Network Traffic Management

8920 Network Traffic Management software

Record Base Administration Guide
Release 17.2

190-406-813
Issue 1.1
October 2011

Alcatel-Lucent - Proprietary
This document contains proprietary information of Alcatel-Lucent
and is not to be disclosed or used except in accordance with applicable agreements.

Copyright © 2011 Alcatel-Lucent.
Unpublished and not for publication. All rights reserved.

This material is protected by the copyright and trade secret laws of the United States and other countries. It may not be reproduced, distributed, or altered in any fashion by any entity (either internal or external to Alcatel-Lucent), except in accordance with applicable agreements, contracts, or licensing, without the express written consent of Alcatel-Lucent and the business management owner of the material.

Notice

Every effort was made to ensure that the information in this document was complete and accurate at the time of printing. However, information is subject to change.

Trademarks

All trademarks and service marks specified herein are owned by their respective companies.

Warranty

Alcatel-Lucent provides a limited warranty to this product.

Customer Notification

The Alcatel-Lucent contract specifies your system configuration (e.g., capacities) and identifies the optional features you have purchased.
The standard NTM Feature Set documentation contains information on all of the features available in the Release, including those you may not have purchased, which are thereby not available for use.
Alcatel-Lucent will not support external use of the third-party software packages included in the NTM Feature Set.

Acknowledgements

We wish to acknowledge:
The NTM product includes software developed by:
Red Hat Enterprise Linux® - Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

APACHE TOMCAT - The Apache License, version 2.0 (http://www.apache.org/licenses/).

APACHE ActiveMQ - The Apache License, version 2.0 (http://www.apache.org/licenses/).

MOD AJP (APACHE Tomcat Connectors) - The Apache License, version 2.0 (http://www.apache.org/licenses/).

Apache Xerces C++ - The Apache License, version 2.0 (http://www.apache.org/licenses/).

Apache Axis2 - The Apache License, version 2.0 (http://www.apache.org/licenses/).

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the Apache Group for use in the Apache HTTP server project (http://www.apache.org/)."

4. The names "Apache Server" and "Apache Group" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact apache@apache.org

5. Products derived from this software may not be called "Apache" nor may "Apache" appear in their names without prior written permission of the Apache Group.

6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the Apache Group for use in the Apache HTTP server project (http://www.apache.org/)."

THIS SOFTWARE IS PROVIDED BY THE APACHE GROUP ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE APACHE GROUP OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

MOD_SSL - Copyright (c) 1998-2004 Ralf S. Engelschall. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

This product includes software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod_ssl project (http://www.modssl.org/).

4. The names "mod_ssl" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact rse@engelschall.com.

5. Products derived from this software may not be called "mod_ssl" nor may "mod_ssl" appear in their names without prior written permission of Ralf S. Engelschall.

6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod_ssl project (http://www.modssl.org/)."

THIS SOFTWARE IS PROVIDED BY RALF S. ENGELSCHALL ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL RALF S. ENGELSCHALL OR HIS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY,

WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Bugzilla - Mozilla Foundation; License: http://creativecommons.org/licenses/by-sa/2.0/

CentOS - CentOS Project;

Dom4J - DOM4J Project; License: http://www.dom4j.org/dom4j-1.6.1/license.html

LDAP C SDK - Mozilla Foundation; License: http://www.mozilla.org/MPL/MPL-1.1.html

mksh - Korn shell by David Korn; Distributed under BSD License. (https://www.mirbsd.org/htman/i386/man7/BSD-Licence.htm)

ncurses - ncurses, GNU 5.5; Distributed under MIT + GPL2+

nmon - IBM nmon; License: http://www.gnu.org/copyleft/gpl.html

PAM_RADIUS_AUTH - This module is a merger of an old version of pam_radius.c, and code which went into

mod_auth_radius.c, with further modifications by Alan DeKok of CRYPTOCard Inc.. The original pam_radius.c code is copyright (c) Cristian Gafton, 1996, redhat.com> The additional code is copyright (c) CRYPTOCard Inc, 1998. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, and the entire permission notice in its entirety, including the disclaimer of warranties.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

ALTERNATIVELY, this product may be distributed under the terms of the GNU Public License, in which case the provisions of the GPL are required INSTEAD OF the above restrictions. (This clause is necessary due to a potential bad interaction between the GPL and the restrictions contained in a BSD-style copyright.)

THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

JAVA JDK - Sun Microsystems Inc. Binary Code License Agreement (http://java.sun.com/j2se/1.5.0/jdk-1_5_0_12-license.txt).

edtFTPj - Enterprise Distributed Technologies under LGPL License (http://www.gnu.org/licenses/lgpl.txt).

Perl DBD - Perl DBD Copyright (c) 1994-2003 Tim Bunce, Ireland is used with permission. Distributions of the standard package can be found through the http://www.cpan.org website.

Perl Convert::ASN1 - Perl DBD Copyright (c) 1994-2003 Tim Bunce, Ireland is used with permission. Distributions of the standard package can be found through the http://www.cpan.org website.

Perl URI - Perl DBD Copyright (c) 1994-2003 Tim Bunce, Ireland is used with permission. Distributions of the standard package can be found through the http://www.cpan.org website.

Prototype - Copyright (c) 2005-2007 Sam Stephenson

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Scmbug - Scmbug by Martin Tomes; License: http://www.subversionary.org/projects/scmbug

SNMP4j - SNMP4J.org; License: http://www.snmp4j.org/LICENSE-2_0.txt

Subversion - CollabNet; License: http://subversion.tigris.org/license-1.html

SWISH-E - Copyright 1995-1998 by Miles O'Neal, Austin, TX, USA. GNU General Public License.

w4ais - Copyright 1995-1998 by Miles O'Neal, Austin, TX, USA. (http://yolo.net/w4ais/license.html)

GNU LESSER GENERAL PUBLIC LICENSE - Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.

59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy. This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form

under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to ecompile the application to use the modified definitions.)

b) Use a suitble shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances. It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

JSch 0.0.* was released under the GNU LGPL license. Later, we have switched over to a BSD-style license.

Copyright (c) 2002-2010 Atsuhiko Yamanaka, JCraft,Inc.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The names of the authors may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL JCRAFT, INC. OR ANY CONTRIBUTORS TO THIS SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Alcatel-Lucent - Proprietary
See notice on first page.

Contents

1 Introduction to the Record Base

Overview of this guide 2
About the NTM record base 3
Record base files and pathnames 4
Notations used in the record base file descriptions 7

2 Managing Record Base Partitions

Background 2
Architecture for subnetwork partitions 4
Subnetwork characteristics 5
Permissions 6

3 Record Base Concepts

Defining sets 4
Checking sets files — ofcset and tgset commands 6
RSPTE concepts 8
RSPTE numbering 10
Using the RSPTE file 11
Working with discretes 13
Background 16
Setting up trunk group files 19
Defining trunk group threshold files 21
Scheduling threshold tables 23
Background 26
Defining domain acronyms 28
Mapping domain acronyms 30
Defining codes 32

4 Data Collection Concentrator Alias File

Interfaces 2

DCC alias file 3

5 Record Base Files

All Point Code (APC) File 4

ATM File 6

ATM Threshold File 8

Code Event File 11

Code Event Threshold File 12

Control Default Domain File 15

Discrete File 16

Domain Acronym File 19

Domestic Code File 21

Event_Alarm File 23

Filter File 25

Final Handling Code (FHC) File 29

INMS File 31

International Code File 33

Job Status File 35

Job Status Threshold File 36

Mass Call Threshold File 38

Office File 40

Initial file entry formats 44

Calculation format 51

Office Domain File 53

Office Type Domain File 55

Packet File 57

Packet Threshold File 60

PAS Code File 63

Password File 65

RSPTE File 67

Sets File 73

Signaling Link File 76

Signaling Link Threshold File 77
TG24HourOfl File 79
TG24HourOfl Threshold File 80
Threshold Table Schedule File 82
Transmitter Timeout (TTO) Thresholds File 84
Trunk Group File 86
Trunk Group Threshold File 96
TYPXREF File 103

6 Record Base Editor

Record base file format 2
Record base file symbols 3
Record format 4
The rbed command 5
Working with record base files 7
Recovering an edited file 8
Editing a record base file with rbed 9
Common editing commands 11

7 Record Base Administration

Record base administration process 3
Creating and modifying database records 6
Defining threshold data 9
Setting up trunk group threshold data 10
Administering subnetworks 12
Modifying record base files for subnetworks 13
Troubleshooting 1A ESS switches with data alignment problems 15
Realigning registers 17
Changing default domain for a control 19
Adding and deleting RSPTE CLLI changes 20
Building the database for 1024 trunk groups 22

8 Record Base Update Procedures

Performing a general update 2
Performing a full create and installdb 3
Performing a single file create and installdb 6

Performing a single office create 9

9 Maintaining the Record Base with BDR

Partitioning for BDR 3
Using the INMS file to define partitioning 5
Resolving errors 6
Configuring the record base files for BDR 7
Synchronizing UDDM/UDNEI files for BDR 9
Global files 12
Independent files 15
Office-related files 17
Shared files 19

10 Adding and Removing Network Elements

Time recommendations 3
Requirements 6
Direct connect TCP/IP interface to data collector 7
Using and testing TCP/IP connections 10
Creating the record base files (DCC) 14
Installing the updated record base (DCC) 15
Structure: DCC office list 16
Performing post-DCC move steps on NTM 20
Performing post-DCC move steps on the EADAS 21
Removing the record base files (DCC) 24
Updating the system after removing a DCC 25
Requirements 28
Setting up the TCIP/IP link between the host and switch 30
Creating the record base files (office) 34
Removing the record base files (office) 36
Updating the system after removing an office 37
Time recommendations 41
Setting up the infrastructure 42
Preparing the non-NTM features 43
Preparing the NTM host 45
Preparing the NTM host for migration to AI 48

Cutting over an office 50
Backing out an office cutover 53
Verifying cutovers 55
Finalize cutovers and deactivate the DCC interface 56
SDM configuration 58
Installing Secure connection 59
Troubleshooting GSP network elements 62

11 Training Objectives and Exercises

GL Glossary

IN Index

List of figures

1 Introduction to the Record Base

2 Managing Record Base Partitions

1 Record base partitions — Directory structure 4
2 Information displayed by snw_info 7

3 Record Base Concepts

1 Sets file example 4
2 ofcset command 6
3 tgset command 7
4 RSPTE diagram 9
5 RSPTE file example 11
6 Discrete file example 13
7 Trunk group thresholding — file relationships 18
8 Trunk group file entries 20
9 Trunk group threshold file 21
10 Threshold table schedule file example 23
11 Relationship of domain files 27
12 Domain acronym file example 28
13 Office domain file example 30
14 Domestic code file example 32
15 International code file example 32

4 Data Collection Concentrator Alias File

1 Entries in the DCC alias file 3

5 Record Base Files

1 All Point Code File entry 5
2 Control Default Domain File entry — 4ESS 15

3 Discrete File entries — 5ESS 17
4 Domain Acronym File entry — subnetworks 20
5 Domain Acronym File entry — no subnetworks 20
6 Domestic Code File entries 21
7 Event_Alarm File entries 23
8 Filter File without Feature 189 27
9 Filter File with Feature 189 27
10 Final Handling Code File entries 29
11 INMS File entries 31
12 International Code File entries 33
13 Office File — Format 1 41
14 Office File — Format 2 41
15 Office File — Format 3 41
16 Office File — Format 4 or Format 10 41
17 Office File — Format 5 42
18 Office File — Format 6 42
19 Office File — Format 7 42
20 Office File — Format 8 42
21 Office File — Format 9 42
22 Office File — Format 10 43
23 Office Domain File entries — 5ESS 54
24 Office Type Domain File 56
25 PAS Code Entries 63
26 RSPTE Entries 71
27 RSPTE entry — Internal network element 72
28 RSPTE entry — External network element 72
29 RSPTE entry — DCC 72
30 RSPTE entry — BDR host and local audit data restoration 72
31 Sets File entries 74
32 Threshold Table Schedule File entries 83
33 Transmitter Timeout File Entries 85
34 Trunk Group File entries 93
35 Trunk Group File entries — 4ESS 93

36 Trunk Group File entries — 5ESS 94
37 Trunk Group File entries — 1A ESS 94
38 Trunk Group File entries — GTD-5 94
39 Trunk Group File entries — GSP 95
40 Trunk group threshold entries without Feature 189 100
41 Last index entry for the calc keyword 101
42 Trunk group threshold entry with Feature 189 102
43 TYPXREF File entries 104
44 Related RSPTE entries 105

6 Record Base Editor

7 Record Base Administration

1 Record base administration process 5

8 Record Base Update Procedures

1 Full create and installdb 4
2 Single file create and installdb 7
3 Single office create 10

9 Maintaining the Record Base with BDR

1 Primary and secondary hosts partitioning 4
2 Entry in the INMS file 5
3 The create process for global files 14
4 The create process for independent files 16
5 The create process for office-related files 18
6 The create process for shared files 21

10 Adding and Removing Network Elements

1 NTM “/etc/hosts” File 6
2 DCC File example 16
3 Migration process 40

11 Training Objectives and Exercises

List of tables

1 Introduction to the Record Base

1 Description of record base files 4

2 Notation used in this guide 7

2 Managing Record Base Partitions

3 Record Base Concepts

4 Data Collection Concentrator Alias File

5 Record Base Files

1 Discrete types and descriptions 17

2 Data type / packet information 49

3 Record base CIC requirement matrix 91

4 Signaling type/switch cross reference 93

5 Explanation: Figure 41 101

6 Record Base Editor

1 Symbols used to format record base files 3

2 vi Cursor and Page Motions 12

3 vi Text Addition 12

4 vi Text Searching 12

5 vi Text Deletion 13

6 vi Text Replacement 13

7 vi Text Movement 13

8 vi Miscellaneous Commands 14

7 Record Base Administration

8 Record Base Update Procedures

1 Single office create record base files and corresponding paths 12

9 Maintaining the Record Base with BDR

10 Adding and Removing Network Elements

1 Recommended time allotment for procedures 3

2 Migrating to TCP/IP connectivity 41

11 Training Objectives and Exercises

1 Introduction to the Record Base

Overview

Purpose

This chapter provides an introduction to the record base and an overview to the rest of the chapters in this guide.

Contents

This chapter contains the following topics:

Overview of this guide	1-2
About the NTM record base	1-3
Record base files and pathnames	1-4
Notations used in the record base file descriptions	1-7

Overview of this guide

Purpose

This document is divided into two major sections:

- Overviews and Conceptual Information
  - Chapter 1, “Introduction to the Record Base”
  - Chapter 3, “Record Base Concepts”
  - Chapter 2, “Managing Record Base Partitions”
  - Chapter 4, “Data Collection Concentrator Alias File”
  - Chapter 5, “Record Base Files”
- Record Base Procedures and Tasks
  - Chapter 6, “Record Base Editor”
  - Chapter 7, “Record Base Administration”
  - Chapter 8, “Record Base Update Procedures”
  - Chapter 9, “Maintaining the Record Base with BDR”
  - Chapter 10, “Adding and Removing Network Elements”

Disclaimer

The terms `exchange` and `office` are used interchangeably throughout the *Record Base Administration Guide*

□

About the NTM record base

Overview

The 8920 Network Traffic Management software record base consists of user-built text files in the "/musr/rb" directory. Users enter records into these files with a standard *Linux* system text editor such as vi.

Reference: Chapter 6, "Record Base Editor"

Record base personnel Tasks

The primary responsibilities of record base personnel are to:

- Create and maintain ASCII record base files

  Reference: See Chapter 5, "Record Base Files" for a discussion of the requirements for each record base file.

- Test and install updates to current database

  Reference: See Chapter 8, "Record Base Update Procedures" for more information on testing and installing record base updates.

- Install updates to records at offices using schedule audit commands (when necessary)

  Reference: See Chapter 2, "Commands for Auditing Network Elements" in the *Input Commands Guide* for more information on schedule audits.

Information contained in record base files

Record base files contain information about the structure of the entire network and additional information about that portion of the network for which 8920 NTM is responsible. Record base files also contain the calculations and thresholds that will be applied to measurement and alarm data received from the surveyed network.

Record Base files contain:

- Thresholds for determining exceptions

  Reference: Chapter 3, "Record Base Concepts"

- Reference data used to identify trunk groups, offices, signaling types, code destinations, etc., in the network.

  Reference: Chapter 5, "Record Base Files"

- Information used to control the display of data

  Reference: Chapter 3, "Record Base Concepts"

Record base files and pathnames

Table

The record base files are described in Table 1 in alphabetical order. The full pathnames indicate whether there will be one of the following:

- one file for each office (CLLI) or network element
- one file for each office type, such as *5ESS* (switch_type)
- one file per NTM (file name or node_name only)

Table 1 Description of record base files

File (see page ...)	Description Full Pathname	Command "file=" option	Valid for ...
"Control Default Domain File" (p. 15)	Set default domains for controls	domain	*4ESS*, *5ESS*,
	"/musr/rb/domain/switch_type"		
"Discrete File" (p. 16)	Categorize discretes and assign severity levels.	discrete	all
	"/musr/rb/discrete/switch_type"		
"Domain Acronym File" (p. 19)	Set up domain acronyms.	domain	*4ESS, 5ESS,*
	"/musr/rb/domain/domain"		
"Domestic Code File" (p. 21)	Associate codes with an office.	domestic	all
	"/musr/rb/codes/domestic"		
"Event_Alarm File" (p. 23)	Defines alert levels for events	alarm	all
	"/musr/rb/gui_alarm/event_alarm"		
"Filter File" (p. 25)	Specify rules to tag data as suspect	filter	all
	"/musr/rb/thresh/filter"		
"Final Handling Code (FHC) File" (p. 29)	Set up a final handling code name.	fhc	*4ESS*
	"/musr/rb/fhc/fhcs"		
"INMS File" (p. 31)	Define partitioning for primary and secondary hosts (BDR only)	inms	all
	"/musr/rb/inms/inms"		

(Sheet 1 of 3)

Table 1 Description of record base files (continued)

File (see page …)	Description Full Pathname	Command "file=" option	Valid for …
"International Code File" (p. 33)	Associate codes with a country.	intl	*4ESS*
	"/musr/rb/codes/intl"		
"Office File" (p. 40)	Office reference data assignments.	office	all
	"/musr/rb/office/clli"		
"Office Domain File" (p. 53)	Associate domains with offices and subnetworks.	office	*4ESS, 5ESS,*
	"/musr/rb/domain/<office type>_dflt" Where <office type> is "ess4" or "ess5".		
"Office Type Domain File" (p. 55)	Define a unique set of domain identifier for a specific office type.	office	*4ESS, 5ESS,* 7revita
	"/musr/rb/domain"		
"PAS Code File" (p. 63)	Define public announcement service codes.	pas	*4ESS*
	"/musr/rb/codes/pas"		
"Password File" (p. 65)	Define the Password File to be used to store the password to the Administrative Services Module (ASM)	office	*GTD-5, 5ESS,* 7/RE
	"/musr/rb/password"		
"RSPTE File" (p. 67)	Define regional, sectional, primary, toll, end office names for internal and external offices.	rspte	all
	"/musr/rb/rspte/rspte"		
"Sets File" (p. 73)	Define names for all trunk group and office sets.	sets	all
	"/musr/rb/sets/sets"		
"Threshold Table Schedule File" (p. 82)	Schedule trunk group threshold tables.	sched	all
	"/musr/rb/thresh/sched"		
(Sheet 2 of 3)			

Table 1 Description of record base files (continued)

File (see page …)	Description Full Pathname	Command "file=" option	Valid for …
"Transmitter Timeout (TTO) Thresholds File" (p. 84)	Set up intercarrier prefixes and their threshold levels.	office	all (except *4ESS* and *GTD-5*)
	"/musr/rb/tto/clli"		
"Trunk Group File" (p. 86)	Trunk group reference data assignments.	office	all
	"/musr/rb/tg/clli"		
"Trunk Group Threshold File" (p. 96)	Set up threshold tables.	thresh	all
	"/musr/rb/thresh/thresh [1-8]"		
"TYPXREF File" (p. 103)	Associate real type and generic names with internally supported type and generic names.	rspte	all
	"/musr/rb/rspte/typxref"		
(Sheet 3 of 3)			

Notations used in the record base file descriptions

Table

Table 2 contains the notation used to describe the record base files.

Table 2 Notation used in this guide

SYMBOL	FUNCTION
`Bold` type	Indicates user-entered input
`Italic` type	Indicates user-entered variables
Square brackets `[ ]`	Encloses an optional statement
CR or **RETURN**	Indicates carriage return or Enter
Semicolon (`;`)	Terminates a command line
`<blank>`	Separates a command from its parameters
Comma (`,`) or `<blank>`	Separates parameters from other parameters
Question mark (?)	Help
exit	Terminates working session
DELETE or **CTRL - D**	Aborts a command
Plus sign (+)	Separates multiple parameter values
Backslash (\)	Separates multiple lines in preplans
Date/Time in either of these forms • YY/MM/DD-HH:mm • DD/MM/YY-HH:mm	Indicates date and time as follows: YY=the numeric year (last 2 digits of the year) MM=the numeric month (1–12) DD=the numeric day (1–31) HH=the hour (0–23) mm=the minutes (0–59)

File description headings

Record Base file descriptions are broken down as follows:

- File Names
- Valid for Office Types
- Restrictions (if applicable)
- Related Record Base files (if applicable)
- Pathname(s)
- File Entry Format(s)
- Variable definitions

- Sample files

2 Managing Record Base Partitions

Overview

Purpose

This chapter describes how Feature 3, “Management of Record Base Partitions and Subnetworks” affects record base administration.

Feature restrictions

Record base partitions are optional. They are available only if they have been purchased.

Contents

This chapter discusses the following topics:

Background	2-2
Architecture for subnetwork partitions	2-4
Subnetwork characteristics	2-5
Permissions	2-6

Background

Overview

A record base partition refers to the separation of the record base files for a subnetwork from other subnetwork record base files. There are two separate concepts involved in partitioned subnetworks:

- Subnetwork — A subnetwork is a group of offices and trunk groups that are managed separately from other offices and trunk groups. Subnetworks restrict the user's ability to manage a particular group of offices and trunk groups.
- Partition — A partition is a group of offices in a separate section of the record base. A partition restricts a user's access to a group of record base files.

Comparison — subnetworks and partitions

A subnetwork allows limited access to monitor, control, and audit a group of offices and trunk groups, while a partition allows limited access to change the record base for a group of offices and trunk groups.

Uses

Subnetworks and partitions can be used in a variety of ways. A subnetwork and a partition can be defined identically with respect to the offices they contain. A partition could also be defined to contain only a portion of the offices assigned to a subnetwork or to contain offices from more than one subnetwork. A subnetwork could also be defined that contains all or a portion of the offices in one or more partitions.

Naming

There must be a one-to-one correspondence between the name of a record base partition that is selected by a user and the name of a subnetwork. However, a subnetwork can be created without a corresponding record base partition.

Maximum number of subnetworks and partitions

The default maximum number of subnetworks is 2. There are purchasable features that will increase the number of subnetworks you can have. With BDR, a maximum of 4 subnetworks may be defined. Two of those 4 (including main) may be a partition. Otherwise, 3 subnetworks may be defined: main and 2 others. With Feature 3, “Management of Record Base Partitions and Subnetworks” a maximum of 15 subnetworks may be defined. Up to 6 of those may be partitions (including main).

References

For information about creating and deleting subnetworks, see Chapter 11, “Subnetwork Administration” in the *System Administration Guide*.

Architecture for subnetwork partitions

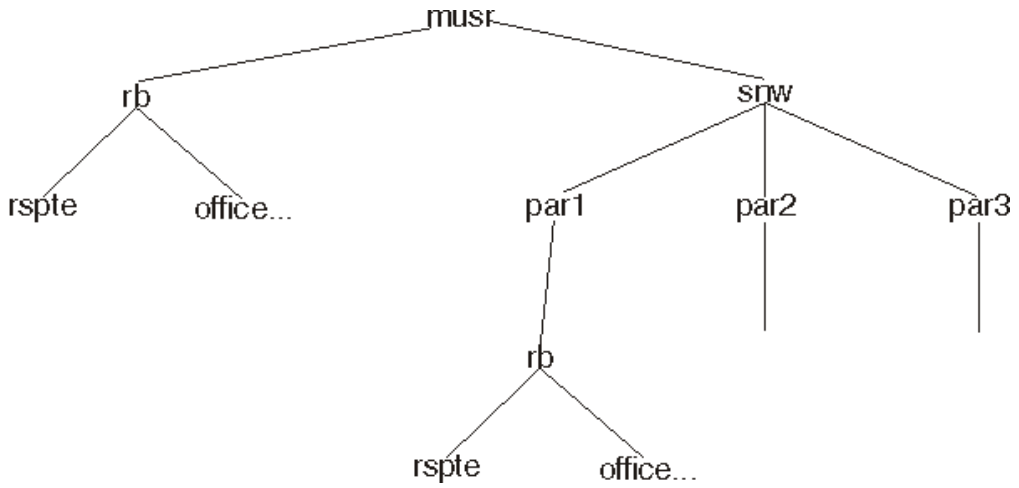
Overview

Partitions use a specific directory structure. The main subnetwork is placed in “/musr/rb” while all other partitions are placed in “/musr/snw/*partition_name*/rb”.

Figure

Figure 1 shows the relationship of these directories:

Figure 1 Record base partitions — Directory structure



Subnetwork characteristics

Subnetworks

All subnetworks:

- use subnetwork permissions to determine which offices and/or trunk groups users can manage
- use permissions in "/nm/etc/permissions" to determine the commands that can be executed by members of a given user group
- are set up and maintained with the `snw_admin` command by an administrator in the `snm` user group

With partitions

If a subnetwork has a corresponding partition, it is referred to as a partitioned subnetwork, which

- allows record base files to be in a separate directory ("/musr/rb/snw/*`partition_name`*")
- allows access to its record base files to be restricted by user group
- can be backed up by BDR

Reference: Chapter 9, "Maintaining the Record Base with BDR"

Permissions

Database modification

The system administrator or another member of the `snm` user group determines which user groups have permission to modify files for each partition. Permissions are set using the `snw_admin` command.

Subnetworks, partitions, and commands

The system administrator also determines which subnetworks should be associated with a partition. By associating a partition with a subnetwork, user permissions can then be limited for the following commands:

- `create` — only a member of the `snm` user group can run a full or a single-file create. However, partitioning allows the administrator to give user groups permission to run single-office creates. If you have permission for the partition that the office is in, you can run a single-office create on it.
- `dbtest` — Again, only a member of the `snm` user group can run a full database test or a single-file test. However, partitioning allows the administrator to give user groups permission to run `dbtest` on single offices for each partition. Also, if you have database modification permission for a partition, you can run `dbtest` on the “rspte”, “thresh”, and any domestic codes files.

  Important! Because the “rspte” and “thresh” files are in more than one partition, errors may result when a `dbtest` is run on these files. This is especially true if another user is modifying his or her partition's “rspte” or “thresh” file in one partition while you are running the `dbtest` command in another.
- `installdb` — Only the user with the `root` login ID, or members of the `snm` user group can install the database.
- `thresh` — any user in the `snm` user group can run the `thresh` command. This command will update the thresholds in all partitions of the threshold file if they have been changed.

  Reference: For information about adding user groups to a partition, see Chapter 11, “Subnetwork Administration” in the *System Administration Guide*.

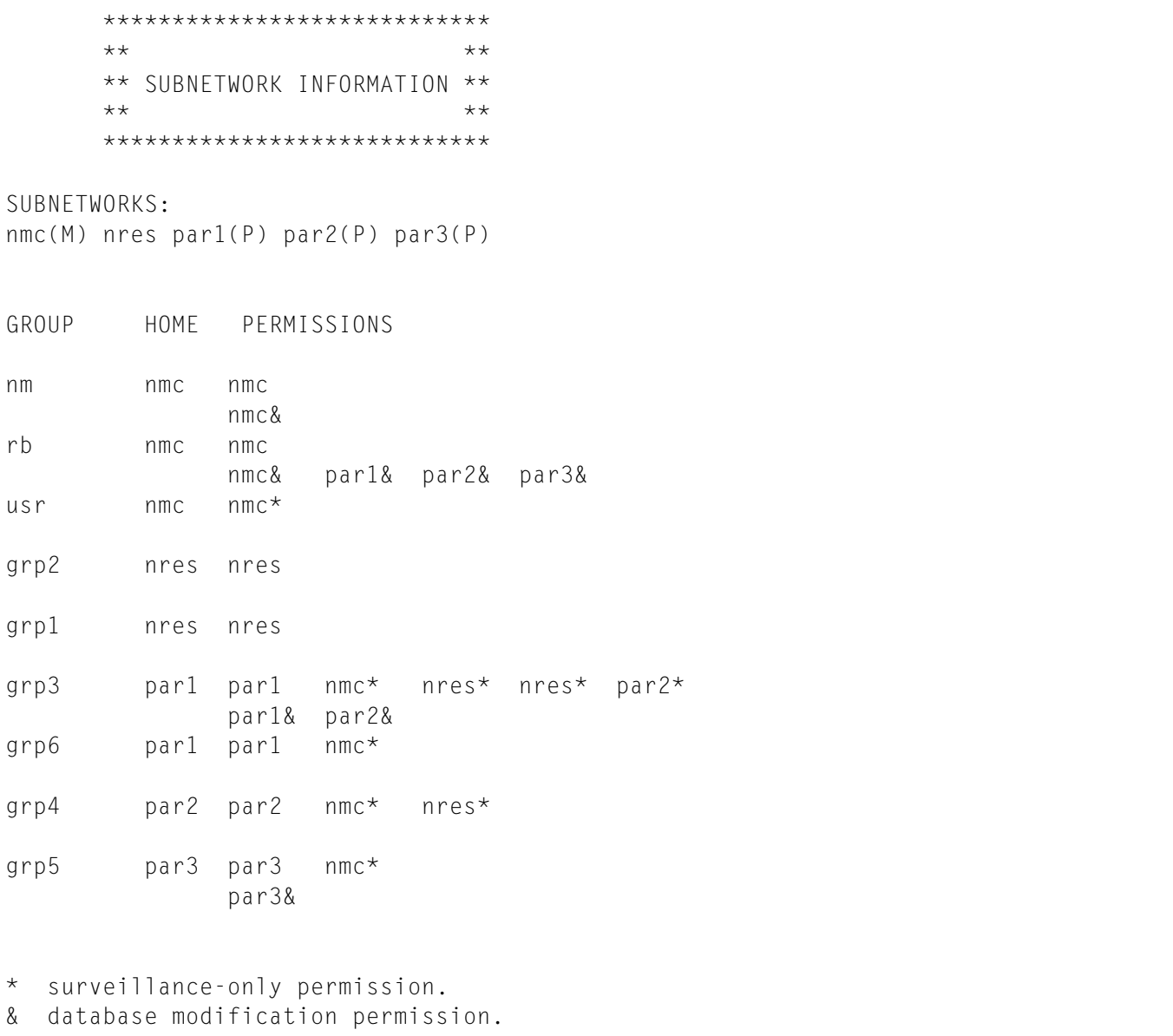
Finding out what you have permission to do

To determine which subnetworks you have access to, you will need to use the `snw_info` command. To display information about all subnetworks, partitions, and permissions, enter `snw_info` at the system prompt.

Figure

Figure 2 shows an example of the information displayed by the `snw_info` command:

Figure 2 Information displayed by snw_info



```
        ***************************
        **                       **
        ** SUBNETWORK INFORMATION **
        **                       **
        ***************************

SUBNETWORKS:
nmc(M) nres par1(P) par2(P) par3(P)


GROUP     HOME   PERMISSIONS

nm        nmc    nmc
                 nmc&
rb        nmc    nmc
                 nmc&    par1&   par2&   par3&
usr       nmc    nmc*

grp2      nres   nres

grp1      nres   nres

grp3      par1   par1    nmc*    nres*   nres*   par2*
                 par1&   par2&
grp6      par1   par1    nmc*

grp4      par2   par2    nmc*    nres*

grp5      par3   par3    nmc*
                 par3&


*  surveillance-only permission.
&  database modification permission.
```

Figure description

The following information appears in Figure 2:

Heading	Description
SUBNETWORKS	all subnetworks defined on the system are listed here. Some are followed by a letter in parentheses: • M — shows the main subnetwork • P — shows that the subnetwork is partitioned • no parenthetical letter — shows that the subnetwork is not partitioned.
GROUP	lists all user groups assigned to any subnetwork
HOME	lists the home subnetwork for each user group
PERMISSIONS	lists for each user group the subnetworks that can be accessed. The subnetwork name can have the following after it: • * — shows that the user group only has permission to monitor this subnetwork • & — shows that the user groups can modify the database of this subnetwork no symbol after the subnetwork name — shows that the user group can monitor, control, and audit the subnetwork.

Reference: “snw_admin” (p. 17) and “snw_info” (p. 22) in the *Input Commands Guide*

□

3 Record Base Concepts

Overview

Purpose

This chapter provides conceptual information about how the record base is set up and how it functions.

Contents

This chapter contains the following topics:

Network data views	3-3
Trunk group exception thresholding	3-15
Control traffic type and code definition	3-25

Network data views

Overview

Purpose

This section provides information about how the record base files affect network data views.

Overview

The following record base files affect how the user views network data on the browser-based GUI:

- Sets — "/musr/rb/sets/sets"

  In the Sets File, you can define office and trunk group sets that are logical groupings of offices and trunk groups. Set membership (specified in other files: the RSPTE file for switches and TG files for trunk groups) can be used to determine which offices and trunk groups are displayed as part of a particular set.

- RSPTE — "/musr/rb/rspte/rspte"

  In the RSPTE File, you can set up a ranking order for network offices by using a numbering scheme and then display only offices having a certain rank number or higher.

- Discrete — "/musr/rb/discrete/*type*"

  In the Discrete File, you can set up the labels you want to use to identify office discretes/alarms and assign severity levels to them.

Contents

This section contains the following topics:

Defining sets	3-4
Checking sets files — ofcset and tgset commands	3-6
RSPTE concepts	3-8
RSPTE numbering	3-10
Using the RSPTE file	3-11
Working with discretes	3-13

Defining sets

Purpose

The purpose of having office or trunk group sets is to enable network managers to determine how they want to view the network on pages. For example, if two offices are in a set and the network manager enters the set name in the search area, data for both these offices is retrieved from the database without retrieving data for offices not in the set.

Sets file

The Sets File is used to define the names for trunk group and office sets and to map the names to identification numbers. Set names can have from 1 to 12 characters. The format for trunk group and office entries is shown in Figure 1.

Index numbers

Index numbers are used internally within the NTM database for cross-reference purposes. You can use an index number only once in the Sets File for a particular type of set. For example, two office sets cannot have the same *ofc*index number and two trunk groups cannot have the same *tg*index number. But you can have an `ofcindex=1` and a `tgindex=1`.

Sets parameter

Set names are assigned as values for the `sets=` parameter in two other record base files. Office sets are assigned in the RSPTE File and trunk group sets are assigned in the Trunk Group Files. You must define a set name in the Sets File before assigning it in the RSPTE or trunk group files.

Limitations

There is a maximum of up to 2,000 office sets for Small/Medium NTM configurations and up to 4,000 office sets for the NTM Large configuration. There can be up to 10,000 trunk group sets in the Sets File. An office can belong to a maximum of 8 sets, and a trunk group can belong to a maximum of four sets.

Example

Figure 1 provides an example of entries in a Sets File.

Figure 1 Sets file example

```
$ view /musr/rb/sets/sets

# tgindex=index,tgset=tgset_name;
# ofcindex=index,ofcset=ofcset_name;
```

```
tgindex=1,tgset=usa;
tgindex=2,tgset=pari;
tgindex=3,tgset=c7;
tgindex=4,tgset=c6;
tgindex=5,tgset=emer;
tgindex=6,tgset=data;
tgindex=7,tgset=i33;
ofcindex=01,ofcset=nort;
ofcindex=02,ofcset=sou;
ofcindex=03,ofcset=gtw;
ofcindex=04,ofcset=locl;
ofcindex=05,ofcset=lk;
ofcindex=06,ofcset=cvd1;
ofcindex=07,ofcset=ffm;
```

Checking sets files — ofcset and tgset commands

Purpose

Two commands are available for checking information about office and trunk group sets: `ofcset` and `tgset`. These commands allow you to find out if a set exists and which offices or trunk groups belong to a specified set.

In all of these procedures, you must know which set you want to check, because you cannot use a question mark (?) to receive prompting during the procedures. Look in the "/musr/rb/sets/sets" file for a list of valid office and trunk group set names.

ofcset command

The `ofcset` command looks for all the offices in a given office set and prints them on your screen.

Figure 2 ofcset command

```
$ ofcset
setname= dm28
Begin ofcset at: Wed Jul 21 14:35:10 EDT 1997

IP

The offices in set dm28 are:

OFFICE
------
bakrca11ds0
enctca12ds0
fntaca11ds0
irvnca11ds1
testewsd025

End ofcset at: Wed Jul 21 14:35:12 EDT 1997
```

tgset command

The `tgset` command looks for all the trunk groups in a given trunk group set and prints them on your screen. You can restrict retrieval of the members of a particular trunk group set to trunk groups originating from a particular from-office or terminating at a particular to-office. If you do not specify a from- or to-office, then the system retrieves all trunk groups in the set.

Figure 3 tgset command

```
$ tgset

setname= cb2
from_office= anhmca11ds0
to_office= all

From_Office     To_Office       Suffix
-----------     ---------       ------
anhmca11ds0     anhmca1176a     a001
anhmca11ds0     anhmca1176a     a002

End tgset at: Wed Jul 23 14:40:07 EDT 1997
```

RSPTE concepts

What does RSPTE mean?

RSPTE is a mnemonic in which each letter stands for a level in a hierarchical switching network. In the past, five levels or ***ranks*** of switching offices were recognized in the U.S. national network: regional, sectional, primary, toll, and end offices.

One characteristic of the hierarchy was that an office was permitted to communicate directly only with another office at its level ***within the same hierarchical chain*** or to the office that was its ***parent or child*** in the chain.

Examples

In the hierarchy in Figure 4, if end office 016 needed to connect a call to end office 015, it could do so either directly or via its ***parent*** toll office 008.

But if end office 016 was required to connect a call to end office 009, the call would have to route: 016 - 008 - 004 - 003 - 005 - 009. Routing was not allowed ***on the diagonal***. End office 016 was not permitted to communicate directly with toll office 005 to complete the call. Calls had to route ***up - over - down***.

Non-hierarchical digital network

This switching concept has given way in recent years to the concept of the ***non-hierarchical digital network***, in which there is great flexibility in routing patterns. But NTM has retained the hierarchical concept for the purposes of managing the display of office data on pages. An imaginary or ***logical*** network hierarchy is constructed in the "/musr/rb/rspte/rspte" file.

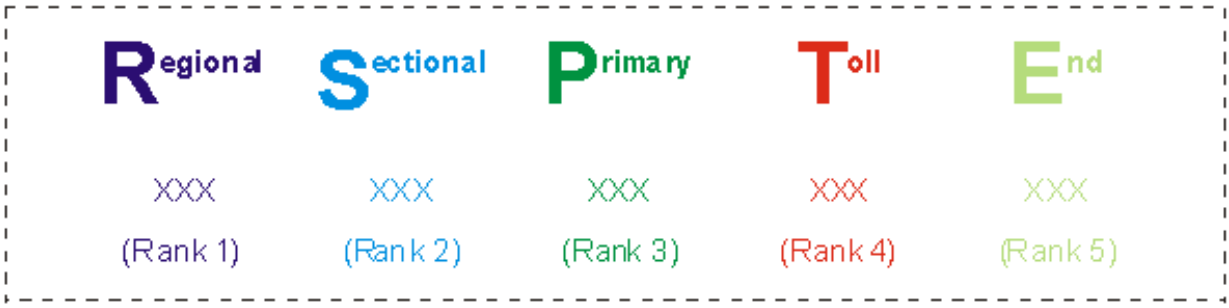
This imaginary hierarchy is used on trunk group page displays (for example, to restrict or expand data display by specifying the levels [ranks] of offices to be considered). Also, the imaginary hierarchy defined in the RSPTE File is used to define "areas" that can be displayed on the pages. For example, if primary office 004 is entered as the "Near End" office in a trunk group search and "AREA" is also selected, the display would include primary office 004, toll offices 007 and 008, and end offices 013, 014, 015, and 016.

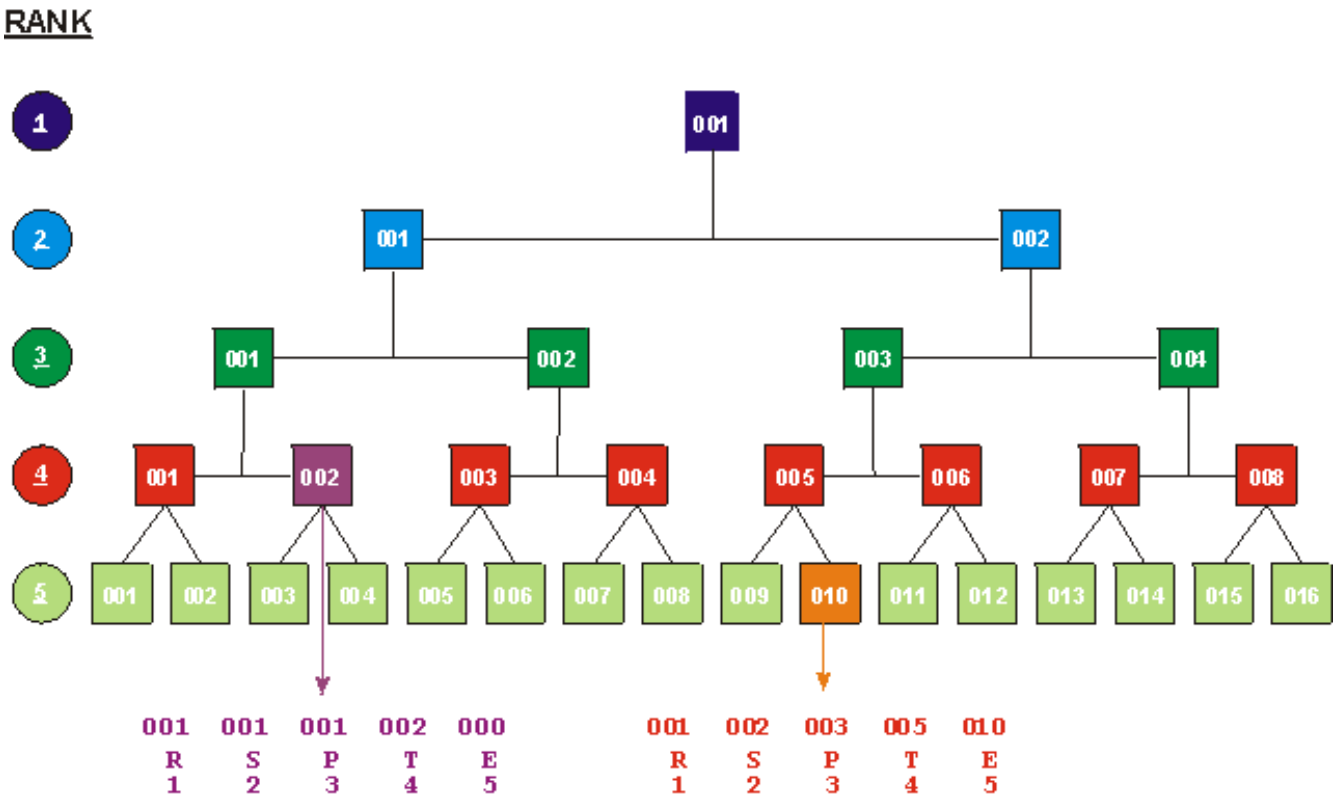
Each office in the RSPTE File will have a unique 15-digit number (five sets of three digits) that defines its position in the 5-rank hierarchy.

Figure

Figure 4 provides a diagram to help explain how RSPTE works.

Figure 4 RSPTE diagram





Important! The RSPTE number is padded with zeros below the rank level of the office.

RSPTE numbering

Overview

The position of an element in the imaginary RSPTE hierarchy is defined by 15 digits, 3 digits per rank or level.

This is best understood by example. In Figure 4, the orange end office is the last office in a chain designated as:

- Regional level = 001
- Sectional level = 002
- Primary level = 003
- Toll level = 005
- End = 010

The RSPTE number assigned in the office file is the combination of these nine digits: 001002003005010.

If an office is higher in the 5-rank level hierarchy, 0's are used for the levels below the element.

For example, the RSPTE number for the purple office in Figure 4 would be 001001001002000.

Numbering of offices in the example network and a real RSPTE file

There can be more than one office at the regional level. If there is a regional office `002`, it will be at the top of its own hierarchical chain, like regional office `001`.

The numbering of the offices within ranks in Figure 4 is shown as consecutive, starting with one. This has been done only for the convenience of discussing the figure.

A more likely pattern of numbering will be to restart numbering from one when you reach the last member of a rank within a subset of the hierarchy. For example, at rank 4 in Figure 4, the offices are probably numbered, from left to right, 001, 002, 001, 002, 001, 002.

There is no requirement on the number of offices that can be in a particular subset or on how those offices are numbered, except that the final RSPTE identifier code must be unique.

□

Using the RSPTE file

Overview

The RSPTE File identifies and describes all internal (surveyed) offices and identifies all external offices. Internal offices are those from which NTM collects data and to which it may apply controls. External offices connect at the far-ends of trunk groups that are connected to internal offices. External offices may belong to another company, or perhaps may be in another country altogether. Although no measurements are received from these external offices, their names are associated on the browser-based graphical user interface display with trunk group data and hard-to-reach destination data.

For each internal office, the following keywords are entered: a 1- to 12-character *clli* (office name); a 15-digit *rspte* identifier code; a *nickname* (maximum six characters) for the office that can be used in place of the full office name in the search area, sending commands to the office, etc.; *sets* to which you wish to assign the office (maximum of four); *subnetwork*s that can access the network element; and the *type*, *generic*, and *issue* of the office. An example of these entries in the RSPTE File is shown in Figure 5.

RSPTE code

The RSPTE File takes its name from the RSPTE code. The 15 digits of the code are arranged into five groups of three digits each to create a 5-level hierarchical office ranking scheme. The names of the levels or office ranks are regional, sectional, primary, toll, and end.

External offices are formatted somewhat differently from internal offices. An external office is identified by an asterisk (*) immediately following the `rspte` code. External offices may have nicknames and may be assigned to sets, but the office type, generic, and issue are not entered, and it is not necessary to indicate the omission of these keywords with commas.

Offices can be entered in any order, but it is usual to separate and identify them by office type (if more than one type exists), and into groupings of internal and external offices.

If your RSPTE File is large, position-defined entry is recommended to limit its size.

> **Reference:** See “Record base file format” (p. 2) for more information on position-defined entry.

Figure

Figure 5 provides an example of an RSPTE File.

Figure 5 RSPTE file example

```
$ view /musr/rb/rspte/rspte
```

```
office rspte nickname set subnetwork type generic issue;
stlsmo0934t 001000000000000 stls seta+setb , ess4 4e14 1;
phxagcsgtd5 004000000000000 agc3 ,, gtd5 1641 1;
antomo50cg0 001000000000002* , setc;
blgrmoxa776 001000000000005* , setc;
blvwmoxa697 001000000000006* , setc;
bnkrmoxa689 001000000000007* , setc;
bossmoxa626 001000000000008* , setc;
stlsmo0905t 001000000000009* , setc;
hnblmoac05t 001000000001000* , setc;
eldnmoex01t 001000000002000* , setc;
eldnmoexdsa 001000000002001* , setc;
lwtwmoxa497 001000000003011* , setc;
mntimoxa767 001000000003012* , setc;
stvlmoxa672 001000000003018* , setc;

#office in pvna subnetworks
galvksxads0 016000000000001* ,, pvna;

#offices in subnetworks
wchtksahds0 016000000000002* , setd pvna+nm;
wchtksands0 016000000000003* , setd pvna+nm;
```

Working with discretes

Purpose

Use the Discrete File to map office discretes to labels that will appear on the browser-based graphical user interface, to define discrete type, and to set alert/alarm levels for the discretes.

There should be 1 discrete file per switch type.

Parameters

The *discrete* parameter is the actual discrete name the office uses. The *label* parameter is the discrete name (label) you want to see on the browser-based graphical user interface displays. Usually the name and the label are kept the same.

The *dsctype* parameter is one of the following:

- AUDCTRL — Assign to discretes that trigger an audit because a control has been executed at the switch.
- AUDADMIN — Assign to discretes that trigger an audit because of an administration change at the switch.
- CTRL — Assign to discretes that indicate a control is in effect at the switch.
- SWAC — Assign to switched-access type discretes.
- SERV — Assign to services type discretes (normally associated with an intelligent network).

The *lvl* parameter is the alert/alarm level 0-10 for the discrete. Level 0 is normally used for AUDADMIN, AUDCTRL, and CTRL discrete types.

Figure

Figure 6 shows an example of a Discrete File. If you do not want to have a discrete reported, you can remove it from this file and perform a `create` and `installdb` to update the current database.

Figure 6 Discrete file example

```
$ view /musr/rb/discrete/ess5
 discrete=mc1,label= mc1,dsctype=swac,lvl=8;
 mc2,mc2,swac,8;
 mc1rcv,mc1rcv,swac,3;
 tmc2rcv,mc2rcv,swac,3;
 atgc,atgc,audctrl,1;
 tgrefc,tgrefc,audadmin,1;
```

```
tgschc,tgschc,audadmin,1;
```

□

Trunk group exception thresholding

Overview

Purpose

This section provides information about how exception thresholding works with trunk groups.

Contents

This section contains the following topics:

Background	3-16
Setting up trunk group files	3-19
Defining trunk group threshold files	3-21
Defining trunk group threshold files	3-21
Using flags	3-21
Scheduling threshold tables	3-23

Background

Overview

Setting up trunk group threshold data requires the use of three record base files:

- Trunk Group Threshold File ("/musr/rb/thresh/thresh[1–8]")
- Trunk Group File ("/musr/rb/tg/*clli*")
- Threshold Table Schedule File ("/musr/rb/thresh/sched") — This file is required only if you have more than one Trunk Group Threshold File.

Trunk group threshold file

Use the Trunk Group Threshold File to define thresholds for trunk groups in the network. This file allows you to define one file of data at a time. Each file contains up to 128 indexes (or entries). In each index you can list up to 10 calculations to be thresholded, with their corresponding threshold and alarm/alert levels. When the threshold files are compiled, they are stored as threshold ***tables*** in the database.

NTM allows you to create more than one Trunk Group Threshold File. When you create more than one of these files, each file must have the same number of threshold indexes. The `thr=` keyword for each trunk group in the Trunk Group File will always point to the same index; however, the calculations in an index may vary from one Trunk Group Threshold File to another.

Trunk group file

Use the Trunk Group File to assign a threshold index to each trunk group. This index is used to select which threshold values (from any Trunk Group Threshold table) are compared to the calculations for the trunk group.

> **Important!** The threshold index determines which calculations to perform on this trunk group. A value of zero (0) indicates that you do not perform exception calculations.

Once the office data is collected, NTM performs calculations on it and compares the results with the threshold values from the appropriate index number within the active threshold table to check for exceptions.

Threshold table schedule file

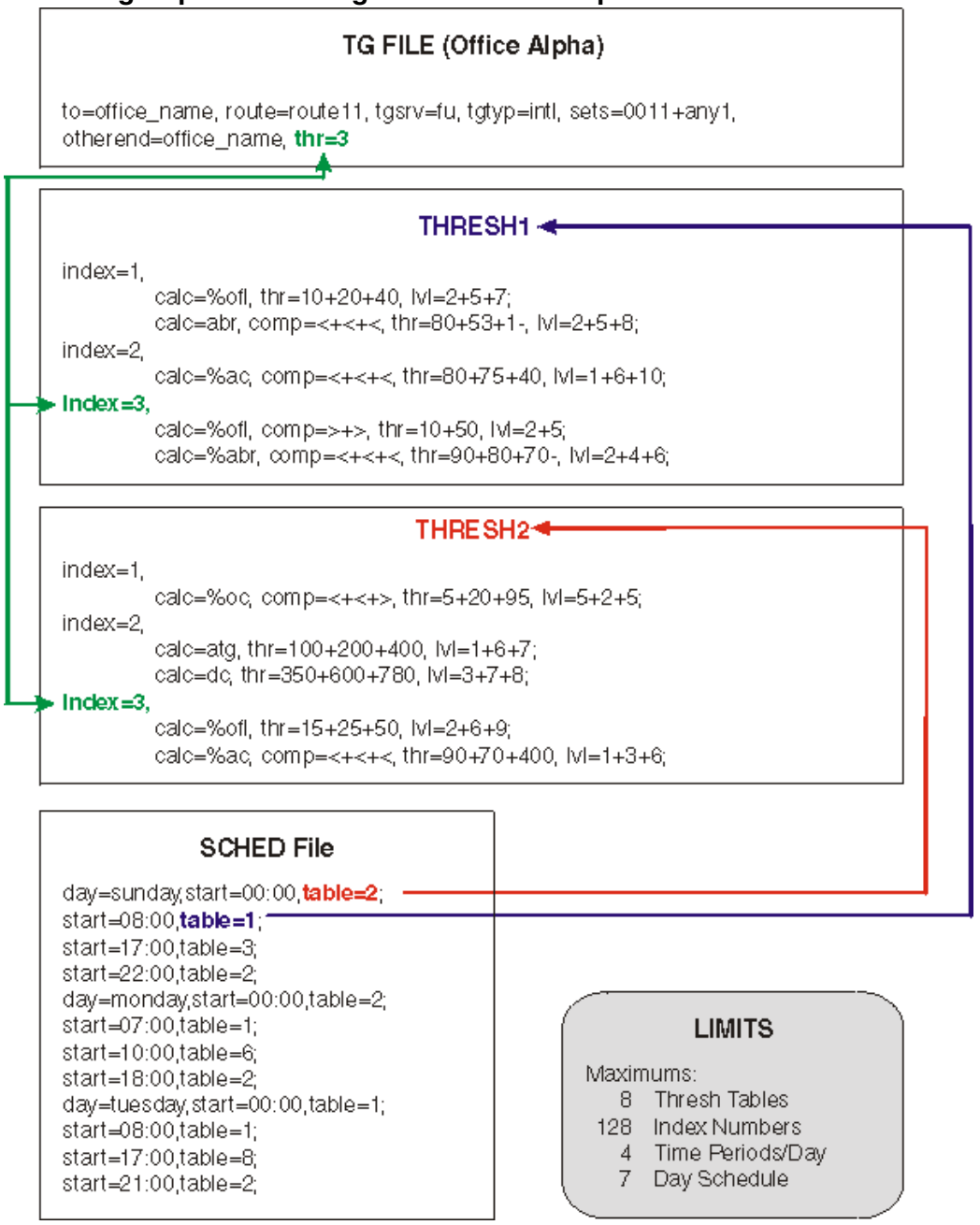
Use the Threshold Table Schedule File to schedule when to make each database threshold table active. You have the option of scheduling each table to be active at different times of the day. For example, you may schedule Table 1 to become active Monday at 10:00 a.m. and Table 5 to become active on the same day at 5:00 p.m. The thresholds used for exception processing are taken from the active table.

Figure

Figure 7 shows how the trunk group, threshold, and schedule files relate to each other.

Reference: "Trunk Group Threshold File" (p. 96)

Figure 7 Trunk group thresholding — file relationships



Setting up trunk group files

Overview

You must have one Trunk Group File for each internal office for which you want NTM to collect and store data. The file name is the full office identifier for the office. This file has one parameter that is required for all office types: the `to office` and `suffix`. Other fields that provide additional description of the trunk group may be required for some office types and optional for others. This includes such information as the trunk group service type and the trunk group type. An example of Trunk Group Files is shown in Figure 8.

Format

The format for one record entry in a *5ESS* Trunk Group File is shown as comment lines in Figure 8. Table 1, "Audit commands and functions" (p. 11) in the *Input Commands Guide* shows the fields that are supplied by audits (such as tg), the fields supplied by the user from the office information, and the fields where entries are user-determined.

Parameters

The *tgsrv* parameters are: hu (high usage, default), fi (final), and fu (full). ***High usage*** trunk groups can overflow traffic to at least one other trunk group. ***Final*** trunk groups receive traffic from other trunk groups, but calls cannot overflow further. Therefore, calls will be lost when a final trunk group is fully occupied unless a reroute control is manually applied. A ***full*** trunk group is a trunk group that does not receive overflow traffic and does not overflow to another trunk group. In other words, a full trunk group is not a part of any routing chain. The *tgsrv* parameter is for display and report output only.

The *sig* type parameter identifies the trunk group signaling type. This parameter is for display and report output only.

The *otherend* parameter specifies the suffix of a trunk group when that suffix is different at the ***other end***. This parameter is used only on the Trunk Group Detail page where it allows you to look at the measurements on a trunk group first as recorded at one end of the trunk group, then as recorded at the opposite end. This is possible only when both ends of the trunk group terminate at internal offices.

For the *thr* parameter, assign an index number (0 is the default). Index zero (0) suppresses exception calculations for the trunk group. The actual trunk group calculations to be performed for each index number and the corresponding threshold values and alert/alarm levels associated with them are defined in the Trunk Group Threshold Files ("/musr/rb/thresh/thresh*[1-8]*"). The threshold tables, compiled from threshold files, are scheduled in the Threshold Table Schedule File.

Reference: Figure 10, "Threshold table schedule file example" (p. 23)

The *options* parameter can be set to sched for trunk groups for which you want to collect measurement data from the office. After you have updated the current database with any changes to the Trunk Group File, you must then run a Trunk group schedule audit (tgsched) to update the office's trunk group schedule.

Reference: See Chapter 2, "Commands for Auditing Network Elements" in the *Input Commands Guide* for more information about schedule audits.

Additionally, the *options* parameter can be set to av or vb to indicate that the trunk group is ***not*** to be presented on reroute analysis as an AV or a VB via option for a reroute.

Figure

Figure 8 provides an example of entries in a Trunk Group File.

Figure 8 Trunk group file entries

```
$ view /musr/rb/tg/alpha

 # to=office-suffix, tgn, tgsrv, tgtyp, sig, n1wi,
 # n1wo, n2w, sets, ofl, otherend, thr, options;
 # fields supplied to current db by tg audit:  n1wi, n1wo, n2w

 to=beta-i5d0,tgn=150,tgsrv=fi,tgtyp=int,sig=isup7,sets=int,
 thr=3,options=sched;
 to=beta-i5d1,tgn=151,tgsrv=hu,tgtyp=int,sig=isup7,ofl=beta-i5d0,
 thr=3,sets=int,options=sched
 to=beta-i5d2,tgn=152,tgsrv=hu,tgtyp=int,sig=isup7,ofl=beta-i5d1,
 sets=int,thr=1,options=sched;
 to=beta-i5d3,tgn=153,tgsrv=hu,tgtyp=int,sig=isup7,ofl=beta-i5d2,
 sets=int,thr=3,options=sched;
 to=beta-i5d9,tgn=159,tgsrv=fu,tgtyp=int,sig=isup7,sets=svcs,
 thr=18,options=sched+av+vb;
```

Defining trunk group threshold files

Limitations

A maximum of up to 8 threshold files, named “thresh1” through “thresh8”, can be defined for the NTM system. Each thresh file can contain up to 128 index IDs with up to 10 calculations for each. Flags count as a calculation. The index IDs are assigned to trunk groups in the “/musr/rb/tg/*clli*” file.

Only one database thresh table (compiled thresh file) can be active in the system at a time. The time (day, hours) when a thresh table is active is scheduled in the “/musr/rb/thresh/sched” file.

Notice in Figure 9 that the index ID needs to be entered only once (with the first calculation record) for all calculations assigned to it. Up to 3 thresholds (*thr*) and three corresponding alert/alarm levels (*lvl*) can be entered for each calculation record.

Reference: Chapter 1, “All Data Fields” in the *Data Tables Guide*

Using flags

Trunk group flags received in a 5-minute measurement package from the *clli* are similar to 30-second discretes in that they signal the occurrence of an event on the trunk group and do not represent counter information. The flags all relate to automatic trunk group controls, which include: SILC, CR and ACC. If a flag is received on a trunk group, it will indicate that at least one call was affected (CANF, CANT, SKIP) by the identified control.

As with discretes, a flag does not have associated thresholds. It is either active or not active, and it can have only one alarm level.

The last entry for index=1 in Figure 9 shows the format of a flag entry.

Reference: See *flags* in the Trunk Group Threshold File for the list of flags that can be included in the thresh files.

Figure

Figure 9 provides an example of flag entries in a Trunk Group Threshold File

Figure 9 Trunk group threshold file

```
$ view /musr/rb/thresh/thresh1

  # index, calc or flag, thr, compare, lvl;

index=1,
        calc=pc,   thr=250+500+1000,   lvl=3+6+9;
        calc=%mb,  thr=99,             lvl=10;
```

```
        calc=sch,  thr=1000,           lvl=3;
        flag=cr,                       lvl=2
index=2,
        calc=%ofl,    thr=5+10+15,     lvl=7+8+9;
        calc=%iasr,   thr=60+20+10,    compare=<+<+<,  lvl=1+5+9;
        calc=isch,    thr=1000,        lvl=1+2+3;
        calc=sch,     thr=10+20+30,    lvl=1+2+3;
        calc=%tocc,   thr=70+80+90,    lvl=3+6+9;
        calc=%occ,    thr=70+80+90,    lvl=3+6+9;
        calc=mht,     thr=60+50+40,    compare=<+<+<,  lvl=1+2+3;
     .
     .
     .
index=128;
```

Scheduling threshold tables

Overview

Figure 7, “Trunk group thresholding — file relationships” (p. 18) shows the relationship between the trunk group, the thresh1- thresh8 file index numbers, and the Threshold Table Schedule File.

Limitations

Up to 4 different threshold tables can be scheduled for each day of the week (Sunday through Monday). Valid start times are 00:00 to 23:59. All 24 hours of the day must be covered.

Examples

Figure 10 shows an example of a Threshold Table Schedule File for all days of the week. In this file, you can schedule threshold tables to become active at a particular time. You may specify the day of the week, the start time, and the table (file) number. The format for entering a record is:

`[day=`*`day`*`] start=`*`start time`* `tg_table=`*`table number`*`;`

Parameters

The `day=` parameter is required only for the first entry for each day. The start=parameter indicates the time when you want the table to become active. The clock time is shown as a 24-hour clock. If you want thresholding scheduled at the beginning of the day, the start time shown for each day should be 00:00.

You may schedule up to 4 start times for one day.

The `table=` parameter value is a number from 1 to 8 that represents a thresh file number (*thresh1* through *thresh8*).

Figure

Figure 10 provides an example of entries in a Threshold Table Schedule File

Figure 10 Threshold table schedule file example

```
$ view /musr/rb/thresh/sched

# day, start, table;

day=sunday,
start=00:00,tg_table=1;
start=08:00,tg_table=2;
```

```
start=17:00,tg_table=3;
start=22:00,tg_table=4;
day=monday,
start=00:00,tg_table=1;
start=08:00,tg_table=3;
start=17:00,tg_table=6;
start=22:00,tg_table=4;
day=tuesday,
start=00:00,tg_table=1;
start=08:00,tg_table=3;
start=17:00,tg_table=4;
start=22:00,tg_table=2;
day=wednesday,
start=00:00,tg_table=1;
start=08:00,tg_table=2;
start=17:00,tg_table=3;
start=22:00,tg_table=4;
day=thursday,
start=00:00,tg_table=1;
start=08:00,tg_table=1;
start=17:00,tg_table=1;
start=22:00,tg_table=1;
day=friday,
start=00:00,tg_table=1;
start=08:00,tg_table=2;
start=17:00,tg_table=4;
start=22:00,tg_table=7;
day=saturday,
start=00:00,tg_table=5;
start=08:00,tg_table=6;
start=17:00,tg_table=7;
start=22:00,tg_table=3;
```

Control traffic type and code definition

Overview

Purpose

This section provides information about controlling traffic using traffic types, domains, and code definitions.

Contents

This section contains the following topics:

Background	3-26
Defining domain acronyms	3-28
Mapping domain acronyms	3-30
Defining codes	3-32

Background

Overview

Some office types allow network managers to restrict controls to specific types of traffic, called domains. At the offices, these domains are known as numbers, and the numbers may vary for each domain from one office type to another.

To simplify domain entry in control commands at NTM, two record base files are used. The first, called the domain acronym file, is used to define the domain names to be used in control commands and to map them to internal ID numbers. The second, called an office domain file, is used to map the defined domain names to the numbers by which the domains are known at the designated office.

When network managers enter data in a domain field of a control command, they use the domain names defined in the first file. The system checks the names against the numbers in the office domain files for the specified offices and substitutes the appropriate office domain ID numbers for the domain names.

Reference: Figure 11, “Relationship of domain files” (p. 27); “Defining domain acronyms” (p. 28); “Mapping domain acronyms” (p. 30)

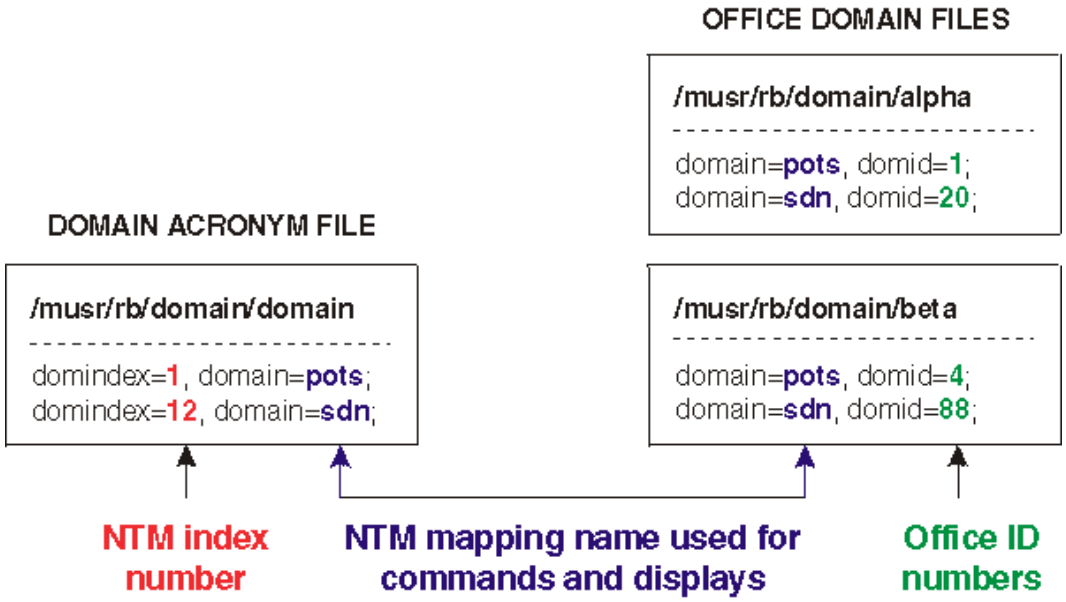
The domestic and international codes record base files are used for associating codes with destinations, normally offices that serve the codes. The office names appear in the browser-based graphical user interface as reference offices for hard-to-reach codes.

Reference: “Defining codes” (p. 32)

Figure

Figure 11 provides a diagram depicting the relationship between the different domain files.

Figure 11 Relationship of domain files



Defining domain acronyms

Overview

Some offices allow controls to be placed on particular domains. Use the domain acronym file to map user-defined domain names to internal domain index numbers.

Various controls can allow or control traffic by domain. These controls include CANT, CANF, SKIP, RR, CG, ACC, and CR.

Predefined domains

The domain acronym file comes predefined with listed domains. You can edit the list by modifying acronym names or deleting entries. An example of a domain acronym file is shown in Figure 12. The domains in the example may not apply to your network. Contact the office personnel to find out which domains apply.

Parameters

For the `domindex` parameter, enter a unique identifier (1 to 254). For the `domain` parameter, enter an actual domain name or a user-defined name (1 to 4 characters). Enter all possible domains for all internal offices. Domains will be cross-referenced to office index numbers in the "/musr/rb/domain/*exch_name*" file.

Figure

Figure 12 provides an example of entries in a Domain Acronym File.

Figure 12 Domain acronym file example

```
$ view /musr/rb/domain/domain
domindex=0, domain=all;
domindex=1, domain=pots;
domindex=2, domain=sknm;
domindex=3, domain=llov;
domindex=4, domain=iddd;
domindex=5, domain=data, subnetwork=pvna;
domindex=6, domain=isdn;
domindex=7, domain=taiw;
domindex=8, domain=orig;
domindex=9, domain=tran;
domindex=10,domain=term;
domindex=11,domain=tern;
domindex=12,domain=sdn;
domindex=13,domain=dev;
domindex=14,domain=ded;
domindex=15,domain=ssp;
```

```
domindex=16,domain=c64;
domindex=17,domain=c384;
```

Mapping domain acronyms

Overview

In an Office Domain File, acronyms that were defined in the Domain Acronym File are mapped to actual domain ID numbers for the office types.

Default office domain files are provided with your system. You will need to customize them for your location.

Format

The format for entering a record in the file is shown below.

`domain=`*`domain`*`, domid=`*`domid`*`;`

Parameters

The `domain` parameter is a domain name defined in the domain acronym file. The `domid` parameter is the appropriate domain identifier number for the office identified in the office domain file name.

Figure

An example of an office domain file is shown in Figure 13. The domains in the file are examples only. Contact your office personnel to get a list of the actual domains.

Figure 13 Office domain file example

```
$ view /musr/rb/domain/ah_2g

# domain=domain, domid=domid;

domain=pots, domid=1;
# international outbound
domain=iddd, domid=81;
# circuit switched data
domain=data, domid=82;
# software defined network
domain=sdn, domid=88;
# dedicated egress - voice
domain=dev, domid=89;
# dedicated egress - data
domain=ded, domid=90;
# 64 KB clear - single circuit
domain=c64, domid=91;
# 64 KB restricted - single circuit
domain=r64, domid=92;
```

```
# dedicated egress voice - CCS7 preferred
domain=devp, domid=97;
# dedicated egress data - CCS7 preferred
domain=dedp, domid=98;
```

Defining codes

Overview

In the Domestic Code File, each defined code is associated with a destination, normally an office name, that serves the code. Names should match network view node names.

In the International Code File, country codes are mapped to country names.

The office names must be defined in the RSPTE File. The codes are 3 or 6 digits. A code can appear only once in the file.

Figures

An example of the Domestic Code File is shown in Figure 14. In the example, the reference office for code 201 is alpha000001.

An example of the International Code File is shown in Figure 15.

Figure 14 Domestic code file example

```
$ view /musr/rb/codes/domestic

# code=code, office=office;
# NPA codes
code=201 office=alpha000001;
code=202 office=alpha000002;
code=203 office=alpha000003;
code=205 office=beta0000001;
code=206 office=beta0000002;
code=207 office=beta0000003;
# Continue for remainder of NPA's
# NPA-NXX's
code=301217 office=delta000001;
code=301221 office=delta000002;
code=301223 office=lambda00001;
code=301224 office=lambda00002;
```

Figure 15 International code file example

```
$ view /musr/rb/codes/intl

# cc=country_code, country=country;
cc=001 country=alemania;
cc=002 country=antillas;
cc=003 country=argentina;
cc=004 country=australia;
cc=005 country=aust
```

4 Data Collection Concentrator Alias File

Overview

Purpose

This document describes the DCC (Data Collection Concentrator) Alias file that is used with the various data collection devices that interface with NTM.

Contents

This document contains the following topics:

Interfaces	4-2
DCC alias file	4-3

Interfaces

EADAS

The EADAS interface is available to collect data from 1A *ESS*, *5ESS*, *DMS*, *EWSD*, *GTD5*, and LSSGR switches. Switch polling order and the data volume for each switch is handled automatically, and the Record Base Administrator does not have to determine any switch-to-EADAS mapping. This is done by automatic polling of the EADAS for the list of offices it serves.

However, it is possible that offices have different names on EADAS from those defined in the NTM system. DCC aliases must be set up to resolve this discrepancy.

Front-end processor interface (FEP)

FEP is available to collect data from *GTD-5*, *DMS* 100/200, and *5ESS* switches. Its interface to NTM is similar to the interface of the enhanced EADAS.

Traffic data management system (TDMS)

NTM supports TDMS or greater.

Network performance monitor (NPM)

NPM is treated by NTM as an EADAS.

DCC alias file

Creation

The DCC Alias file is ***not*** generated by the `create` command. The system searches this file for cases when the office name assigned in the RSPTE File is different from the office name assigned by the DCC. For example, a given office may function as both a toll office for some traffic and an end-office for other traffic. The DCC may call it the end-office name but you may always want to refer to it by its highest ranking function name in the RSPTE File.

Important! If BDR is in use, use the `bdr_commit` and `bdr_chgstat` commands to synchronize the DCC alias file between hosts.

Reference: Chapter 9, "Maintaining the Record Base with BDR"

DCC alias file format

The DCC Alias File is called "/musr/rb/*dcc_alias*". In the file, list the "alias" name used by the DCC along with the corresponding NTM CLLI code.

Use the following format for entering a record in this file:

`alias=`*`clli`*

Where:

`alias`	Office name assigned by the FEP, TDMS, or NPM
`clli`	Corresponding NTM CLLI code for the office

Examples

Figure 1 shows an example of entries in the DCC Alias File ("/musr/rb/*dcc_alias*").

Figure 1 Entries in the DCC alias file

```
brbovtmads0=brbovtma02t
brpkmawids0=brpkmawi1gt
burlvtmads0=burlvtma04t
dovrnhthds0=dovrnhth02t
eprvrinbds0=eprvrinb1gt
frmnmaunds0=frmnmaun04t
hnvrmacods0=hnvrmaco1gt
hnvrnhscds0=hnvrnhsc01t
mnchnhcods1=mnchnhco04t
spfdmawods0=spfdmawo01t
stbyvtsmds0=stbyvtsm02t
wrjtvtgads1=wrjtvtga03t
```

The recognized aliases are recorded automatically for each FEP, TDMS, or NPM in the "/musr/ofclst" directory. The CLLI code to DCC channel mapping is also recorded. This file has two types of information:

- The alias in use for a given office
- Any offices having data collected by the DCC that are not defined in the RSPTE File (these offices may need aliases)

References

For more information on the DCC interfaces, see Chapter 2, "System Functions" and Chapter 10, "NTM Engineering Guidelines" in the *System Overview*.

For more information on using the files in the "/musr/ofclst" directory, see the "Structure: DCC office list" (p. 16).

5 Record Base Files

Overview

Purpose

This chapter provides complete descriptions of all of the record base files in alphabetical order. For each record base file, there is a description of the file, an example of an entry or entries, the format for making entries in the file, and a description of the parameters.

Contents

This chapter contains the following topics:

All Point Code (APC) File	5-4
ATM File	5-6
ATM Threshold File	5-8
Code Event File	5-11
Code Event Threshold File	5-12
Control Default Domain File	5-15
Discrete File	5-16
Domain Acronym File	5-19
Domestic Code File	5-21
Event_Alarm File	5-23
Filter File	5-25
Final Handling Code (FHC) File	5-29
INMS File	5-31
International Code File	5-33
Job Status File	5-35
Job Status Threshold File	5-36
Mass Call Threshold File	5-38
Office File	5-40
Office Domain File	5-53
Office Type Domain File	5-55
Packet File	5-57
Packet Threshold File	5-60
PAS Code File	5-63
Password File	5-65
RSPTE File	5-67
Sets File	5-73
Signaling Link File	5-76
Signaling Link Threshold File	5-77
TG24HourOfl File	5-79

TG24HourOfl Threshold File	5-80
Threshold Table Schedule File	5-82
Transmitter Timeout (TTO) Thresholds File	5-84
Trunk Group File	5-86
Trunk Group Threshold File	5-96
TYPXREF File	5-103

All Point Code (APC) File

Description

Defines point codes for a network element. This is a global file.

Point codes must be defined in the All Point Code file for each internal and external office used for signaling.

The All Point Code file should exist if any of the network elements receive signaling data. Point codes should be defined and should include the associated office, and optionally the signaling point ID. Internally the system will pass data by point code, for ease of use NTM will translate this information to a *clli*-code from the RSPTE File.

Related information

Newer offices such as 5e16 can have multiple signaling points within the same network element. These require and entry in the the All Point Code (APC) File and in addition, an entry in the Signaling Link File. See the Signaling Link File for information on how to define multiple point codes within the same network element.

Valid for office type(s)

5ESS

Restrictions

5ESS switches prior to 5e16 allow one signaling points per office.

Pathname

"/musr/rb/rspte/apc"

Format(s)

`ne=`*`office`*`, pc=`*`pc`*`, sp_id=`*`Signaling Point ID`*`,`

Parameters

`office` The office name for the corresponding point code as defined in the RSPTE File.

`pc` The pc or "point code" is required to be made of three fields separated by colons. Each of the three fields has a possible value of 0 – 255. All three fields are required.

`Signaling Point ID` Valid Values of 1– 192. This is an optional field and necessary only for those offices with multiple point codes. The office and signaling point ID number uniquely identify a point code.

Examples

Figure 1 shows an example of an All Point Code file.

Figure 1 All Point Code File entry

```
ne=tst5e16,     sp_id=1, pc=001:000:000;
ne=tstna012,    sp_id=1, pc=001:000:001;
ne=tstncs1024,  sp_id=1, pc=001:000:002;
ne=artnca1135l, sp_id=1, pc=001:000:003;
ne=artnca11ds0, sp_id=1, pc=001:000:004;
ne=balbca01ds0, sp_id=9, pc=001:000:005;
```

Related record base file(s) and command(s)

"RSPTE File" (p. 67)

References

"Signaling link set audit (sls)" in the *Input Commands Guide*

□

ATM File

Description

All ATM Succession offices which receive NTM Passport CSV data, should have an ATM file set up for their links, otherwise thresholding on the link's data cannot occur. This file defines ATM Passport reference data for a Succession office. This data includes:

- links as reported in the Passport CSV file
- thresholding index which NTM uses to perform thresholding
- far end information associated with the link
- service type
- comment field

Valid for office type(s)

Succession (sn06+)

Restrictions

This file is only available if you have purchased Feature 404, "Additional Data Support for Nortel Networks Sucession Switch".

This file is restricted to a maximum of 200 entries.

The threshold index defined in the "ATM Threshold File" (p. 8), determines which calculations to perform on these links. If no entry is made for a link, it is assigned a default index value.

If entries are created in this file without assigning a threshold value a default value of 1 will be assigned. A value of zero (0) suppresses exception calculations.

Pathname

"musr/rb/atm/<*atm succession office name*>"

Format(s)

```
linkid=linkid atmsrv=atmsrv to=to thr=thr [comment=comment];
```

Parameters

`linkid` Up to a 30 characters used to identify the Passport 15K link. This should match, exactly, the LINKID records found or received in the Passport CSV file.

`atmsrv` Link type. Valid values are:

- pnni - links between Passport 15k's
- uni - links between a Passport 15k and a MG4000
- amdi - links between a Passport 15k and the Call Server

`to` Customer defined far end connection. This field is up to 30-characters. This is often the corresponding MG4000.

`thr` Threshold value. See the ATM Threshold File.

`comment` A comment of up to 80 characters.

Examples

```
linkid=EM/CINCINNATI3 ATMIF/651,atmsrv=pnni, to=CINCINNATI2, thr=2,
   comment=first and formost this is the linkid we want to monitor;
linkid=EM/CINCINNATI3 ATMIF/803,atmsrv=pnni, to=COLUMBUSOH4, thr=1,
   comment=second;
linkid=EM/CINCINNATI3 ATMIF/550,atmsrv=uni, to=CINCINNATI, thr=2,
   comment=third;
linkid=EM/CINCINNATI3 ATMIF/800,atmsrv=amdi, to=COLUMBUS, thr=1,
   comment=fourth;
linkid=EM/CINCINNATI3 ATMIF/661, atmsrv=pnni, to=MG4K_3, thr=1,
   comment=fifth;
linkid=EM/CINCINNATI3 ATMIF/551,atmsrv=pnni, to=KALIDAOHIO, thr=1,
   comment=sixth;
linkid=EM/CINCINNATI3 ATMIF/650, atmsrv=pnni, to=COLUMBUSOH4FL, thr=1,
   comment=seventh;
linkid=EM/CINCINNATI3 ATMIF/653, atmsrv=uni, to=CINCINNATITXS, thr=2,
   comment=eighth;
linkid=EM/CINCINNATI3 ATMIF/662,atmsrv=amdi, to=COLUMBUSTXS, thr=1,
   comment=ninth;
linkid=EM/CINCINNATI3 ATMIF/652, atmsrv=pnni, to=MG4K_333, thr=1,
   comment=tenth;
```

ATM Threshold File

Description

Defines for all Passport ATM succession office thresholds for the raw and calculated ATM data.

Valid for office type(s)

Succession (sn06+)

Reference: ATM data for Succession ATM MG4k is thresholded using the Office File.

Restrictions

- The table may have 256 indexes.
- Each index supports up to 20 data_fields.
- Each index supports up to 20 simple statements.
- The sum of the number of statements plus mathematical operators plus logical operators should not exceed 60.
- This file is only available if you have purchased Feature 404, "Additional Data Support for Nortel Networks Sucession Switch".
- When the value provided as a part of comparison clause is grater than 2 147 483 647(MAX_INT32) then it is implicitly converted to float data type.

Pathname

“musr/rb/thresh/atm”

Format(s)

```
index index;
   if [condition] then [data_field] level=[level_number];
```

Parameters

`index` Threshold index (a number from 0–256). This index is required as the first entry for each index record within the file.

`condition` Logical operator relating to the *`data_field`*

- and
- or
- =

- < (less than)
- < = (less than or equal to)
- > (greater than)
- >= (greater than or equal to)
- <> (not equal to)

You may also include the following expression delimiters

- (
-)

Conditional thresholding allows ***some*** field-to-field comparisons, but not others.

While all thresholdable numeric fields can be compared to integer numbers, only those fields displayed with decimal points can be compared to decimal numbers.

It is also permissible to test thresholdable fields against other thresholdable fields, but only of the same type.

> **Important!** Thresholds for max calc value entry can be 1 to 4,000,000,000. This is much higher than typical thresholds used in NTM.

`data_field` Select Record Base File = ATM Threshold file on the Search NTM Documentation page to list the valid raw and derived measurements that can be thresholded in this file. Refine the search by Switch Type or Calc Type, if desired.

`level_number` Indicates the exception level to be associated with a data field (1-10).

Examples

```
index 1;
if linkcap >= 1 then linkcap level = 8;
if sigstat >= 1 then sigstat level = 6;
if sysutil >= 40 then sysutil level = 2;
if sysutil >= 60 then sysutil level = 5;
if sysutil >= 80 then sysutil level = 9;
if incells >= 3000 then incells level = 2;
if incells >= 4000 then incells level = 5;
if incells >= 4000000000 then incells level = 9;
if insetup >= 500 then insetup level = 1;
if insetup >= 1500 then insetup level = 4;
if insetup >= 39005000 then insetup level = 9;
if outsetup >= 500 then outsetup level = 1;
if outsetup >= 1500 then outsetup level = 4;
if outsetup >= 39005000 then outsetup level = 9;
```

Related record base file(s) and command(s)

For defining ATM Succession Passport 15k offices see the ATM File.
See “Defining thresholds” in the *System Overview* for more information on defining threshold levels.

Code Event File

Description

The Code Event file allows users to define threshold indexes for code controls on the NTM System for Code Event Analysis job purposes.

Valid for office type(s)

All

Restrictions

This file is available only if you have purchased Feature 437, "Enhanced Thresholding and Analysis".

Pathname

“musr/rb/uddm/codeevent_netevent”

Format(s)

`CTLD_CODE=`*`code`*`, thr_idx=`*`index`*

Parameters

`code`	Control Code
`index`	Threshold index

Examples

```
CTLD_CODE= 1455521, thr_idx=1;
CTLD_CODE= 9764000, thr_idx=2;
```

□

Code Event Threshold File

Description

Defines all Code Event thresholds for the raw and calculated data.

Valid for office type(s)

All

Restrictions

- The table may have 256 indexes.
- Each index supports up to 20 data_fields.
- Each index supports up to 20 simple statements.
- The sum of the number of statements plus mathematical operators plus logical operators should not exceed 60.
- This file is only available if you have purchased Feature 437, "Enhanced Thresholding and Analysis".
- When the value provided as a part of comparison clause is grater than 2 147 483 647(MAX_INT32) then it is implicitly converted to float data type.

Pathname

“musr/rb/thresh/codeevent_thesh(n)”

Format(s)

```
index index;
   if [condition] then [data_field] level=[level_number];
```

Parameters

`index` Threshold index (a number from 0–256). This index is required as the first entry for each index record within the file.

`condition` Logical operator relating to the *data_field*

- and
- or
- =
- < (less than)
- < = (less than or equal to)
- > (greater than)

- >= (greater than or equal to)
- <> (not equal to)

You may also include the following expression delimiters

- (
-)

Conditional thresholding allows ***some*** field-to-field comparisons, but not others.

While all thresholdable numeric fields can be compared to integer numbers, only those fields displayed with decimal points can be compared to decimal numbers.

It is also permissible to test thresholdable fields against other thresholdable fields, but only of the same type.

Thresholds for maximum calculation value entry can be 1 to 4,000,000,000.

`data_field` Available data files for thresholding:

- tot_cg_att - Total number of call attempts for a particular call gap this period. This data file has impact on `starttime` and `stoptime`.
- tot_cg_blk - Total number of calls blocked for a particular call gap in this period. This data file has impact on `starttime` and `stoptime`.
- tot_cg_succ - Total number of call successes for a particular call gap this period. This data file has impact on `starttime` and `stoptime`.
- tot_cg_att_event - Total number of call attempts for a particular call gap during the event.
- tot_cg_blk_event - Total number of call blocked for a particular call gap during the event.
- tot_cg_succ_event - Total number of call successes for a particular call gap during the event.

`level_number` Indicates the exception level to be associated with a data field (1-10).

Examples

```
index 1;
if tot_cg_att > 0 then tot_cg_att level = 4;
if tot_cg_blk > 10 then tot_cg_blk level = 1;
if tot_cg_succ > 15 then tot_cg_succ level = 9;
if tot_cg_att_event > 20 then tot_cg_att_event level = 3;
if tot_cg_blk_event > 22 then tot_cg_blk_event level = 4;
if tot_cg_succ_event > 25 then tot_cg_succ_event level = 5;

index2;
if tot_cg_att > 0 then tot_cg_att level = 4;
if tot_cg_blk > 15then tot_cg_blk level = 1;
```

```
if tot_cg_succ > 20then tot_cg_succ level = 9;
if tot_cg_att_event > 30 then tot_cg_att_event level = 3;
if tot_cg_blk_event > 42 then tot_cg_blk_event level = 4;
if tot_cg_succ_event > 55 then tot_cg_succ_event level = 5;
```

Control Default Domain File

Description

Defines a set of default domains for specific controls. The Control Default Domain files specify how the DOMAIN field on control pages is populated. The domain identifier numbers are switch specific.

Valid for office type(s)

4ESS, *5ESS*

Pathname

"/musr/rb/domain/<office type>_dflt"

Where <office type> is "ess4" or "ess5".

Format(s)

```
cntrl=control domain=domain;
```

Parameters

`control`	Abbreviation for a control (cg — call gap; rr — reroute, etc.)
`domain`	Domain acronym (same name as the one assigned in the Domain Acronym File)

Examples

Figure 2 shows an example of a Control Default Domain file for a *4ESS* switch.

Figure 2 Control Default Domain File entry — 4ESS

```
# ess4 control default domains
cntrl=cg, domain=pots;
cntrl=rr, domain=pots;
cntrl=cg, domain=all;
```

Related record base file(s) and command(s)

The domain acronyms are defined in the "Domain Acronym File" (p. 19).

References

"Changing default domain for a control" (p. 19)

Discrete File

Description

Use the Discrete file to define a set of discretes to be monitored by the system.

A discrete is an on/off indicator generated by the switch that represents the status of an event message or alerting function in the switch itself.

Default entries are provided.

Valid for office type(s)

All

Restrictions

You must create a separate Discrete file for each office type supported.

Pathname

"/musr/rb/discrete/<type>"

Format(s)

```
discrete=discrete label=label dsctype=dsctype lvl=lvl;
```

Parameters

`discrete` NTM-defined discrete name.

Select Record Base File = Discrete on the Search NTM Documentation page for a list of valid discrete names. Refine the search by Switch Type or Calc Type, if desired.

Reference: HTML search

`label` User-defined discrete label that appears on the pages

`dsctype` Discrete type. Valid discrete types are listed in Table 1.

`lvl` Exception level of the discrete (if the discrete is set)

- Zero (0) shows that the discrete is not an alarm or alert

  Important! Use level zero (0) for the AUDADMIN, AUDCTRL, and CTRL discrete types.
- 1–5 shows an alert
- 6–10 shows an alarm

Table

Table 1 lists valid discrete types and descriptions.

Table 1 Discrete types and descriptions

Discrete Type	Valid Switch / Generic	Description	Corresponding Exception Level (*1 v 1*)
AUDADMIN	Not valid for *GTD-5* switches.	A discrete that triggers an audit because of an administration change at the switch (for example, a new trunk group has been added)	0 (zero)
AUDCTRL		A discrete that triggers an audit because a control has been executed at the switch site	
CTRL	All	A discrete that indicates a control is in effect at the switch	
SWAC		A switch surveillance-type discrete	1–5 — alert 6–10 — alarm
SERV		A services-type discrete	

Examples

Figure 3 shows an example of entries in a Discrete File for a *5ESS* switch.

Figure 3 Discrete File entries — 5ESS

```
# This 5ESS discrete file defines discretes and their (alarm and alert)
   levels

discrete=mc1,label= mc1,dsctype=swac,lvl=8;
mc2,mc2,swac,8;
mc1rcv,mc1rcv,swac,3;
mc2rcv,mc2rcv,swac,3;
slcinh,slcinh,swac,3;
rsmtbl,rsmtbl,swac,8;
trctl,trctl,ctrl,0;
esp,esp,swac,3;
tgctl,tgctl,ctrl,0;
cgctl,cgctl,ctrl,0;
acgctl,acgctl,serv,8;
e5dsmf,e5dsmf,serv,8;
silclc,silclc,audctrl,0;
atgc,atgc,audctrl,0;
mtgc,mtgc,audctrl,0;
tgrefc,tgrefc,audadmin,0;
iectgc,iectgc,audadmin,0;
tgschc,tgschc,audadmin,0;
```

```
mcgc,mcgc,audctrl,0;
pkschc,pkschc,audadmin,0;
rsmchg,rsmchg,audadmin,0;
trinh,trinh,serv,3;
tglchg,tglchg,swac,8;
tgldmd,tgldmd,swac,8;
e_aintfcg,aintfacg,serv,8;
dln1,dln1,swac,8;
dln2,dln2,swac,8;
hpcxmpnmc,hpcxmptgc,serv,2
hpcnc,hpcnc,serv,2
```

Domain Acronym File

Description

Defines a set of domain acronyms available for all offices, domain acronyms used on the NTM Pages and in the commands, and subnetworks that are allowed to use the domain on the controls. (A ***domain*** is a type of network traffic.)

Reference: "Defining domain acronyms" (p. 28); "Mapping domain acronyms" (p. 30)

Valid for office type(s)

4ESS; *5ESS*

Restrictions

You can define up to 255 domain acronyms.

Pathname

"/musr/rb/domain/domain"

Format(s)

```
domindex=index domain=domain [subnetwork=subnetwork];
```

Parameters

`index`	Unique numeric identifier for domain (1–254) An entry of zero (0) is equal to an entry of "all." Each domain is assigned an index that identifies the domain internally in the database. You must run the full `create` and `installdb` process if these indices change.
`domain`	Domain acronym (1 to 4 alphanumeric characters long) See DOMAINTYPE in *Data Tables Guide*.
`subnetwork`	Subnetworks that are permitted to control this domain of traffic. You can specify up to three subnetworks; the default is the main subnetwork or partition. If Feature 3, "Management of Record Base Partitions and Subnetworks" or one of the BDR (Backup and Disaster Recovery features — Feature 8, "Disaster Recovery (Duplex)"and Feature 40, "Enhanced Disaster Recovery" — is being used, the subnetwork keyword must be used to define which partitions will be allowed to use each domain. Otherwise, only main partition users will be able to execute controls containing a domain value. Users logged in under a non-main partition will not be able to successfully execute controls containing a domain value.

In the current NTM product this includes:

- *5ESS* switch (generic 5e5 or later) manual call gapping, cancel-to, cancel-from, skip, and reroute controls
- *4ESS* switch (generic 4e12) manual call gapping control
- *4ESS* switch (generic 4e12 or later) reroute control

Examples

Figure 4 and Figure 5 show examples of entries in the Domain Acronym file.

Figure 4 shows a record entry with a subnetwork entry.

Figure 4 Domain Acronym File entry — subnetworks

```
domindex=2 domain=data subnetwork=pvna;
```

Figure 5 shows a record entry without a subnetwork entry.

Figure 5 Domain Acronym File entry — no subnetworks

```
domindex=1 domain=pots;
```

These are examples only; they may not apply to your network. Contact the office personnel to find out which domains apply.

Related record base file(s) and command(s)

"Office Domain File" (p. 53); "Control Default Domain File" (p. 15)

□

Domestic Code File

Description

Defines codes for the following:

- NPA (Numbering Plan Area)
- NPA-NXX (Numbering Plan Area-Central Office Code Digits)

Defines codes for the domestic codes in the network. The codes defined in this file are associated with the reference office that serves each code.

Valid for office type(s)

All

Pathname

"/musr/rb/codes/domestic"

Format(s)

```
code=code office=office [set=set];
```

Parameters

`code`	3- or 6-digit character string
`office`	Office that services the code
`set`	Office set (optional). If no set name is provided, the default is "all internal offices".

Examples

Figure 6 shows an example of a Domestic Code file.

Figure 6 Domestic Code File entries

```
# NPA codes
code=201 office=nwrknj0208t;
code=202 office=washdcsw06t;
code=203 office=whplny0504t;
code=205 office=brhmalmt01t;
code=206 office=sttlwa0604t;
code=207 office=ptldmefo02t;
code=209 office=sktnca0107t;
code=212 office=nycqnyrp08t;
code=213 office=lsanca0292t;
code=214 office=dllstxtl34t;
```

```
code=215 office=waynpala42t;
code=216 office=clevoh0203t;
code=217 office=peorilpj51t;
code=218 office=mplsmndt18t;
code=219 office=sbndin0504t;
code=301 office=bltmmdch01t;
code=302 office=waynpala42t;
code=303 office=dnvrcozj05t;
code=304 office=chtnwvle25t;
code=305 office=orldflma03t;
code=306 office=mplsmndt18t;
code=307 office=dnvrcozj05t;
code=308 office=omahnenw14t;
code=309 office=peorilpj51t;
# Continue for remainder of NPA's

# NPA-NXX's
code=301217 office=rkvlmdrvcg0;
code=301221 office=cmbrmdcmmg0;
code=301222 office=bltmmddt22a;
code=301223 office=wlptmdwpmg0;
code=301224 office=annpmdancg0;
code=301225 office=bltmmdmdmg1;
code=301226 office=estnmdes07t;
code=301227 office=bthsmdwamg0;
code=301228 office=cmbrmdcmmg0;
code=301229 office=bthsmdwamg0;
```

Related record base file(s) and command(s)

All office names must be defined in the “RSPTE File” (p. 67).

Sets must be defined in the “Sets File” (p. 73).

“htr_codes” and “htr_ref” in *Input Commands Guide*.

□

Event_Alarm File

Description

Use the event_alarm file to define alert levels for events monitored by the system.

Default entries are provided.

Valid for office type(s)

All

Pathname

"/musr/rb/gui_alarm/event_alarm"

Format(s)

```
alarm=event alarm_level=lvl;
```

Parameters

`event` For definitions of the event levels, see the EVENT_LVL file.

`lvl` Alert level of the event

- Zero (0) shows that the event is not an alarm or alert
- 1–10 shows an alert level

Examples

Figure 7 shows an example of an event_alarm file.

Figure 7 Event_Alarm File entries

```
alarm=EXC_DCOLFAIL, alarm_level=2;
alarm=EXC_MANOOS,   alarm_level=1;
alarm=EXC_LATE,     alarm_level=1;
alarm=EXC_MORE,     alarm_level=1;
alarm=EXC_TTOFAIL,  alarm_level=2;
alarm=EXC_DESTFAIL, alarm_level=5;
alarm=DATA_MISSING,alarm_level=2;
alarm=TIME_DIFF,    alarm_level=1;
alarm=SYNC_OFC,     alarm_level=1;
```

References

See “Link Status Schematic” in the *User Guide* for information about displaying event alarms.

□

Filter File

Description

Specifies rules that will tag trunk group or machine data as suspect. Suspect data may then be filtered out of the pages that support Feature 74, “Improved Filtering and Reporting of Data”.

The Filter File works with the “Trunk Group Threshold File” (p. 96), which supports two types of thresholding:

- Traditional thresholding
- Enhanced thresholding (based on whether or not a site has purchased Feature 189, “Replacement Thresholding Capability for Trunk Group Data”)

Refer to the appropriate section based on the configuration of your system.

Valid for office type(s)

All

Feature impact

This file is available only with the purchase of Feature 74, “Improved Filtering and Reporting of Data”.

A different file format is used if Feature 189, “Replacement Thresholding Capability for Trunk Group Data” has been purchased.

Pathname

“/musr/rb/thresh/filter”

Format(s)

Traditional Thresholding (without Feature 189)

```
datatype=datatype esstype=esstype id=ID
   calc=calc compare=compare thr=thr;
```

Enhanced Thresholding (with Feature 189)

```
datatype=datatype esstype=esstype;
   if rule then set filter_tags suspect;
```

Parameters

`datatype` Type of data. This is required for the first calculation entry only.

- tg (trunk group)

- ma (machine)

`esstype` Office type

- ess1a
- ess4
- ess5
- dms
- gtd5
- lssgr
- ewsd
- scsnsn
- gsx

`ID` Rule number (1–5). You may specify up to five rules for each combination of datatypes and switch types.

`rule` An expression relating the *`data_fields`* that uses the following logical operators and mathematical signs:

- and
- or
- =
- <
- <= (less than or equal to)
- >
- >= (greater than or equal to)
- <> (not equal to)

Important! Each of these logical operators and mathematical signs requires a space character before and after it when used in a rule. In addition, the rules may include the following expression delimiters: left and right parentheses [`( )`].

`calc` Calculations. You can have up to three calculations per rule. If there is more than one calculation, use calc1, calc2 and calc3.

Select Calc Type = Calculated on the Search NTM Documentation page for a list of calculated fields. Refine the search by Switch Type or other option, if desired.

Reference: HTML search

`compare` Comparison of exception and threshold levels. You can select up to two comparisons using:

- < (less than)

- > (greater than)
- eq (equal to)

`thr` Threshold value (value depends on the calculation specified)

Examples

Traditional Thresholding (without Feature 189)

Figure 8 shows an example of a Filter file without Feature 189.

Figure 8 Filter File without Feature 189

```
datatype=tg esstype=ess1 id=1
        calc1=pc compare1=> thr1=5000
        calc2=ofl compare2=eq thr2=0
        calc3=ach compare3=> thr3=600;
datatype=tg esstype=ess1 id=2
        calc1=pc compare1=> thr1=200
        calc2=pc compare2=< thr2=560
        calc3=ofl compare3=eq thr3=555;
datatype=tg esstype=ess1 id=3
        calc1=pc compare1=> thr1=560
        calc2=ofl compare2=> thr2=558
        calc3=%ofl compare3=< thr3=100;
datatype=tg esstype=ess1 id=4
        calc1=ach compare1=< thr1=600
        calc2=pc compare2=> thr2=5000
        calc3=%ofl compare3=eq thr3=0;
datatype=tg esstype=ess1 id=5
        calc1=pc compare1=eq thr1=0
        calc2=ofl compare2=> thr2=50
        calc3=ach compare3=eq thr3=0;
datatype=tg esstype=ess4 id=1
        calc1=pc compare1=eq thr1=0;
datatype=tg esstype=ess5 id=1
        calc1=pc compare1=eq thr1=0;
datatype=tg esstype=dms id=1
        calc1=pc compare1=eq thr1=3;
```

Enhanced Thresholding (with Feature 189)

Figure 9 shows an example of a Filter file with Feature 189.

Figure 9 Filter File with Feature 189

```
datatype=tg, esstype=ess1;
if  pc > 200 and %ofl > 100 then set filter_tags suspect;
datatype=tg, esstype=ess4;
if  pc = 0 then set filter_tags suspect;
```

```
datatype=tg, esstype=ess5;
if  pc = 0 then set filter_tags suspect;
datatype=tg, esstype=dms;
if  pc = 0 then set filter_tags suspect;
datatype=tg, esstype=gtd5;
if  pc = 0 then set filter_tags suspect;
datatype=tg, esstype=ess4;
if  ofl > 10 then set filter_tags suspect;
if  %ofl > 50 then set filter_tags suspect;
datatype=tg, esstype=ess5;
if  ofl > 10 then set filter_tags suspect;
if  ht > 2 then set filter_tags suspect;
```

Related record base file(s) and command(s)

The rules filtering is enabled or disabled using the `exptrules` command.

Reference: See the `exptrules` command in the *Input Commands Guide* for more information about turning on or off the exception processing rules.

□

Final Handling Code (FHC) File

Description

Defines handling code reference information for FHC data for the *4ESS* switch. The FHC codes that are set by the switch are displayed on the Final Handling Codes element of the Network Element Details page.

Valid for office type(s)

4ESS

Restrictions

You can define up to 2,047 FHC codes in the file.

Pathname

"/musr/rb/fhc/fhcs"

Format(s)

`fhcid=`*`fhcid`* `name=`*`name`* `trap=`*`trap`* `priority=`*`priority`*`;`

Parameters

`fhcid`	FHC identifier number (1–2047)
`name`	FHC name that appears on the pages (up to 24 characters)
`trap`	Trap name for the FHC (up to 4 characters)
`priority`	Priority of the FHC that determines the order in which the FHCs appear on the pages; priority must be a single number from 1 to 2,047

Examples

Figure 10 shows an example of entries in the Final Handling Code File.

Figure 10 Final Handling Code File entries

```
fhcid=1 name=code_block trap=mnm priority=1;
fhcid=2 name=acc trap=anm priority=2;
fhcid=3 name=cr trap=anm priority=3;
fhcid=4 name=cant trap=mnm priority=4;
fhcid=5 name=canf trap=mnm priority=5;
fhcid=6 name=acc trap=anm priority=6;
fhcid=7 name=tg_access_restrict_block trap=mnm priority=7;
fhcid=8 name=cg trap=mnm priority=8;
fhcid=9 name=rr trap=mnm priority=9;
```

```
fhcid=10 name=no_idle_trunk trap=mnm priority=10;
```

INMS File

Description

The INMS (Inter-Network Management System) File defines the partitioning of the NTM network for data distribution and backup support. The information in this file includes the primary and secondary host that supports each subnetwork partition.

Valid for office type(s)

All

Feature impact

This is a global file. This file is used as part of the BDR (Backup and Disaster Recovery) features (Feature 8, “Disaster Recovery (Duplex)”and Feature 40, “Enhanced Disaster Recovery”).

Restrictions

Both a primary and secondary host name must be defined as NMS offices in the appropriate RSPTE File.

Pathname

“/musr/rb/inms/inms”

Format(s)

```
partition=name primary=primary _host_name
   secondary=secondary_host_name;
```

Parameters

`name` Legitimate partition name. An incorrect partition name results in an error.

`primary _host_name`Primary NTM host.

`secondary_host_name` Secondary NTM host.

Examples

Figure 11 shows an example of an entry in the INMS File.

Figure 11 INMS File entries

```
partition=nma primary=hosta secondary=hostb;
partition=nmb primary=hostb secondary=hosta;
```

In this example, the first entry defines the partition nma, which is a primary partition on host hosta. Its backup host is hostb.

The second entry defines the partition nmb, which is a primary partition for host hostb. Its backup host is hosta.

Related record base file(s) and command(s)

See Chapter 9, “Maintaining the Record Base with BDR” for more information about subnetwork partitioning.

□

International Code File

Description

Defines codes for the international codes in the network. The codes defined in this file are associated with the reference office that serves each code.

Valid for office type(s)

4ESS

Restrictions

- This file should not contain more than 100,000 entries
- No code should appear more than once.
- You are not required to define the office names in the RSPTE File.
- Deletions do not take effect until the `create all` and `installdb all` commands have been executed.

Pathname

"/musr/rb/codes/intl"

Format(s)

`cc=`*`cc`* `country=`*`country`*`;`

Parameters

`cc`	Country code (1- to 6-digit string)
`country`	Country name (1- to 12-character string)

Examples

Figure 12 shows an example of entries in the International Code file.

Figure 12 International Code File entries

```
cc=35 country=liechtenstein;
cc=401 country=nicaragua;
cc=3 country=cyprus;
cc=162 country=venezuela;
cc=2 country=argentina;

#Continue for remainder of country codes
```

Related record base file(s) and command(s)

"htr_codes" and "htr_ref" in *Input Commands Guide*.

Job Status File

Description

The Job Status file allows users to define threshold indexes for specific job.

Valid for office type(s)

All

Restrictions

This file is available only if you have purchased Feature 437, "Enhanced Thresholding and Analysis".

Pathname

“musr/rb/uddm/job_status_netevent”

Format(s)

`jobname=`*`job`*`, thr_idx=`*`index`*

Parameters

`job`	Name of the job executable file.
`index`	Threshold index.

Examples

```
jobname=mass_call.sh,thr_idx=2;
jobname=24hour_ofl.sh,thr_idx=2;
jobname=code_event.sh,thr_idx=65;
```

Job Status Threshold File

Description

Defines all Job Status thresholds for the raw and calculated data.

Valid for office type(s)

All

Restrictions

- The table may have 256 indexes.
- Each index supports up to 20 data_fields.
- Each index supports up to 20 simple statements.
- The sum of the number of statements plus mathematical operators plus logical operators should not exceed 60.
- This file is only available if you have purchased Feature 437, "Enhanced Thresholding and Analysis".
- When the value provided as a part of comparison clause is grater than 2 147 483 647(MAX_INT32) then it is implicitly converted to float data type.

Pathname

“musr/rb/thresh/job_status_thresh(n)”

Format(s)

```
index index;
   if [condition] then [data_field] level=[level_number];
```

Parameters

`index` Threshold index (a number from 0–256). This index is required as the first entry for each index record within the file.

`condition` Logical operator relating to the *data_field*

- and
- or
- =
- < (less than)
- < = (less than or equal to)
- > (greater than)

- >= (greater than or equal to)
- <> (not equal to)

You may also include the following expression delimiters

- (
-)

Conditional thresholding allows ***some*** field-to-field comparisons, but not others.

While all thresholdable numeric fields can be compared to integer numbers, only those fields displayed with decimal points can be compared to decimal numbers.

It is also permissible to test thresholdable fields against other thresholdable fields, but only of the same type.

Thresholds for maximum calculation value entry can be 1 to 4,000,000,000.

`data_field` Available data files for thresholding:

- Interval - Time how long job worked in seconds..
- ExitCode - Argument for the job exit function.

`level_number` Indicates the exception level to be associated with a data field (1-10).

Examples

```
index 1;
if exitcode = 2 then exitcode level = 6;
if interval > 5 then interval level = 4;
```

□

Mass Call Threshold File

Description

Defines all Mass Call Event thresholds for the raw and calculated data.

Valid for office type(s)

All

Restrictions

- The table may have 256 indexes.
- Each index supports up to 20 data_fields.
- Each index supports up to 20 simple statements.
- The sum of the number of statements plus mathematical operators plus logical operators should not exceed 60.
- This file is only available if you have purchased Feature 437, "Enhanced Thresholding and Analysis".
- When the value provided as a part of comparison clause is grater than 2 147 483 647(MAX_INT32) then it is implicitly converted to float data type.

Pathname

“musr/rb/thresh/masscall_thresh(n)”

Format(s)

```
index index;
   if [condition] then [data_field] level=[level_number];
```

Parameters

`index` Threshold index (a number from 0–256). This index is required as the first entry for each index record within the file.

`condition` Logical operator relating to the *data_field*

- and
- or
- =
- < (less than)
- < = (less than or equal to)
- > (greater than)

- >= (greater than or equal to)
- <> (not equal to)

You may also include the following expression delimiters

- (
-)

Conditional thresholding allows ***some*** field-to-field comparisons, but not others.

While all thresholdable numeric fields can be compared to integer numbers, only those fields displayed with decimal points can be compared to decimal numbers.

It is also permissible to test thresholdable fields against other thresholdable fields, but only of the same type.

Thresholds for maximum calculation value entry can be 1 to 4,000,000,000.

`data_field` Available data files for thresholding:

- tot_ssp_ns_5min - Total number of service attempts this period. This data file has impact on `starttime` and `stoptime`.
- tot_ssp_mass_5min - Total number of calls blocked by mass calling controls during this period. This data file has impact on `starttime` and `stoptime`.
- tot_ssp_ns_event - Total number of service attempts during the event.
- tot_ssp_mass_event - Total number of calls blocked by mass calling controls during the event.

`level_number` Indicates the exception level to be associated with a data field (1-10).

Examples

```
index 1;
if tot_ssp_ns_5min > 50 then tot_ssp_ns_5min level = 6;
if tot_ssp_ns_event > 5000 then tot_ssp_ns_event level = 9;
if tot_ssp_mass_5min > 50 then tot_ssp_mass_5min level = 8;
if tot_ssp_mass_event > 5000 then tot_ssp_mass_event level = 7;
```

□

Office File

Description

The office file defines:

- Packets scheduled for data collection
- Which calculations you want performed on an office
- Threshold levels for office calculations
- Maximum trunk group exceptions allowed per office
- Maximum hard-to-reach exceptions allowed per office
- Maximum machine exceptions allowed per office
- Additional office reference information
- A DCC (Data Collection Concentrator) dialstring
- A TCP/IP dialstring

Reference: Chapter "8920 NTM Engineering Guidelines" in the *System Overview*

Valid for office type(s)

All

Restrictions

Office names cannot be the same as sets names.

Pathname

"/musr/rb/office/*clli*"

Where *clli* is the office-identifier code of an office.

Format(s)

This file contains multiple formats and topics as follows:

Initial file entry formats	5-44
Calculation format	5-51

Examples

The following figures provide examples of Office File entries using the different Initial Entry Formats and Calculation formats.

Reference: See the "/musr/rb/office directory" for example office files.

Figure 13 shows examples of entries in the Office file that uses Format 1.

Figure 13 Office File — Format 1

```
hnpa=212 max_maxcpt=20 max_tgxcpt=50;
calc=%tot_ima thr=1.1+2.1+3.7 lvl=1+3+5;
calc=%ima thr=10+20+30 lvl=1+3+5;
calc=%nc thr=10+20+30 lvl=1+3+5;
calc=%op_cama thr=10+20+30 lvl=1+3+5;
calc=%mc_rt thr=10+20+30 lvl=1+3+5;
calc=%mc_mf thr=10+20+30 lvl=1+3+5;
calc=%mc_dp thr=10+20+30 lvl=1+3+5;
```

Figure 14 shows examples of entries in the Office file that uses Format 2.

Figure 14 Office File — Format 2

```
packets=all max_maxcpt=20 max_tgxcpt=50;
calc=%mc1 thr=1.1+2.1+3.7 lvl=1+3+5;
calc=%mc2 thr=10+20+30 lvl=1+3+5;
calc=%origdly thr=10+20+30 lvl=1+3+5;
calc=%incdly thr=10+20+30 lvl=1+3+5;
calc=%tot_ima thr=10+20+30 lvl=1+3+5;
calc=%misc_ima thr=10+20+30 lvl=1+3+5;
calc=%tdec_ima thr=10+20+30 lvl=1+3+5;
calc=%hlsc_ima thr=10+20+30 lvl=1+3+5;
calc=%frtofl thr=10+20+30 lvl=1+3+5;
```

Figure 15 shows examples of entries in the Office file that uses Format 3.

Figure 15 Office File — Format 3

```
max_maxcpt=20 max_tgxcpt=50
hilo=comb
nmdoc=yes
dtstyp=dp+tt+dp+tt
ttpm=100
cgcnt=63 ppcnt=63 flxcnt=127 rrcnt=127
rcvrscan=10+100+10+100+10+100
xmtrscan=10+100+10+100+10+100+10+100
rcvrtgn=100+101+102 xmtrtgn=103+104+105+106
crcvrtgn=107+108 anntgn=109+110+111+112+113+114+115+116
```

Figure 16 shows examples of entries in the Office file that uses Format 4.

Figure 16 Office File — Format 4 or Format 10

```
calc=%mc1 thr=10+30+90 lvl=1+2+3;
calc=%mc2 thr=10+30+90 lvl=1+2+3;
calc=%mc3 thr=10+30+90 lvl=1+2+3;
```

```
calc=%origdly thr=10+30+90 lvl=1+2+3;
calc=%incdly thr=10+30+90 lvl=1+2+3;
calc=totld thr=10+30+90 lvl=1+2+3;
calc=%orig thr=10+30+90 lvl=1+2+3;
calc=%inc thr=10+30+90 lvl=1+2+3;
calc=%outg thr=10+30+90 lvl=1+2+3;
calc=%term thr=10+30+90 lvl=1+2+3;
w4rcvrtgn=117+118 w4xmtrtgn=119+120
w4anntgn=121+122+123+124+125+126+127+128;
```

Figure 17 shows examples of entries in the Office file that uses Format 5.

Figure 17 Office File — Format 5

```
dialstring=TCP.fep1.1010;
```

Figure 18 shows examples of entries in the Office file that uses Format 6.

Figure 18 Office File — Format 6

```
packets=all,
dialstring=TCP.tstna013.9553,
dialstring2=TCP.tstna013.9554,
dialstring3=TCP.tstna013.9555,
authentication=Secure,
```

Figure 19 shows examples of entries in the Office file that uses Format 7.

Figure 19 Office File — Format 7

```
hybrid=y
packets=all,
dialstring=TCP.tstna013.9553,
dialstring2=TCP.tstna013.9554,
dialstring3=TCP.tstna013.9555,
authentication=Secure,
```

Figure 20 shows examples of entries in the Office file that uses Format 8.

Figure 20 Office File — Format 8

```
packets=all dialstring=TCP.tst5e15t.60005, cpnode=1;
calc=vct thr=1.1+2.1+3.7 lvl=1+3+5;
calc=hpc_acc_exmp thr=10+20+30 lvl=1+3+5;
calc=hpc_acg_blk thr=10+20+30 lvl=1+3+5;
calc=hpc_acg_exmp thr=10+20+30 lvl=1+3+5;
```

Figure 21 shows examples of entries in the Office file that uses Format 9.

Figure 21 Office File — Format 9

```
packets=all,
dialstring=TCP.tst5e61.13015,
dialstring2=TCP.tst5e61.13016,
```

```
dialstring3=TCP.tst5e61.13017;
```

Figure 22 shows examples of entries in the Office file that uses Format 10.

Figure 22 Office File — Format 10

```
packets=all,
dialstring=TCP.tstgsx5_1.7400;
```

Initial file entry formats

Description

Multiple initial file entry formats are available, based on network element and connection types.

Format(s)

Format 1

For *4ESS* offices:

```
hnpa=hnpa max_maxcpt=max_maxcpt max_tgxcpt=max_tgxcpt
   dialstring=dialstring;
```

Format 2

Important! Format 2 applies to switches without TCP/IP direct connect. If you have TCP/IP direct connections, see Format 6 (for *DMS*), Format 8 (for 5e15 and later), or Format 10 (for Sonus).

For a *5ESS*, *DMS, EWSD*, or LSSGR87 switch:

```
packets=packets [max_maxcpt=max_maxcpt max_tgxcpt=max_tgxcpt
   max_htrxcpt=max_htrxcpt];
```

Format 3

For the 1A *ESS* switch:

```
[hilo=hilo nmdoc=nmdoc dtstyp=dtstyp ttpm=ttpm
   cgcnt=cgcnt ppcnt=ppcnt flxcnt=flxcnt rrcnt=rrcnt
   rcvrscan=rcvrscan xmtrscan=xmtrscan
   rcvrtgn=rcvrtgn xmtrtgn=xmtrtgn
   crcvrtgn=crcvrtgn anntgn=anntgn
   w4rcvrtgn=w4cvrtgn w4xmtrtgn=w4xmtrtgn
   w4anntgn=anntgn
   max_maxcpt=max_maxcpt max_tgxcpt=max_tgxcpt;
```

Format 4

For a *GTD-5* switch:

```
max_maxcpt=max_maxcpt max_tgxcpt=max_tgxcpt mf_rec=mf_rec
   dtmf_rec=dtmf_rec;
```

Format 5

For the DCC file:

```
dialstring=dialstring;
```

Format 6

For a *DMS* 100/200 switch (generics na013 and later), *DMS* 250 (generic ucs13 and later), *DMS* 500 (ncs13 and later), using a TCP/IP direct connection:

```
packets=packets [max_maxcpt=max_maxcpt max_tgxcpt=max_tgxcpt
   max_htrxcpt=max_htrxcpt], dialstring=dialstring,
   dialstring2=dialstring, dialstring3=dialstring,
   authentication=authentication;
```

Format 7

For an SCSN switch using a TCP/IP direct connection or FTP connection:

```
hybrid=hybrid packets=packets [max_maxcpt=max_maxcpt
   max_tgxcpt=max_tgxcpt max_htrxcpt=max_htrxcpt] [uaip=uaip],
   dialstring=dialstring, dialstring2=dialstring,
   dialstring3=dialstring, authentication=authentication;
```

Format 8

For *5ESS* switch (generic 5e15 and later) and 7 R/E using a TCP/IP direct connection:

```
packets=packets [max_maxcpt=max_maxcpt max_tgxcpt=max_tgxcpt
   max_htrxcpt=max_htrxcpt] dialstring=dialstring cpnode=cpnode;
```

Format 9

For *5ESS* switch (generic 5e4 and later) and using a TCP/IP direct connection via AI:

```
packets=packets [max_maxcpt=max_maxcpt max_tgxcpt=max_tgxcpt
   max_htrxcpt=max_htrxcpt], dialstring=dialstring,
   dialstring2=dialstring, dialstring3=dialstring;
```

Format 10

For Sonus using a TCP/IP direct connection:

```
packets=packets [max_maxcpt=max_maxcpt max_tgxcpt=max_tgxcpt]
   dialstring=dialstring;
```

Format 11

For GSP using a TCP/IP direct connection:

Important! No initial file entry format is required. Proceed to the Calculation format.

Parameters

`hnpa` Home NPA (Numbering Plan Area) of the *4ESS* switch

`max_maxcpt` Maximum number of bad machine counts that can occur on an individual office before the exception system determines that the data is bad and discontinues processing machine data for that office. This can be any number from 0–65; the default is 65.

`max_tgxcpt` Maximum number of trunk groups with bad data that can occur on an individual office before the exception system determines that the data is bad and discontinues processing trunk group data for that office. This can be any number from 0–2000; the default is 2000.

`max_htrxcpt` Maximum number of hard-to-reach exceptions that can occur on the office before the exception system determines that the data for this office is bad. This can be any number from 0–1,000; the default is 1,000.

`uaip` Universal Access IP. Valid values are “yes” or “no”. To collect data from NTM Feature 404, "Additional Data Support for Nortel Networks Sucession Switch" this option should be defined as “no”.

- uaip=yes means that the office is set up as a Universal Access IP office.
- uaip=no means that the office is not setup as a Universal Access IP office.

`hybrid` Must be placed before the packets parameter. Valid values are: “y” or “n”

- hybrid=y means that the office is used as a packet AND a circuit office.
- hybrid=n means that the office is only used as a packet office.

`packets` Types of data to schedule. Valid types are listed in Table 2. If using multiple data types (not “all”), separate the data types with the plus sign (+).

Important! If you purchased Feature 263, “DMS 100/200 Switch Surveillance of 1024 Trunk Groups Via FEP”, a packet value of `all` will include a new “Trunk Group Data” packet that can contain data for up to 1024 trunk groups.

`hilo` Hilo feature of the switch. Valid values are:

- 2wire — 2-wire switch
- 4wire — 4-wire switch
- comb — combined switch

`nmdoc` Office equipped for DOC (Dynamic Overload Control) transmit. Valid values are:

- yes
- no (default)

`dtstyp` Dial tone sender types. Up to six dial tone sender types may be entered. Valid types are:

- dp — dial pulse
- tt — touch tone

`ttpm` Number of trunk-to-trunk path memory registers. This is the value of the 1A *ESS* switch parameter set card NTM. Valid values are: 0–32767, defaults to 0

`cgcnt` Number of call gap controls. This is the value of the 1A *ESS* switch parameter set card NMCODE. Valid values are: 0–63, defaults to 0

`ppcnt` Number of preprogram controls. This is the value of the 1A *ESS* switch parameter set card NMTGPP. Valid values are: 0–63, defaults to 0

`flxcnt` Number of flexible controls. If no entry is made, the system defaults to 0. This is the value of the 1A *ESS* switch parameter set card NMFLXC. Valid values are:

- 0–127 for pre-1AE11 switches
- 12–127 for 1AE11 and subsequent generics equipped with CCS7 signaling

`rrcnt` Number of reroute controls. This is the value of the 1A *ESS* switch parameter set card NMFLXC. If the 1A *ESS* switch parameter set card NMSNGLE is zero (0), then this parameter should be 0. Valid values are: 0–127, defaults to 0

`rcvrscan` Receiver scan rate. Up to six scan rates can be entered for MF (multifrequency), DP (dial pulse), and RP (revertive pulse) total and maintenance usage scan rates.

`xmtrscan` Transmitter scan rate. Up to eight scan rates can be entered for MF, DP, RP, and PCI total and maintenance usage scan rates.

`rcvrtgn` Receiver TGNs (Trunk Group Numbers). Up to three TGNs can be entered for MF, DP, and RP receiver TGNs.

`xmtrtgn` Transmitter TGNs. Up to four TGNs can be entered for MF, DP, RP, and PCI transmitter TGNs.

`crcvrtgn` Customer receiver TGNs. Up to two TGNs can be entered for DP and TT customer receiver TGNs.

`anntgn` Announcement TGNs (2-wire and 4-wire). Up to 8 TGNs can be entered for:

- regular overflow tone
- common overflow tone
- VCA (Vacant Code Announcement)
- NCA (No Circuit Announcement)
- NCA/NM (No Circuit Announcement/NM control)
- ROA (Re-Order Announcement)
- EA1 (Emergency Announcement 1)

- EA2 (Emergency Announcement 2) announcement TGNs

`w4cvrtgn` 4-wire receiver TGNs. Up to two TGNs can be entered for MF and DP receiver TGNs.

`w4xmtrtgn` 4-wire transmitter TGNs. Up to two TGNs can be entered for MF and DP transmitter TGNs.

`mf_rec` Number of multifrequency receivers (0–99999)

`dtmf_rec` Number of dual-tone multifrequency receivers (0–99999)

`dialstring` TCP/IP dialstring in the format "TCP.*`clli`*.*`socket`*", where:

- *`clli`* — the CLLI name of the office
- *`socket`* — socket number to connect to on the specified switch and later:
  - For *5ESS*, this value is normally 60005
  - For *4ESS* (4e12 and later) (Datatek port should be assigned here)
  - For *GTD-5* (gtd4003 and later), this value is normally 10724
  - For DCC's ***two*** dialstrings can be used although only one is required.
  - For SCSN, *DMS* 100/200 (na013 and later), *DMS* 250 (ucs13 and later), *DMS* 500 (ncs13 and later) or 5ESS (5e4 and later using direct connection via AI) switches ***three*** dialstrings are needed. First *`dialstring`* connects to the high channel, *`dialstring2`* for the medium channel, and *`dialstring3`* for the low channel.

Example: TCP.5e15.60005

`authentication` Optional field that indicates whether security software is to be used for authentication. This parameter can be used only with features: Feature 422, "Enhanced Security for Nortel Networks TR-746 Interface", Feature 432, "Enhanced Security for Nortel Networks Using sftp". Valid values are:

- Secure
- Insecure (default)

`cpnode` (5e15 and later). Node to which the office is connected. Valid values are: 0–15.

Table

Table 2 provides data types, descriptions, and valid switch types for packets.

Table 2 Data type / packet information (Sheet 1 of 2)

Data Type	Description	5ESS	DMS	EWSD	LSSGR	ics02+	sn02+	Sonus GSX	Sonus PSX
5e_hpcofc	GETS HPC Office Counts	5e13+							
5e_hpctgc	GETS HPC TG Counts	5e13+							
acg	AIN ACG control data								
aintf	AIN toll free service	5e11+							
all	All packets appropriate to the generic of the switch	X	X	X	X	X	X	X	X
atmmk4k	ATM MK4000 Packet Data						sn06+		
atmpassport	ATM Passport 15k Packet Data						sn06+		
bicc	Bearer Independent Call Control	5e16_2+							
bicchpc	Bearer Independent Call Control High Probability of Completion	5e16_2+							
ccs	Common Channel Signaling and 800	X							
cd	Call direction	X	X	10.5+	X	X	X	X	
cg	Code controls	X	X	10.5+	X	X	X		X
cmix	Call mix	5e16_2+							
ctrl	NM controls	X	X	10.5+ RR 13+	X	X	X	X	
dly	Delayed readiness	X	X	10.5+	X	X*	X	X	
dms_hpctgc	GETS HPC TG Counts		dms24+, na009+, ucs07+, sn05tdm+, sn02+						
dmsmb250	Trunk group data 250 MB extended		na014+, ucs14+, ncs14+			X	X		
dmsmb1024	Trunk group data 1024 MB extended		na014+, ucs14+, ncs14+			X	X		
dmsmb250ext †	Trunk group data 250 MB extended					ics04+	sn04+		
dmsmb1024ext	Trunk group data 1024 MB extended					ics04+	sn04+		
dpt_ctrl	Dynamic packet trunk group controls					ics04+	sn04+		
ewsd_hpctgc	GETS HPC TG Counts			16+					
flag	Trunk group flags	X							
gets	Government Emergency Telecommunications Service	5e13+	na009+, dms24+, sn05_250+	16+			X		

Table 2 Data type / packet information (Sheet 2 of 2)

Data Type	Description	5ESS	DMS	EWSD	LSSGR	ics02+	sn02+	Sonus GSX	Sonus PSX
hpcofc	GETS HPC Office Counts		na009+, dms24+, ucs07+, sn05tdm+, sn02+	16+					
htr	Hard-To-Reach	5e16h+							
ic	IC (Interexchange carrier) shared trunk group	X	na009+, dms24+, ncs06+, sn02+	12.1+	X	X			
ima	Additional ineffective machine attempts	X	X	10.5+	X	X	X	X	
lnp	Local Number Portability Service	5e12+							
mact	Processor occupancy data		X	12.1+	X	X	X		
nc	Matching loss/no circuit	X	X	10.5+	X	X	X	X	
ovld	Overload	X	X	12.1+	X	X	X	X	
rr	Reroute controls	X	X	13+	X	X	X	X	
siglnk	Signaling link data	5e16+							
ssp	Service switching point	X	na009+, dms24+, ncs06+, sn02+	13+	X	X			
svc	Critical service circuits	X	X		X	X	X		
tg	Trunk group	X	X	10.5+	X	X	X	X	
tgpart	Trunk Group Part (1024 TG Data)		dms24+, na007+, ucs08+, ncs07+, ics02+			X	X		
tto	IC start signal	X	X	12.1+	X	X	X		

* Hybrid office only

† **Note:** Offices must be configured with the associated extended packet feature. When extended TG packets are used, they replace the standard TG packets.

Calculation format

Description

This is the format of an example calculation entry. These entries show the calculations performed on the specified office. Any calculations not specified are not performed.

Restrictions

Calculations are not applicable for DCC network elements.

Format(s)

```
calc=calc thr=thr [compare=compare] lvl=lvl;
```

Parameters

`calc` Calculation type. Enter the names in lowercase.

Select Record Base File = Office on the Search NTM Documentation page for a list of the valid raw and derived measurements that can be thresholded. Refine the search by Switch Type or Calc Type, if desired. See HTML search.

`thr` Threshold value (up to 3 values)

Important! Thresholds for max calc value entry can be 1 to 2,000,000,000 for ATMMG4k offices. This is much higher than typical thresholds used in NTM.

`compare` Comparison of exception and threshold levels. You can select up to 3 comparisons using:

- < (less than)
- > (greater than); this is the default.
- The comparison > includes >= (greater than or equal to).

`lvl` Threshold level (1-10); you can select up to three threshold levels. Threshold level determines the color in which an exception is displayed on the browser-based graphical user interface. Default levels are:

- 1–3 — low level exception
- 4–7 — medium level exception
- 8–10 — high level exception

Reference: See Chapter “Thresholds” in the *System Overview* for more information on determining exception threshold levels.

Important! If there is a compare statement, the system evaluates the exception threshold and the compare statement to determine which values are true. It then

assigns the highest alarm level corresponding to the highest threshold that produces a value of true.

Special calculations for the *GTD-5* switch

In order to enter peripheral unit and host remote link calculations in the Office File, you need to use flags to signify starting points for the following calculations:

- host remote link calculations (hrlk;). The hrlk; flag must precede any host remote link calculations to be thresholded.
- peripheral unit (pru;). The pru; flag must precede any peripheral unit calculations to be thresholded.

These two groups of calculations should be entered after all other Office File calculations.

□

Office Domain File

Description

Defines a unique set of domain identifier/domain acronym pairs for a specific office. The office domain files are provided for domain identifiers that are different between office types. If a particular office domain file is not found in the domain directory, the office type file is used as a default.

Valid for office type(s)

4ESS; *5ESS*

Restrictions

You can define up to 127 domains for *4ESS* switches with generics prior to 4e22 and *5ESS* switches with generics prior to 5e16.

You can define up to 255 domains for *5ESS* switches with generics 5e16 and later.

Pathname

"/musr/rb/domain/<office type>_dflt"

Where <office type> is "ess4" or "ess5".

Format(s)

`domain=`*`domain`* `domid=`*`domid`*`;`

Parameters

`domain` Domain acronym (the same name as the one assigned in the Domain Acronym File)

`domid` Domain identifier (switch value returned.) Values may be from 0-255.

Important! *5ESS* switches do not supply a POTS domain when the switch is installed; instead, POTS routing must be specified using Recent Change and Verify procedures. Therefore, the domain for POTS could be different in each *5ESS* switch. You must coordinate with your routing organization to identify which Digit Analysis Selector (DAS) value was selected for routing calls using the North American Numbering Plan (NANP). The following information is part of the *5ESS* Database:

Digital Analysis Selector
Recent change view 9.1
Recent change view form: RC_DAF
View ID: RDVAF

ODA form name: DAF
ODA form title: Digital Analysis Selector
ODA Office Record: 5300-1

Examples

Figure 23 shows an example of an Office Domain file for a *5ESS* switch.

Figure 23 Office Domain File entries — 5ESS

```
#ess5 domains
#all domains
domain=all domid=0;
```

Related record base file(s) and command(s)

Domain Acronym File
Control Default Domain File
Office Type Domain File

□

Office Type Domain File

Description

Defines a unique set of domain identifier for a specific office type. If a particular office domain file is not found in the domain directory, the office type file is used as a default.

Valid for office type(s)

4ESS; *5ESS*

Restrictions

You can define up to 127 domains for *4ESS* switches with generics prior to 4e22 and *5ESS* switches with generics prior to 5e16.

You can define up to 255 domains for *5ESS* switches with generics 5e16 and later.

Pathname

"/musr/rb/domain/switch-type"

Format(s)

`domain=`*`domain`*`; domid=`*`domid`*

Parameters

`domain`	Domain acronym (1 to 4 alphanumeric characters long) See DOMAINTYPE in *Data Tables Guide*.
`domid`	Domain identifier (switch value returned.) Values may be from 0-254.

Important! *5ESS* switches do not supply a POTS domain when the switch is installed; instead, POTS routing must be specified using Recent Change and Verify procedures. Therefore, the domain for POTS could be different in each *5ESS* switch. You must coordinate with your routing organization to identify which Digit Analysis Selector (DAS) value was selected for routing calls using the North American Numbering Plan (NANP). The following information is part of the *5ESS* Database:

Digital Analysis Selector
Recent change view 9.1
Recent change view form: RC_DAF
View ID: RDVAF
ODA form name: DAF
ODA form title: Digital Analysis Selector
ODA Office Record: 5300-1

Examples

Figure 4 shows an example of the Office Type Domain file.

Figure 24 Office Type Domain File

```
#ess5 domains
domain=all, domid=0;
domain=pots, domid=1;
#international outbound
domain=iddd, domid=81;
#circuit switched data
domain=data, domid=82;
#software defined network
domain=sdn, domid=88;
```

Important! This is an example only; it may not apply to your network. Contact the office personnel to find out which domains apply.

Related record base file(s) and command(s)

Domain Acronym File
Office Domain File
Control Default Domain File

Packet File

Description

All IP Succession offices which receive NTM Passport CSV data, should have a packet file set up for their links, otherwise thresholding on the link's data cannot occur. This file defines IP Passport reference data for a Succession office. This data includes:

- links as reported in the Passport CSV file
- component type supported by the Passport 15k
- far end information associated with the link
- thresholding index which NTM uses to perform thresholding
- comment field

Valid for office type(s)

Succession (sn07+)

Restrictions

This file is only available if you have purchased Feature 416, "Support of Nortel Succession IP Solution".

This file is restricted to a maximum of 300 entries.

The threshold index defined in the "Packet Threshold File" (p. 60), determines which calculations to perform on these links. If no entry is made for a link, it is assigned a default index value.

If entries are created in this file without assigning a threshold value a default value of 1 will be assigned. A value of zero (0) suppresses exception calculations.

Pathname

"musr/rb/packet/<*IP succession office name*>"

Format(s)

```
linkid=linkid component=component to=to thr=thr [comment=comment];
```

Parameters

`linkid` Up to a 40 characters used to identify the Passport 15K link. This should match, exactly, the LINKID records found or received in the Passport CSV file.

`component` Link type. Valid values are:

- shelf - Passport 15k shelf
- card - Passport 15k CPU Card number. Value can be 0 – 15.
- fabric - Passport 15k fabric card for which NTM monitors the maximum temperature.
- ip - Internet Protocol layer.
- pvg - packet voice gateway

`to` Customer defined far end connection. This field is up to 30-characters. This is often the corresponding MG4000.

`thr` Threshold value. See the Packet Threshold File.

`comment` A comment of up to 80 characters.

Examples

```
linkid=EM/CINCINNATI3 LP/651 ETHERNET/10,component=ip,
   to=CINCINNATI2,thr=2,comment=first and formost this is the linkid we
   want to monitor;
linkid=EM/CINCINNATI3 LP/803 ETHERNET/11,component=ip,
   to=COLUMBUSOH4,thr=1,comment=second;
linkid=EM/CINCINNATI3 LP/550 ETHERNET/12,component=ip,
   to=CINCINNATI,thr=2,comment=third;
linkid=EM/CINCINNATI3 LP/800 ETHERNET/13,component=ip,
   to=COLUMBUS,thr=1,comment=fourth;
linkid=EM/CINCINNATI3 LP/661 ETHERNET/14,component=ip,
   to=LP,thr=1,comment=fifth;
linkid=EM/CINCINNATI3 LP/551 ETHERNET/15,component=ip,
   to=KALIDAOHIO,thr=1,comment=sixth;
linkid=EM/CINCINNATI3 LP/650 ETHERNET/16,component=ip,
   to=COLUMBUSOH4FL,thr=1,comment=seventh;
linkid=EM/CINCINNATI3 LP/653 ETHERNET/17,component=ip,
   to=CINCINNATITXS,thr=2,comment=eighth;
linkid=EM/CINCINNATI3 LP/662 ETHERNET/18,component=ip,
   to=COLUMBUSTXS,thr=1,comment=ninth;
linkid=EM/CINCINNATI3 LP/652 ETHERNET/19,component=ip,
   to=LP33,thr=1,comment=tenth;
linkid=EM/CINCINNATI3 LP/654 ETHERNET/20,component=ip,
   to=LP34,thr=1,comment=eleventh;
linkid=EM/CINCINNATI3 LP/663 ETHERNET/21,component=ip,
   to=LP34,thr=1,comment=twelve;
linkid=EM/CINCINNATI3 NSTA/655 VOICEGATEWAY,
   component=pvg,to=PVG_334,thr=1,comment=thirteen;
linkid=EM/COLUMBUSOH4 NSTA/803 VOICEGATEWAY,
   component=pvg,to=PVG_336,thr=1,comment=fourteen;
linkid=EM/COLUMBUSOH4 NSTA/651 VOICEGATEWAY,
   component=pvg,to=PVG_337,thr=1,comment=fifteen;
linkid=EM/COLUMBUSOH4 NSTA/551 VOICEGATEWAY,
   component=pvg,to=PVG_338,thr=1,comment=sixteen;
linkid=EM/COLUMBUSOH4 NSTA/650 VOICEGATEWAY,
   component=pvg,to=PVG_339,thr=1,comment=seventeen;
```

```
linkid=EM/COLUMBUSOH4 NSTA/550 VOICEGATEWAY,
   component=pvg,to=PVG_340,thr=1,comment=eighteen;
linkid=EM/COLUMBUSOH4,component=shelf,to=SHELF_341,thr=1,comment=ninetee
   n;
linkid=EM/COLUMBUSOH4 SHELF CARD/661,component=card,
   to=CARD_342,thr=1,comment=twenty;
```

Packet Threshold File

Description

Defines for all Passport IP succession office thresholds for the raw and calculated IP data.

Valid for office type(s)

Succession (sn07+)

Restrictions

- The table may have 256 indexes.
- Each index supports up to 20 data_fields.
- Each index supports up to 20 simple statements.
- The sum of the number of statements plus mathematical operators plus logical operators should not exceed 60.
- This file is only available if you have purchased Feature 416, "Support of Nortel Succession IP Solution".
- When the value provided as a part of comparison clause is grater than 2 147 483 647(MAX_INT32) then it is implicitly converted to float data type.

Pathname

“musr/rb/thresh/packet”

Format(s)

```
index index;
   if [condition] then [data_field] level=[level_number];
```

Parameters

`index` Threshold index (a number from 0–256). This index is required as the first entry for each index record within the file.

`condition` Logical operator relating to the *`data_field`*

- and
- or
- =
- < (less than)
- < = (less than or equal to)
- > (greater than)

- >= (greater than or equal to)
- <> (not equal to)

You may also include the following expression delimiters

- (
-)

Conditional thresholding allows ***some*** field-to-field comparisons, but not others.

While all thresholdable numeric fields can be compared to integer numbers, only those fields displayed with decimal points can be compared to decimal numbers.

It is also permissible to test thresholdable fields against other thresholdable fields, but only of the same type.

Thresholds for maximum calculation value entry can be 1 to 4,000,000,000.

`data_field` Select Record Base File = IP Threshold file on the Search NTM Documentation page to list the valid raw and derived measurements that can be thresholded in this file. Refine the search by Switch Type or Calc Type, if desired.

`level_number` Indicates the exception level to be associated with a data field (1-10).

Examples

```
index 1;
if ip_linkcap >= 5651320 then ip_linkcap level = 8;
if ip_inbytes >= 1000000 then ip_inbytes level = 6;
if ip_outbytes >= 1000000 then ip_outbytes level = 6;
if ip_inpackets >= 200000 then ip_inpackets level = 6;
if ip_outpackets >= 200000 then ip_outpackets level = 6;
if ip_sysutil >= 100 then ip_sysutil level = 2;
if ip_sysutil >= 60 then ip_sysutil level = 5;
if ip_sysutil >= 80 then ip_sysutil level = 9;
if ip_inutil >= 30 then ip_inutil level = 2;
if ip_inutil >= 40 then ip_inutil level = 5;
if ip_inutil >= 80 then ip_inutil level = 9;
if ip_oututil >= 5 then ip_oututil level = 1;
if ip_oututil >= 15 then ip_oututil level = 4;
if ip_oututil >= 20 then ip_oututil level = 9;
if ip_outpktsize >= 500 then ip_outpktsize level = 1;
if ip_outpktsize >= 1500 then ip_outpktsize level = 4;
if ip_outpktsize >= 20005 then ip_outpktsize level = 9;
if ip_inpktrate >= 5000 then ip_inpktrate level = 2;
```

Related record base file(s) and command(s)

For defining IP Succession Passport 15k offices see the Packet File.
See “Defining thresholds” in the *System Overview* for more information on defining threshold levels.

PAS Code File

Description

Define the PAS (Public Announcement Service) codes for which the *4ESS* switch sends data and specify the PAS announcement name record. The PAS data contains counts of attempts and overflows to each PAS code. Use the `pas` command to display the PAS data and reference information.

Valid for office type(s)

4ESS

Restrictions

You can have up to 512 entries in this file.

Pathname

"/musr/rb/codes/pas"

Format(s)

`pasid=`*`pasid`* `pasname=`*`pasname`* `pascode=`*`pascode`*`;`

Parameters

`pasid`	PAS identifier (offset into PAS data). The valid range is 0–511.
`pasname`	PAS announcement name (a 1- to 21-character string). Numbers, letters, and underscores (_) are the only valid characters.
`pascode`	PAS code (a 10-digit string, NPA-NXX-LINE)

Important! Although valid entries include symbols, it is recommended that only alphanumeric characters and underscores be used.

Examples

Figure 25 shows examples of entries in the PAS Code File:

Figure 25 PAS Code Entries

```
pasid=0 pasname=stock_quotes pascode=9009761515;
pasid=1 pasname=weather pascode=9009761212;
pasid=2 pasname=sports_results pascode=9009761313;
pasid=3 pasname=time pascode=9009761616
```

Related record base file(s) and command(s)

See the `pas` command in the *Input Commands Guide*.

Password File

Description

Define the Password File to be used to store the password to the Administrative Services Module (ASM).

Valid for office type(s)

5e15 and later, 7R/E, GTD5 4003 and later, and Succession sn06 and later.

Restrictions

- Available only with the purchase of:
  - Feature 282, “TCP/IP Interface to 5ESS 5E15 Generic switches”
  - Feature 381, “TCP/IP Interface to GTD-5 Switches”
  - Feature 404, "Additional Data Support for Nortel Networks Sucession Switch"
- Available only to users with `nmadm` permissions.

Pathname

“/musr/rb/password”

Format(s)

```
clli=clli login=login password=passwd sitename=sitename
   [nofiles=nofiles]
```

Parameters

`clli`	Name of the switch to which you wish to connect
`login`	User login
`passwd`	User’s password
`nofiles`	Optional data file type. Valid only if the data file does not exist for an Succession entity. The only allowed value is MG or PP. Only one file type can be specified (MG or PP). In order to stop collect either do not activate the CSV channel.

5ESS 5e16.2 and later Password conventions

5ESS 5e16.2 and later offices must follow these passwords guidelines:

- The first 6 characters of the password must contain at least two alphabetic characters, one numeric and one special character.

  It is required that the one “special character” be a punctuation mark or other ASCII printable character such as “!”, “?”, “=”.
- The password must not contain the login name string.
- Password must differ by at least 3 positions.

After establishing an initial password, users must login and change their password again as a rendundant security feature. This second “final” password is what needs to be recorded in the NTM system “/musr/rb/password” file.

`sitename` Sitename may be up to twenty four characters and may be any contiguous series of ASCII, alphanumeric characters. Space and punctuation are not allowed.

References

A sample password file, “password.example”, is provided in the “/musr/rb” directory. This file can be renamed to “password” and used to populate the logins and passwords for each office.

□

RSPTE File

Description

Use the RSPTE (Regional, Sectional, Primary, Toll, End Office) file to define the following for all internal and external network elements:

- Network element names
- An RSPTE identifier
- An associated network element nickname
- Set name(s) of which the network element is a member
- Subnetworks that can access the network element
- Type
- Generic
- Issue
- Maximum number of trunk groups for data collection (*DMS* only)

  Reference: "Building the database for 1024 trunk groups" (p. 22)
- Report
- Direct

Valid for office type(s)

All

Pathname

"/musr/rb/rspte/rspte"

Format(s)

```
office=clli rspte=rspte [nickname=nickname] [sets=sets]
   [subnetwork=subnetwork] [type=type] [generic=generic]
   [issue=issue] [max_tg=max_tg] [report=report] [direct=direct]
   [udneitype=UDNEITYPE];
```

Parameters

`clli` User-defined full CLLI code name; a 1- to 12-character string is allowed. Alphanumerics, including underscores (_), and asterisks (*), are valid characters. Only dash sign (-) is not allowed in the clli name. When an office name is changed or deleted and the record base is created and installed, it is no longer possible to look at data for that office in the current database.

Important! For Feature 86, “Local Audit Data Restoration” without BDR, a hostname must be defined. It must have the type variable defined as “nms”. For an example, see “RSPTE entry — BDR host and local audit data restoration” (p. 72)

`rspte` RSPTE Office; the format is *rrrssspppttteee*. Where:

Where …	Means …	And is a number from …
rrr	region number	001–255
sss	section number	000–255
ppp	primary number	000–255
ttt	toll number	000–255
eee	end number	000–255

The rspte number is a numerical representation of a 5-level hierarchical network of offices. Offices with portions of the RSPTE number that match are connected. In general, the last non-zero number in the rspte string gives the office rank. An office with zero in the last 3 digits of the rspte numbers (eee above) is not an end office. An asterisk at the end of the string signifies an external network element.

`nickname` A 1- to 6-character string used to identify the network element.

`sets` Office sets of which the network element is a member. These sets must be defined in the Sets File as office sets.

- You can specify up to 8 sets per network element (up to 12 if you purchase Feature 29, “Increased Set Membership for Offices”).
- Set names may be up to 8 characters (up to 12 with Feature 160, “Increased Number of Characters in Set Names”).

Reference: See the “Sets File” (p. 73) for more information on defining trunk group sets.

Notes:

1. When converting DCS-based displays to GUI map displays, the automated script run by Alcatel-Lucent field support adds a “g” to the set name for offices displayed on the GSD maps. For more information about adding nodes, see the “Types of nodes” in the *User Guide*.
2. Any entry in the RSPTE file can be used as a network element on the map.

`subnetwork` Subnetworks of which the network element is a member. If you do not specify a subnetwork, the subnetwork value defaults to the main subnetwork or, if you have partitions, to the partition to which the office belongs.

Important! If you purchased Feature 23, “Switch Type Specification Enhancement”, see the “TYPXREF File” (p. 103) for additional type and generic entries. These entries may be used in place of the NTM internally supported type and generic.

`type` Type of switch or network element supported by NTM (choose one):

• ess1a • ess4 • ess5 • dcc • dms • dms250	• dms500 • ewsd • gsp • gsx • gtd5	• lssgr • nms • psx • scsnsn • UDNE • nextone

`generic` GENERIC type supported by NTM, as follows:

• 1ae8	• 5e11	• gtd1732	• nms3
• 1ae9	• 5e12	• gtd4003	• npm6_0
• 1ae10	• 5e13	• ics02	• pl3_9
• 1ae11	• 5e14	• ics03	• psx5_1
• 1ae12	• 5e15	• ics04	• psx5_2
• 1ae13_0	• 5e16	• ics05	• rsm5_0
• 4e12	• 5e16_1	• lssgr87	• rsm5_1
• 4e13	• 5e16_1h	• na007	• sn02
• 4e14	• 5e16_2	• na009	• sn03sn04
• 4e15	• dms24	• na010	• sn04tdm
• 4e16	• dms25	• na012	• sn05
• 4e17	• dms26	• na013	• sn05_100
• 4e18	• dms27	• na014	• sn05_250
• 4e19	• dms28	• na016	• sn05_500
• 4e20	• ewsd10	• na017	• sn06
• 4e21	• ewsd11	• ncs06	• sn07
• 4e22	• ewsd12	• ncs07	• tdms1
• 4e23	• ewsd13	• ncs10	• tdms2
• 4e27	• ewsd13a	• ncs12	• tdms3
• 4e28	• ewsd16	• ncs13	• UDNE1
• 5e4	• fepr1	• ncs14	• ucs07
• 5e5	• gsp07	• ncs16	• ucs08
• 5e6	• gsx5_1	• ncs17	• ucs09
• 5e7	• gsx5_2	• nms1	• ucs12
• 5e8	• gtd1641	• nms2	• ucs13
• 5e9	• gtd1711		• ucs14
• 5e9_2	• gtd1721		• ucs16
• 5e10	• gtd1722		

Reference: For a switch type-to-generic reference, see Table "8920 NTM supported switch GENERIC" in the *System Overview*.

`issue` Issue number (0–127)

`max_tg` Maximum number of trunk groups for data collection

- (*DMS*) This can be 250 or 1024. The default is 250. This field is valid only if you have purchased
  - Feature 263, "DMS 100/200 Switch Surveillance of 1024 Trunk Groups Via FEP"

– Feature 264, “DMS 100/200 Switch Surveillance of 1024 Trunk Groups Via TDM”

- (For 5e12 and later). This can be 500, 1024, or 2000 (5e15 and later). The default is 500. This field is valid only if you have purchased
  – Feature 283, “Surveillance of 2000 Trunk Groups in a 5ESS Switch”.

`report` y or n (default is y). This field is valid only if you have purchased Feature 272, “NTM Report Writer”.

Important! Depending on the feature purchased by the customer, collecting data is restricted to 50, 100, 250 or 810 internal entities.

`direct` ai, tcp or blank (default is blank). “Tcp” value is valid if you have purchased:

- Feature 277, “TCP/IP Interface to DMS 100/200 Switches”
- Feature 282, “TCP/IP Interface to 5ESS 5E15 Generic switches”
- Feature 293, “TCP/IP Interface to DMS 250 Switches”
- Feature 296, “TCP/IP Interface to DMS 500 Switches”
- Feature 376, “Sonus GSX9000 5.1 Support”
- Feature 381, “TCP/IP Interface to GTD-5 Switches”
- Feature 403, "Nortel DMS GSP Network Element Support"

This field is valid if you are linking to a SCSNSN, GSP or Sonus switch.

“Ai” value is valid if you have purchased:

- Feature 409, “TCP/IP Interface to 5ESS Switches via AI”
- Feature 410, “TCP/IP Interface to DMS Switches via AI”.

`UDNEITYPE` UDNEIType name. Any character string of size less or equal to 20 characters. The following chracters must be restricted: plus-sign (+), semi-colon (;), backslash (\), equal (=), at-sign (@), or spaces “whitespace”.

Examples

Figure 26 shows examples of entries in the RSPTE file. Figure 27 through Figure 30 show examples of specific types of entries in the RSPTE file.

Figure 26 RSPTE Entries

```
#office rspte nickname set subnetwork type generic issue;
stlsmo0934t 001000000000000 stls seta+setb , ess4 4e14 1;
phxagcsgtd5 004000000000000 agc3 ,, gtd5 1641 1;
antomo50cg0 001000000000002* , setc;
blgrmoxa776 001000000000005* , setc;
blvwmoxa697 001000000000006* , setc;
```

```
bnkrmoxa689 001000000000007* , setc;
bossmoxa626 001000000000008* , setc;
stlsmo0905t 001000000000009* , setc;
hnblmoac05t 001000000001000* , setc;
eldnmoex01t 001000000002000* , setc;
eldnmoexdsa 001000000002001* , setc;
lwtwmoxa497 001000000003011* , setc;
mntimoxa767 001000000003012* , setc;
stvlmoxa672 001000000003018* , setc;

#Office in pvna subnetworks
galvksxads0 016000000000001* ,, pvna;

#Offices in subnetworks
wchtksahds0 016000000000002* , setd pvna+nm;
wchtksands0 016000000000003* , setd pvna+nm;

#DCC entries
db1bed5ent30 100001001000000 bed5 seta , dcc 1bed5 1;
db1bed6ent31 100001002000000 bed6 seta , dcc fepr1 1;

#BDR Host entry
cbnmha 100200300400500 cbnmha ,,, nms nms1;
```

Figure 27 RSPTE entry — Internal network element

```
snfcca2143t 001000000000000 snfcca gate+hier, ess4 4e13 1;
```

Figure 28 RSPTE entry — External network element

```
losangel04t 001001001000000* la04 , nm+pvna;
```

Figure 29 RSPTE entry — DCC

```
whpldcc01 001001000000000 edwp ,, dcc 1bed5 1;
```

Figure 30 RSPTE entry — BDR host and local audit data restoration

```
cbnmha 100200300400500 cbnmha ,,, nms nms1;
```

References

"Adding and deleting RSPTE CLLI changes" (p. 20)

"Building the database for 1024 trunk groups" (p. 22)

Sets File

Description

Defines ***office set*** names and ***trunk group set*** names. Sets are logical groupings of network elements (offices or trunk groups). Set membership determines which offices and trunk groups are displayed on the browser-based graphical user interface.

The grouping of offices and trunk groups into sets is an alternative to using hierarchical areas provided by the RSPTE record base for partitioning the network. For example, sets can be used for partitioning customers or services.

Set names can be used to limit the amount of data shown.

> **Important!** Office names cannot be the same as office set names and trunk group names cannot be the same as trunk group set names.

Valid for office type(s)

All

Restrictions

- Each office can be a member of up to 8 office sets. With the purchase of Feature 29, “Increased Set Membership for Offices” each office can be a member of up to 12 office sets.
- Each trunk group can be a member of up to 8 trunk group sets. With the purchase of Feature 32, “Increased Set Membership for Trunk Groups” each trunk group can be a member of up to ten trunk group sets.
- You can have up to 10,000 trunk groups or offices in a set.
- The limit on the number of trunk groups or offices in a given set is the system-wide limit on the number of trunk groups or offices that can be defined.
- A combination of trunk groups ***and*** offices in a set is invalid

Pathname

“musr/rb/sets/sets”

Format(s)

Office Sets

```
ofcindex=index ofcset=set_name;
```

Trunk Group Sets

```
tgindex=index tgset=set_name;
```

Parameters

`index` Single numeric identifier for office set

- (1–2,000) Small/Medium NTM configuration
- (1–4,000) Large NTM configuration.

If you change the set index, you must assign a corresponding set name that identifies the set internally in the database. You must run a full `create` and `installdb` process if these indices change.

`set_name` Set name (1 to 8 characters long, up to 12 characters if you have purchased Feature 160, “Increased Number of Characters in Set Names”). Depending on which NTM configuration you have purchased, you can define set names for up to:

- 2,000 set names for the Small/Medium NTM configuration

  or

- 4000 set names for the Large NTM configuration.

Notes:

1. Any set in the sets file can be used as a grouped node on the map.
2. When converting DCS-based displays to GUI map displays, the automated script run by Alcatel-Lucent field support adds a “g” to the set name for offices displayed on the GSD maps. For more information about adding nodes, see “Types of nodes” in the *User Guide*.

Examples

Figure 31 shows examples of entries in the Sets file.

Figure 31 Sets File entries

```
tgindex=1 tgset=seta;
tgindex=2 tgset=setb;
tgindex=3 tgset=setc;
tgindex=4 tgset=setd;
tgindex=5 tgset=sete;
tgindex=6 tgset=setf;
ofcindex=1 ofcset=setj;
ofcindex=2 ofcset=setk;
ofcindex=3 ofcset=setl;
ofcindex=4 ofcset=setm;
ofcindex=5 ofcset=setn;
ofcindex=6 ofcset=seto;
```

Notes:

1. The entries that begin with "`tgindex`" are Trunk Group Set Entries.
2. Those that being with "`ofcindex`" are Office Set Entries.

Related record base file(s) and command(s)

The Sets file is used to ***define*** sets. In order to use trunk group sets and office sets, you must enter the trunk group set names in the Trunk Group File and the office set names in the RSPTE File.

□

Signaling Link File

Description

With newer switches such as the 5e16 the standard relationship of one point code to one far end does not apply. These offices can have multiple signaling connection points. This file uses APC codes defined in the All Point Code (APC) File and Near End offices to locate Far End offices. The Signaling Link file is required to be present to complete the rspte build process.

Valid for office type(s)

5e16 and later.

> **Important!** When defining signaling points for offices earlier than 5e16 , use the All Point Code (APC) File to define the signaling points.

Pathname

"/musr/rb/rspte/siglink"

Format(s)

`fpc=`*`fpc`*`, sls=`*`sls`*`, tpc=`*`tpc`*`;`

Parameters

`fpc`	From Point Code. This may be referred to as the Near End.
`sls`	Signaling Link Set number.
`tpc`	Terminating Point Code. This may be referred to as the Far End.

Examples

The following line represents an example entry in the Signaling Link File:

```
fpc=001:000:004, sls=1, tpc=001:000:003;
```

Signaling Link Threshold File

Description

Defines threshold levels for signaling link exceptions.

Valid for office type(s)

5e16_1h and later.

Restrictions

- Each threshold file can contain up to 15 link thresholds.
- Create one threshold file for each office that has signaling functionality.
- When the value provided as a part of comparison clause is grater than 2 147 483 647(MAX_INT32) then it is implicitly converted to float data type.

Pathname

"/musr/rb/link/*clli*"

Where *clli* is the office-identifier code of an office.

Format(s)

```
calc=calc thr=thr [compare=compare] lvl=lvl;
```

Parameters

`calc`	Calculation type. Select Record Base File = Signaling Link Threshold file on the Search NTM Documentation page for a list of the valid raw and derived measurements that can be thresholded. Refine the search by Switch Type or Calc Type, if desired. See HTML search.
`thr`	Threshold value (up to 3 values)
`compare`	Comparison of exception and threshold levels. You can select up to 2 comparisons using:

- < (less than)
- > (greater than); this is the default. The comparison > includes >= [greater than or equal to].

Use the following ranges:

- 0–100 for all percentage calculations.
- 0–999,999 for the remaining calculations.

`lvl` Threshold level (a number from 1–10). You can select up to 3 threshold levels. The threshold level determines whether an exception is an alert (1–5) or an alarm (6–10).

Examples

The following lines represent example entries in the Signaling Link Threshold File:

```
calc=sl_octxmit thr=10+40+70 lvl=2+3+4;
calc=sl_octrexmit thr=10+40+70 lvl=2+3+4;
calc=sl_msuxmit thr=10+40+70 lvl=2+3+4;
calc=sl_msurexmit thr=10+40+70 lvl=2+3+4;
calc=sl_msudiscard thr=10+40+70 lvl=2+3+4;
calc=%octrexmit thr=10+40+70 lvl=2+3+4;
calc=%msurexmit thr=10+40+70 lvl=2+3+4;
calc=%msudiscard thr=10+40+70 lvl=2+3+4;
```

Important! If thresholds are defined within an office's link file, and a value like `SL_MSUXMIT=1024` falls true on more than one comparison calculation, the highest exception level value will be assigned. For example, in the line shown below, an MSUXMIT value of 1024 appears to fall within the exception level (5) range. However, it is also true that the 1024 value is greater than 0, which yields a higher exception level value of (6).

```
"/musr/rb/link/;"
calc=sl_msuxmit, thr=0+500+1500,
compare=>+>+>, lvl=6+5+9;
```

□

TG24HourOfl File

Description

The TG24Hour_Ofl file allows users to define threshold index for code controls on the NTM System for 24-Hour Final TG Overflow Event Analysis job purposes.

Valid for office type(s)

All

Restrictions

This file is available only if you have purchased Feature 437, "Enhanced Thresholding and Analysis".

Pathname

“musr/rb/uddm/tg24hourofl_netevent”

Format(s)

`ent_id=`*`clli`*`, to_id=`*`clli`*`, suffix=`*`suffix`*`, thr_idx=`*`index`*

Parameters

`clli`	Name of Network Element
`suffix`	Trunk group suffix
`index`	Threshold index

Examples

```
ent_id=kydms4,to_id=ky5e10,suffix=4,thr_idx=5;
ent_id=kydms4,to_id=ky5e10,suffix=5,thr_idx=122;
ent_id=kydms4,to_id=ky5e10,suffix=6,thr_idx=1;
ent_id=kydms4,to_id=ky5e10,suffix=7,thr_idx=1;
ent_id=kydms4,to_id=ky5e10,suffix=8,thr_idx=4;
ent_id=kydms4,to_id=ky5e10,suffix=9,thr_idx=1;
```

□

TG24HourOfl Threshold File

Description

Defines all 24-Hour Final TG Overflow Event thresholds for the raw and calculated data.

Valid for office type(s)

All

Restrictions

- The table may have 256 indexes.
- Each index supports up to 20 data_fields.
- Each index supports up to 20 simple statements.
- The sum of the number of statements plus mathematical operators plus logical operators should not exceed 60.
- This file is only available if you have purchased Feature 437, "Enhanced Thresholding and Analysis".
- When the value provided as a part of comparison clause is grater than 2 147 483 647(MAX_INT32) then it is implicitly converted to float data type.

Pathname

“musr/rb/thresh/tg24hourofl_thresh(n)”

Format(s)

```
index index;
   if [condition] then [data_field] level=[level_number];
```

Parameters

`index` Threshold index (a number from 0–256). This index is required as the first entry for each index record within the file.

`condition` Logical operator relating to the *data_field*

- and
- or
- =
- < (less than)
- < = (less than or equal to)
- > (greater than)

- >= (greater than or equal to)
- <> (not equal to)

You may also include the following expression delimiters

- (
-)

Conditional thresholding allows ***some*** field-to-field comparisons, but not others.

While all thresholdable numeric fields can be compared to integer numbers, only those fields displayed with decimal points can be compared to decimal numbers.

It is also permissible to test thresholdable fields against other thresholdable fields, but only of the same type.

Thresholds for maximum calculation value entry can be 1 to 4,000,000,000.

`data_field` Available data files for thresholding:

- tg_ofl - Trunk group overflow this period.
- tot_tg_ofl - Trunk group overflow this event. This data file has impact on `starttime` and `stoptime`.

`level_number` Indicates the exception level to be associated with a data field (1-10).

Examples

```
index 1;
if tg_ofl >= 100 then tg_ofl level = 4;
if tot_tg_ofl >= 850 then tot_tg_ofl level = 6;
```

□

Threshold Table Schedule File

Description

This file allows you to schedule a time for a particular Trunk Group Threshold Table to become active. You may specify the:

- Day of the week
- Start time
- Table number

Important! You do not need a Threshold Table Schedule file if you only have one Trunk Group Threshold File.

Valid for office type(s)

All

Pathname

"/musr/rb/thresh/sched"

Format(s)

```
[day=day] start=start time tg_table=table number;
[day=day] start=start time <UDDMType>_table=table number;
```

Parameters

`day` Day of the week (required for first entry only for each day)

- monday
- tuesday
- wednesday
- thursday
- friday
- saturday
- sunday

`start time` Actual starting time for table to become active. There is a maximum of 4 start times allowed per day. If you want thresholding scheduled at the beginning of the day, the first start time should be `00:00`.

`table number` Number of the table you are scheduling to become active (a number from 1–8)

Examples

Figure 32 shows an example of entries in a Threshold Table Schedule file.

Figure 32 Threshold Table Schedule File entries

```
day=monday start=00:00 tg_table=1;
start=08:00 tg_table=2;
start=17:00 uddm_table=3;
start=22:00 uddm_table=4
```

This table indicates that on Monday:

- Table 1 will be in effect from midnight to 8:00 am.
- Table 2 will be in effect from 8:00 am to 5:00 pm.
- Table 3 will be in effect from 5:00 pm to 10:00 pm.
- Table 4 will be in effect from 10:00 pm to midnight.

Related record base file(s) and command(s)

The Threshold Table Schedule file is used to activate specific Trunk Group Threshold Files. In order to use trunk group schedule files, you must enter the trunk group threshold exception indexes in the Trunk Group File and define exception levels in the Trunk Group Threshold File.

□

Transmitter Timeout (TTO) Thresholds File

Description

Defines the exception thresholds to be used for transmitter timeout exceptions.

Valid for office type(s)

All except *GTD-5* and *4ESS* switches.

Restrictions

- Up to 99 individually assigned thresholds can be made. The remainder of the thresholds may not be individually assigned.
- One default threshold can be specified for all carriers that do not have a carrier-specific threshold.
- When the value provided as a part of comparison clause is grater than 2 147 483 647(MAX_INT32) then it is implicitly converted to float data type.

Pathname

"/musr/rb/tto/*clli*"

Where *clli* is the office-identifier code of an office.

Format(s)

```
icprefix=icprefix fgp=fgp thr=thr lvl=lvl;
```

Parameters

`icprefix` Interexchange carrier prefix for IEC shared trunk group. A maximum of 100 defined IEC prefixes per Trunk Group is allowed (not including the default). Any icprefix not specified will be thresholded using the "default" icprefix, if one is defined.

Reference: Table 3, "Record base CIC requirement matrix" (p. 91)

`fgp` Feature group prefix.

Reference: Table 3, "Record base CIC requirement matrix" (p. 91)

`thr` Threshold value (up to three values) (0–99999) Threshold value (up to three values) (0–1048576 for 5e15+). The threshold values automatically apply to the IC_TTO count.

`lvl` Exception level of the TTO

Examples

Figure 33 shows an example of an entry in the TTO file.

Figure 33 Transmitter Timeout File Entries

```
icprefix=default thr=10+20+30 lvl=1+4+8;
icprefix=0111 thr=15+25+35 lvl=3+7+10;
icprefix=0333 thr=20+30+40 lvl=3+7+10;
icprefix=0444 thr=15+25+35 lvl=lvl=3+7+10;
```

Trunk Group File

Description

Specifies different types of trunk groups for each office and is also used to define trunk group threshold exception indexes.

Valid for office type(s)

All

Restrictions

A Trunk Group file must be created for each internal office.

Pathname

"/musr/rb/tg/*clli*"

Where *clli* is the office-identifier code of an office.

Format(s)

```
to=office-suffix [tgn=tgn] | [icprefix=icprefix]
   [fgp=fgp] [sfgn=sfgn] [btfn=btfn] [tgsrv=tgsrv]
   [tgtyp=tgtyp] [sig=sig] [n1wi=n1wi] [n1wo=n1wo]
   [n2w=n2w] [sets=sets] [trk_key_info=trk_key_info]
   [subnetwork=Trunk group name used by Nortel SCSN switch to identify
   the trunk group in the OM TRK CSV files. Prior to SN07, this name is
   defined in the following format:]
   [ofl=ofl] [otherend=otherend] [thr=thr]
   [options=options] [comment=comment];
```

Parameters

`office-suffix` To Office Name and Trunk Group Suffix separated by a hyphen (-).

Example: albynyss05t-aaaa

Where: "albynyss05t" is the To Office Name and "-aaaa" is the Trunk Group Suffix.

Important! It is invalid to use "-tgn" or "-to" as a Trunk Group Suffix.

Other-end trunk groups are directly determined by the "otherend" keyword in NTM.

The *otherend* keyword is only required if the true other-end of the trunk group uses a different suffix in the NTM database. If not, the system default is the same suffix with the *to* and *from* CLLIs reversed.

`tgn` Trunk Group Number

- 1–1024 — 1A *ESS*
- 1–4095 — *4ESS*
- 1–8191 — *5ESS* (5e14 and earlier)
- 1–2000 — *GTD-5* generics prior to 1721
- 1–9999 — 5e15 and later, 7R/E*, DMS*, *EWSD*, GSP, LSSGR, SCSN, Sonus
- 1–6000 — *GTD-5* generics 1721 and later

`icprefix` Interexchange carrier prefix for IEC shared trunk group. A maximum of 100 defined IEC prefixes per Trunk Group is allowed (not including the default).

Reference: Table 3, “Record base CIC requirement matrix” (p. 91)

`fgp` Feature group prefix.

Reference: Table 3, “Record base CIC requirement matrix” (p. 91)

`sfgn` 1A *ESS* switch type simulated facility group number (1–4096)

`btfn` Base Traffic Number

– (0–9976) (*4ESS*)

Important! For a *4ESS*, you must supply the BTFN for proper operation of the TGLIST Audit.

– (0–16 characters) (GSP)

`tgsrv` Trunk Service Type

- For non-7R/E and non-SCSN switches:
  – hu (high usage) (default)
  – fi (final)
  – fu (high usage and final)
- For *5ESS* (5E16_2 and later), SCSN switches with a *tgtyp* of virtual:
  – vhu (virtual high usage)
  – vfi (virtual final)
  – vfu (virtual high usage and final)
- For *5ESS* (5E16_2 and later), SCSN switches with a *tgtyp* of physical:
  – phu (physical high usage)
  – pfi (physical final)
  – pfu (physical high usage and final)

`tgtyp` Trunk Group Type

- dis (dial-it service) — *4ESS*
- dismix (shared between dis and normal traffic) — *4ESS*
- dom (domestic) —all switch types
- ic (Interexchange Carrier) — all switch types
- intl (international) — *4ESS*, *GTD-5,* GSX
- pool — all switch types
- wbtg (wideband trunk group) — *5ESS* (5e9_2 and later)
- virtual — 7R/E, SCSNSN, *5ESS* (5E16_2 and later)

Important! Only wbtg can be specified with one other trunk group type, the others can't be specified with each other.

`sig` Signaling Type. Valid Signaling Types are listed in Table 4, "Signaling type/switch cross reference" (p. 93).

- For *4ESS, 5ESS, DMS,* GSP, LSSGR87, or *EWSD* switches — you are not required to enter a signaling type. The trunk group reference audit for all these switch types can determine if a trunk group is "isup7" or not. When the audit response indicates that the trunk group uses in-band signaling, the audit stores the signaling type as "noncc" for *4ESS* switches or "mf" for *5ESS*, *DMS*, LSSGR87, and *EWSD* switches, regardless of the value in the trunk group file. If the audit response indicates that the trunk group uses out-of-band signaling (i.e. CCS7) and is therefore capable of supporting ISDN (Integrated Services Digital Network) ISUP (User Part) calls, the audit stores the signaling type as "isup7".
- For the *GTD-5* switch — you are not required to enter a signaling type. The trunk group list audit provides detailed signaling type information for *GTD-5* trunk groups.
- For the 1A *ESS* — if no signaling type is entered, the signaling type may be treated as "nosig".
- For 5E16_2 and 7R/E IVTA virtual trunk groups, the signaling type may be "bicc".
- For SCSN switches with a *`tgtyp`* of virtual, values can be: "nosig", "isup7", or "sip-t".
- For SCSN switches with a *`tgtyp`* of physical, values can be: "nosig", "isup7", "mf", "dp".

Important! The *`n1wi`*, *`n1wo`*, and *`n2w`* fields are not required because the switch reference audit updates the number of circuits on 1A *ESS* switches. The sfgn circuits are not provided by the switch audit, so `n1wo` should be entered.

`n1wi` Number of 1-way incoming circuits

`n1wo` Number of 1-way outgoing circuits

`n2w` Number of 2-way circuits

`sets` Trunk Group Sets. These sets must be defined in the Sets File as trunk group sets. Valid values are:

- Up to 4 trunk group sets are allowed, with a 1- to 12-character string.
- Up to 10 trunk group sets can be associated with a network element if you purchase Feature 32, "Increased Set Membership for Trunk Groups".

Reference: See the "Sets File" (p. 73) for more information on defining trunk group sets.

`trk_key_info` Trunk group name used by Nortel SCSN switch to identify the trunk group in the OM TRK CSV files. Prior to SN07, this name is defined in the following format:

`TGNAME.TRKDIR.NCCT.NWCCT`

where `TGNAME` is similar to the destination CLLI,

`TRKDIR` = 2W or IC or OG,

`NCCT` = the number of circuits,

`NWCCT` = the number of circuits in service.

For generic SN07 and later, the new format is:

`TGID.TGNAME.TRKDIR.NCCT.NWCCT`

with the addition of the `TGID` at the beginning of the name.

Because the trunk group name includes the `TGID`, it is no longer necessary to include the keyword `trk_key_info` in the record base file for generics SN07 and later generics.

`subnetwork` Subnetwork to which this trunk group belongs. If you do not specify a subnetwork, the default becomes the union of the "From Office" and "To Office" of the trunk group. For example, if the "From Office" is in "nmc" and "snwa" and the "To Office" is in "snwa," the trunk group is assigned to "snwa" and "nmc." The record base administrator can:

- assign the subnetwork by entering this parameter in the record base
- allow the `create` command to automatically assign the default

`ofl` Overflow Office Name and Trunk Group Suffix; suffix must be a 1- to 5-character string. This field is intended for 2-way and 1-way out trunks.

`otherend` Suffix of trunk group from the "To Office" to this office; must be a 1- to 5-character string. This parameter shows the trunk group that is at the "other end" in the trunk group record base of the "To Office." The `otherend` keyword is only required if the true other-end of the trunk group uses a different suffix in the NTM database. If not, the system default is the same suffix with the ***to*** and ***from*** CLLIs reversed.

`thr` Exception Threshold Index; valid values are 0–256 (the default is zero). This index is found in the thresh [*n*] (where *n* equals 1–8) file. The threshold index determines which calculations to perform on this trunk group. A value of zero (0) suppresses exception calculations.

`options` Options on the trunk group (multiple options are allowed, separated by a "+" sign). Valid values are:

- sched — schedule trunk group in the trunk group schedule audit or Modified Trunk Subgroup schedule audit; not valid for 1A *ESS* switches or 7R/E, pts3 generic.)

  Important! `options=sched` is only valid for *4ESS* switches with generics 4e17 or later and with Feature 71, "4ESS Switch Generics 4E14(R4) - 4E18(R1) Support" enabled. If this is not the case, trunk group scheduling must be done by setting up a study group at the *4ESS* switch.
- av — not to be used as AV via on the reroute
- vb — not to be used as VB via on the reroute
- mtd — identifier for Modified Trunk Subgroup Data
  - Any trunk group assigned "`options=mtd`" will be automatically treated as if it were assigned "`options=mtd+av+ab`". MTD trunk subgroups cannot be used for rerouting calls.
  - For the *4ESS* switch, you can schedule up to 255 MTD trunk groups above the 1023 (4027 with generic 4e21 or later) regular trunk group limit. However, you must first add the "`sched+mtd`" flags to the options field for the desired trunk group.

    Next, create the office (using a single office `create`) so that MTD trunk groups can be added to the NTM database. Finally, run the regular trunk group schedule (tgsched) audit which will schedule the regular and MTD trunk groups in the *4ESS* switch.

`comment` A comment of up to 80 characters. This will be available for display on the Trunk Group Detail page.

Important! Although most alphanumeric characters are valid in the comment field, you cannot use a semi-colon (;), backslash (\), equal (=), or at-sign (@).

Tables

The following tables provide more details for the Trunk Group File parameters.

Table 3 Record base CIC requirement matrix

Switch Type	Generic	FGP	rb/tg	rb/tto
ESS1A	1ae11-	Illegal	0001–0999	0001–0999
	1ae12+	D	0001–9999	0001–9999
ESS4	4e17-	Illegal	0001–0999	Not Applicable
	4e18+	D	0001–9999	Not Applicable
ESS5	5e7-	Illegal	0001–0999	0001–0999
	5e8	B	0001–9999	0001–9999
	5e8	D	0001–0999	0001–0999
	5e9+	B or D	0001–9999	0001–9999
DMS, DMS250, DMS500	BCS36-	Illegal	0001–0999	0001–0999
	na012+, ucs12+, ncs12+	D	0001–9999	0001–9999
EWSD	ewsd13-	Illegal	0001–0999	Not Applicable
	ewsd_13a+	D	0001–9999	Not Applicable
GSP	gsp07+	D	0001–9999	0001–9999
LSSGR	87 Version	Illegal	0001–0999	0001–0999
SCSNSN	all	B or D	0001–9999	0001–9999
GTD5	all	B	0001–9999	Not Applicable
		C	0001–9999	Not Applicable
		D	0001–9999	Not Applicable
GSX	all	B or D	0001–9999	Not Applicable

Table 4 Signaling type/switch cross reference

Value	Description	1A ESS	4ESS	5ESS	DMS	GSP	EWSD	GTD-5	LSSGR	SCSN	Sonus GSX
bicc	Bearer Independent Call Control			X							
comb	combined dial pulse/dual-tone multifrequency							X			
dp	dial pulse			X	X	X	X	X	X		
dtmf	dual-tone multifrequency							X			
fast	multifrequency-fast							X			
isup7	integrated services digital network user part (ISUP) number 7		X	X	X	X	X		X	X	X
mf	multifrequency			X	X	X	X	X	X		X
noncc	non-common channel		X								
nosig	no signaling	X	X	X	X	X	X	X	X		
pri	Primary Rate Interface							X			
sip-t	Signaling IP									X	
ss7	Signaling System 7							X			

Examples

Figure 34 shows an example of entries in the Trunk Group file. The second trunk group entry is for a “pvna” trunk group.

Figure 34 Trunk Group File entries

```
to=albynyss05t-aaaa
tgn=100 tgsrv=hu sig=ccs7 sets=seta
ofl=albynyss05t-bbbb otherend=dddd thr=3
options=sched+vb;

to=phlapasl40t-aaaa
tgn=101 btfn=1001 tgsrv=hu sig=noncc
sets=setb subnetwork=pvna thr=65;
```

Figure 35 shows an example of a Trunk Group file entry for a *4ESS* switch.

Figure 35 Trunk Group File entries — 4ESS

```
to=sim4e14ent03-001 tgn=1 n2w=100 thr=1 btfn=9001;
```

```
to=sim4e14ent03-002 tgn=2 n2w=100 thr=1 btfn=4001;
to=sim4e14ent03-003 tgn=3 n2w=100 thr=1 btfn=9001;
to=sim4e14ent03-004 tgn=4 n2w=100 thr=1 btfn=2001;
to=sim4e14ent03-005 tgn=5 n2w=100 thr=1 btfn=4001;
to=sim4e14ent03-006 tgn=6 n2w=100 thr=1 btfn=4001;
to=sim4e14ent03-007 tgn=7 n2w=100 thr=1 btfn=4001;
to=sim4e14ent03-008 tgn=8 n2w=100 thr=1 btfn=4001;
to=sim4e14ent03-009 tgn=9 n2w=100 thr=1 btfn=4001;
to=sim4e14ent03-010 tgn=10 n2w=100 thr=1 btfn=4001;
```

Figure 36 shows an example of a Trunk Group file entry for a *5ESS* switch that includes an IEC (Inter-Exchange Carrier) trunk group.

Figure 36 Trunk Group File entries — 5ESS

```
to=sim4e14ent03-001 tgn=1 tgsrv=hu sig=mf sets=hier+eo+mas+acct
   ofl=sim4e14ent03-002 otherend=001 options=sched thr=1;
to=sim4e14ent03-002 tgn=2 tgsrv=hu sig=isup7 sets=hier+nsc
   ofl=sim4e14ent03-003 otherend=001 options=sched thr=1;
to=sim4e14ent03-003 tgn=3 tgsrv=fi sig=isup7 sets=hier+spac+vdms+hun1
   ofl=sim4e14ent03-004 ,otherend=001 thr=1;
to=sim4e14ent03-004 icprefix=1234 fgp=d tgsrv=hu tgtyp=dis+wbtg
   sig=isup7 sets=hier ofl=sim4e14ent03-005 otherend=001 options=sched
   thr=1;
```

Figure 37 shows an example of a trunk group file entry for a 1A *ESS* switch.

Figure 37 Trunk Group File entries — 1A ESS

```
to=sim4e14ent03-001 tgn=1 tgsrv=hu sig=nosig sets=hier ofl=sim4e14ent03-
   002 otherend=001 thr=1;
to=sim4e14ent03-002 tgn=2 tgsrv=hu sig=nosig sets=hier ofl=sim4e14ent03-
   003 otherend=001 thr=1;
to=sim4e14ent03-003 tgn=3 tgsrv=fi sig=nosig sets=hier ofl=sim4e14ent03-
   004 otherend=001 thr=1;
```

Figure 38 shows an example of a trunk group file entry for a *GTD-5* switch.

Figure 38 Trunk Group File entries — GTD-5

```
to=anhmca01amd-fg tgn=8 thr=16 tgsrv=fu options=sched ;
to=anhmca01amd-se tgn=3 thr=16 tgsrv=fi options=sched ;
to=anhmca01amd-cm tgn=4 thr=07 tgsrv=fi options=sched ;
to=anhmca01ds0-ph ofl=anhmca0295t-af tgn=5 thr=02 tgsrv=fi
options=sched ;
to=anhmca0152t-da tgn=2 thr=05 tgsrv=fi options=sched ;
to=anhmca0152t-cn tgn=125 thr=07 tgsrv=fi options=sched ;
to=anhmca0152t-nc tgn=126 thr=07 tgsrv=fi options=sched ;
to=anhmca0177k-ph ofl=anhmca0295t-af tgn=094 thr=02 tgsrv=hu
options=sched ;
to=anhmca0295t-af tgn=124 thr=01 tgsrv=fi options=sched otherend=af;
to=anhmca0295t-ct tgn=187 thr=01 tgsrv=fi options=sched
otherend=a001;
```

```
#iec's
to=alnxfdic444-ic n1wo=0252 tgsrv=fi icprefix=444 ;
to=aepxfdic729-ic n1wo=0252 tgsrv=fi icprefix=729 ;
to=mcixfdic022-ic n1wo=0252 tgsrv=fi icprefix=022 ;
to=mcjxfdic088-ic n1wo=0252 tgsrv=fi icprefix=088 ;
to=tvtxfdic408-ic n1wo=0252 tgsrv=fi icprefix=408 ;
to=gtd5extern-ic1 n1wo=0252 tgsrv=fi icprefix=9996 fgp=b;
to=gtd5extern-ic2 n1wo=0252 tgsrv=fi icprefix=9998 fgp=c;
to=gtd5extern-ic3 n1wo=0252 tgsrv=fi icprefix=9997 fgp=d;

#exercise tgn field.
to=gtd5extern-tst1 tgn=1 options=sched;
to=gtd5extern-tst2 tgn=2000 ;
```

Figure 39 shows an example of a trunk group file entry for a GSP switch.

Figure 39 Trunk Group File entries — GSP

```
to=tstna017t-0003 btfn=abc3 tgn=0003 thr=1 sig=mf sets=tg1 tgtyp=dom
   tgsrv=hu comment=Manually Out of Service;
to=tstna017t-0004 btfn=abc4 tgn=0004 thr=1 sig=mf sets=tg1 tgtyp=dom
   tgsrv=hu comment=Under Repair;
to=tstna017t-0005 btfn=abc5 tgn=0005 thr=1 sig=mf sets=tg1 tgtyp=dom
   tgsrv=hu comment=;
to=tstna017t-0006 btfn=abc6 tgn=0006 thr=1 sig=mf sets=tg1 tgtyp=dom
   tgsrv=hu comment=;
to=tstna017t-0007 btfn=abc7 tgn=0007 thr=1 sig=mf sets=tg1 tgtyp=dom
   tgsrv=hu comment=;
to=tstna017t-0008 btfn=abc8 tgn=0008 thr=1 sig=mf sets=tg1 tgtyp=dom
   tgsrv=hu comment=;
to=tstna017t-0009 btfn=abc9 tgn=0009 thr=1 sig=mf sets=tg1 tgtyp=dom
   tgsrv=hu comment=testing;
to=tstucs17t-0010 btfn=abc10 tgn=0010 thr=1 sig=dp tgsrv=fu
   comment=Gateway;
```

Related record base file(s) and command(s)

The Trunk Group file is used to define trunk group threshold exception indexes. These indexes identify which set of calculations or flags in a Trunk Group Threshold File to use in defining exception levels, which are then activated by the active compiled threshold table as scheduled in the Threshold Table Schedule File.

References

See Chapter “8920 NTM Engineering Guidelines” in the *System Overview* for valid threshold ranges and for trunk groups that may be scheduled.

□

Trunk Group Threshold File

Description

The Trunk Group Threshold File is used in two different ways. Refer to the appropriate section based on the configuration of your system.

- Traditional thresholding
- Enhanced thresholding — Based on whether or not a site has purchased Feature 189, “Replacement Thresholding Capability for Trunk Group Data”. This feature increases the maximum number of threshold levels in a threshold rule from 3 to 10.

Valid for office type(s)

All

Restrictions

- Use the trunk group threshold files (“musr/rb/thresh/thresh*[1-8]*”) to specify values for each threshold index.
- NTM supports up to 8 trunk group threshold files in the record base.
- There is no limit to the number of *flags*. However, 9 *calc*s and all the *flags* for a given index count as 10 *calc* entries. Therefore, all *flags* together are seen as a single *calc*.
- It is recommended that primary subnetworks use indices 1–64.
- Network managers for other subnetworks should cooperate to define the use of index ranges above 64.
- When the value provided as a part of comparison clause is grater than 2 147 483 647(MAX_INT32) then it is implicitly converted to float data type.

Pathname

“/musr/rb/thresh/thresh*[n]*”

Where *[n]* is a number from 1–8 that specifies a threshold index.

Format(s)

Formats differ between Traditional Thresholding and Enhanced Thresholding, as follows:

Traditional thresholding (without feature 189)

Calculation Entry Format

```
[index=index]
   calc=calc thr=thr
   [compare=compare] lvl=lvl;
```

Flag Entry Format

```
[index=index] flag=flags lvl=lvl;
```

Enhanced thresholding (with feature 189)

Calculation Entry Format

```
[index index]
   if rule then calc level=lvl;
```

Flag Entry Format

```
[index index]; if flags has any of flags then flags level=lvl;
```

OR

```
index index; if flags has all of flags then flags level=lvl;
```

Parameters

`index` Threshold index. This is required for the first calculation entry only.

- 1–128
- 1–256 (if Feature 3, “Management of Record Base Partitions and Subnetworks”, is purchased)

`calc` Calculations that can be thresholded. Any calculations that you do not specify for a threshold index are not performed. You can have up to 10 calculations per threshold index. All CCS flags combined count as only one calculation.

Important! You can have up to 60 calculations w/Feature 189, “Replacement Thresholding Capability for Trunk Group Data”.

Select Record Base File = Trunk Group Threshold file on the Search NTM Documentation page to list the valid raw and derived measurements that can be thresholded in this file. Refine the search by Switch Type or Calc Type, if desired. See HTML search.

`thr` Threshold value (up to 3 values). If no calc is specified, the threshold value defaults to zero (0).

- For non-SCSN switches:
  - Use the values 0.0–100 for percentage calculations.

  - Use the values 0–9999 for the remaining calculations.
- For SCSN switches:
  - Use the values 0.1–100 for percentage calculations.
  - Use the values 0–1,048,575 for the remaining calculations.

`compare` Comparison of exception and threshold levels. You can select up to 2 comparisons using:

- < (less than)
- > (greater than)

`lvl` Threshold level 1–10. Each level determines if the exception is an alert (1–5) or an alarm (6–10).

Traditional Thresholding

- Calculations — You can select up to three levels.
- Flags — Specify only one level per flag. Up to three different levels are allowed for one index for all flags.

Enhanced Thresholding

- The exception level to be associated with the *`data_field`*
- Each rule entry supports only one exception level
- Specify only one level per flag rule

`data_field` A measurement item. Up to 10 unique measurement items can be put under the same index.

Select Record Base File = Trunk Group Threshold file on the Search NTM Documentation page to list the valid raw and derived measurement items. Refine the search by Switch Type or Calc Type, if desired. See HTML search.

Important! You can have up to 20 unique measurements items under the same index w/Feature 189, “Replacement Thresholding Capability for Trunk Group Data”.

`flags` A single flag from the list below:

- bofl — Buffer Full/Processor Signaling Congestion
- ler — Link Emergency Restart
- tfp — Transfer Prohibited
- iuf — Integrated Services Digital Network User Part (ISUP) User Failure
- gsc — Group Signaling Congestion/Transfer Controlled
- cr — Circuit Reservation
- sdoc — Selective Dynamic Congestion Control/Automatic Congestion Control

- If you want to indicate more than one flag, enclose any combination of flags from the preceding list in parentheses and separate them by commas [for example: (ler, gsc, tfp)].
- If multiple flags are specified in a "has any of" statement, the reception of any one of the listed flags shall identify an exception. In a "has all of" statement, all the listed flags must have been received for an exception to be identified.

`rule` An expression relating the *`data_field`* that uses the following logical operators and mathematical signs:

- and
- or
- =
- <
- <= (less than or equal to)
- >
- >= (greater than or equal to)
- <> (not equal to)

Each of these logical operators and mathematical signs requires a space character before and after it when used in a rule. In addition, the rules may include the following expression delimiters: left and right parentheses [( )].

Up to 30 (60 w/Feature 189, "Replacement Thresholding Capability for Trunk Group Data") rules or comparisons ("if**…**then" clauses) can be put under the same index.

All the flags identified in a single index count as one of the unique measurements allowed in an index. Each rule statement counts as one of the allowable comparisons in an index.

Rule processing

In the absence of expression delimiters, all rules are processed from left to right with `and` logical operators taking precedence over **or** logical operators. The "truth" of each comparison will be verified as it is encountered in the rule. Logical operators will relate that portion of the expression to the left of the operator with the comparison to its immediate right. If expression delimiters are present, those comparisons and logical operators within the "innermost" set of delimiters will be processed first, with processing proceeding "outward" until all portions of the expression within delimiters have been processed. Then processing proceeds from left to right with `and` logical operators taking precedence over **or** logical operators.

Consider a situation where pc = 110, %ofl = 65, and occh = 3, and the following rules are processed:

- Rule 1: if pc >= 100 and %ofl > 75 or occh <= 5 then …
- Rule 2: if pc >= 100 and (%ofl > 75 or occh <= 5) then …

The first rule begins by checking pc >= 100, which is true. The `and` operator is then exercised against a check of %ofl > 75, which is not true. Since only one of the comparisons is true, this rule does not detect an exception.

The second rule begins by checking %ofl > 75, which is not true. The logical `or` operator is then exercised against a test for occh <= 5, which is true. Since one of the comparisons is true, the portion of the expression within the delimiters is true. Having no more delimited sections to process, the rule checks pc >= 100, which is true. The `and` operator is then exercised against the delimited portion of the statement and, since it is also true, this rule does detect an exception.

The entire list of operators available with Feature 189, “Replacement Thresholding Capability for Trunk Group Data” is:

- <
- <=
- =
- =>
- >
- and
- or

Important! The placement of expression delimiters within a rule can have a significant effect on whether or not an exception is detected. Care should be taken to ensure that expression delimiters are properly paired to group together those portions of the conditional statement that need to be evaluated together.

Examples

Traditional Thresholding (without Feature 189)

Figure 40 shows an example of a Trunk Group Threshold file without Feature 189.

Figure 40 Trunk group threshold entries without Feature 189

```
index=1 calc=pc thr=200+300+400 lvl=2+3+4;
  calc=ofl thr=10+30+50 lvl=2+3+4;
  calc=%ofl thr=50+60+70 lvl=7+8+9;
  calc=ach thr=20+40+60 lvl=2+3+4;
  calc=occh thr=20+30+40 lvl=2+3+4;
  calc=%mfto thr=16+30+50 lvl=7+8+9;
  calc=%rej thr=95+96+98 lvl=7+8+9;
  calc=%mb thr=25+50+75 lvl=2+3+4;
```

```
   calc=%occ thr=10+5+90 compare=<+<+> lvl=2+3+4;
   flag=sdoc lvl=3;
   flag=cr lvl=3;
   flag=ler lvl=3;
   flag=gsc lvl=3;
   flag=tfp lvl=8;
   flag=bofl lvl=3;
index=2 calc=%ofl thr=1+5+10 lvl=7+8+9;
   calc=ach thr=28+35+42 lvl=2+3+4;
   calc=occh thr=40+60+80 lvl=2+3+4;
   calc=icch thr=30+40+50 lvl=2+3+4;
   calc=%mfto thr=16+30+50 lvl=7+8+9;
   calc=%rej thr=95+96+98 lvl=7+8+9;
   calc=%mb thr=25+50+75 lvl=2+3+4;
   flag=sdoc lvl=3;
   flag=cr lvl=3;
   flag=ler lvl=3;
   flag=gsc lvl=3;
   flag=tfp lvl=8;
   flag=bofl lvl=3;
```

Notice that there are 9 calc entries and a number of flag entries. This combination counts as 10 calc entries, which is the maximum allowed.

To understand how these entries relate to establish a threshold level, see Figure 41 and Table 5.

Figure 41 Last index entry for the calc keyword

```
calc=%occ thr=10+5+90 compare=<+<+> lvl=2+3+4;
```

The *compare* (comparison) keyword allows you to indicate you want the directionality changed for %occ so that the following occurs:

Table 5 Explanation: Figure 41

Calculation	Threshold Level	Exception Level	Indicates
%occ	Less than 10 (First thresh entry)	2 (First level entry)	Alert
%occ	Less than 5 (Second thresh entry)	3 (Second level entry)	Alert
%occ	Greater than or equal to 90 (Third thresh entry)	4 (Third level entry)	Alert

Enhanced Thresholding (with Feature 189)

Figure 42 shows an example of a Trunk Group Threshold file with Feature 189.

Figure 42 Trunk group threshold entry with Feature 189

```
index 1;
     if (PC > 50) AND (HT <= 2) AND (%OCC >= 70) AND (%OCC <= 90)
     then %OCC level = 5;
     if (%OFL > 90) AND (%OCC >= 75)
     then %OFL level = 9;
     if flags has any of sdoc then flags level = 3;
     if flags has any of (cr, ler, gsc) then flags level = 4;
     if flags has all of (bofl, ler, tfp, cr) then flags level = 5;
index 2;
```

Notice the following in the example:

- A space character instead of an equal sign is between the “index” keyword and the index number.
- The index number is followed by a semicolon (;).
- Operators in the “if” statements have one space character on either side of them.
- Multiple flags in an “if” statement for flags are enclosed in parentheses and separated by commas.

Related record base file(s) and command(s)

See “Defining thresholds” in the *System Overview* for more information on defining threshold levels.

See the `thrconvert` command in the *Input Commands Guide* if you have Feature 189, “Replacement Thresholding Capability for Trunk Group Data” and you want to convert your “thresh” files to the new format.

See Chapter 3, “System Security, User Groups, and Group Permissions” in the *System Administration Guide* for more information on user permissions.

For more information about available threshold indices, see Chapter “8920 NTM Engineering Guidelines” in the *System Overview*.

□

TYPXREF File

Description

The TYPXREF (Type Cross-Reference) file associates real-type and real-generic names of network elements to internally supported type and generic names.

This is a global file. If you have BDR, you must make the status of the file primary after making any changes before you can run the `create rspte` command.

Valid for office type(s)

All

Restrictions

- The total number of types allowed (both real and internally supported) is 50.
- The total number of generics allowed (both real and internally supported) is 120.

Pathname

"/musr/rb/rspte/typxref"

Format(s)

```
realtype=realtype inttype=inttype;
   realgen=realgen intgen=intgen;
```

Important! When adding entries to this file, you must use name-defined syntax. Position-defined syntax is invalid for this file.

Parameters

`realtype` User-defined real-type name that is used as a network element type; 7-character maximum. This cannot be an internally supported type.

`inttype` Internally supported network element type, as follows:

• ess1a	• dms250	• lssgr
• ess4	• dms500	• nms
• ess5	• ewsd	• psx
• dcc	• gsp	• scsnsn
• dms	• gsx	
	• gtd5	

`realgen` User-defined real-generic name that is used as a network element generic; 8-character maximum. This cannot be an internally supported generic.

`intgen` Internally supported network element GENERIC, as follows:

• 1ae8	• 5e10	• gtd1721	• ncs17
• 1ae9	• 5e11	• gtd1722	• nms1
• 1ae10	• 5e12	• gtd1732	• nms2
• 1ae11	• 5e13	• gtd4003	• nms3
• 1ae12	• 5e14	• ics02	• npm6_0
• 1ae13_0	• 5e15	• ics03	• pl3_9
• 4e12	• 5e16	• ics04	• psx5_1
• 4e13	• 5e16_1	• ics05	• psx5_2
• 4e14	• 5e16_1h	• lssgr87	• sn02
• 4e15	• 5e16_2	• na007	• sn03sn04
• 4e16	• dms24	• na009	• sn04tdm
• 4e17	• dms25	• na010	• sn05
• 4e18	• dms26	• na012	• sn05_100
• 4e19	• dms27	• na013	• sn05_250
• 4e20	• dms28	• na014	• sn05_500
• 4e21	• ewsd10	• na016	• sn06
• 4e22	• ewsd11	• na017	• tdms1
• 4e23	• ewsd12	• ncs06	• tdms2
• 4e27	• ewsd13	• ncs07	• tdms3
• 4e28	• ewsd13a	• ncs10	• ucs07
• 5e4	• ewsd16	• ncs12	• ucs08
• 5e5	• fepr1	• ncs13	• ucs09
• 5e6	• gsp07	• ncs14	• ucs12
• 5e7	• gsx5_1	• ncs16	• ucs13
• 5e8	• gsx5_2		• ucs14
• 5e9	• gtd1641		• ucs16
• 5e9_2	• gtd1711		

Examples

Figure 43 shows an example of records in the TYPXREF File.

Figure 43 TYPXREF File entries

```
realtype=xyztype inttype=dms;
realgen=xyzgen intgen=dms24;
realgen=5e99 intgen=5e8;
realgen=1741 intgen=gtd1721;
```

The records shown in the example above would allow the values shown in Figure 44 for the generic and issue keywords of the records in the RSPTE File.

Figure 44 Related RSPTE entries

```
#clli rspte nick sets snw type generic issue;
timbucktoo 123123123123121 ,,, xyztype xyzgen 1;
new5e 12312123123121 ,,, ess5 5e99 1;
```

Even though xyztype, xyzgen, and 5e99 are not supported by NTM, these values can now be entered into the RSPTE File. The names will be seen on the appropriate interface pages and on the `linkstat` command output. Issue gtd1741 will be treated as issue gtd1721.

Related record base file(s) and command(s)

For more information on name-defined and position-defined syntax, see Chapter 6, "Record Base Editor".

□

6 Record Base Editor

Overview

Purpose

This chapter provides information about the record base editor.

Contents

This chapter contains the following topics:

Record base file format	6-2
Record base file symbols	6-3
Record format	6-4
The rbed command	6-5
Working with record base files	6-7
Recovering an edited file	6-8
Editing a record base file with rbed	6-9
Common editing commands	6-11

Record base file format

Overview

The format for entering input records into a record base file is similar to the format for entering NTM commands (but these are simply line entries in a file, not commands). A record can be entered as ***name-defined*** or ***position-defined***.

> **Important!** A file can have a name-defined format or a position-defined format, but it cannot have both.

It is recommended that entries be name-defined except possibly for the RSPTE Files, where the number of entries can be quite large. Generally, the format for the file is defined in a comment line (prefaced with the **#** symbol so the machine will ignore the line when reading the file) at the top of the file. For clarity and consistency, everyone uses that format when working in the file.

Name-defined format

To enter a record in name-defined format, you must use keyword phrases, as shown below. You can input the keyword phrases in any order. Keywords in the database can be shortened to three or more characters by truncation (for example, the name `office` can be shortened to `off`).

`keyword=`*`value`*`+...+`*`value`* `keyword=`*`value`*`+...+`*`value`*

For example:

```
to=alpha_exch-011 tgn=11 tgsrv=hu sets=acct otherend=221
   options=sched thr=1;
```

can be changed to the following using truncated keywords,

```
to=alpha_exch-011 tgn=11 tgs=hu set=acct oth=221 opt=sched
   thr=1;
```

Position-defined format

To enter a record in position-defined format, enter only the keyword ***values***, but enter them in the correct order as shown in the file description. For any unused parameters, use a comma (,) as a place holder. Be careful not to confuse place-holder commas with separation commas. For each record base file type, the file description shows the format in the correct order for position-defined entry.

`value``+...+`*`value`* *`value`*`+...+`*`value`*

```
alpha_exch 010001000000000 , ohio+clmb , ess5 5e4 2;
beta_exch 010001000001000 , ohio+clmb , ess5 5e6 2;
```

Record base file symbols

Table

Table 1 shows the symbols used to format record base files.

Table 1 Symbols used to format record base files

Symbol	Description
Pound sign (#)	Use as the first character on a line within a record base file to comment out that line; the system considers the line to be a comment and does not process it as a record. `Note`, a comment (#) cannot appear within a record.
Plus sign (+)	Separates multiple values for a a keyword within a record entry. `Example: keyword=`***value+value+value+value***
Semicolon (`;`)	Terminates each record entry. The semicolon (;) must be the last character in a record entry to indicate the end of the record.
Comma (`,`)	Separates fields in record entry. Both a comma and any number of blank spaces (including tabs and returns) can also be used.
Space ( )	

Record format

Overview

The following examples show several ways a record can be entered in the Trunk Group File. The examples are in name-defined format. Some keywords were not used in the examples.

> **Important!** Although the system is very forgiving in the variations of entry it will accept, it is recommended that a simple and consistent entry style be used across the files to avoid confusion and errors.

Examples

The following paragraphs provide examples of different types of formats.

Space only

```
to=asd_2h-1 tgn=1 tgsrv=fi tgtyp=dom sig=ccis6 n1wi=0 n1wo=0 n2w=1
   sets=auto ofl=asd_2h-2+asd_2h-3 thr=1 options=sched;
```

Comma only

```
to=asd_2h-2,tgn=2,tgsrv=hu,tgtyp=intl,sig=tup,n1wi=0,n1wo=0,n2w=1,
   sets=auto,ofl=asd_2h-3+asd_2h-4,thr=1,options=sched;
```

Comma + space

```
to=asd_2h-3, tgn=3, tgsrv=fu, tgtyp=dom, sig=mfev1, n1wi=0, n1wo=0,
   n2w=1, sets=auto,  ofl=asd_2h-4+asd_2h-5, thr=1, options=sched;
```

Comma + multiple spaces

```
to=asd_2h-4,  tgn=4,  tgsrv=fi,  tgtyp=intl,  sig=mfev2,  n1wi=0,
   n1wo=0, n2w=1, sets=auto, ofl=asd_2h-5+asd_2h-6, thr=1,
   options=sched;
```

CR + multiple spaces

```
to=asd_2h-5
     tgn=5    tgsrv=hu    tgtyp=dom    sig=ccis6
     n1wi=0    n1wo=0    n2w=1    sets=auto    ofl=asd_2h-6+asd_2h-7
     thr=1     options=sched;
```

The rbed command

Overview

In the course of record base administration, you will need to edit (make changes to) record base files. The `rbed` command:

- allows you to modify any ASCII file in the record base directory ("/musr/rb") by placing you in a text editor of your choice
- "locks" out other users who attempt to execute `rbed` on a file you are editing. This prevents multiple users from editing a file with the `rbed` command at the same time and overwriting each other's changes.

Uses

You may use the `rbed` command to edit the files under the "/musr/rb" directory. Use the `rbed` command to:

- Add, modify, and delete records in the record base files
- Search for a particular record or string in a record base file
- Edit any available field in a record base file
- Create new record base files

Saving changes

After you make a change with the `rbed` command, the change can be written to the record base file. Use the `create` command to compile the new changes to the database. Use the `installdb` command to install your changes.

Syntax

Use the following command format to access a record base file with the `rbed` command:

`rbed` *`file`*

Parameters

`file`	File name of the record base file to edit (valid pathname is required if you are not in the directory where the file resides).

Examples

For example, to edit the Sets File

- If you are in the "/musr/rb/sets" directory, enter:

```
rbed sets
```

- If you are not in the “/musr/rb/sets” directory, enter:

```
rbed /musr/rb/sets/sets
```

□

File locking

While you are editing the file with `rbed`, it is locked to other users. It will remain locked until you exit `rbed`.

> **Important!** If you exit `rbed` in any abnormal way, such as pressing the delete key or deleting a window, the file will be unlocked.

On rare occasions, such as a system crash, a lock will not be detected. Although `rbed` frequently is able to detect when a lock is obsolete, it is not always possible to do so. To help you determine whether the locked file is still in use, the owner process ID is written into the locked file. You can check with the owner to see if the process is still running. If it is, then the lock is probably valid. You and the NTM System Administrator are responsible for investigating files that you think may be locked in error, and for deleting the lock.

File locking with BDR

Because the file-locking protocol is only used by `rbed`, it is possible that the original file may be changed while you are editing a file from the record base. Backup and Disaster Recovery may update the original file if you edit the copy on the non-primary system. If the original file is changed while you are editing, `rbed` will detect and report this.

You may discard the copy of the file you are editing, save it to another file, or overwrite the original file with your changes. You are responsible for evaluating the changes and assuring the validity of the record base.

Defining the text editor

You are able to select the editor that `rbed` uses. RBEDITOR, the environment variable, defines the choice of editor. If undefined, RBEDITOR defaults to $EDITOR. If EDITOR is also undefined, then RBEDITOR defaults to “vi”.

Although you can select the text editor you wish to use, the editor of choice for NTM is the *Linux* System vi Text Editor. Much of the information provided in this chapter assumes use of the vi text editor.

Changing record base file security

Since the files in the “/musr/rb” directory are *Linux* system files, you can change permissions on them to make them more secure. To do this, use `chmod 664` for all files and `chmod 775` for all directories in the structure.

Recovering an edited file

Overview

If an abnormal event such as a disconnection or a system crash occurs, you may need to recover an edited file. `rbed` assumes that the editor you select will have a recover file option, and that you will know the option specification for that editor. The *Linux* System vi Text Editor provides the "`-r`" option to perform this function. Assuming use of the *Linux* System vi Text Editor, use the following information to recover an edited file:

> **Important!** If you are ***not*** using the *Linux* System vi Text Editor, refer to user documentation for your editor of choice for information on recovering lost files.

Syntax

To recover an edited file, enter the following command:

```
rbed -r file
```

Parameters

`file`	File name of the record base file to recover.

Examples

For example, to recover the Sets File, enter:

```
rbed -r sets
```

Command output

After this command is run, the recovered file will appear on the screen. Upon reviewing the recovered file, you will find that one of three possible degrees of recovery has taken place:

1. All of the changes you made were saved and recovered. If this is the case, save the changes and exit the file.
2. Some percentage of your changes were saved and some were lost. If this is the case, review the file and re-enter any changes that were not saved. Save the re-entered changes and exit the file.
3. None of the changes you made were saved. If this is the case, discard the recovered file. Re-edit the original file, save the changes and exit the file.

Editing a record base file with rbed

Purpose

Use the following procedure when editing a record base file with the `rbed` command. In this example, assume you are in the "/musr/rb" directory and are editing the Sets File.

Instructions

1 Enter `rbed sets`

Result: If no one else is accessing the file, the sets file appears.

Important! If the file is being edited (with the `rbed` command) by someone else, it is considered "locked," and you receive a response similar to the following:

```
rbed: file /musr/rb/sets/sets is locked by user jsmith
If lock is in error, have administrator delete
/usr/spool/locks/rb00001a0a5008
```

If the lock appears to be in error (i.e. an old lock resulting from a system problem, etc.), contact the System Administrator so that the lock can be removed manually.

2 Make changes to the file as needed, using the *Linux* Visual Editor (vi) editing commands found in the "Common editing commands" (p. 11).

Important! You can select the text editor you wish to use; however, the editor of choice for NTM is the *Linux* System vi Text Editor.

3 When you have finished, you can take one of the following actions:

1. Close (quit) the file and save the changes

Result: You are presented with the following options:

```
Select action ([n]ew file, [s]ave & exit, save & [r]e-edit,
[d]iscard & exit)
```

These options are defined as follows:

- `n` — create a copy of this file with a new filename. You will be asked to define the new filename.
- `s` — save the changes to this file and exit the file
- `r` — re-edit the file

- `d` — discard the changes you made and exit the file

2. Close (quit) the file ***without*** saving the changes

   Result: You are presented with the following options:

   ```
   File unchanged, select action ([n]ew file, [e]xit or [r]e-edit)
   ```

   These options are defined as follows:

   - `n` — create a copy of this file with a new filename. You will be asked to define the new filename.
   - `e` — exit the file without saving changes
   - `r` — re-edit the file

□

Common editing commands

Overview

Although you can select the text editor you wish to use, the editor of choice for NTM is the *Linux* System vi Text Editor. Like other text editors, vi is an interactive program that allows you to create and edit text.

The purpose of this section is to present vi keys and functions commonly used while editing.

Only basic commands that are applicable to NTM tasks are covered. This section is not a comprehensive lesson in vi.

Working with vi

Keep in mind that:

- vi distinguishes between upper- and lower-case letters. It is important for you to observe this distinction when you are typing vi commands.
- If you get lost in vi, press `ESC`. This allows you to escape any input mode. If you are not sure about a change you have made and would like to start over, type `u` to undo the last change.
- If you must exit vi and do not wish to save your changes, press `ESC` and type `:q!`

  Typing this command gets you out of the file without making any of your changes permanent. Thus the file remains in its original state for either you or your successor to re-enter.
- If you wish to save changes (write) to a file but the file has read-only permissions (you are alerted to this by a message appearing at the bottom of the screen when you attempt to write the file normally), press `ESC` and type `:w!`

vi text editor keys and their functions

The vi Text Editor keys and key combinations are divided into the following tables according to their functions:

- Table 2, “vi Cursor and Page Motions” (p. 12)
- Table 3, “vi Text Addition” (p. 12)
- Table 4, “vi Text Searching” (p. 12)
- Table 5, “vi Text Deletion” (p. 13)
- Table 6, “vi Text Replacement” (p. 13)
- Table 7, “vi Text Movement” (p. 13)
- Table 8, “vi Miscellaneous Commands” (p. 14)

Table 2 vi Cursor and Page Motions

Key	Function
[line number] **G**	Move the cursor to the first character of the line number specified. Pressing 1 and **Shift g** moves the cursor to line 1 (beginning of the file). Pressing **Shift g** moves the cursor to the last line of the file.
-	Move the cursor up the screen to the previous line.
Return or **+**	Move the cursor down the screen to the next line.
Spacebar	Move the cursor to the right one character.
Backspace	Move the cursor to the left one character.
Control f	Move the cursor forward through the file in 1-page increments.
Control b	Move the cursor backward through the file in 1-page increments.
w	Move the cursor from left to right to the beginning of the next word.

Table 3 vi Text Addition

Important! You must press **ESC** to exit Text Addition modes.

Key	Function
a	Start appending text immediately following (right of) the cursor position.
A	Start appending text at the end of the current line.
i	Start inserting text immediately preceding (left of) the cursor position.
o [letter]	Start a new line of text below the cursor position.
O [letter]	Start a new line of text above the cursor position.

Table 4 vi Text Searching

Key	Function
/ [search expression] **Return**	Search the file for the next occurrence of the indicated search expression.
? [search expression] **Return**	Search the file for the preceding occurrence of the indicated search expression.
/ or **n**	Search in the forward direction for the next occurrence of the previously defined search expression.
? or **N**	Search in the backward direction for the preceding occurrence of the previously defined search expression.

Table 5 vi Text Deletion

Key	Function
x	Delete the character at the current cursor position.
d w	Delete the character at the current cursor position and all characters to the end of the word, including the space following the word.
d d	Delete the line at the current cursor position.

Table 6 vi Text Replacement

Key	Function
r [character]	Replace the character at the current cursor position with the character selected. This is a 1-character replacement and ESC does not need to be pressed.
R [characters]	Overwrite the characters beginning at the current cursor position until ESC is pressed.
c w [word(s)]	Replace the specified word with the word(s) entered. (You must press ESC to exit this mode.)

Table 7 vi Text Movement

Key	Function
[number] **y y**	Yank a copy of the **[number]** of lines indicated from the current cursor position down. Place the lines elsewhere in the current file, using P (see below).
[number] **d d**	Delete the **[number]** of lines indicated from the current cursor position down. Place the lines elsewhere in the current file, using the P key.
P	Place the line(s) below the current cursor position after one of the above two commands has been executed.

Table 8 vi Miscellaneous Commands

Key	Function
:wq Return	Write the file to disk and return to the system prompt.
:w Return	Write the current file to disk, but do not quit the vi editor.
:q!	Exit the file without incorporating changes made since the last write (`: w`) and return to the system prompt.
: . = Return	Display the current line number.
u	Undo the last vi text modifying command.
J	Join the current line and the following line, separating them by a space.
ESC	Quit adding text and return to the vi command mode.
Ctrl g	Display the current file name, line number of the cursor, and percentage through the file.
`:set nu`	Display all line numbers.

7 Record Base Administration

Overview

Purpose

This chapter provides descriptive and procedural information about administering the record base.

Contents

This chapter contains the following topics:

Record base administration process	7-3
Creating and modifying database records	7-6
Defining threshold data	7-9
Setting up trunk group threshold data	7-10
Administering subnetworks	7-12
Modifying record base files for subnetworks	7-13
Troubleshooting 1A ESS switches with data alignment problems	7-15
Valid machine data/invalid trunk group data	7-15
Invalid machine and trunk group data	7-16
Realigning registers	7-17
Changing default domain for a control	7-19
Adding and deleting RSPTE CLLI changes	7-20
Building the database for 1024 trunk groups	7-22

Record base administration process

CAUTION

Do not attempt to follow this process until you have read this chapter and Chapter 8, "Record Base Update Procedures".

Overview

Record base administration refers to the process of creating, configuring, initializing, and maintaining the reference database of trunk groups and offices.

The NTM reference database consists of user-built text files. In general, the information in these files falls into two categories:

- Data about the network management center itself (such as the configuration of the center and threshold tables)
- Data about the network being monitored (such as switching systems and trunk groups in the network management center's cluster)

These files are stored in the "/musr/rb" directory; they are edited, deleted, or modified with the `rbed` command or the *Linux* Visual (vi) Editor.

In addition to the current database, NTM maintains an offline database. The offline database is copied to a temporary database area, thus keeping the current database available to the rest of the system users during the `create` process.

Sequence of commands

The record base administration process is accomplished by a sequence of record base commands. This sequence is listed below.

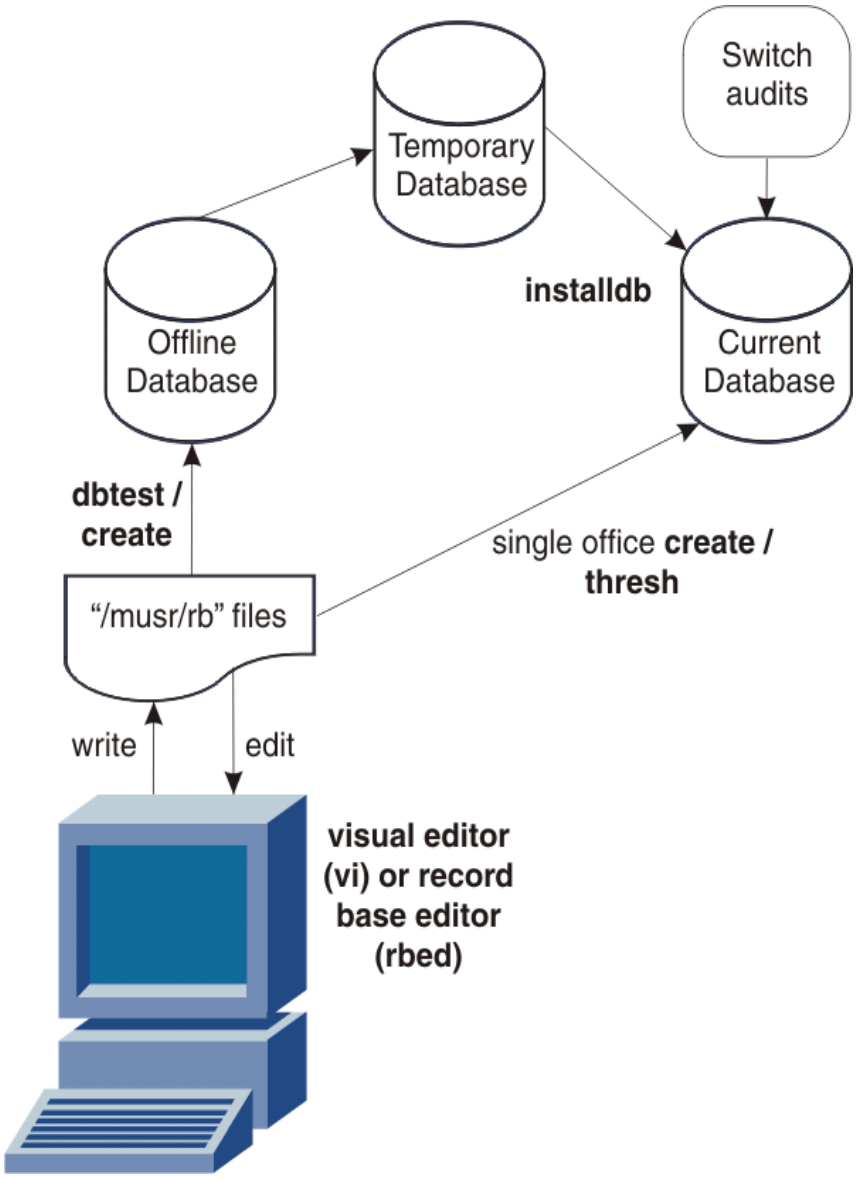
1. Edit the "/musr/rb" files using the *Linux* system vi editor or `rbed`, the record base editor command.
2. Verify the proper entry of the records in the files you edited, using the `dbtest` command.
3. Create a new offline database that uses the "/musr/rb" files, using the `create` command.
4. Halt the NTM exception processing and data collection, using the `stopsys` command.
5. Move the newly created database to the current database, using the `installdb` command.

6. If you have halted the NTM exception processing and data collection with the `stopsys` command, then start the NTM exception processing and data collection using the `startsys` command.

Figure

The record base administration process is illustrated in Figure 1.

Figure 1 Record base administration process



References

See the *Input Commands Guide* for more information about all of the record base commands.

□

The rbed command

You can use the rbed command to edit and write changes to the "/musr/rb" files. Once your changes are written to the file(s), you can execute the appropriate version of the dbtest command, followed by the full, single office, or single file version of the create command or the recreate command by itself.

The dbtest command

The dbtest command checks for syntax errors or inconsistencies in the data, compiles the specified ASCII files, and updates the offline database. Always run the dbtest command before any version of the create command. Otherwise, the current database will be corrupted by errors. You can run the same dbtest procedures (full, single office, single file) as those for the create command.

The create command

Full create

Once the database files are prepared, you can use the full create procedure to construct the reference portion of the current database. This procedure modifies the offline database and copies it to the temporary database.

Important! It is recommended that the full create procedure be performed at least once every 30 days. Failure to do so can result in database problems.

Single office and single file create

WARNING

There is only one trunk group reference data assignment for trunk group registers per database. If you execute a single office create during the day, the trunk group reference data is changed and no longer agrees with earlier trunk group reference data.

A single office create modifies the database from the "/musr/rb" files for one office only. A single office create acts directly on the current database; no installdb is performed. The offline and temporary databases are not updated by the single office create.

The single file create creates individual record base files. Use the installdb command to install these files to the current database.

Reference: For a list of files you can enter for single file `create`, see the `create` command (5-5) in the *Input Commands Guide*. See Chapter 8, "Record Base Update Procedures" for a more detailed flowchart and step procedure.

The recreate command

Use the `recreate` command to directly update the current database with record base file changes. The `recreate` command looks for:

- record base files that have been modified since the time when the last `installdb` or `recreate` command was run.
- offices that have been defined but have not been created properly.

It then runs a combination of the following commands (as needed) on each file to be updated:

- `create`
- `stopsys`
- `installdb`
- `startsys`
- `local_audit`
- `audit`

The `recreate` command is automatically executed every night as part of the end-of-day procedures.

CAUTION

This command, if necessary, will stop and later restart NTM exception processing and data collection. It may also deactivate and reactivate data collection for offices while it runs a single office `create` process for each one. For this reason, it may be appropriate to allow the `recreate` command to run automatically at the end of the day.

The `recreate` command has several advantages over a full `create`. The `recreate` command updates a complete list of recently updated offices or files, rather than just one office (as the single office `create` process does) or just one file (as the single file `create` process does). There is no need to do a separate execution of the `installdb` command. Only reference audits are updated, rather than all audits. A combination of local audits and reference audits is used to update the reference data. The `recreate` command minimizes the length of time the system is stopped.

If BDR is in use, the `recreate` command also synchronizes the:

- Global record base files with those in the primary state on other NTM hosts
- Record base files in backup subnetwork partitions from NTM hosts that are primary for those partitions (as defined in the INMS record base file)

References

See the *Input Commands Guide* for more information about all of the record base commands.

□

Defining threshold data

Purpose

In addition to constructing and modifying database files, defining trunk group threshold data is also a part of the NTM record base administration process. Trunk group threshold data is entered into special record base files for use in exception processing. The `thresh` command compiles a specified threshold table from the *"/musr/rb"* files and updates the current database directly.

Reference: Chapter 5, "Thresholds" in the *System Overview*

Setting up trunk group threshold data

Purpose

Use this procedure to set up trunk group threshold data.

Before you begin

Three record base files are required:

1. Trunk Group Threshold File("/musr/rb/thresh/thresh*[n]*"), where *[n]* = a number from 1–8
2. Trunk Group File ("/musr/rb/tg/*clli*")
3. Threshold Table Schedule File ("/musr/rb/thresh/sched")

Instructions

Follow these steps to set up trunk group threshold data:

1 Define the thresholds for trunk groups in the network, one data table at a time.

Each entry for an index contains all the threshold values needed for a trunk group.

You can define up to 128 indices (or entries) in the Trunk Group Threshold File. If Feature 3, "Management of Record Base Partitions and Subnetworks" is purchased, the threshold tables have 256 indices.

2 In the Trunk Group File, assign a threshold index to each trunk group to select which threshold values are compared to the calculations.

Hint: If you do not want exception processing done on a trunk group, assign that trunk group a threshold index of zero (0).

Result: Once the data is collected from the switch, calculations are made on the data and compared to the threshold values defined in the Trunk Group Threshold File for the corresponding threshold index in the Trunk Group File. Data that exceeds a threshold is considered to be in exception.

3 Create up to 8 different thresh*n* files. NTM allows you to create more than one table of thresholds. When you create more than one table, however, each table must have the same number of threshold indices.

4 Schedule when to make each table active, using the Threshold Table Schedule File.

Important! Before attempting to install the new Trunk Group Threshold File, you must update the Threshold Table Schedule File ("/musr/rb/thresh/sched") to include the new thresh file.

The `thresh` command installs the file, but the Threshold Table Schedule File indicates which thresh table is to be used currently.

You have the option of scheduling each table to be active at different times of the day.

Example: You can schedule Table 1 to become active Monday at 10:00 a.m. and Table 5 to become active on the same day at 5:00 p.m.

The thresholds used for exception processing are taken from the active table.

END OF STEPS

Administering subnetworks

Overview

NTM supports subnetworks, allowing parts of the network to be monitored and controlled independently of the main network. Offices and trunk groups can be assigned to and managed by these subnetworks. You must include subnetwork record base files in the `create` and `installdb` command processes. There are two ways of maintaining these files:

1. The record base administrator can make changes to these files in "/musr/rb"
2. The files or parts of files that belong to a subnetwork can be copied to the subnetwork record base area, "/musr/snw/<*snw_name*>/rb." The subnetwork record base administrator maintains these files. These files must be copied or merged with the "/musr/rb" files when the subnetwork record base administrator wants to change these files, or during normal `create` and `installdb` command procedures.

Permissions

Subnetwork users cannot read or write to the "/musr/rb" area, regardless of *Linux* system file permissions. Files must be copied to the "/musr/snw/<*snw_name*>/rb" directory to be seen and/or edited by the subnetwork record base administrator.

Some versions of the `create` command can only be run by a record base administrator of group "`snm`". Additionally, subnetwork users can only run a single office `dbtest`.

Modifying record base files for subnetworks

Purpose

Two record base files contain the subnetwork field:

1. RSPTE File
2. Trunk Group File

For trunk groups to be assigned to a subnetwork, the office for those trunk groups must be assigned to the same subnetwork. The trunk groups are assigned in the Trunk Group File for the office and the office is assigned in the RSPTE File. The example below shows how to update these two files.

Example: Assume that you have the following subnetworks: “A”, “B”, and “nmc”. Also assume that user group “alpha” is assigned to subnetwork A, user group beta to subnetwork B, and user group nmc to subnetwork nmc.

If you want user group alpha to see only trunk groups that belong to subnetwork A and user group beta to see only trunk groups that belong to subnetwork B, set up your record base files using the procedure below.

Instructions

Follow these steps to modify record base files for subnetworks:

1 In the RSPTE File, assign the office to all three subnetworks by entering:
`subnetwork=a+b+nmc`

2 In the Trunk Group File for the office, assign trunk groups to subnetworks as shown below.

- Trunk groups for subnetwork A `subnetwork=nmc+a`
- Trunk groups for subnetwork B `subnetwork=nmc+b`

Subnetwork nmc is included in each case so that members of the nmc group will be able to look at all trunk groups.

END OF STEPS

References

For more information on subnetwork permissions, see Chapter 3, “System Security, User Groups, and Group Permissions” in the *System Administration Guide*.

□

Troubleshooting 1A ESS switches with data alignment problems

Overview

Two types of data alignment problems can occur on a 1A *ESS* switch:

1. Valid machine data/invalid trunk group data
2. Invalid machine and trunk group data

For either problem, first verify with the 1A *ESS* switch personnel that the parameter set card values correspond with the control counts in the 1A *ESS* Office File. If the two correspond, continue with the procedures below.

Table

Table 7-1 shows 1A *ESS* TG valid values.

Table 7-1 1A ESS TG valid values

TRUNK TYPE	DIRECTION	END	PC	OFL	USG	IPC
1 (1-way) 2	out incoming	A Z	tmc1	tmc2	tmc0 tmc0	 tmc1
3 (2-way)	2-way	A Z	tmc4 tmc4	tmc2 tmc2	tmc0 tmc0	tmc3 tmc3
Unsupported:						
3 (2-way used as 1-way) 2	1-way out 1-way in	A Z	tmc4	tmc2	tmc0 tmc0	 tmc3

Valid machine data/invalid trunk group data

This situation happens infrequently, although it can occur on all releases of the 1A *ESS* switch. This problem may be caused by the addition of a register at the switch when the end of the machine data falls at the end of a 250-register data block from the switch. The

most common method of solving this problem is to have the personnel responsible for administering the switch H and C schedules add or subtract a register on the H schedule to realign the data.

Invalid machine and trunk group data

In the NTM database, the raw data for 1A *ESS* switches is stored in the following order:

- Control counts — keywords are cgcnt, ppcnt, flxcnt, rrcnt
- Dynamic overload control counts (if applicable for the switch) — keyword is nmdoc (uses 16 registers)
- Machine counts
- Traffic counts

If all machine count and trunk group data for a switch appears to be invalid, the problem may be the number of registers allowed for control counts in the record base Office File.

A maximum of 250 control count registers can be sent to the1A *ESS*. The total number of control count values is calculated in the following way:

- `nmdoc` = if set to `yes`, 16 registers
- `cgcnt` = 2*cgcnt registers
- `ppcnt` = ppcnt registers
- `flxcnt` = 2*flxcnt registers
- `rrcnt` = rrcnt registers

If the total number of control count registers in these five values is greater than 250, then the following message is displayed:

```
"Warning: Significant potential for data corruption exists.
  Changes in control count parameters are required."
```

The easiest way to correct this problem is to output raw data from the database to check the register position of the EECYC (E-to-E cycles) count in the raw data block. If the position of this count is wrong, adjustments can be made to the `rrcnt` parameter in the record base Office File to realign the registers. For example, if the count is four registers beyond where it should be, you can adjust the rrcnt value by subtracting four (4) from the existing rrcnt value.

□

Realigning registers

Purpose

While this section refers primarily to 1A *ESS* switches, this procedure can be used to output raw data for any switch type supported by NTM.

Instructions

Follow this procedure to realign registers:

1 Enter `/nm/dbutil/opentref clli`

The first line of the output contains information about the switch, including the *clli* code, type, generic, and issue. It also indicates the date when the last `create` was executed.

The lines beginning with “numtg” (number of trunk groups) contain information from the record base Office File and the switch database related to the 5-minute collected data.

The next section contains data addresses. Each address consists of a packet number followed by a count offset number. The packet number for all 1A *ESS* switches is 1. A packet number of -1 indicates that the count (or packet) is not scheduled. The count offset number is the count offset position in the packet.

2 Locate EECYC in the data addresses and write down the count offset number.

3 Enter `/nm/dbutil/opblock -o clli [-f d]`.

This command outputs the data counts stored in the raw data blocks in the database. The first line of the output contains the ending time of the 5-minute block of data.

The second section identifies the office and gives information about the raw block number, packet names, and their offset positions in the raw block, length of the packet, and any flags associated with the data.

The last section of the output contains the counts that are stored in the raw data blocks, beginning with a starting offset number at the beginning of each line, followed by ten counts.

4 Find the packet offset number (in the first few lines of output), then add the count offset number from Step 2. The sum of these numbers tells you where the EECYC count should be.

Typically, the EECYC count for a 1AE8 generic is approximately 3001, while the EECYC count for a 1A *ESS* generic is in the range 4000-9999.

Example: If the packet offset number is 2038 and the register count offset number is 295, their sum is 2333, which also is the offset position where the EECYC register count should be in the opblock output.

5 Look at the value in the offset position that should contain the EECYC count.

- If the count appears to be valid for EECYC, STOP, YOU HAVE COMPLETED THIS PROCEDURE.
- If the count appears to be invalid for EECYC, look at the values 4 to 5 spaces to the right and left where the EECYC count should be.

6 When you locate the EECYC count, determine how many places it is from where it should be.

Example: If the EECYC count should be in offset position 2333, but it actually is in 2337, it is four places from where it should be.

7 Edit the `rrcnt` parameter in the record base Office File to reflect the difference between where the EECYC count should be and where it actually is stored.

Example: If the EECYC count should be in offset position 2333, but it actually is in 2337, subtract four from the value of rrcnt.

8 Update the database using `dbtest` and `create`. A single office `dbtest` command will display an error message if the control counts are out of range. However, `create` still will update the current database with the changed control count.

END OF STEPS

Changing default domain for a control

Instructions

Follow these steps to change default domains.

1 Edit the Control Default Domain file for the desired switch (*4ESS* or *5ESS*.)

2 Find the line in the file that pertains to the control you wish to change.

3 Change the domain acronym to the desired domain. Note that the acronym must exist in the Domain Acronym File.

4 Save the changes, then run the `dbtest`. `create`, and `installdb` commands against the affected Control Default Domain file.

END OF STEPS

□

Adding and deleting RSPTE CLLI changes

Purpose

When you make changes to CLLI names in the RSPTE file, you may need to follow the Delete/Add procedure. The system can support up to 865 internal entities. If the number of internal entity CLLIs that you are going to change plus the number of existing internal entities is more than 865, you must use the Delete/Add procedure. By following the Delete/Add procedure from the beginning of the updates, you can avoid surpassing the maximum limit.

Instructions

Use Step 1 through Step 4 to ignore the entities you want to change and make more space available. Use Step 5 through Step 8 to add the new entities to the system.

1. Comment out (add a pound sign in front of) all of the lines in the RSPTE file that contain the CLLI that you want to change or that you have changed since the last `installdb rspte`.

2. Run `dbtest rspte` and resolve any errors.

3. Run `create rspte`.

4. Run `installdb rspte` (install with system running is appropriate if you have Feature 41, "Install RSPTE Without Stopsys").

5. Remove the comments and change the CLLI information as needed.

6. Run `dbtest rspte` and resolve any errors.

7. Run `create rspte`.

8 Run `installdb` **rspte** (places changes in the online database).

☐

Building the database for 1024 trunk groups

Purpose

This procedure is used to set up the database for Feature 264, "DMS 100/200 Switch Surveillance of 1024 Trunk Groups Via TDM" and Feature 265, "DMS 100/200 Surveillance of 1024 Trunk Groups Via DCOS-2000".

Before you begin

Use of this feature requires that the System Administrator has set up the links to the TDM and DCOS and that the Alcatel-Lucent site manager has enabled the appropriate features.

References

"Setting up DMS 1024 trunk group surveillance — DCC" (p. 5) in the *System Administration Guide*

Instructions

Follow these steps to build the database:

1. Add variable `max_tg=1024` to the switch entry in the RSPTE file.
2. Update switch generic to at least `na007` in the RSPTE file.
3. (TDMS only) Update TDMS generic for associated TDMS in RSPTE file to `tdms3`. (If *DMS **does not*** have surveillance of 1024 trunk groups, the TDMS generic should be set to `tdms2`).
4. (DCOS only) Update DCOS generic for associated DCOS in RSPTE file to `npm6_0`.

□

8 Record Base Update Procedures

Overview

Purpose

This chapter provides procedure for updating the record base.

Notes

See Chapter 5, "Record Base and Database Commands" in the *Input Commands Guide* for more information on the commands referred to in this chapter.

Depending on optional features you may have purchased, some command functions may differ from those presented here. Refer to the *Input Commands Guide*.

Contents

This chapter contains the following topics:

Performing a general update	8-2
Performing a full create and installdb	8-3
Performing a single file create and installdb	8-6
Performing a single office create	8-9

Performing a general update

Instructions

Follow these steps to update the record base.

1 Edit the record base files that need to be updated, using the *Linux* system `vi` command.

2 Run `dbtest` on the edited files. If errors are reported, edit the files that have errors and rerun `dbtest`. Continue until no errors are reported.

3 Run `create` on the tested files.

Three different procedures are available for the `create` command, depending on the specified variables: full `create`, single file `create`, and single office `create`. These procedures are given in this chapter.

Important! If you want to update a single trunk group threshold file, see "thresh" (p. 72) in the *Input Commands Guide*.

END OF STEPS

Performing a full create and installdb

Purpose

Use `create files=all` to perform a full `create`. Use `installdb files=all` to copy all the newly created files from the temporary database into the current database. The options for the `installdb` command are:

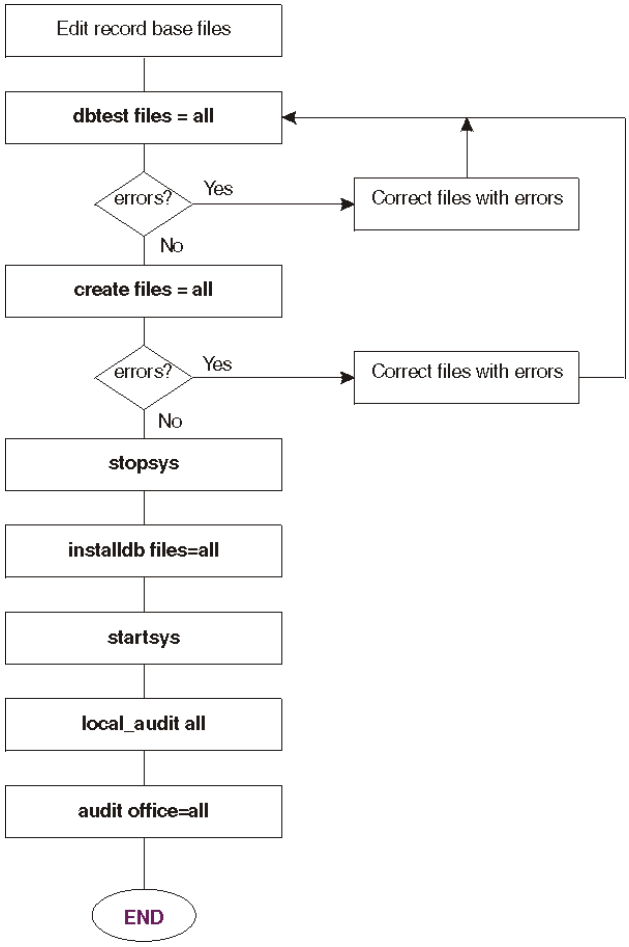
- `files=all` (installs reference data and initializes control records)

  Important! In some instances, the number of entries in the RSPTE File will exceed the configuration limit. This will generate an error message. See the error message INP 114 in the *System Responses Guide* for information on correcting this problem.

Figure

Figure 1 illustrates the full `create` and `installdb` procedure, followed by a detailed description.

Figure 1 Full create and installdb



Instructions

The following steps refer to Figure 1, “Full create and installdb” (p. 4).

1 Edit the record base files in their proper directories, using the vi command.

Reference: See Chapter 5, “Record Base Files” for more information on the full pathname to be used for each NTM record base file.

2 Execute `dbtest files=all`.

3 Were errors reported?

- If no, continue with the next step.

- If yes, the `dbtest` command outputs the line number and name of the record base file(s) containing errors. Edit the files with errors. Execute the `dbtest` command again. Continue editing and testing until there are no more errors.

4 Execute `create files=all`.

5 Were errors reported?

- If no, continue with the next step.
- If yes, edit the files with errors. Go back and repeat Step 2 and Step 3 until there are no more errors, then continue with the next step.

6 Execute `stopsys`.

7 Execute `installdb files=all when=now` to copy data from the temporary database to the current database.

CAUTION

Each time a full `create` (`create files=all`) is performed, it should be immediately followed by a full `installdb` (`installdb files=all when=now`). If you choose to install the files at dayend, any reference data changes made between the full `create` and dayend may be lost. Also, if the `create files=inms` command is run between the full `create` and dayend, changes to all except the inms file will be lost.

8 Execute `startsys`.

9 Execute the `local_audit all` command to receive a quick approximation of the synchronization of the NTM database with the switch database.

10 Execute `audit office=all` to synchronize the NTM database with the switch database.

END OF STEPS

□

Performing a single file create and installdb

Purpose

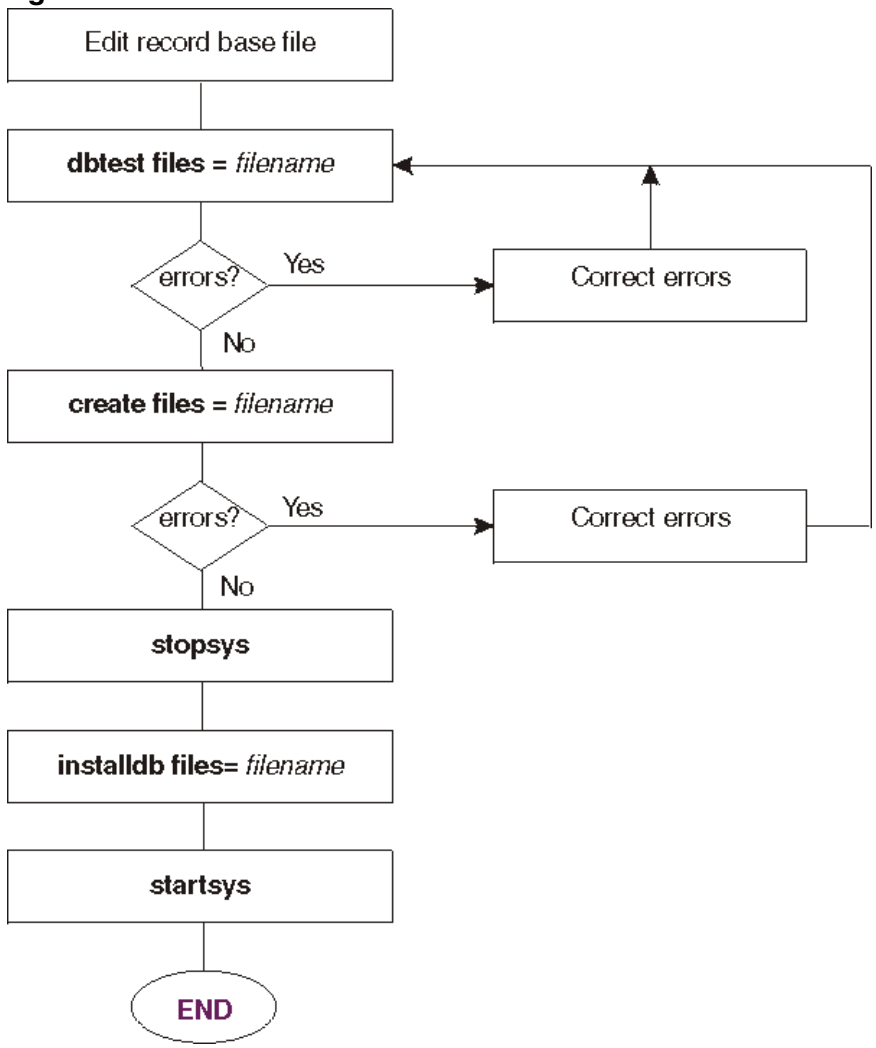
Use `create files=filename` to perform a single file `create`. Use `installdb files=filename` to copy the newly created file from the temporary database into the current database.

> **Important!** This procedure can be used with any variable for the files keyword except `office`. Use the single office `create` procedure for this variable.

Figure

Figure 2 illustrates the single file `create` and `installdb` procedure. A detailed description of this figure follows.

Figure 2 Single file create and installdb



Instructions

The following steps refer to Figure 2, "Single file create and installdb" (p. 7).

Important! The `files=office` option is not available for this procedure. To create the files associated with this option, use "Performing a single office create" (p. 9).

1 Enter `dbtest files= file`

2 Were errors reported?

- If no, continue with the next step.

- If yes, the `dbtest` command outputs the line number and name of the record base file(s) containing errors. Edit the files with errors. Execute the `dbtest` command again. Continue editing and testing until there are no more errors.

3 Enter `create files=` *`file`*

4 Execute `stopsys`.

5 Execute `installdb` for the desired file.

6 Execute `startsys`.

END OF STEPS

□

Performing a single office create

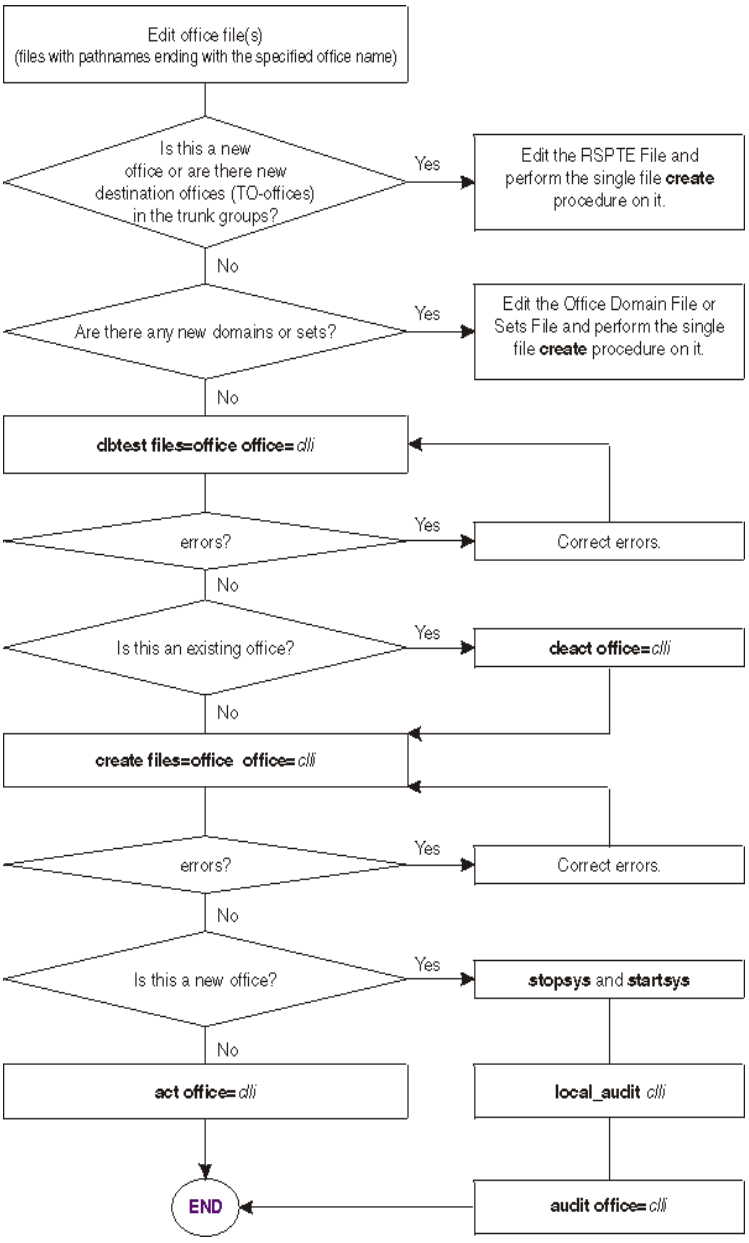
Purpose

Use `create files=office office=office` to perform a single office `create`. This procedure affects all files for a single office that have pathnames ending with the specified office name.

Figure

Figure 3 illustrates the single office `create` procedure. A detailed description of this figure follows.

Figure 3 Single office create



Instructions

The following steps refer to Figure 3, “Single office create” (p. 10).

Reference: See Table 1 for the pathnames for record base files that are updated with this procedure.

1 Is this a new office or are there new destination (to) offices in the trunk groups?

- If yes, add the new office names to the RSPTE File and use "Performing a single file create and installdb" (p. 6) to update the RSPTE File.
- If no, continue with the next step.

2 Are there any new domains or sets?

- If yes, edit the Office Domain File or Sets File and use the "Performing a single file create and installdb" (p. 6) to update the domain or sets file.
- If no, continue with the next step.

3 Execute `dbtest files=office office=`*`office name`*.

4 Are there any errors in the office files?

- If yes, edit the "/musr/rb/office/*office* files to correct the errors. Rerun the `dbtest` command. Continue to edit and test the files until there are no more errors.
- If no, continue with the next step

5 Is this an existing office?

- If yes, execute `deact office=`*`clli`*.
- If no, continue with the next step.

6 Execute `create files=office office=`*`clli`*.

7 Is this a new office?

- If yes, execute `stopsys` followed by `startsys`.
- If no, continue with the next step.

8 Execute the `act office=`*`clli`* command to activate the office.

9 Execute the `local_audit` *`clli`* command to quickly synchronize the NTM database with the switch database.

10 Execute the `audit office=cli` command to synchronize the NTM database with the switch database.

END OF STEPS

Table

Table 1 provides pathnames for record base files that are updated with this procedure.

Table 1 Single office create record base files and corresponding paths

Record Base File Name	Found In
Office File	"/musr/rb/office"
Trunk Group File	"/musr/rb/tg"
Office Domain File	"/musr/rb/domain"
Transmitter Timeout (TTO) Thresholds File	"/musr/rb/tto"

9 Maintaining the Record Base with BDR

Overview

Purpose

This chapter provides background information and procedures for working with BDR and the record base.

Much of record base administration has to do with the `create` command and the process behind it. Simplified, the `create` process generates the reference data portion of the NTM database. The process gathers user-entered information from record base files in the "/musr/rb" directories, creates the reference data portion of the database, and installs the data into the database. This involves the use of the `create`, `stopsys`, `installdb`, and `startsys` commands.

The use of these commands is no different for BDR. What ***is*** different is the internal process of updating reference data using the additional record base directories for partitions ("/musr/snw/<*partition*>/rb"). In most cases, the command will execute on the primary host, then re-execute on the secondary host or hosts.

Reference: Chapter 7, "Record Base Administration"

Restrictions

BDR (Backup and Disaster Recovery) features — Feature 8, “Disaster Recovery (Duplex)”and Feature 40, “Enhanced Disaster Recovery” — are optional. They are available only if purchased.

Contents

This chapter contains the following topics:

Partitioning for BDR	9-3
Using the INMS file to define partitioning	9-5
Resolving errors	9-6
Configuring the record base files for BDR	9-7
Synchronizing UDDM/UDNEI files for BDR	9-9
Differences in record base files	9-11

Partitioning for BDR

Overview

BDR works by “partitioning” the record base on each host. The record base on each host contains at least two partitions, which the system administrator creates with the `snw_admin` command.

Description

A partition is a collection of offices and record base files containing information about the offices that belong to the partition.

The types of partitions are:

- ***primary*** partition, which contains the record base files for which data collection and monitoring occurs under normal operating conditions.
- ***backup*** partitions, which contains a copy of the record base files for the subnetwork partitions residing on the secondary hosts (also referred to as the backup hosts).

Primary partition

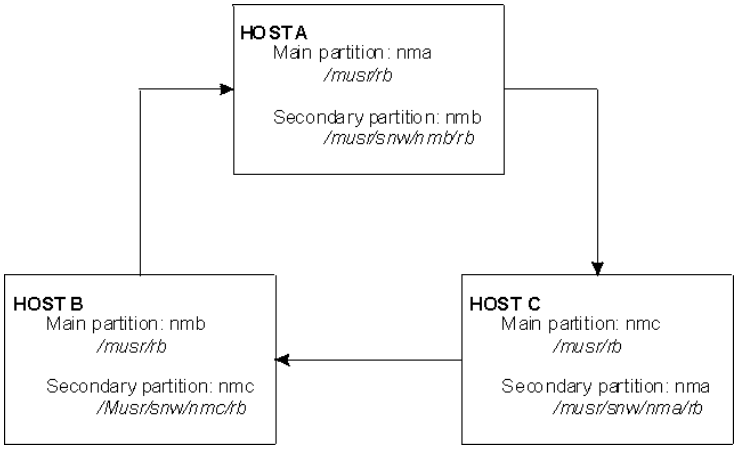
The main partition, which must be a primary partition, has its record base files in the “/musr/rb” directory.

With BDR, record base files belonging to primary partitions are backed up onto the backup or secondary host (specified in the “/musr/rb/inms/inms” file), in the “/musr/snw/<*partition*>/rb” directory.

Figure

Figure 1 illustrates how three hosts and their partitions are set up, and how they interact in a daisy chain environment.

Figure 1 Primary and secondary hosts partitioning



Using the INMS file to define partitioning

INMS File

The INMS File (Inter-Network Management System) reflects partitioning information on both the primary and secondary hosts. It is used to define the partitioning of the NTM network for data distribution and backup support. The information in this file includes the primary and secondary host that supports each subnetwork partition.

All partitions must be included in the INMS File.

Reference: "INMS File" (p. 31)

Format(s)

The following format is used for entering subnetwork partitions and host information in this file:

```
partition=name primary=primary_host_name
   secondary=secondary_host_name;
```

Important! Both the primary and secondary NTM names must be defined as NTM offices in the appropriate RSPTE File.

Examples

Figure 2 shows an example of an entry in the INMS File ("/musr/rb/inms/inms").

Figure 2 Entry in the INMS file

```
partition=nma primary=hosta secondary=hostc;
partition=nmb primary=hostb secondary=hosta;
partition=nmc primary=hostc secondary=hostb;
```

In this example, the first entry defines the partition ***nma***, which is a primary partition on host ***hosta***. The partition is backed up on ***hostc***.

The second entry defines the partition ***nmb***, which is a primary partition on host ***hostb***. The partition is backed up on ***hosta***.

The third entry defines the partition ***nmc***, which is a primary partition on *hostc* and is backed up on ***hostb***.

□

Resolving errors

Purpose

During the `create` and `bdr_create` processes, some errors will be output on the screen in the standard manner of the `create` command. When the `create` command has successfully run on the host from which it was invoked, it calls `bdr_create` and the output of that process is also output on the screen. Errors in transmission are also reported in the "/musr/log/bdrlog" file.

Important! The `create` command invokes the `bdr_create` executable (this is not a user command).

Instructions

If errors occur in the create process during the transmission of data from one host to another, perform the following steps:

1. Determine the cause of the failure (e.g., a link problem).
2. Correct the cause of the failure.
3. Rerun the `create` command, watching the output messages to ensure that both the `create` and the `bdr_create` commands have run successfully.

END OF STEPS

□

Configuring the record base files for BDR

Purpose

The following procedure details the steps to be taken by the Record Base Administrator to configure the record base files for BDR.

Before you begin

Before this procedure may be performed, the System Administrator must perform "Performing system administration tasks" (p. 24) in the *System Administration Guide*.

Instructions

Follow these steps to configure the record base files for BDR.

1 Move or copy the RB files for all partitions to the proper partitioned RB directory.

The main partitioned subnetwork record base files reside under the "/musr/rb" directory structure. The remaining partitioned subnetwork record base files reside under the "/musr/snw/<*partition*>/rb" directories.

2 Add all hosts to the "musr/rb/rspte/rspte" file.

One entry for each host needs to exist in the appropriate RSPTE File.

For example, using the north/south scenario, the north host entry is added to the "/musr/rb/rspte/rspte" file on the north host machine. The south host entry is added to the "/musr/snw/<south partition>/rb/rspte/rspte" file which is also on the north host machine.

Likewise, on the south host machine, the south host entry is added to the "/musr/rb/rspte/rspte" file and the north host entry is added to the "/musr/snw/<north partition>/rb/rspte/rspte" file.

Reference: See the expanded explanation in "RSPTE File" (p. 67).

3 Create an empty Office File for each host in the "/musr/rb/office" directory.

4 Create and install the RSPTE File.

The main partitioned subnetwork record base files reside under the “/musr/rb” directory structure. The remaining partitioned subnetwork record base files reside under the “/musr/snw/<*partition*>/rb” directories.

5 Modify the “/musr/rb/inms/inms” file to reflect any new partitions.

The INMS File (“/musr/rb/inms/inms”) lists the valid partitions and the primary and secondary hosts the partitions reside on.

- The primary host is the NTM host where the primary partition resides.
- The secondary host is the partition's backup host for BDR.

For example, if two hosts are used, north host and south host, with two partitions, north and south partitions, the north host is the primary host for the north partition, and its record base files are backed up to the secondary host, the south host. The south host is the primary host for the south partition, and its record base files are backed up to the secondary host, the north host.

On both hosts, the primary partitioned subnetwork(s) is the collection of network elements for which data collection and monitoring occurs under normal operating conditions.

6 Create and install the “/musr/rb/inms/inms” file.

Reference: See the expanded explanation in “INMS File” (p. 31).

END OF STEPS

Synchronizing UDDM/UDNEI files for BDR

Purpose

The following procedure details the steps to be taken by the Record Base Administrator to replicate models and udneitypes to BDR host.

Instructions

Follow these steps to synchronize the record base files for BDR.

1 Copy all files in the "*/musr/uddm"* directory to the secondary host.

2 Copy reference file "*/musr/rb/udnei/udneitype"* to the secondary host. This file maps the UDNEITYPE to a DCOL and to a datasource.

3 Copy "*/musr/rb/udnei/<dcol>/dcol_parms file"* to the secondary host.

END OF STEPS

□

Differences in record base files

Overview

Purpose

With BDR, record base files are split into four types:

- global
- independent
- office-related
- shared (or merged)

Global files are available at, and are the same on, all hosts. They reside in the appropriate "/musr/rb" directory.

Independent files are maintained separately on both hosts and are not shared between hosts.

Depending on which partition the office belongs to, office-related files reside in either the "/musr/rb" directories or the "/musr/snw/<*partition name*>/rb" directories. They are files that contain information relative to specific offices.

Shared files contain mutually exclusive data, are available at both hosts, and are merged when the `dbtest` and `create` commands are used.

The following sections detail which record base files fit into these categories, and the processes that `dbtest`, `create`, and `installdb` execute on them.

Contents

This section contains the following topics:

Global files	9-12
Independent files	9-15
Office-related files	9-17
Shared files	9-19

Global files

File types

Files considered to be ***global*** are:

- Sets File
- Domain Acronym File
- Event_Alarm File
- INMS File
- International Code File
- PAS Code File
- Password File
- Discrete File
- Final Handling Code (FHC) File
- TYPXREF File
- DCC alias file
- All Point Code (APC) File
- Filter File

Exceptions

The DCC alias file resides on each host. Since it is not part of the BDR process, you must manually update it and keep it in sync. Since it is not part of the create process, the file is not part of BDR. Use the `bdr_commit` command to make manual backups of the DCC alias file on the backup host.

The Domain Acronym File is not updated directly with the `dbtest` and `create` commands. If you want updates to the Domain Acronym File to be transferred to the backup host machine, you must make sure the file is in the primary state before you run these commands on it. If you do not want updates to be transferred, run `dbtest` and `create` with the `noxfer` parameter, for example: `dbtest file=sched noxfer`.

The Password File is kept in sync using the dayend process. If updates are required more frequently, manual backups between NTM hosts are required.

Rules

Global files share the same rules:

- Only one version of the file exists on each host in the “/musr/rb” directories.

- The dbtest or create <*record base file*> command is executed on the primary host. If the file is in the primary state when the command is executed, and is in the backup state on the backup host, the file is transferred to the appropriate "/musr/rb" directory on the backup host and is also created there, but not installed.

  Important! If you do not want a global file to transfer to the backup host when you run dbtest or create on it, use the noxfer parameter on the command line, as shown below.

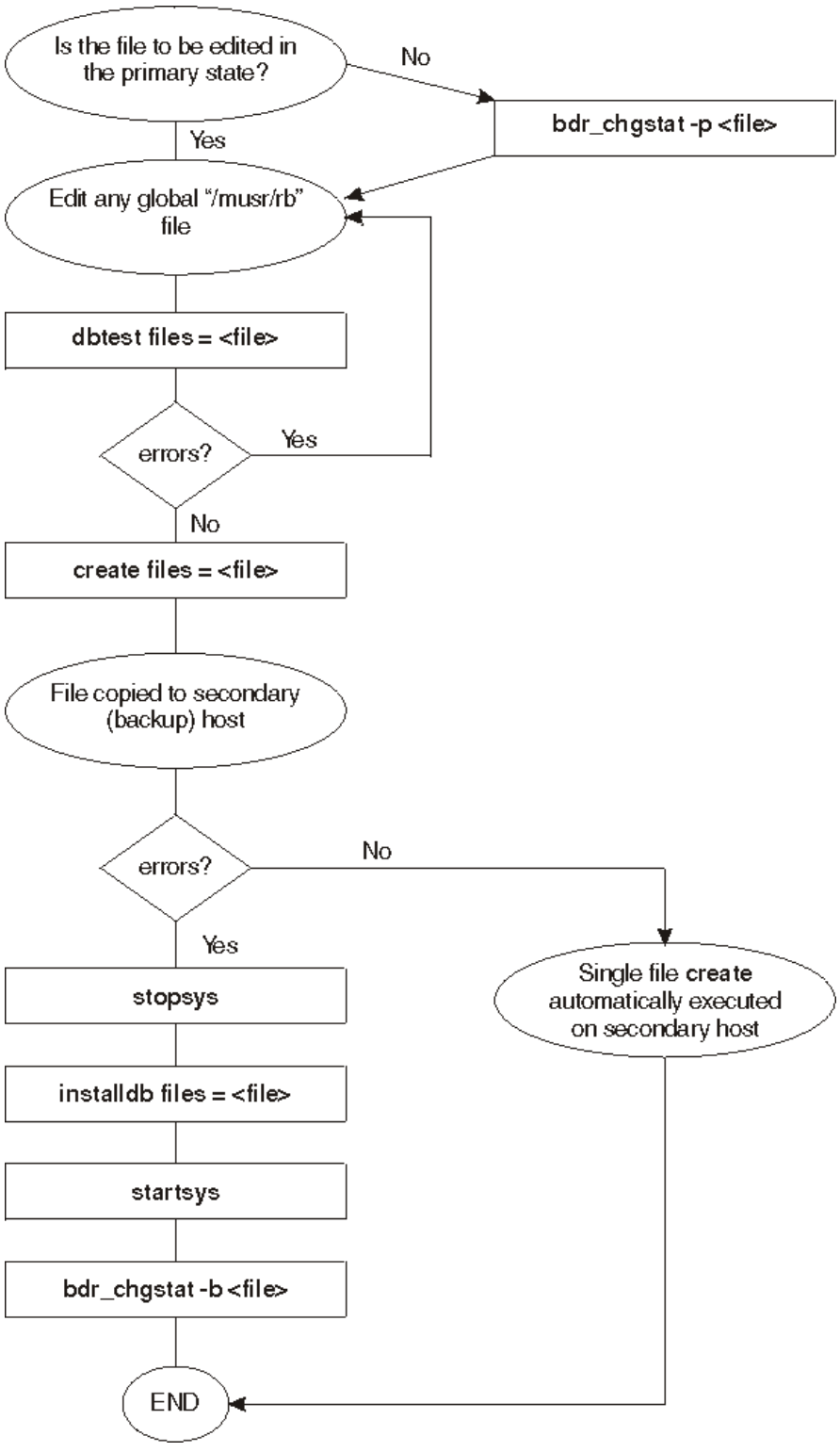
  ```
  $ dbtest file=sets noxfer
  ```

- To change the state of a file, use the bdr_chgstat command. See the in the *Input Commands Guide*.
- If the global file is in the primary state on the primary host, and in the backup state on the backup host, existing information on the backup host is overwritten when the file is copied to the backup host.
- The user may run stopsys and installdb on the primary host to install the new file; otherwise, it is not installed until dayend.
- If they wish, users on the backup host may run stopsys and installdb. Otherwise, the file is installed on the backup host at dayend.

Figure

Figure 3 illustrates the create process for a global file.

Figure 3 The create process for global files



Independent files

File types

The Threshold Table Schedule File is an ***independent*** file.

Rules

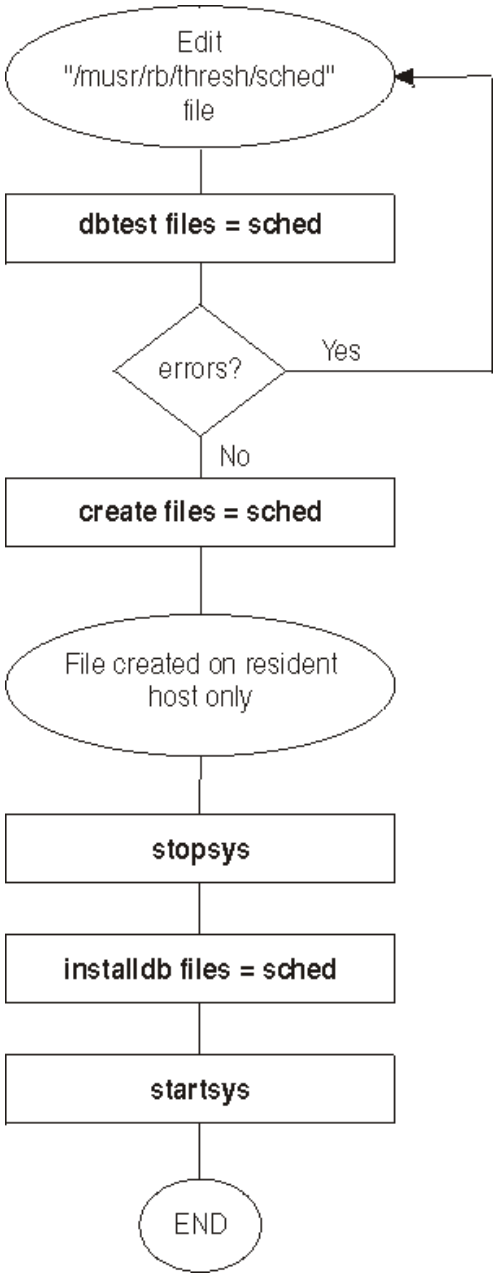
The following rules apply to the Threshold Table Schedule File.

- Each host has its own file.
- The file is not transferred to the backup host via the `create` and `installdb` commands. Instead, it is transferred to the backup host via `dayend` to the "/musr/snw/<*partition*>/rb/thresh" directory on the backup host.
- You may run `stopsys` before installing with `installdb` <*file*>. Otherwise the changes will update the database at dayend.

Figure

Figure 4 illustrates the `create` process for an independent file.

Figure 4 The create process for independent files



Office-related files

File types

Files considered to be ***office-related*** are:

- Office File
- Office Domain File
- Trunk Group File
- Transmitter Timeout (TTO) Thresholds File

Rules

Rules for office-related files are:

- The partition to which an office belongs is the partitioned record base directories in which the office files reside.
- When the command `dbtest` or `create office <clli>` is executed for an office belonging to a primary partition on the host, all of its office-related files are transferred to the "/musr/snw/<*partition*>/rb" directories on the backup or secondary host. The `dbtest` or `create` command is also executed on the backup host.

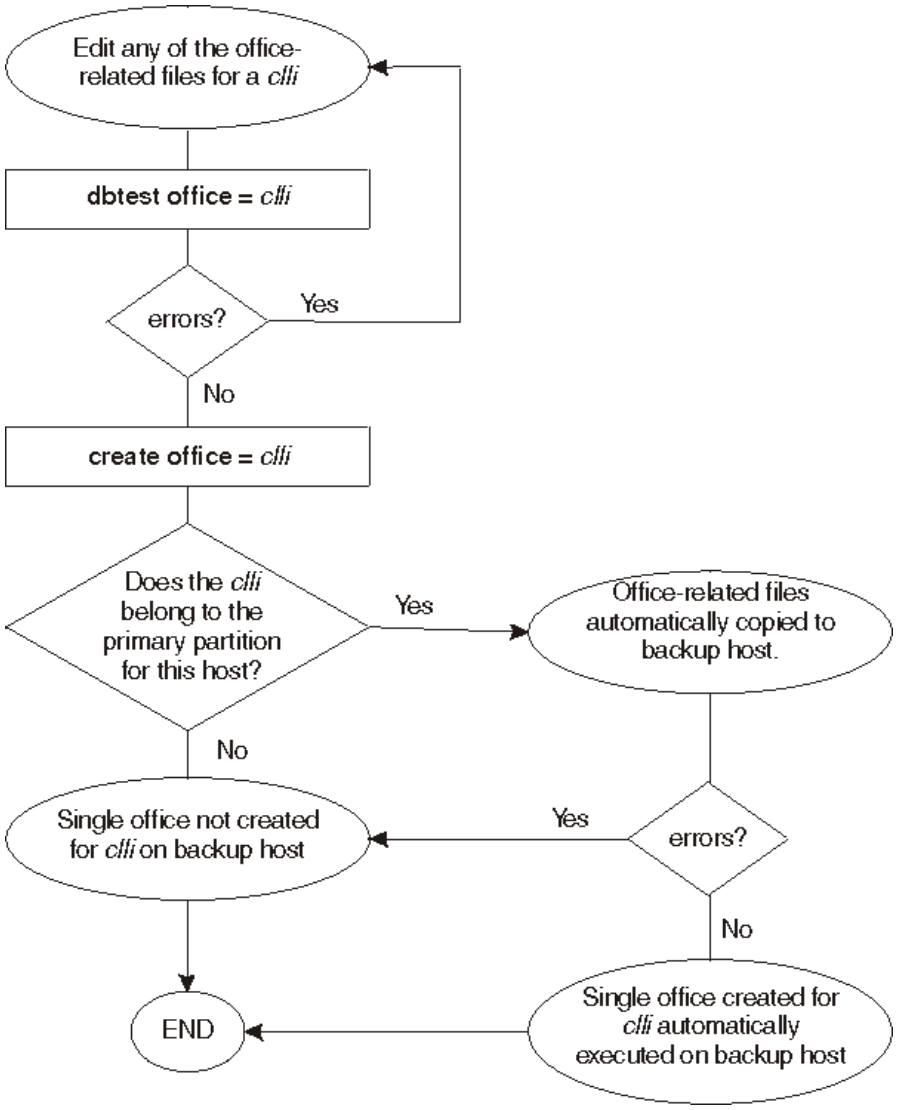
  Important! If you do not want a global file to transfer to the backup host when you run `dbtest` or `create` on it, use the `noxfer` parameter on the command line, as shown below.

  ```
  $ dbtest file=office office=beta0000001 +noxfer
  ```
- When the command is executed for an office not belonging to a primary partition on the host, the office-related files are not transferred to the backup host, and `dbtest` or `create` does not execute on the backup host.
- No `stopsys` and `installdb` is needed.
- For DCC office files, the complete dialstring must be used.

Figure

Figure 5 illustrates the `create` process for office-related files.

Figure 5 The create process for office-related files



Shared files

File types

Files considered to be ***shared*** (or ***merged***) are:

- RSPTE File
- Trunk Group Threshold File
- Domestic Code File

Shared files are record base files that are split among the partitioned subnetworks. The files within a partitioned subnetwork contain a portion of the total network information. During a `dbtest` or `create`, the information from the partitioned subnetwork record base directories is combined (merged).

Treatment of these shared record base files is detailed in the text that follows.

> **Important!** If you do not want a shared file to transfer to the backup host when you run `dbtest` or `create` on it, use the `noxfer` parameter on the command line, as shown below.
>
> ```
> $ dbtest file=rspte noxfer
> ```

RSPTE file

Executing a `dbtest` or `create rspte` causes the following to occur:

- The system processes RSPTE Files from the "/musr/rb/rspte" and "/musr/snw/<*partition*>/rb/rspte" directories.
- If an invalid subnetwork name exists, an error is printed and the record is processed, defaulting to the partitioned subnetwork name.
- If no subnetwork name exists, it defaults to the partitioned subnetwork name.
- If duplicate office names exist, the duplicates are not processed and an error message is printed. The user must edit the RSPTE File to correct these duplicates.
- If duplicate RSPTE numbers or nicknames exist, an error message is printed. The user must edit the proper RSPTE File to correct these duplicates.
- The RSPTE Files belonging to the primary partitions are transferred to the backup hosts in the "/musr/snw/<*partition*>/rb/rspte" directory.
- Installing changes after a successful `create rspte` on the primary host with `installdb` causes the changes to be installed on both the primary and secondary hosts.

Trunk group threshold file

Each threshold file contains 128 indices (contains 256 indices if Feature 3, “Management of Record Base Partitions and Subnetworks” is purchased). The indices must be shared or specifically designated for all partitions. No duplicate indices should exist within a threshold file.

Executing a `dbtest`, `create` or `thresh` command causes the following to occur:

- The system processes the “/musr/rb/thresh/thresh(1-8)” and “/musr/snw/<*partition*>/rb/thresh/thresh(1-8)” files.
- The threshold files in the primary partitions are transferred to the “/musr/snw/<*partition*>/rb/thresh” directory on the backup host and are created on the backup host.
- At the primary host, the user may execute `stopsys` and `installdb` (after a `create`) to place the changes in the database. Otherwise, the changes will be installed during dayend.
- Users on the backup host may run `stopsys` and `installdb` (after a `create`) but it is not required, as the file is installed on the backup host at dayend.

Domestic code file

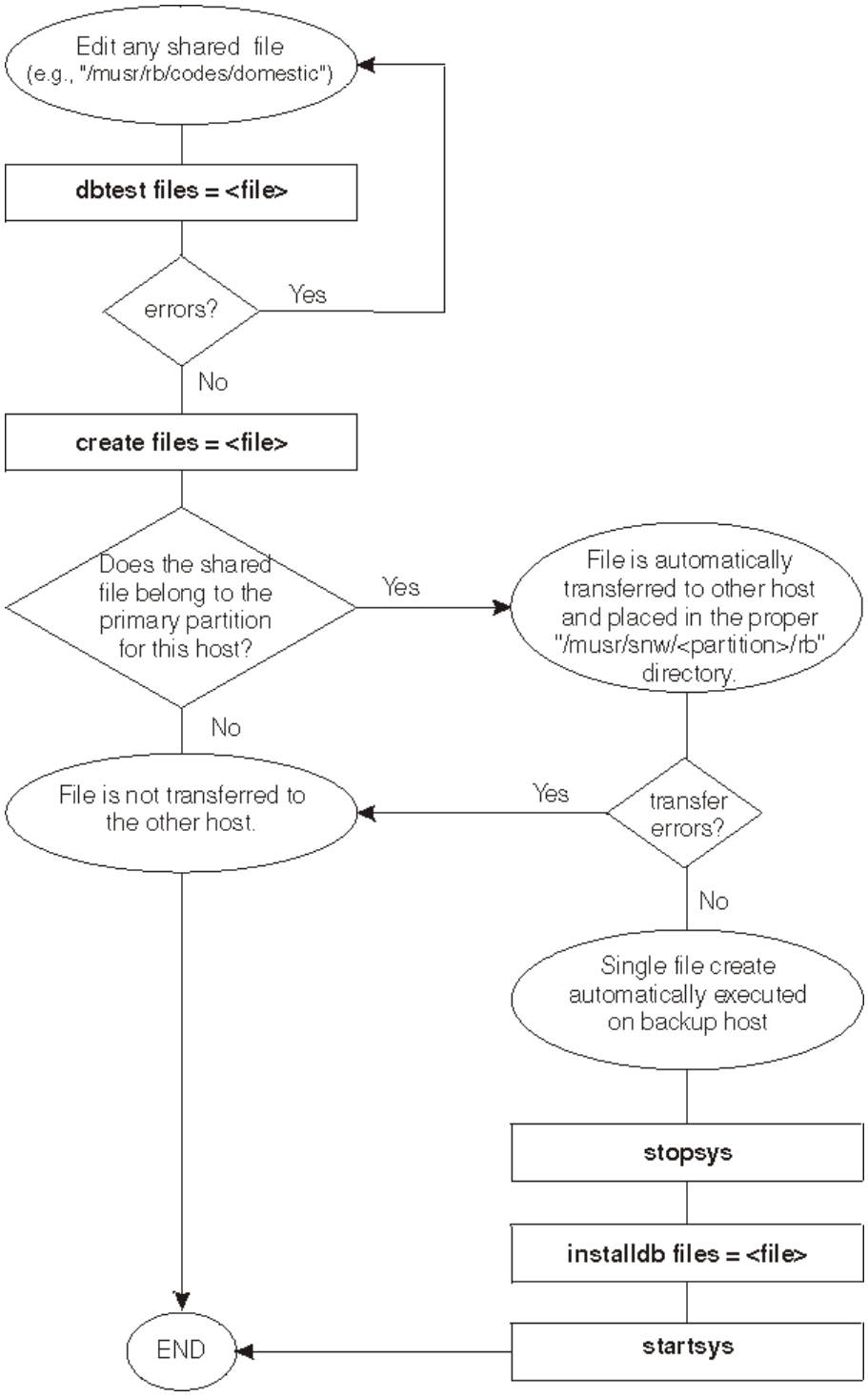
Executing a `dbtest` or `create domestic` command causes the following to occur:

- The system processes the “/musr/rb/codes/domestic” and “/musr/snw/<*partition*>/rb/codes/domestic” files.
- A maximum of 100,000 combined codes is allowed. If duplicate codes are encountered, they are skipped. In either case, an error message is printed.
- When the command is executed, the primary partitions' files are transferred to the “/musr/snw/<*partition*>/rb/codes/” directory on the backup host and are created on the backup host.
- A `stopsys` and `installdb` may be executed (after a `create`) to install the changes in the database. This can be done at any time on the primary host, or is automatically installed on the backup host during dayend.

Figure

Figure 6 illustrates the `create` process for a shared file.

Figure 6 The create process for shared files



10 Adding and Removing Network Elements

Overview

Purpose

This chapter discusses how to add and remove network elements. The primary method for connecting network elements to the NTM host is through TCP/IP connections.

DCC migration

During the migration away from DCC's and to connect network elements to the NTM host directly through TCP/IP, we have included a section for "Migrating to TCP/IP connectivity" (p. 39).

Before you begin

If the system does not have *4ESS* switches, you must make the following change in "/nm/ubin/start.all" before running DCOL_4E. This change prevents the system from trying to collect *4ESS* entity information.

Change the line:

```
DCOL0:0:0:respawn:export SRVID=20;DCOL_4E -s
   DCAUDSVC0,DCADMSVC0,DCCTRLSVC0 -o /dev/null -e /dev/null -- -i 0
```

to:

```
DCOL0:0:0:respawn:export NO4ESS=1; export SRVID=20; DCOL_4E -s
   DCAUDSVC0,DCADMSVC0,DCCTRLSVC0 -o /dev/null -e /dev/null -- -i 0
```

Contents

This chapter contains the following components:

Time recommendations	10-3
TCP/IP interface to a DCC	10-5
Adding a DCC	10-13
Moving a switch to a new DCC	10-19
Removing a DCC	10-23
TCP/IP interface to offices	10-27
Adding or removing an office	10-33
Migrating to TCP/IP connectivity	10-39
Secure shell for Succession switches	10-57
Troubleshooting network elements issues	10-61

Time recommendations

Table

Table 1 lists estimated times to perform each procedure.

Table 1 Recommended time allotment for procedures

Procedure	Approximate Time Required
DCC	
Creating the record base files (DCC)	15 minutes
Installing the updated record base (DCC)	20 minutes
Performing post-DCC move steps on NTM	30 minutes
Performing post-DCC move steps on the EADAS	30 minutes
Removing the record base files (DCC)	15 minutes
Setting up the TCIP/IP link between the host and switch	1 hour
OFFICE (Non-4ESS)	
Creating the record base files (office)	15 minutes
Removing the record base files (office)	15 minutes
Updating the system after removing an office	90 minutes
Migrating to TCP/IP connectivity	1 hour
Setting up the infrastructure	1 hour
Preparing the non-NTM features	1 hour
Preparing the NTM host	3 hours
Cutting over an office	10–60 minutes
Backing out an office cutover	15 minutes
Verifying cutovers	10–30 minutes
Finalize cutovers and deactivate the DCC interface	1 hour

TCP/IP interface to a DCC

Overview

Purpose

This section discusses procedural and supporting information for DCCs.

Contents

This section contains the following components:

Requirements	10-6
Direct connect TCP/IP interface to data collector	10-7
Using and testing TCP/IP connections	10-10

Requirements

Prerequisit features

The following FEP releases are supported with Feature 124, “TCP/IP Interface to FEP”: FEP (Release 2) and later

The following TDMS release is supported with Feature 245, “TCP/IP Interface to TDM”:TDMS Release 3.1 and later

The following NPM release is supported with Feature 369, “TCP/IP Interface to NPM”: NPM Release 6.0 and later

Coordination

It is necessary to coordinate use of this feature with record base personnel, as a change must be made to the record base “Office” file. A dialstring must be added for the TCP/IP connection.

Reference: “Required entries in the “/etc/hosts” file” (p. 6)

Required entries in the “/etc/hosts” file

Each DCC that will interface to an NTM using the TCP/IP interface must have an entry in the “/etc/hosts” file. Likewise, an entry must exist in the hosts file on the DCC that defines the host name and IP address of each NTM that it will interface to.

Here is an example NTM “host” file.

Figure 1 NTM “/etc/hosts” File

```
192.7.41.82     ntmos1 “optional alias”
192.7.41.82     ntmos2 “optional alias”
192.7.41.82     fepone "optional alias"
192.7.41.82     tdms1 "optional alias"
```

Reference: Sets File in the *Record Base Administration Guide*

Communicating with DCCs over the TCP/IP network

Ethernet interface connections between NTM and a DCC must exist. Additionally, network route(s) must exist so that the systems can communicate with each other.

Depending on the method of implementation, static or dynamic routing can be established.

NTM to DCC communications using TCP/IP may share the same Ethernet interface on the system that is used for normal data traffic to the host NTM machine.

Direct connect TCP/IP interface to data collector

Specifying a new far end destination remote host to the TCP/IP protocol database

System administration personnel are responsible for modifying the TCP/IP host and routing data.

This TCP/IP data exists on the NTM systems for other system functions (for example, rlogin, ftp, telnet...); however, the WAN that these functions use may not contain a route to the required switching system. In addition, even if the WAN supports basic transfers of data between NTM and the switch, there exists the strong possibility that the route taken by the data to/from the far end is insufficient in one or more of the following ways:

- Number of hops (physical path); could cause delays in data delivery
- Quality of service (will the data arrive in a timely manner)
- Bandwidth (size of the data pipe); this issue occurs when NTM must compete on the same LAN/WAN with other normal business functions. It is STRONGLY recommended that NTM **NOT** be provisioned on the same physical LAN that carries “regular business” functions. The practice of assigning realtime communication traffic to business LANs has been known to cause multiple anomalies in network systems.
- Hardware configuration; failure of a single hardware unit could cause an NTM outage to certain switches (or groups of switches, or ALL switches in the worst case scenario). There should be planned hardware redundancy in the case of ALL interfaces that route to target switches. This affects all hardware on path to the far end: Network Interface Cards (NICs), routers, physical connections. In the ideal case NTM would use two different physically diverse paths on two separate interfaces to one target switch (for example, one path via land-line, the other via microwave channel).
- WAN/LAN carrier; the method and size of the pipe that connects NTM to the far end switch must be considered. The delivery of TCP/IP data will be adversely affected if the carrier is not sized properly or is not of a high quality.

Adding routing data

It is necessary to add routing data for each switch from which NTM will collect data. This is accomplished by the system administrator (requires root privilege) in one of several methods outlined in the RHEL manual.

The simplest method is to simply add an entry in the “/etc/hosts” file on NTM for each target switch specifying the CLLI (Common Language Location Identifier) that NTM recognizes.

This “/etc/hosts” file entry is of the form:

```
# The form for each entry is:
# <internet address> <official hostname> <aliases>
     130.88.47.172       switch_name     possible_switch_alias
```

This method is only one of several methods used to determine how the switch CLLI is translated to the proper interface for TCP/IP communication. Other methods, Domain Name Service (DNS) and Network Information Service (NIS/BIND), accomplish the resolution of the switch CLLI to TCP/IP address. These methods are specified in the appropriate RHEL documents. You must add the name resolution capability for each and every data collection switch.

The "/etc/nsswitch.conf" file determines the method used to perform the CLLI to IP address translation: Linux files database, Domain Name Service (DNS) or Network Information Service (NIS). From "/etc/nsswitch.conf" the system will find the translation method.

The "/etc/nsswitch.conf" file possibly needs to be modified to reflect the method chosen to resolve a CLLI to an IP address. If the basic Linux file method is chosen then the file would look like the following example file, "/etc/nsswitch.files":

```
passwd:       files
group:        files
hosts:        files
services:     files
networks:     files
protocols:    files
rpc:          files
publickey:    files
netgroup:     files
automount:    files
aliases:      files
```

Also, if an implicit route to the far end switch is not available through the "default" route then an explicit route must be added so that the IP protocol knows how to reach the far end. This can be accomplished using the following methods:

- manually using the /usr/sbin/route command (refer to the "route(1M)" command in your *Linux* operating system documentation or use the online `man <`*`command_name`*`>` command.)

Operating system checks

The condition of the route/path to the far end of a TCP/IP link may be determined using a few *Linux* commands: /usr/sbin/ping, /bin/telnet, /usr/contrib/bin/traceroute. First try using ping specifying the CLLI or IP address of the target switch. If the after a length of

time (thirty seconds) the control-C key combination (*Linux* INTR signal) will display the packet loss statistics. If the packet loss statistics are greater than approximately ten percent (10%) then a problem exists in the route chosen to reach the far end.

□

Using and testing TCP/IP connections

Before you begin

Prior to activating a new DCC on NTM, verify that the communications path is available between NTM and the DCC.

Important! It is not recommended that a DCC be left active for extended periods of time on NTM if the communications path is not operational. This causes many connection attempts and messages to be logged in the "/musr/log/errors" file.

Operating system checks

There are commands provided as part of the *Linux* operating system that may be used to verify the communications and status of the network. Refer to the "ping", "telnet", and "netstat" commands in your *Linux* operating system documentation, or use the online `man <command_name>` command, to obtain more information about these commands.

"Ping" is a command that can help determine how far down the communications path a signal is getting. It can be used to send a message for basic loopback to the sending hosts or can be targeted to any intermediate point in the route if the "host name" or "IP address" is known. Ultimately, a "ping" should execute end-to-end.

Application checks

The NTM application code contains a command that may be used to send a test message to the DCC.

Reference: "sendmsg" (p. 20) in the *Input Commands Guide*.

Once the communications path has been verified and all the necessary administration work in both NTM and the DCC has been completed, the link can be activated. The log files and the `linkstat` command may be used to determine the status of the link. Also, the `linkstat` command output shows which interface is active to the FEP or TDMS.

Reference: "linkstat" (p. 9) in the *Input Commands Guide*.

Communications link

The *Linux* "netstat" command can be useful in determining the amount of traffic, routing table information, and certain network conditions, such as packets rejects, etc.

Refer to the "netstat" command in your *Linux* operating system documentation, or use the `man <command_name>` command, to obtain more information about the "netstat" command.

Routing table changes

The *Linux* “route” command can be used to update the routing table.

Refer to the “route” command in your *Linux* operating system documentation, or use the online `man <command_name>` command, to obtain more information about the “route” command.

Network bandwidth

As with any network, successful transmission and effective communications are dependent on appropriate bandwidth being available. Obviously, with a network traffic management system it is very important that the bandwidth be adequate for busy periods as well as for typical loads.

□

Adding a DCC

Overview

Purpose

This section provides procedures and related information to add a new DCC to be controlled by NTM. To add a new DCC to be controlled by NTM, you must create the record base files for the new network element and then install the updated record base.

Contents

This section contains the following components:

Creating the record base files (DCC)	10-14
Installing the updated record base (DCC)	10-15
Structure: DCC office list	10-16

Creating the record base files (DCC)

Instructions

Follow these steps to create the record base files:

1 Establish links to the DCC.

2 Add the DCC to the RSPTE File.

Reference: "RSPTE File" (p. 67) in the *Record Base Administration Guide* explains how to add the DCC to this file.

3 Add an Office File for the DCC.

Reference: "Office File" (p. 40) in the *Record Base Administration Guide* explains how to add an office file.

4 Enter `dbtest` to check the RSPTE File for errors.

END OF STEPS

□

Installing the updated record base (DCC)

Instructions

Follow these steps to install the updated record base files:

1 Enter `create rspte` to create the RSPTE File.

Reference: See Chapter 7, "Record Base Administration" in the *Record Base Administration Guide*.

2 Enter `stopsys` to stop the system.

3 Enter `installdb rspte now` to install the updated RSPTE DCC entry in the current database.

4 Enter `dbtest` to check the DCC office file for errors.

5 Enter `create all` to create the new DCC office file entry.

6 Enter `startsys` to start the system.

7 Enter `act` to activate the DCC.

END OF STEPS

References

See the *Input Commands Guide* for information on each of these commands.

□

Structure: DCC office list

Overview

When the connection to a DCC is established, the DCC sends NTM a list of offices to which it is connected. NTM uses this list to determine which offices it may communicate with through that particular DCC. NTM can also request this list if an active DCC requests it.

Important! Individual switch offices (entities) must be activated at the DCC to enable NTM to collect data for the offices from the DCC. Refer to the *Front-End Processor (FEP) Administration Guide* for information on activating FEP entities.

Output

The DCC output (list of connected offices) is written to the "/musr/ofclst" directory. There is a file for each DCC in this directory where the name of the file is the name of the DCC. In this file, a CLLI may be alias to another CLLI name. The format of the file is shown in Figure 2.

Figure 2 DCC File example

```
clli =  hrclca11ds0, type = DMS100, channel =  0
clli =  igncca1288l, type =  1AESS, channel =  1
clli =  labtolab5eh, type =   ESS5, channel =  2
clli =  lrksca11ds0, type = DMS100, channel =  3
clli =  lsbnca12ds0, type =   ESS5, channel =  4
clli =  mlbrca11ds0, type =   ESS5, channel =  5
clli =  nhldca11ds0, type =   ESS5, channel =  6
clli =  nlmtest1111, type = DMS100, channel =  7
clli =  npvlrs07e5h, type =   ESS5, channel =  8
clli =  nvcyca11ds0, type = DMS100, channel =  9
clli =  okdlca1184e, type =   ESS5, channel = 10
clli =  okldca03ds2, type = DMS100, channel = 11
clli =  okldca04ds0, type = DMS100, channel = 12
clli =  ptvlca1178e, type = DMS100, channel = 13
clli =  washdcut11t, type =   ESS5, channel = 14
clli =  nycmnyby01t, type =   ESS5, channel = 15
clli =  boston5esst, type =   ESS5, channel = 16
clli =  wtvlmeap02t, type =   ESS5, channel = 17
clli =  brtnmaco03t, type = DMS100, channel = 18
clli =  glflnygfds0, type =   ESS5, channel = 19  * NOT IN NM DATABASE *
clli =  dovrnhth02t, type = DMS100, channel = 20
```

In Figure 2

- "clli" is the name of the offices on the DCC

- “type” is the switch type
- “channel” is the DCC channel number
- The last field indicates those switches that are not in the NTM database or are offline at the FEP.

  Reference: Chapter 4, “Data Collection Concentrator Alias File” in the *Record Base Administration Guide*

□

Moving a switch to a new DCC

Overview

Purpose

Several procedures are required to make sure NTM and the DCC know that an office has been added or removed.

Contents

This section contains the following components:

Performing post-DCC move steps on NTM	10-20
Performing post-DCC move steps on the EADAS	10-21

Performing post-DCC move steps on NTM

Instructions

Follow these steps on the NTM:

1. Make sure the DCC procedure for building an office is followed in the DCC to which the office was moved and that the proper procedure is followed in the DCC from which the office was moved.

2. If the name of the office used in the DCC is different from that used in NTM, make an entry in the “/musr/rb/dcc_alias” file.

3. If the office's entry does not exist in the “/musr/rb/dcc_alias” file, then add it to that file.

4. Make sure you follow the DCC procedure for building an office.

5. Deactivate and activate the affected DCCs to move the office from the old interface data collector.

   Reference: See the `deact_dcc` command (7-13) and the `act_dcc` command (7-7) in the *Input Commands Guide*.

6. Enter `linkstat type=dcc`. Make sure that the DCC to which the office is connected is active and collecting information.

7. Execute `linkstat` on the office that was moved. Make sure that it is associated with the new DCC.

END OF STEPS

Performing post-DCC move steps on the EADAS

Instructions

Follow these steps on the EADAS:

On the EADAS *FROM* which the switch was moved:

1 Deactivate the entity.

2 Edit the entities file (under "/eusr/na/entity/rbasexx/entities/xxxx") and change the "`nm enabled`" parameter from "yes" to "no."

3 Execute `ice compile` on the entity.

4 Activate the entity (in order to get the change into DCC memory).

5 Deactivate the entity.

On the EADAS *TO* which the switch was moved:

6 Deactivate the entity (if already active).

7 Edit the entity file and change the "`nm enabled`" parameter from "no" to "yes."

8 Execute `ice compile` on the entity.

9 Activate the entity.

END OF STEPS

□

Removing a DCC

Overview

Purpose

When removing a DCC from NTM's control, you must remove the record base files for the DCC and then install the updated record base. These procedures show the required steps and provide references to more detailed information.

Contents

This section contains the following components:

Removing the record base files (DCC)	10-24
Updating the system after removing a DCC	10-25

Removing the record base files (DCC)

Instructions

Follow these steps to remove the record base files:

1 Remove all switches from the DCC.

Reference: “Adding or removing an office” (p. 33)

2 Enter `deact` to deactivate the DCC for collection of measurements, audits, controls, and discretes.

3 Remove the DCC from the RSPTE File.

Reference: “RSPTE File” (p. 67) in the *Record Base Administration Guide*

4 Remove the Office File for the DCC.

Reference: “Office File” (p. 40) in the *Record Base Administration Guide*

END OF STEPS

□

Updating the system after removing a DCC

Instructions

Follow these steps to remove the record base files:

1. Enter `create all` to copy the record base files to the offline database.
2. Enter `stopsys` to stop the system.
3. Enter `installdb all now` to install the offline database into the current database.
4. Enter `startsys` to start the system.

END OF STEPS

References

Chapter 7, "Record Base Administration" in the *Record Base Administration Guide*

□

TCP/IP interface to offices

Overview

Purpose

This section explains the TCP/IP (Transmission Control Protocol/Internet Protocol) interface to the offices.

Background

The customer may select the direct-connect TCP/IP interface to the switch, or the previously existing DCC interface to the switch, when both exist.

It is necessary to coordinate use of this feature with record base personnel, as a change must be made to the record base Office File and RSPTE File for this feature to function properly. This includes adding a dialstring to the “Office” file for the TCP/IP connection, entering security settings in the “Office” file, and setting the “direct” connection option in the “RSPTE” file.

Contents

This section contains the following components:

Requirements	10-28
Setting up the TCIP/IP link between the host and switch	10-30

Requirements

Equipment

TCP/IP Interface to the Switch requires the following:

- A properly equipped and engineered Ethernet between the NTM Feature Set and the Switch(es) from which data is to be collected
- The DMS 100/200 Switch must be equipped with a Supernode Data Manager loaded with a compatible TCP/IP and Ethernet protocol “stack”
- A properly configured security environment

Prerequisite features

This section applies when you are establishing a TCP/IP link to offices. Connections to SCSNSN (generic sn02 and later) type can only be made by directly connecting them to the NTM hosts via TCP/IP.

The TCP/IP Interface to offices prior to Release 13 was optional. Now it is required and is available through these features:

- DMS 100/200 Switches Generic NA013 and later only if Feature 277, “TCP/IP Interface to DMS 100/200 Switches” has been purchased.
- DMS 250 Switches Generic UCS13 and later only if Feature 293, “TCP/IP Interface to DMS 250 Switches” has been purchased. This feature expands from 200 to 800 simultaneous direct connect TCP/IP connections to switches from NTM. It is recommended the TCP/IP network used should be dedicated to the direct connect interfaces of NTM to avoid performance problems.
- DMS 500 Switches Generic NCS13 and later only if Feature 296, “TCP/IP Interface to DMS 500 Switches” has been purchased.
- *5ESS* Switches 5E15 Generic and later only if Feature 282, “TCP/IP Interface to 5ESS 5E15 Generic switches” has been purchased.
- Feature 381, “TCP/IP Interface to GTD-5 Switches”
- Feature 394, "TCP/IP Interface to 4ESS Switches via Datatek DT-4180"
- Feature 431, "TCP/IP Interface to 4ESS Switches via AI Switch"
- Feature 409, "TCP/IP Interface to 5ESS Switches via AI"
- Feature 410, "TCP/IP Interface to DMS Switches via AI"

Troubleshooting

In the event that all NTM data for a DMS switch being sent through a TDMS/FEP is missing at NTM, you will need to contact TDMS/NetMinder Customer Support for assistance.

The *DMS* switch can receive polls using either the EADAS interface (supporting up to 250 TGs) or the newer NTM interface (supporting up to 1024 TGs.)

One possible scenario is that NTM and the *DMS* switch are set up for 1024 TG support, but TDMS/FEP is not. In this case, TDMS/FEP will send polls for all NTM data for a given *DMS* switch along the EADAS interface, while the switch expects NTM polls only along the NTM interface.

Such a condition will result in no NTM data for this switch being sent to NTM. In this case, TDMS/FEP should be reconfigured to send NTM polls along the NTM interface.

If there is trouble connecting to the network element, verify port availability on the networl element using the netstat command.

Examples might be:

5ESS

```
“netstat -an | grep 60005"
```

DMS

```
“netstat -an | grep 9553"
“netstat -an | grep 9554"
“netstat -an | grep 9555"
```

□

Setting up the TCIP/IP link between the host and switch

Purpose

This procedure establishes the TCIP/IP link between the host and the DMS 100/200, DMS 250, DMS 500, *5ESS,* SCSNSN, Sonus GSX, and Sonus PLXswitch.

Instructions

Follow these steps to set up the link:

1 Create the link on the NTM host machine:

1. Enter `tcp` at end of entry for the value of the `direct` parameter for switch in RSPTE File.
2. Create the RSPTE File (`create rspte`).
3. Enter `stopsys`.
4. Install the RSPTE file (`installdb rspte`).
5. Enter `startsys`.
6. Deactivate the office if it is activated (`deact`).
7. Modify the Office File:
   - If establishing a link to DMS or SCSN office, add values for all three `dialstring` parameters and the `authentication` parameter.
   - If establishing a link to *5ESS* or 7R/E office, add values for the `dialstring` and `cpnode` parameters. Add an entry for the parameters in the PAS Code File.
8. Create the office (`create` office).
9. Add the clliname and the IP address of the office to the “etc/hosts” file.

   Important! If you have purchased the Backup and Disaster Recovery Features, this step will need to be done on each host.
10. Activate the office (`act`).
11. Enter `audit all`
12. Verify data collection from the office.

2 Contact switch personnel to activate their features that correspond to Feature 277, 282, 293, or 296 on the switch itself.

3 Activate the switch.

END OF STEPS

References

"Office File" (p. 40), "PAS Code File" (p. 63), and "RSPTE File" (p. 67) in the *Record Base Administration Guide*

See the related commands in the *Input Commands Guide*.

□

Adding or removing an office

Overview

Purpose

To add an office which is to be controlled by NTM, you must create the record base files for the new office and then install the updated record base.

> **Important!** DCC's such as FEPs, TDMs, etc. and Protocol converters (Datatek 4180) should be configured before adding offices.

When removing an office from NTM's control, you must remove the record base files for the network element and then install the updated record base.

Contents

This section contains the following components:

Creating the record base files (office)	10-34
Removing the record base files (office)	10-36
Updating the system after removing an office	10-37

Creating the record base files (office)

Instructions

Follow these steps to create the record base files:

1 Add the office to the RSPTE File.

2 Enter `dbtest rspte` to check this file for errors.

3 Enter `create rspte` to update the offline database.

4 If you have Feature 41, "Install RSPTE Without Stopsys", continue with Step 6.

5 If you do not have Feature 41, "Install RSPTE Without Stopsys":

- Enter `stopsys` to stop the system.
- Enter `installdb rspte` to move the newly built database from the offline area to the current area.
- Enter `startsys` to start the system.

6 Add an Office File for the switch.

7 Add an Office Domain File for the office if you are adding a *4ESS*, *5ESS*, or 7R/E switch.

8 Add a Trunk Group File for the office.

9 Enter `dbtest office <office_name>` to check the record base files for errors.

10 Enter `create office <office_name>` to update the offline database.

11 Enter `stopsys` to stop the system.

12 Enter `startsys` to start the system.

13 Enter `act <office_name>` to activate the office.

14 Enter `audit <office name> all`

END OF STEPS

References

Chapter 7, “Record Base Administration” in the *Record Base Administration Guide*

□

Removing the record base files (office)

Instructions

Follow these steps to remove the record base files for an office:

1 Remove all active controls from the office, including any manual HTR (Hard-To-Reach) codes.

2 Enter `purglog` to remove all matched entries from the database for all switches.

3 Enter `deact <office name> all` to deactivate the switch for data collection.

4 Remove the office from the RSPTE File.

Important! This step can only be done if all other references to this CLLI code are removed throughout the NTM record base.

5 Remove the Office File for the office.

6 Remove the Office Domain File for the office if you are removing a *4ESS*, *5ESS*, or 7R/E office.

7 Remove the Trunk Group File for the office.

8 Enter `dbtest all` to check the record base files for errors.

END OF STEPS

Updating the system after removing an office

Purpose

Once the office's record base files have been removed, you must update the current database.

Instructions

Follow these steps to update the system:

1. Enter `create all` to update the offline database for all record base file types.
2. Enter `stopsys` to stop the system.
3. Enter `installdb all now` to install reference data.
4. Enter `startsys` to start the system.

END OF STEPS

□

Migrating to TCP/IP connectivity

Overview

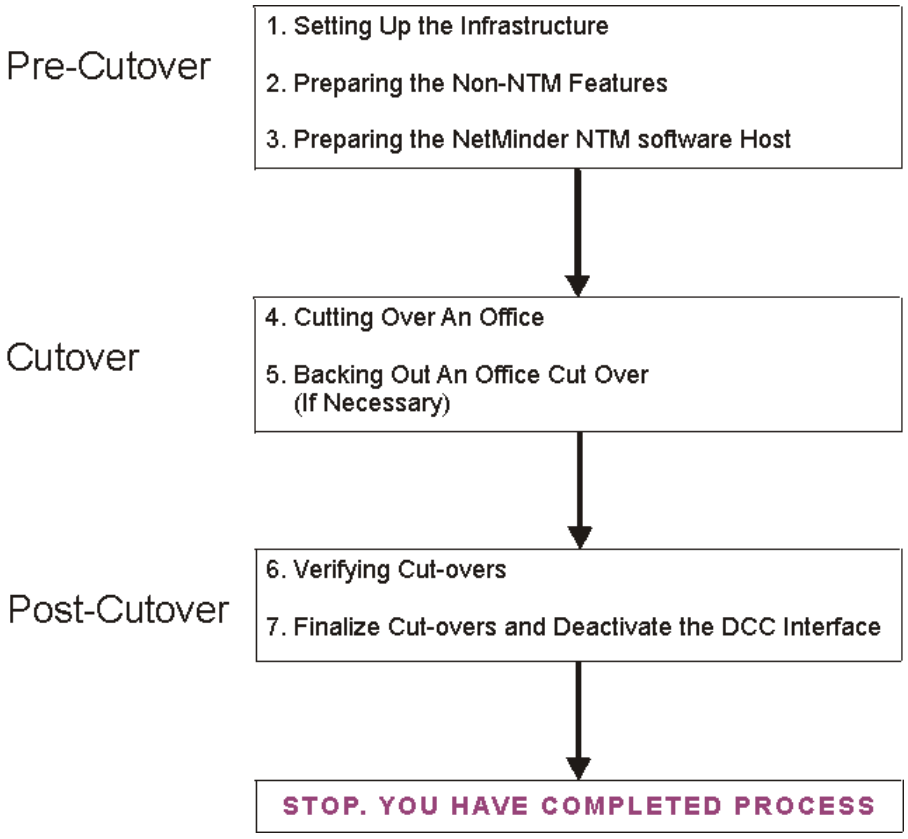
Purpose

This section describes the steps required to convert the NTM system to communicate with a *5ESS* or *DMS* office via TCP/IP.

Figure

Figure 3 provides a flowchart of the migration process.

Figure 3 Migration process



Contents

This section contains the following components:

Time recommendations	10-41
Setting up the infrastructure	10-42
Preparing the non-NTM features	10-43
Preparing the NTM host	10-45
Preparing the NTM host for migration to AI	10-48
Cutting over an office	10-50
Backing out an office cutover	10-53
Verifying cutovers	10-55
Finalize cutovers and deactivate the DCC interface	10-56

Time recommendations

Table

Table 2 lists estimated times to perform each procedure.

Table 2 Migrating to TCP/IP connectivity

Procedure	Approximate Time Required	Disrupt NTM Activities?
Setting up the infrastructure	1 hour	No
Preparing the non-NTM features	1 hour	No
Preparing the NTM host	1 hour	No
Preparing the NTM host for migration to AI	1 hour	No
Cutting over an office	3 hours	Yes
Backing out an office cutover	10–60 minutes	Yes
Verifying cutovers	15 minutes	No
Finalize cutovers and deactivate the DCC interface	10–30 minutes	No

Setting up the infrastructure

Instructions

Follow these steps to set up the infrastructure:

1 Update the "/etc/hosts" file on the NTM host with new IP addresses of the office, using the format:

`XXX.XXX.XXX.XXX` *`office_name`*

2 For *5ESS*, 7R/E, and *GTD-5* offices, update the Password File on the NTM host with an ID and password for each office.

3 Verify that "/etc/nsswitch.conf" file on the NTM host is defined properly. The "hosts" line should indicate that "files" are first as opposed to "dns".

4 Verify TCP/IP protocol and Ethernet stack compatibility between the NTM host and the offices.

Between each office and the NTM host, execute:

`ping`

END OF STEPS

Time synchronization

It is highly recommended that the network have a solution for time synchronization available, as the DCC/FEP will no longer be able to mask time differences between the switches and the NTM host. All switches have a lockout period during which no NTM requests will be received. Synchronization is required to ensure that the NTM requests occur on or after the five-minute boundary for data collection. NTM has some tolerance for time differences (3-10 seconds depending on switch type) and will repoll if blocked, but data may be marked late or suspect in those cases.

The HP's operating system (HP-UX) supports an ntp-based time synchronization package. It requires the IP address of the machine to be used as the master time source. If no time synchronization is established, it will be the Customer's responsibility to keep the switches in sync with the NTM host.

Reference: "Time synchronization — 4ESS" (p. 3) in the *System Administration Guide*

Checklist

The Office Administrators must prepare each office to support the new TCP/IP interface.

Network Element	Ensure that each network element …
5ESS	• is equipped with Administrative Services Module (ASM) • has the correct feature package (ASM feature 99-5E-7133) installed and configured The office administrator must supply: – IP address for ASM module – Username and password for NTM port (60005) (established on the ASM via the addnusr command) • has networking addresses in place • loaded with at least the 5e15 generic
DMS	• is equipped with the Supernode Data Manager (SDM) • has the correct feature packages installed and configured (including the SDM/SNM feature NMDC001) • has networking addresses in place • is loaded with at least the ucs13 generic.

Network Element	Ensure that each network element …
GTD-5	• is loaded with at least the gtd4003 generic.

The DCC Administrator must be prepared to remove entities to no longer have the data forwarded to NTM.

For the new TCP/IP interface via AI switch the Office Administrators must prepare the following tasks.

Network Element	Ensure that each network element …
5ESS	• is connected with properly configured AI Switch • has networking addresses in place • is loaded with at least the 5e4 generic
DMS	• is connected with properly configured AI Switch • has networking addresses in place • has loaded generic with at least the DMS24, UCS07 and NCS06 for DMS, DMS 250 and DMS 500 respectively.

Reference: Installing and Configuring AI Switch in the *Installation Guide*

References

Refer to the following documents regarding this feature on the *5ESS*/ASM.

- "*5ESS* Switch OneLink Manager Administrative Services Module User's Guide, ASM Release 6.0 or earlier", Document Number 235-200-145, Issue 3.00A, August 2002. Section 8.12 (starting on page 8-38)
- "7R/E *5ESS* Switch Local and Toll System Features, Feature Document, 5E13 and Later Software Releases", Document Number 235-190-115, Issue 10.00, November 2000. Section 12.4 (starting on page 12-13)

Supporting 1024 trunk groups involves adding hardware to the DMS and configuring it for the correct NTM ports (9553, 9554, 9555). Customers should review this "growth procedure" from Nortel before implementing that upgrade.

□

Preparing the NTM host

Instructions

Prepare the NTM host for the conversion by:

- Collecting information required from the office
- Networking Setup (define switches in "/etc/hosts", check "/etc/nsswitch.conf")
- Record Base Changes

1 Make sure that both the network element and the NTM host recognize each others IP addresses. For the NTM hosts, this can be done through the "/ets/hosts" file.

2 Edit the "/nm/ubin/start.all" file.

If this is a change from a data collector to TCP/IP and ALL offices are moved off the old DCOLs, please turn off the DCOLs for the data collector after moving the offices to the TCP/IP DCOLs.

Change "`off`" to "`respawn`" for the DCOL_<*`office type`*>

Default DCOL's are; 10 for *DMS* and 8 for *5ESS*

Example for a DMS:

```
DCOL10:0:0:respawn:export SRVID=30;DCOL_DMS -s
   DCAUDSVC10,DCADMSVC10,DCCTRLSVC10 -o /dev/null -e /dev/null
   -- -i 10
```

Example for a 5ESS:

```
DCOL8:0:0:respawn:export SRVID=28;DCOL_5E -s
   DCAUDSVC8,DCADMSVC8,DCCTRLSVC8 -o /dev/null -e /dev/null --
   -i
```

3 In case the cutover needs to be backed out, save a copy of the original files for the:

- Office File
- RSPTE File
- Password File (*5ESS,* 7R/E, *GTD-5*)

4 Update the office file for each office to be converted by replacing the "`;`" after `packets=all` with a "`,`" and inserting the following lines after the "`packets=all,`" line:

5ESS:

```
## Lucent Technologies 5ESS TECHNOLOGY
packets=all,
dialstring=TCP.<office_name>.60005,
cpnode=1;
```

DMS:

```
##  DMS SWITCH TECHNOLOGY
packets=all,
dialstring=TCP.<office_name>.9553,
dialstring2=TCP.<office_name>.9554,
dialstring3=TCP.<office_name>.9555,
authentication=Insecure,
max_maxcpt=20, max_tgxcpt=1024;
```

GTD5:

```
##  GTD5 SWITCH TECHNOLOGY
packets=all,
dialstring=TCP.<office_name>.10724,
max_maxcpt=65, max_tgxcpt=2000;
```

Some offices have only one dialstring that needs to be defined. By standard, that port number is 60005 for the *5ESS* and 10724 for the *GTD-5*. The *DMS* can have multiple dialstrings which can vary between *DMS* network elements.

The office name in all instances must be all lower case.

5ESS:

The cpnode number is also based on the office and assigned here. Unless there are multiple offices attached to the same ASM this should remain 1.

The <*office_name*> must match what is listed in the "/etc/hosts" file and what is used in the NTM system. It must also match what the ASM thinks the office is called.

5 In the "/musr/rb/tg" file add additional trunk groups to the trunk group file for any office utilizing enhanced trunk group monitoring.

This step is necessary only if you have purchased Surveillance of 1024 trunk groups.

6 In the "/musr/rb/rspte/rspte" file, add or modify a line for each office.

Ensure that the `direct=tcp` is at the end of the syntax as shown in these examples:

```
(5ESS) <office_name>,<hierarchy>,,<sets>,,
   ess5,5e15,1,y,tcp;
(DMS) <office_name>,<hierarchy>,,<sets>,,
   dms,na013,1,max_tg=1024 ,n,tcp;
(GTD5) <office_name>,<hierarchy>,,<sets>,,
   gtd5,gtd4003,1, ,n, tcp;
```

END OF STEPS

Preparing the NTM host for migration to AI

Instructions

Prepare the NTM host for the conversion by:

- Collecting information required from the office
- Networking Setup (define switches in “/etc/hosts”, check “/etc/nsswitch.conf”)
- Record Base Changes

1 Make sure that both the network element and the NTM host recognize each others IP addresses. For the NTM hosts, this can be done through the “/etc/hosts” file.

2 Edit the “/nm/ubin/start.all” file.

In the file “/nm/ubin/start.all” the new data collectors must be defined: DCOL# where # is between 11 and 26. In total up to 16 new DCOLs can be defined. The numbering of the following DCOLs must be preserved for each type of DCOL.

Example for DCOL numbering:

```
DCOL11 - DCOL_5E
DCOL12 - DCOL_5E
DCOL15 - DCOL_DMS
DCOL16 - DCOL_DMS
DCOL17 - DCOL_DMS
```

3 In case the cutover needs to be backed out, save a copy of the original files for the:

- Office File
- RSPTE File

4 Update the office file for each office to be converted by replacing the “;” after `packets=all` with a “,” and inserting the following lines after the “`packets=all,`” line:

5ESS:

```
## Lucent Technologies 5ESS TECHNOLOGY
packets=all,
dialstring=TCP.<office_name>.60005;
```

DMS:

```
##  DMS SWITCH TECHNOLOGY
packets=all,
dialstring=TCP.<office_name>.9553,
dialstring2=TCP.<office_name>.9554,
dialstring3=TCP.<office_name>.9555,
max_maxcpt=20, max_tgxcpt=1024;
```

The office name in all instances must be all lower case.

The <*office_name*> must match what is listed in the "/etc/hosts" file and what is used in the NTM system.

The port numbers (e.g. "60005') are dependent on AI Switch configuration.

5 In the "/musr/rb/tg" file add additional trunk groups to the trunk group file for any office utilizing enhanced trunk group monitoring.

This step is necessary only if you have purchased Surveillance of 1024 trunk groups.

6 In the "/musr/rb/rspte/rspte" file, add or modify a line for each office.

Ensure that the `direct=ai` is at the end of the syntax as shown in these examples:

```
(5ESS) <office_name>,<hierarchy>,,<sets>,,
   ess5,5e15,1,y,ai;
(DMS) <office_name>,<hierarchy>,,<sets>,,
   dms,na013,1,max_tg=1024 ,n,ai;
```

END OF STEPS

□

Cutting over an office

Purpose

Switches do not support multiple, simultaneous interfaces for Network Management data. For this reason, the DCC interface cannot be maintained while the TCP/IP interface is in place. Removal of the entity definition from the DCC is necessary for this process. Otherwise, NTM will continue to associate the office with the DCC and not recognize the TCP/IP interface.

The following table outlines how to cut over an office from DCC to TCP/IP connectivity.

Instructions

Follow these steps to cut over an office:

1 Verify that the system time on the NTM host matches the system time on the office. The DCC/FEP will no longer be available to handle time differences. Execute the following command on each machine at the same time.

```
$ date
```

2 Verify the system time of the office is in synchronization with the NTM host.

Responsibility: This should be performed by the office administrator.

3 Switch the interface to TCP/IP

Responsibility: This should be performed by the office administrator.

4 DCC deprovision the entity.

Responsibility: This should be performed by the DCC administrator.

5 If the cutover will occur during the `dayend` process, comment out the “dayend” entry in the root crontab on the NTM host.

6 Verify that the system time on the NTM host matches the system time on the office. The DCC will no longer be available to handle time differences. Execute the following on each machine at the same time.

```
$ date
```

7 Deactivate the office by executing:

```
$ deact <office name>
```

8 Copy the modified RSPTE File and Office File into the appropriate directories; "/musr/rb/rspte/" and "/musr/rb/office/" respectively.

9 Test the RSPTE File by executing:

```
$ dbtest rspte
```

10 Examine the ouput to detect errors. If there are syntax errors, correct and repeat this step. If there are errors you are unable to correct, STOP and call Alcatel-Lucent support.

11 Update record base changes by entering:

```
$ create rspte
```

12 Enter:

```
$ stopsys
```

13 Enter:

```
$ installdb rspte now
```

14 Test the Office File by executing:

```
$ dbtest <office name>
```

15 Enter:

```
$ create office <office name>
```

16 Enter:

```
$ startsys
```

17 Check the link status of the converted office to verify that it is defined as TCP/IP direct connect and not associated with the DCC

```
$ linkstat <office name>
```

18 Verify the dcol assignment for the office.

```
$ /nm/dbutil/openstat m <office name>
```

Values should be:

- *5ESS* = DCOL 8
- *DMS* = DCOL 10
- *GTD5* = DCOL 12

19 Activate the converted office by entering:

```
$ act <office name>
```

20 Enter:

```
$ audit <office name> all
```

21 If you commented out the “dayend” entry in the root crontab on the NTM host in Step 5, uncomment the entry.

END OF STEPS

Backing out an office cutover

CAUTION

This activity should only be used if the conversion encounters a major problem and the decision is made to revert to the DCC interface. It is not part of the normal conversion procedure.

Some procedures cannot be reversed without significant hardware and/or software changes. This includes migrating 4ESS offices to TCP/IP connect via the DT4180.

Instructions

Follow these steps to change the office connection back to the DCC configuration.

1 Create and activate the entity on the DCC.

Responsibility: This should be performed by the DCC administrator.

2 Switch the interface to support the EADAS channel (TDM) or GPU (*GTD5*).

Responsibility: This should be performed by the Office Administrator.

3 Deactivate the office.

```
$ deact <office name>
```

4 Copy over the old RSPTE File, Office File, and Password File (*5ESS*) record base files.

5 Test the RSPTE File by executing:

```
$ dbtest rspte
```

Examine the ouput to detect errors. If there are syntax errors, correct and repeat this step. If there are errors you are unable to correct, STOP and call Alcatel-Lucent support.

6 Update record base changes by:

```
$ create rspte
```

7 Enter:

```
$ stopsys
```

8 Enter:

```
$ installdb rspte now
```

9 Test the office file by executing:

```
$ dbtest <office name>
```

10 Enter:

```
$ create office <office name>
```

11 Enter:

```
$ startsys
```

12 Check the link status of the converted office to verify that it is associated with a data collector.

```
$ linkstat <office name>
```

13 Activate the reverted office by entering:

```
$ act <office name>
```

14 Audit the reverted office by entering:

```
$ audit <office name> all
```

END OF STEPS

Verifying cutovers

Instructions

Follow these steps to verify cut overs:

1 Run linkstat to verify active state and data collection status.

```
$ linkstat <office name>
```

Verify that the Connection Status for each office on all three channels (HI, MED, LOW) all say “conn” (connected).

2 Run audits.

```
$ audit <office name> all
```

Verify that each audit runs to completion without any connectivity errors.

3 View data collection status by executing:

```
$ datastat <office name>
```

Verify that all configured packets (may not be all the listed packets) have FLAGS set to “GOOD”.

4 Execute sample controls (specific allowable controls must be determined by the customer for this test.) Verify that each properly defined control request is transmitted successfully to the office.

```
$ <ctrl> <office name> <parameters>
$ audit <office name> <equivalent control audit type>
```

Verify that the audit confirms the state your control should have established.

END OF STEPS

□

Finalize cutovers and deactivate the DCC interface

WARNING

This procedure should only be done when all offices have been removed from all DCC's and the DCC's are being decommissioned.

Instructions

Follow these steps to finalize cutovers and deactivate the DCC interface:

1 Remove or comment out DCC entries in the RSPTE File.

2 Remove or archive DCC Office Files.

3 Remove unused DCCs from the "/musr/ofclst/" directory.

4 Modify "/nm/ubin/start.all", turn off DCC DCOLs. (Set "respawn" to "off")

```
DCOL2:0:0:respawn:export SALI_MODE=urp;export
   SRVID=22;DCOL_FEP -s
DCAUDSVC2,DCADMSVC2,DCCTRLSVC2 -o /dev/null -e /dev/null -- -i
   2
```

Let the `dayend` process implement these changes.

END OF STEPS

Secure shell for Succession switches

Overview

Purpose

Procedures in this section provide information on configuration and installation of Secure shell for Succession switches.

Prerequisite Features

Secure connection for Succession switches is available only if all these features are purchased and installed:

- Feature 422, "Enhanced Security for Nortel Networks TR-746 Interface",
- Feature 432, "Enhanced Security for Nortel Networks Using sftp",
- Feature 433, "Support of Nortel Networks Succession SN08 Interface from SDM/CBM".

NTM is collecting data for Succession switches over a secure interface using the OPENSSH software package.

Generics

Succession (sn08+).

Contents

This section contains the following components:

SDM configuration	10-58
Installing Secure connection	10-59

Instructions

Verify the following on your system:

- SSH is installed.
- SSHD is running.
- HOST Key is created.
- Any other vendor based configuration.
- A default user is configured in the "/musr/rb/password" file. (This will be used to make the secure connections to the SDM. We recommend this default user to be defined as "vital".)
- The user vital has a home directory defined.
- For an existing office, the Secure Port numbers are the same as the port numbers in the Record Base Office File.
- Make sure the nmadm's public key is copied to vital's .ssh directory on the SDM (Step 3 in Installing Secure connection).
- Verify vital's home directory has permission of 755.
- Verify "~vital/.ssh" directory has permission of 700.
- Verify the "~vital/.ssh/authorized_keys2" has permission of 644.

Important! If authorized_keys2 file already exists, append the public key to the file.

Installing Secure connection

Instructions

Follow these steps to install Secure connection on NTM:

1 Login as nmadm.

2 Create the public key file /musr/nmadm/.ssh/id_rsa.pub for user nmadm by executing:

```
/usr/bin/ssh-keygen -t rsa
```

3 Copy the nmadm's public key to vital's authorized_keys2 file under the ".ssh" directory on SDM

Important! The public key should be created on all NTM systems that connect to a secure Succession office. The public key should also be copied to all the secure Succession elements that have the security enabled. Keys from multiple NTM systems (BDR) should be appended to the authorized_keys2 file. (Chapter 12, "BDR Administration on a Host")

4 If the NE is a new office, perform the following steps to create a new office:

- Add the NE information to the "/etc/hosts file",
- Add the login information to the "/musr/rb/password",
- Create the entry in the RSPTE File,
- Create the Office File in the office directory,
- In the Office File, make sure the authentication flag is set to Secure (`authentication=Secure;`)
- Create and Install the RSPTE and OFFICE files.

5 If the NE is an existing office, perform the following steps:

- In the office file, modify the authentication flag to Secure (`authentication=Secure;`)
- Create the office.

6 Start the NTM system by executing `startsys`.

7 Verify the data collection has resumed and is stable on all Successions.

□

Troubleshooting network elements issues

Overview

Purpose

This section contains information about common network connectivity issues.

Contents

This section contains the following components:

Troubleshooting GSP network elements	10-62

GSP connection problem

If error messages persist for any or all GSP switches, stating "can't communicate with DCOL X". Deactivate any recently modified switches or switch known to have network connectivity issues. This should resolve the error message. If the message persists, please contact Alcatel-Lucent customer support.

11 Training Objectives and Exercises

Overview

Purpose

This Appendix contains objectives and exercises that accompany Alcatel-Lucent Learning course number OS3190.

Objectives

This course covers the topics needed to maintain the NTM record base and database. The record base files and audits are explained, along with the procedures for adding, deleting, and modifying record base information. This course is designed to enable the student to:

- Identify record base files related to reference data
- Perform database tests and creates
- Identify the location and format requirements of record base files

Course locations

Courses can be taught at your location. Call 1-614–860–5040 for suitcasing requirements. Enrollment: https://www.lucent-product-training.com/sabaweb, or 1-888-Lucent8 (888-582-3688), prompt 2, prompt 2

□

Chapter 1, “Introduction to the Record Base”

Objectives

This lesson is designed to teach you how to:

- Know where information is located in the *Record Base Administration Guide*
- Describe the responsibilities of Record Base Administrators
- Find record base file locations on the NTM host
- Interpret record base file descriptions

Exercises

1 In what directory are record base files located?

2 What are the two primary responsibilities of record base personnel?

3 Match the record base file format to the correct example:

1. Name-defined syntax

2. Position defined syntax

a) clmboh17ds0, 001020003004051, clbm17, oh5e,, ess5, 5e16, 1,y;

b)to=clmboh17ds0,tgn=172,tgsrv=fi,sets=ohfinal+clmbfin,thru=9,options=sched;

□

Chapter 3, “Record Base Concepts”

Objectives

This lesson is designed to teach you how to:

- Use record base files to control network views
- Enable trunk group exception thresholding
- Use domains to control various traffic types

Exercises

1 Which of the following statements are true?

a. Offices and trunk groups may be combined in the same set.

b. Offices are given set membership in the office files.

c. Trunk group set membership is specified in the trunk group threshold file.

2 How many trunk group threshold files may be present on one NTM system?

3 How many of these trunk group files may be in use at one time?

4 In which record base file are domain acronyms mapped to switch traffic domains?

□

Chapter 2, “Managing Record Base Partitions”

Objectives

This lesson is designed to teach you how to:

- Create and manage subnetworks and partitions

Exercises

1 Can a record base partition be created without creating a corresponding subnetwork?

2 Can a subnetwork be created without a corresponding partition?

3 In general, what is the path for a subnetwork’s record base files?

4 Which command is used to create subnetworks and partitions?

5 Which command would a user employ to determine permissions?

□

Chapter 5, “Record Base Files”

Objectives

This lesson is designed to teach you how to:

- Identify the record base files and describe their functions
- Identify the format requirements for each record base file
- Identify required and optional keywords for each record base file

Exercises

1 Use the `view`, `more`, or `browse` command to view your sets file. Select one trunk group set and one office set name. Then use the appropriate commands to determine how many trunk groups are assigned to your trunk group set at a particular office and how many offices are assigned to your office set (if there are many of either type, do not bother counting, just note `many`).

- Commands used:

- Trunk group set:

- Number assigned:

- Office set:

- Number assigned:

Important! If your sets file has not yet been customized to your location, there may be many set names that are not assigned to offices or trunk groups. To get results using your commands, you may need to check the RSPTE and a Trunk Group file actually being assigned.

2 View your RSPTE file. On a separate piece of paper, map out your RSPTE hierarchy as it is presently defined in the file for at least one vertical chain, showing at least two offices per level.

3 Is the present RSPTE hierarchy appropriate for your network management center needs? Note any thoughts you have on this below and we will discuss this as a group in class.

□

Chapter 7, "Record Base Administration"

Objectives

This lesson is designed to teach you how to:

- Maintain the NTM record base
- Identify the primary responsibilities of record base personnel
- Describe name-defined and position-defined formats for record entry
- Match symbols used for entering records in record base files with their functions

Important! Information on record base file formats and symbols is found in "Record base file format" (p. 2) and "Record base file symbols" (p. 3).

Exercises

1 In what directory will you find the record base files?

2 `True or False:` The record entry below is in name-defined format.

```
clmbohtst5e,000031040000000,clmb5e,intl,,ess5,5e15,1;
```

3 The record entry below has how many omitted keywords?

```
test5e15,000031010000000,test2,,,ess5,5e15,1;
```

4 `True or False:` The record entry below is in position-defined format.

```
to=AH_1B-i4do,tgn=150,tgsrv=hu,n2w=270,options=sched;
```

5 In the blank space before each symbol on the left, write the letter of the statement on the right that describes the function of the symbol.

_____ 1.	;	A. Separates fields in record.
_____ 2.	+	B. Ends record entry.
_____ 3.	=	C. Separates parameters
_____ 4.	#	D. Separates multiple values.
_____ 5.	,	E. Indicates comment.

6 Match the command with its function.

Command	Function
create	Checks record base files for errors.
dbtest	Installs changes to the current database
installdb	Produces a binary version of the record base

□

Chapter 8, "Record Base Update Procedures"

Objectives

This lesson is designed to teach you how to:

- Use the `dbtest`, `create`, `installdb` and `recreate` commands.
- Database testing (`dbtest`).
- Full create and install (`create` and `installdb`).
- Single office create (`create`).
- Single file create and install (`create` and `installdb`).
- Single threshold file `create` and install (`thresh`).
- Use of the `recreate` command.

Exercise 1

1 What is the function of the dbtest command?

2 I just added a new entry to RSPTE. Should I run single file create or single office create?

3 I just added new trunk groups to clmboh150ds0. Should I run single file create or single office create?

4 Can I run recreate from the command line, or only as part of the dayend process?

5 `True or False:` The command `dbtest files=all` tests all applicable record base files.

6 `True or False:` To perform the command `installdb files=thresh when=now`, you must first stop the exception system.

7 List three office files updated in the current database when you type the `create files=office` command:

8 Which command must you run ***before*** performing the single office create procedure?

9 Which two commands should you run ***after*** performing the single office create procedure?

10 `True or False:` The `thresh` command can be used to create a threshold file that does not currently exist in the "/musr/rb/thresh" directory.

11 `True or False:` The `thresh` command does not change the number of the "thresh" file currently being used by the exception system.

Exercise 2

For this exercise, the class will be divided into teams to run dbtest against trunk group files and correct any errors found. The instructor will give each team the name of a file to test. Your instructor has already made backup copies of the files, so do not worry (too much) about destroying your file. Once you have your assignment, follow the steps below:

1 Change directions (cd) to the directory that contains the file in your assignment.

2 Run the `dbtest` command on the file. Save the output by redirecting it to a temporary file (for example, "group1.save").

3 View your temporary file. Write down the first error on the list.

4 Correct the error above in your record base file. Run `dbtest` on the file again, saving the output. Was the error corrected?

5 Were any other errors corrected when you corrected the first error?

6 Continue correcting errors in the same way until `dbtest` reports no more errors.

□

Chapter 9, "Maintaining the Record Base with BDR"

Objectives

This lesson is designed to teach you how to:

- Configure the record base for BDR
- Perform record base tasks related to BDR

- Differentiate record base file types for BDR

Exercises

1 To enable BDR, what two types of partitions are created on each host?

2 Consider the following entries from an INMS file ("/musr/rb/inms/inms"):

```
partition=nma primary=hosta secondary=hostc;
partition=nmb primary=hostb secondary=hosta;
partition=nmc primary=hostc secondary=hostb;
```

For each host, list the backup machine.

- Host A
- Host B
- Host C

3 Match the term in List A with the definition in List B:

List A	List B
Global files	Not shared between hosts.
Independent files	Available on all hosts; are merged when dbtest and create commands run.
Shared files	Maintained separately on each host.

□

Chapter 10, "Adding and Removing Network Elements"

Objectives

This lesson is designed to teach you how to:

- Add various types of switches to NTM
- Remove various types of switches from NTM
- Add and remove a DCC

Exercises

1 From the list below, put the record base file and the actions to be performed in the correct order.

Order to be Performed	Record Base File/Action
	Run DBTEST
	Add an Office file for the new network element
	Run CREATE ALL
	Add a Trunk Group file for the new network element.
	Add the new network element to the RSPTE file
	Run INSTALLDB
	Run audits
	Run STOPSYS
	Activate the new network element for data collection
	Run STARTSYS

2 In the list above, what step(s) may be omitted when adding a DCC?

□

Glossary

%%OCC Percent Occupancy

The fraction of time that a circuit or a piece of equipment is in use, expressed as a decimal. Numerically, it is the Erlangs carried, and it equals the carried CCS divided by 36. Percent occupancy measurements include both message time and setup time.

%OFL Percent Overflow

The relationship between the total attempts offered in a specific time period to a route or a destination and the number of attempts not finding an idle circuit.

AAB A-B trunk group

A trunk group that connects an originating office (A) directly to a terminating office (B). See "AV" (p. 3) and "VB" (p. 25).

ACC Automatic Congestion Control

Senses machine congestion and activates preplanned internal and external overload controls. Also called/see also DOC. See the acc command (4-9) in the *Input Commands Guide*.

ACG

Automatic Call Gap

ACH Attempts per Circuit per Hour

Relationship between the number of attempts that result in an answer signal and the total number of attempts.

ACM Address Complete Message

A messages sent in the backward direction indicating that all the address signals required for routing the call to the called party have been received.

Activate
To make an office active for data collection.

ADL-V
AT&T Digital Link — Phase 5

Aggregated Trunk Group
An aggregated trunk group is not a physical trunk group but rather a collection of all traffic information on trunk groups to a particular "to office", represented with a unique trunk group ID. In this way, controls can be sent to a 7R/E switch for a given "to office" by specifying the tg ID of the aggregated trunk group.

Aggregation Limit
Date and time limit you can set on the aggregation view to limit the number of records that will appear in your report.

AIC Available Idle Circuits
A traffic measurement used by network managers to determine which trunk groups have capacity available for rerouting traffic from an overloaded trunk group.

AIN Advanced Intelligent Network Also called an Intelligent Network) A network:

- That affects the routing of calls within it from moment to moment based on a criteria other than simply finding a path through the network for the call
- Where the originator or the ultimate receiver of the call can inject intelligence into the network and affect the flow of his call (either outbound or inbound).

Intelligent networks generally include SCP, SSP, and STP components.

Alarm
Visible report of a trouble condition in the network. Alarms usually require immediate attention from network personnel.

Alert
Visible report of a potential trouble condition in the network.

Alerting Discrete
An on/off indicator that notifies network managers of changes to the status of the office. An alerting discrete provides a message to NTM that starts a corresponding audit (unless that audit has been previously inhibited by the network manager).

Allow
Indicates the permitting of an action, such as permitting automatically triggered audits to run.

Alternate Routed Traffic
Traffic that has been offered to a previous trunk group and has not been able to find an idle circuit. The switching system handling the traffic then offers it to an "Alternate Route," based on its internal routing tables.

Alternate Routing
A means of selectively distributing traffic over a number of routes, ultimately leading to the same destination.

APC
Adjacent Point Code

APR Allow Previously Rerouted
A trunk group reroute control option that allows previously rerouted traffic to reroute. Only *4ESS* and *5ESS* offices support this reroute control option.

APS
Attached Processor System

ASCII American Standard Code for Information Interchange
A 7-bit code for providing as many as 128 different characters. An eighth bit can be added as a parity check for error detection purposes.

ASP
Advanced Services Platform

ATM Asynchronous Transfer Mode
A high bandwidth, low-delay, connection-oriented, packet-like switching and multiplexing technique that allows very high speed transmission.

Attempt
An attempt to seize a circuit in a route. An attempt may be successful or unsuccessful.

Audit
An integrity check through which NTM corrects differences between its own database and office databases.

AV
A-V (via) trunk groups. A trunk group that connects an originating office (A) to a via office (V). See "AB" (p. 1) and "VB" (p. 25).

BBacking Up

The process of copying data onto a separate medium for the purpose of data retention.

BDR Backup and Disaster Recovery

See Feature 8, “Disaster Recovery (Duplex)”and Feature 40, “Enhanced Disaster Recovery” in the *System Overview*.

Blocking

The inability of the calling party to be connected to the called party because either all suitable trunk paths are busy or a path between a given inlet and any suitable free outlet of the switching network is unavailable.

Broadcast Message

A text message sent out by personnel using the NTM to other users on the system.

CCalculation

Calculated counts used to signify changing network conditions and, when thresholded, to alert network managers to events that might require action to prevent excessive network congestion.

CAMA Centralized Automatic Message Accounting

Specific version of AMA in which the ticketing of toll calls is done automatically at a central location for several central offices.

CANF Cancel From

A post-hunt protective trunk group control that prevents a percentage of overflow traffic for a selected originating trunk group from advancing to any alternate route. See the canf/cant/skip command (4-13) in the *Input Commands Guide*.

CANT Cancel To

A pre-hunt protective trunk group control that prevents a percentage of traffic from accessing a selected destination trunk group. See the canf/cant/skip command (4-13) in the *Input Commands Guide*.

CCIS Common Channel Interoffice Signaling

Carries telephone signaling information along a path different from the path used to carry voice.

CCITT

Consultative Committee on International Telegraphy and Telephony

CCS Centi (Hundred) Call Seconds
A unit of traffic used to express the average number of calls or the average number of devices in use. One CCS is equal to the continuous load for 100 seconds. The CCS for an hour is 36.

CCS Common Channel Signaling
A form of signaling in which a group of circuits share a signaling channel.

CCS7-NA
North American Version of CCITT#7

CG Call Gap
A protective control that allows a fixed number of calls to succeed to a code (telephone number) in a 5-minute interval. See the cg command (4-21) in the *Input Commands Guide*.

CGX
Call Gaps with an IC prefix (*1AESS* only)

CICR Cancel In-Chain Return
A reroute trunk group control option. When set to YES, does not allow traffic to return to in-chain routing. When set to NO, allows traffic to return to in-chain routing.

CLI
Caller Line Identification

Client
A client uses the resources of another device (computer) or application. Client is another term for a PC on a local area network.

CLLI
Common Language Location Identifier

CNI
Common Network Interface

Code
A numbering system for telephone addresses, for example, 614-555-1234 (NPA-NXX-XXX).

Connection
An attempt for a circuit that succeeds in obtaining a circuit. Also called a seizure.

Container Page
One of the five basic types of pages used in the GUI. It displays the results of a search or a map of a network area.

Control Data
Data that describes the actual controls in place for the network.

CPE
Customer Premises Equipment

CPU
Central Processing Unit

CR
Critical Alarm

CR Circuit Reservation
An automatic trunk group control that reserves the last few trunks of a trunk group for critical users exclusively and eliminates the need to queue critical users for inter-switch trunks. See also/also called STR. See the cr command (4-32) in the *Input Commands Guide*.

Crash Dump
The output from the hardware registers, the hardware stack, and the CPU.

CRO Cancel Rerouted Overflow
A reroute trunk group control option that prevents overflow traffic on a via route (VB) from overflowing back to the direct route (AV). Not activating the CRO can result in an external loop.

CSL
Communications Software Launcher

Customer Premises Equipment
All telecommunications terminal equipment located on the customer premises.

DDatabase
A collection of data organized for rapid search and retrieval by a computer.

DCC
Data Collection Concentrator

DCE
Distributed Computing Environment

DCS
Display Construction Set

Deactivate
To make an office inactive for data collection.

Demand Data

Data retrieved by the demand command (5-20) from the system database. The User Report Writer feature and SQL files use this data to create informational reports.

Destination

A specified area or country in which the called subscriber is located. A destination is identified by its destination code (the digits used for routing the call).

Detail Page

One of the five basic types of pages used in the GUI. It provides information (such as reference data) on specific network elements or network connections.

Direct Routed Traffic

Traffic that is being offered to the trunk group for the first time, not having been previously offered to a different trunk group. This traffic, which has not alternate routed, is sometimes called “First Routed” traffic.

Discrete

An on/off indicator that notifies network managers that:

- Changes have been made to the status of the office
- Significant events have taken place within the office

NTM polls the offices for discretes at regular intervals.

Disk Array

A disk subsystem combined with management software that controls the operation of the physical disks and presents them as one or more virtual disks to the host computer.

DOC Dynamic Overload Control

Also called/see also ACC

Domain

A type of calling service, such as POTS (Plain Old Telephone Service), ACNT (*Accunet*), SDN (Software Defined Network), or ISDN (Integrated Services Digital Network).

Dot Profile (.profile)

A file located in your home directory that alters your default *Linux* system environment. You can use your .profile to define environmental variables such as your terminal type, prompt string, or mailbox address.

DP

Dial Pulse

DPT

Dynamic Packet Trunks

DPTPRI
Dynamic Packet Trunks Prioritization

DPTRES
Dynamic Packet Trunks Reservation

DPTTID
Dynamic Packet Trunks Terminal Identifier

DSC
Dynamic Service Control

DSDC Direct Services Dialing Capability
Network services provided by local switches interacting with remote databases via CCIS.

DTMF
Dial Tone Multifrequency

DTS
Dial Tone Speed

EEA Equal Access
A trunk group reroute option for switches that limits the reroute to equal access traffic.

EADAS Engineering and Administration Data Acquisition System
A system in which traffic data are measured at switching systems by electronic devices, transmitted to a centrally located minicomputer, and recorded on magnetic tape in a format that is suitable for computer processing and analysis. Performs data collection in NTM for certain switch types.

Erlang
A measurement of traffic load equal to the continuous occupancy of one circuit (or unit of equipment) for one hour. An Erlang can express the capacity of a system; for example, a trunk group of 30 trunks, which in a theoretical peak sense might carry 30 Erlangs of traffic, would have a typical capacity of perhaps 25 Erlangs averaged over an hour.

Error Code
An identification field used to identify the module or feature reporting the error. See the **ERR_CODE** field help file.

Error Log
The error log is a file that contains the error messages being generated by NTM. See the errlog command (9-7) in the *Input Commands Guide*.

Error Messages
System responses resulting from software-detected errors, changes in the system status, or non-executable commands.

Error Number
Number associated with error codes that help identify specific messages. See the **ERR_NUM** field help file.

ESP
Essential Service Protection Triggered

ESS
Electronic Switching System

ETR Easy To Reach
A code (telephone number) is determined to be easy to reach because the attempts and failures to the code do not exceed user-defined thresholds.

Exception
A calculation based on office or trunk group data that exceeds a user-defined threshold. It indicates an abnormal working condition in the network.

Exception Level
A number associated with an exception, indicating the severity or priority of the exception. High-numbered exception levels are more severe.

Exception Processing
Process used to collect raw data from the switch, perform calculations on the data, and, as a result, find exceptions based on predefined thresholds.

Exception Report
Formatted report of all exceptions that have occurred during the most recent 5-minute period.

Execution Error
The NTM GUI presents error messages in response to conditions such as improper permission, execution errors, etc. Execution errors are related to the execution of requests that affect the network elements to which the NTM host is connected (e.g., control requests or HTR administration).

External Network Element
A network element that is defined in the NTM Record Base but for which surveillance data is not received by NTM.

FFEP Front-End Processor

An application that acts as a DCC. Available with purchase of Feature 214, "FEP Release 4" or Feature 257, "FEP Release 5".

FHC

Final Handling Code

Final Trunk Groups

A trunk group that acts as a final route for traffic. Traffic can overflow to a final group from high-usage groups that are busy. Traffic cannot overflow from a final trunk group. Calls that overflow a Final Trunk Group are terminated unless they are rerouted by an NTM Reroute control. See the rr command (4-44) in the *Input Commands Guide*.

FML Field Manipulation Language

A set of C-language functions for defining and manipulating data storage structures called fielded buffers.

FOO

A foo is a term universally substituted for something real when discussing ideas or presenting examples.

From Office

Internal network element that originates the trunk group.

FSD

Feature Specification Document

Full Create

The process of constructing the database itself (once the database files have been prepared) or making major database modifications through the use of the `create` command with no arguments. This process also modifies the offline database.

Full Trunk Group

A trunk group that does not overflow calls to another trunk group because enough trunks are provided to give an acceptable blocking probability.

GGeneric

The version released to provide specific services, features, or functions.

GETS

Government Emergency Telecommunications Service

GSC
Group Signaling Congestion

GSM
Global Switching Module

GUI Form Elements
The elements that appear within a form on a web page. Form elements may consist of a label and one or more fields when they are used outside a table. See "GUI form elements" (p. 20) in the *User Guide*.

Hhecto
A unit of measure meaning 10 to the power of 2.

High-Usage Trunk Group (HU)
A trunk group that is the primary direct route between two switching systems. The group is designed for high average occupancy. To provide an overall acceptable probability of blocking, an alternate route must be provided for overflow traffic.

Host Computer
Computer (machine) used to run the NTM.

HPC High Probability of Completion
A phase of GETS that extends the enhanced routing and priority service to LEC networks traversed by the call.

HT Holding Time
The average duration of phone calls.

HTR Hard-To-Reach
A code (telephone number) is designated as hard-to-reach because the number of attempts and failures to the code exceed user-defined thresholds. See Chapter 7, "Hard-To-Reach (HTR)" in the *System Overview*.

HU High Usage
A trunk group that is the primary direct route between two switching systems. The group is designed for high average occupancy. For an overall acceptable probability of blocking, an alternate route must be provided for overflow traffic.

Hunt Types
The three hunt types for reroutes are ***regular***, ***order***, and ***spray***.

- The regular hunt uses only one out-of-chain engineering route for the reroute. Order and spray hunts can have from two to seven out-of-chain engineering reroutes.

- For the order hunt, an ordinary route-advance pattern is specified for the out-of-chain engineering reroutes, and the same route is always used as the starting point for the trunk hunt.
- For the spray hunt, rerouted traffic is divided evenly among the out-of-chain engineering routes through a rotation scheme.

See the HUNT field help file.

Hysteresis
The minimum amount of change required to make a difference.

ICCH Incoming Connections per Circuit per Hour
The incoming peg count divided by the number of equivalent 2-way circuits.

IEC
InterExchange Carrier

IMA
Ineffective Machine Attempts

Immediate Reroute
A reroute that diverts calls to one or more specified via trunk groups prior to the hunting of the "reroute from" trunk group.

IMS
IP (Internet Protocol) Multimedia Subsystem

INA
Ineffective Network Attempts

Incoming Calls
Incoming trunk seizures at the office.

Inhibit
Indicates the blocking of an action, such as blocking automatically triggered audits from running.

Input Command
User-invoked instructions to a system, entered in the command shell. Also called an input message and command. See the *Input Commands Guide*.

Internal Calls
Originating calls intended to complete on lines served by the switch.

Internal Error Message
An error message reported in the error log and on the system console.

Internal Network Element
Network elements from which surveillance data is collected.

INWATS Inward Wide Area Telephone Service
A service that allows subscribers to receive calls from specified areas with no charge to the person who's calling.

IP
In Progress

IRR Immediate Reroute
A pre-hunt trunk group control option that causes a percentage of a specified type of traffic to be rerouted before it is offered to the regular in-chain trunk group.

ISA
Integrated Service Assurance

ISDN Integrated Service Digital Network
A set of standards for digital transmission over ordinary telephone copper wire as well as over other media. ISDN integrates analog or voice data together with digital data over the same network.

Issue
Office generic issue number.

ISUP Integrated Service Digital Network User Part
Defines the protocol and procedures used to set up, manage, and release trunk circuits that carry voice and data calls over the public switched telephone network (PSTN). ISUP is used for both ISDN and non-ISDN calls. Calls that originate and terminate at the same switch do not use ISUP signaling.

IWBM
Inter-working Bridge Measurements.

LLATA
Local Access and Transport Area

Launch page
One of the five basic types of pages used in the GUI. It is used to select high-level data types to monitor.

LEC
Local Exchange Carrier

Link Status
The signaling system connection status of an office.

LNP
Local Number Portability

Logical Database
A logical database consists of a computer program system database and a *Linux* operating system file area.

LRN
Location Routing Number

LSSGR
LATA Switching System Generic Requirements

MMB Maintenance Busy
Conditioning a circuit, a terminal, or a termination to be unavailable for service. When unavailable, it is generally necessary that it appear busy to circuits that seek to connect to it. Sometimes referred to as “make busy”. See the MB field help file.

MC
Machine Congestion Level

Menu Mouse Button
Mouse button used to display context-sensitive menus. (Usually the right mouse button.) Click the menu mouse button once to display the menu, then use the Select Mouse Button to select an item (or subitem) from the menu.

MF
Multifrequency

Mnemonic
Executable name used to access menus, menu items, and pages on the terminal screen. A mnemonic is a word or string that is intended to be easier to remember than the thing it stands for.

Monitoring
Comparing the traffic on selected trunk groups with assigned thresholds.

MSU
Message Signaling Unit

MTP Message Transfer Part
The part of the SS7 protocol that provides for basic routing of signaling messages between signaling points.

NNC
No Circuits

NCP Network Control Point
A routing, billing, and call control database system.

NEA Non-Equal Access
A trunk group reroute control option for switches that limits the reroute to non-equal access traffic.

Network Traffic Management
A system that provides near-real time surveillance of the network elements connected to it for the purpose of managing network congestion.

Network Data
Traffic data that is collected from the network elements on a periodic basis, typically 5 or 15 minutes.

Network Management
A set of procedures, equipment, and operations designed to keep a traffic network (a telephone network, for example) operating near maximum efficiency when unusual loads or equipment failures would otherwise force the network into a congested, inefficient state.

Network Management Data
A combination of data collected from the switches and data entered in the record base. This data describes the base of the network and what occurs in the network.

NFS Network File System
A distributed-file-system protocol that allows a computer on a network to use the files and peripherals of another networked computer as if they were local.

NHR Not Hard-to-Reach
A code (telephone number) determined to be not hard-to-reach because the attempts and failures to the code do not exceed user-defined thresholds.

NMC Network Management Center
A centralized location at the network management layer used to consolidate input from various network elements to monitor, control, and manage the state of a network in a telecommunications organization.

NOCS Network Operation Center
A group responsible for the day-to-day care of a network.

NPA Numbering Plan Area
A geographic division within which telephone directory numbers are subgrouped. A 3-digit NXX (local office) code is assigned to each NPA, where:

- N=any digit 2 through 9
- X = any digit 0 through 9

NPR
NTM Performance Reporting

NS
Number Service

NTM
Network Traffic Management

NTM **Host**
The server on which the NTM is run.

OOCC Occupancy
The time a circuit or switch is in use.

OCCH Outgoing Connections per Circuit per Hour
The outgoing peg count divided by the number of equivalent 2-way circuits.

Office
A local switch, DCC, or FEP connected to your host computer.

OFL Overflow
Number of attempts failing to find an idle circuit in a group of circuits.

One-Way Trunk
A trunk that can be seized at only one end.

Ongoing Data
Data retrieved by the `ongoing` command from the system's shared memory.

Originating Calls
Line seizures at the office.

ORR Overflow Reroute
A reroute post-hunt trunk group control option that takes the overflow traffic on a trunk group and reroutes it to a trunk group with idle capacity.

Outgoing Calls
Calls intended to complete on trunks to points outside the system (same as outgoing seizures).

Overflow Peg Count
Peg count overflowing to another trunk group or to a circuit busy signal.

OVLD Overload
An increase in offered load beyond the capacity for which the network components (for example, trunks and switching systems) are engineered.

PPage
A page is a universal resource locator (URL), part of the NTM application. A page is displayed inside a Window. The user selects, changes and transfers pages within the same window.

Parameter area
The area of a control request display that contains various control parameters.

Parameter Set
A predefined group of control parameter values that may be used to quickly apply a control to one or more switches.

PAS
Public Announcement Service

PATR Performance and Troubleshooting Reports
This feature enables NTM personnel to collect various office and application performance data, and to output reports on request. Depending on the report type selected, the data may be real-time or hourly. The hourly data may be for a 24-hour period or less. Seven days of data are collected and stored for report access.

PC Peg Count
A count of all calls offered to a subgroup during a measurement interval.

PCI
Panel Call Indicator

PIIT Prohibit International Inbound Traffic
A reroute trunk group control option. When set to YES, does not allow inbound international traffic to be rerouted. When set to NO, allows inbound international traffic to be rerouted. See the rr command (4-44) in the *Input Commands Guide*.

Post-Hunt Control
A trunk group control that may affect a call that is attempting to alternate route to the next designated trunk group, for example: CANF.

PP
Preprogram

PPC
Peripheral Processor Complex

Pre-Hunt Control
A trunk group control that may affect a call before it is offered to a particular trunk group, for example: CANT, SKIP.

Preplan
Command used to create and manage pre-designated control plans to be used in emergency situations. See the preplan command (4-72) in the *Input Commands Guide*.

PS/UT
Pseudo-Subunit / Unit Type

PTS
Public Telecommunications Systems

QQOR
Query on Release

RRADR
Receiver Attachment Delay Readiness

RC
Routing Code

RDB
Routing Data Block

Real Time Usage
The percentage of time used out of total available real time, not including multi-task time.

Record Base
A collection of ASCII files containing reference information about the network to be managed by NTM.

Record Base Administration
The process of creating and maintaining the reference data portion of the NTM database.

Reference Data
Data that describes what the network is managing. This consists of either data about the network management center itself (such as the configuration of the center and threshold tables) or data about the network being monitored (such as the switching systems and trunk groups in the network management center's cluster). User-defined reference data is stored in the “/musr/rb” directory. Some reference data is supplied to the database by audits. This data typically changes infrequently.

Regular Expressions
A way of searching for patterns of characters in text strings. In NTM, it applies to Network Element search fields used to find particular switches or trunk groups.

Reorder Tone
A tone that is applied 120 times per minute to indicate all switching paths busy, all toll trunks busy, equipment blockages, unassigned code dialed, or incomplete registration of digits at a tandem or a toll office. Also called **Channel Busy** or **Fast Busy Tone**.

Request Page
One of the five basic types of pages used in the GUI. It is used to display control parameters before a control is applied.

Reroute
See “RR” (p. 20).

Reservation Level
The Circuit Reservation (CR) control allows the user to specify a maximum number of idle circuits to reserve and what the switch is to do with direct and/or alternate routed traffic when the reservation level is reached.

RLU
Remote Line Unit

ROA
Re-Order Announcement

Route
One or more trunk groups providing a connection between offices.

Route Group
A route group consists of one or more routes that may be used for a given destination. A route group may be accessed by more than one combination of destination and additional parameters.

RP Revertive Pulse
Revertive Pulsing is a method of signaling between switching systems in which information is conveyed from System A to System B. System B sends a sequence of pulses to System A, where the pulses are counted. System A signals System B when the correct number of pulses has been received.

RR ReRoute
An expansive trunk group control that is used to take traffic from congested or failed routes to other trunk groups not normally included in the route advance chain. These other trunk groups, called "vias," should have available idle circuits (AIC) to be used for the reroute. See the rr command (4-44) in the *Input Commands Guide*.

RSPTE Regional, Sectional, Primary, Toll, and End office
See the "RSPTE File" (p. 67) in the *Record Base Administration Guide*.

RSU
Remote Switching Unit

SSCCP Signaling Connection Control Part
A signaling protocol that provides additional routing and management functions for transfer of messages other than call setup between signaling points.

SCP Service Control Point
A remote database within the SS7 network that supplies the translation and routing data needed to deliver advanced network services. Also called Signal Control Point.

SDM
Supernode Data Manager

SDN Software Defined Network
A service developed for multi-location businesses that allows network managers to tailor their network to their own specific communications needs.

SDOC
Selective Dynamic Congestion Control/Automatic Congestion Control

Search Page
One of the five basic types of pages used in the GUI. It is used to request data on network elements, network connections, and controls. It can be used in simple or advanced modes.

Seizure
An attempt for a circuit in a trunk group that succeeds in obtaining a circuit.

Select Mouse Button
Mouse button used to specify an object to operate on and to manipulate objects and controls. (Usually the left mouse button.)

Set
Logical grouping of network elements (offices or trunk groups). NTM with standard features allows each office to be a member of up to four office sets, and each trunk group to be a member of up to four trunk group sets.

Shared Memory
A RAM-based data structure on the host that is used to store discrete, control, and exception data. Portion of memory accessible to multiple processes.

Signaling
The transmission of address (pulsing), supervision, or other switching information (including any information required for billing) between stations and switching systems, and between switching systems.

SILC Selective Incoming Load Control
An automatic trunk group control that can be enabled or disabled on a selected trunk group in a "From Office" when the office encounters machine congestion. See the silc command (4-55) in the *Input Commands Guide*.

Single File Create
The process for creating (compiling) individual record base files.

Single Office Create
The process for creating (compiling) all office-related files for one office only. A single office `create` acts directly on the current database; no `installdb` command is necessary to install the changes to the database. See the *Record Base Administration Guide*.

SKIP Skip route control
A pre-hunt trunk group control that allows all or a percentage of traffic to bypass a specific route and to advance to the next route in its normal routing pattern. See the canf/cant/skip command (4-13) in the *Input Commands Guide*.

SMS Service Management System
Allows provision and updating of information on subscribers and services in near-real time for billing and administrative purposes.

SQL Structured Query Language
Database language used for creating, maintaining, and viewing database data. See Chapter 3, "SQL Interpreter" in the *Data Tables Guide*.

SQL File

A data request file that lets you specify what data should be retrieved from the database or the ongoing shared memory and to define the format of the data.

SS7 Signaling System 7

Signaling protocol that uses destination routing, octet-oriented fields, variable length messages and a maximum message length allowing for 256 bytes of data. The four basic sub-protocols of SS7 are: MTP, SCCP, ISUP, and TCAP.

SSP Service Switching Point

A switch that can recognize IN (Intelligent Network) calls and route and connect them under the direction of an SCP. Also called **Signal Switching Point**.

STP Signal Transfer Point

A message switching system that permits signaling messages to be sent from one switching system to another by way of one or more other offices at which STPs are located. It reduces the number of data links required to serve a network.

STR Selective Trunk Reservation

An automatic trunk group control that reserves the last few trunks of a trunk group for critical users exclusively and eliminates the need to queue critical users for inter-switch trunks. Also called CR/TSR. See the cr command (4-32) in the *Input Commands Guide*.

Subnetwork

A subdivision of the network that allows parts of the network to be monitored and controlled independently of the main network.

Suffix

A user-defined string (up to 5 characters long) used to identify a particular office or trunk group. The suffix is separated from the office or trunk-group name by a hyphen.

Surveillance Data

Discrete and measurement data collected periodically from the switch.

SVC Switched Virtual Circuit

A virtual circuit connection established across a network on an as-needed basis and lasting only for the duration of the transfer.

Switch

A computer system that channels telephone calls from one place to another and keeps track of each call that it transfers.

Switch Name

A code name that identifies an office.

Syntax
The format in which a command is entered, including the input command name, parameters, and action options.

System Error
The NTM GUI presents error messages in response to conditions such as improper permission, execution errors, etc. A system error is presented when an error occurs on the NTM host during the generation of a web page or during the processing of a request from a web page (except certain control related requests).

TTandem Office
In general, an intermediate switching system for interconnecting local and toll offices. All toll offices are tandem offices. A more specific meaning of local tandem or metropolitan tandem office is an office that connects end offices to other end offices or to other tandem offices within a metropolitan area.

TCAP Transaction Capabilities Application Part
A signaling protocol that provides for transfer of non-circuit related information between signaling points.

TCU
Time Switch and Peripheral Control Unit

TDM
Time Division Multiplexing

Terminating Calls
Calls intended to complete on lines served by the system.

TFP
Transfer Prohibit

TG Trunk Group
A group of trunks with similar electrical characteristics that go between two geographical points. A trunk group performs the same function as a single trunk, except that on a trunk group multiple conversations can be carried. Trunk groups are used as traffic demands them.

Threshold
A preset limit of exceptions that each network element must exceed during each 5-minute period before NTM determines that the office is experiencing patternable trouble.

Thresholding
The process of setting values to be compared against data values (raw counts) collected from the switches every 5 minutes to determine exception conditions.

TID
Terminal Identifier

To Office
Internal or external network element that is the termination of a trunk group.

TPC
Telephony Processor Complex

Traffic Network
An arrangement of channels, such as loops and trunks, associated switching arrangements, and station equipment designed to handle a specific body of traffic; a subset of the facility network.

Trunk
A telephone communication path or channel between two points, one of them usually being a telephone company central office or switching center.

Trunk Group
See "TG" (p. 23).

Trunk Group Number
Number assigned to a trunk group in the switch.

TSG
Trunk Subgroup

TTO
Transmitter Time-Out

Two-Way Trunk
A trunk that can be seized at either end.

UUDTS
Unitdata Services

URW User Report Writer
The User Report Writer consists of the transaction processing system report writer software package and a system command set. The transaction processing system generates informational reports based on data that changes periodically.

Usage

A measure of trunk or equipment occupancy expressed in Erlangs or CCS.

V

VVacant Code

An unassigned numbering plan area, central office, or station code. A call placed to a vacant code is normally directed to a VCA (vacant code announcement).

Validate

A command used to verify that the values and actions specified are correct for a specific display or page.

VB

V-B (terminating) trunk group. A trunk group that connects a via office (V) to a terminating office (B). See “AB” (p. 1) and “AV” (p. 3).

Via Office

An office that transits a rerouted call between the originating office and the terminating office.

Via Trunk Group

A trunk group designated to carry the calls redirected by a reroute control activated on the “reroute from” trunk group of the reroute control. If a trunk group is identified as a “via trunk group” it is the “AV” portion of the “AV”-“VB” path for rerouted calls.

VRTO Via Route Turnoff Override

VRT is a reroute option that protects regular traffic from rerouted traffic, by not allowing rerouted traffic to use a via TG that is filling with regular traffic. VRTO overrides the VRT option so that network managers can use the via trunk group anyway. See the rr command (4-44) in the *Input Commands Guide*.

W

WWindow

A window is box-type graphic displayed when specific buttons, icons, function keys or hot keys are selected in a windows operating system environment. Each window contains various control attributes including a means to close the box, typically an “X” in the upper right corner. The window identifier is displayed in the task bar. The user opens and closes windows.

Index

1024 trunk groups
surveillance, 7-22

1A *ESS* switch
initial office file entry format, 5-44

1A ESS Switches with Data Alignment Problems, Troubleshooting, 7-15

4ESS
tglist audit, 5-87

5ESS switch
discrete file entries, 5-17
POTS domain, 5-53, 5-55

A

Administering Subnetworks, 7-12

Administration
record base
command sequence, 7-3
process, 7-3
subnetwork, 7-12

After a Switch Has Been Moved to a New DCC, 10-19

Application Checks, 10-10

Architecture for Subnetwork Partitions, 2-4

B

Backup and Disaster Recovery File Locking, 6-7

Backup and Disaster Recovery (BDR), 9-1

BDR
Configuring the Record Base Files, 9-7
DCC alias file, 4-3
File locking, 6-7
Partitioning, 9-3

BDR - see Backup and Disaster Recovery, 9-1

BDR (Backup and Disaster Recovery)
Feature 40, “Enhanced Disaster Recovery”, 9-2
Feature 8, “Disaster Recovery (Duplex)”, 9-2

BDR, Record Base Administration for, 9-1

bdr_create executable, 9-6

BTFN
tglist audit, 5-87

C

Calc keyword
last index entry, 5-101

Calculations
format, 5-51

Changing Record Base File Security, 6-7

Checking Sets Files — ofcset and tgset Commands, 3-6

child, 3-8

CIC Requirement Matrix, 5-91

Codes
Defining, 3-32

Combinations in rules, 5-26

Commands
Common Editing, 6-11
create, full, 7-6
create, single file, 7-6
create, single office, 7-6
dbtest, 7-6
installdb, 8-3
rbed, 7-6
recreate, 7-7
sequence, record base, 7-3

Common Editing Commands, 6-11

Communicating with DCCs over the TCP/IP Network, 10-6

Communications Link, 10-10

Concepts, RSPTE, 3-8

Configuration limit, 8-3

Configuring the Record Base Files for BDR, 9-7

Consistency
file formats, 6-4

Control Default Domain File Entry — 4ESS, 5-15

Control Default Domain Files, 5-15

Control Traffic Type and Code Definition, 3-25

create, 7-6
Full, 7-6

create Command, 7-6

create Process, 8-5

create Process for Global Files, 9-14

create Process for Independent Files, 9-16

create Process for Office-Related Files, 9-18

create Process for Shared Files, 9-21

create, Single Office and Single File, 7-6

Creating and Modifying Database Records, 7-6

D

DAS, 5-53, 5-55

Data Alignment Problems, Troubleshooting 1A ESS Switches, 7-15

Data collection
restrictions, 5-71

Data Collection Operations System, 4-2

Data Type Information, 5-49

Data views, 3-3

Database
define threshold, 7-9
NTM reference, 7-3

Database Modification Permission, 2-6

Database Records
Creating and Modifying, 7-6

dbtest Command, 7-6

DCC
Office file format, 5-44
office list, 10-16

DCC Alias File, 4-3

DCC alias file
with BDR, 4-3

DCC, RSPTE Entry, 5-72

DCOS, 4-2

Default Domain Files Control, 5-15

Defining Codes, 3-32

Defining Domain Acronyms, 3-28

Defining Sets, 3-4

Defining the Text Editor, 6-7

Defining Threshold Data, 7-9

Defining Trunk Group Threshold Files, 3-21

Delimiters
expression, 5-100

Differences in Record Base Files, 9-11

Digit Analysis Selector, 5-53, 5-55

Discrete
file entries for *5ESS* switch, 5-17

Discrete File, 5-16

Discrete Types and Descriptions, 5-17

Discretes, Working With, 3-13

DMS 100/200 Switch TCP/IP Interface, 10-28

Domain
definition, 5-19

Domain Acronym File, 5-19

Domain Acronym File Entry — No Subnetworks, 5-20

Domain Acronym File Entry — Subnetworks, 5-20, 5-56

Domain Acronyms
Defining, 3-28

Domain Acronyms, Mapping, 3-30

Domains
POTS, 5-53, 5-55

Domestic Code File, 5-21, 9-20

E

EADAS, 4-2

EADAS Interface, 4-2

Editing Commands, 6-11

Editing record base files, 6-9

Editing record base files(**rbed**), 6-5

Enhanced Thresholding (with NTM Feature 189), 5-25, 5-27, 5-97, 5-101

Entering
logical operators, 5-26
mathematical signs, 5-26

Error messages
RSPTE file, 8-3

Event_Alarm File, 5-23

Exceptions, Specifying Machine, 3-13

Expression delimiters, 5-100

External Network Element, RSPTE Entry, 5-72

F

Feature 189
Enhanced Thresholding, 5-25, 5-27, 5-97, 5-101
Filter File, with, 5-27
Traditional Thresholding, 5-25, 5-27, 5-97, 5-100
Trunk Group Threshold Entries, with, 5-102
Trunk Group Threshold Entries, without, 5-100

FEP
interface, 4-2

FEP Interface, 4-2

FHC File Entries, 5-29

File

Control Default Domain, 5-15
DCC entry format, 5-44
Discrete, 5-16
Domain Acronym, 5-19
Domestic Code, 5-21
Event_Alarm, 5-23
Filter, 5-25
Final Handling Code, 5-29
global, 9-12
HTR, 11-2
independent, 9-15
INMS, 5-31, 9-5
International Code, 5-33
Office, 5-40
Office Domain, 5-53
Office Type Domain, 5-55
office-related, 9-17
Password, 5-65
record base, editing, creating, and searching (**rbed**), 6-5
RSPTE, 5-67
Sets, 5-73
Signaling Link Threshold, 5-77
Threshold Table Schedule, 5-82
Transmitter Timeout (TTO) Thresholds, 5-84
Trunk Group, 5-86
Trunk Group Threshold, 5-96
trunk group threshold, 5-96
TYPXREF, 5-103
File formats, 6-2
recommendations, 6-4
File Locking
Backup and Disaster Recovery, 6-7
File locking, 6-7
File Security
Changing, 6-7
Files
Recovering lost, 6-8
Files, Office-Related, 9-17
files=office option, 8-7
Filter File, 5-25
with Feature 189, 5-27
without Feature 189, 5-27
Final Handling Code File, 5-29
Final trunk groups, 3-19
Flags, Using, 3-21
Flowcharts and procedures
single exchange create, 8-9
Format
DCC, 4-3
Records, 6-4
Format, Name-Defined, 6-2
Frequency
full **create** procedure, 7-6
Full create, 7-6

G
General Flow of Update Procedures, 8-1
Global Files, 9-12
Global files
backup host, 9-13, 9-17
noxfer, 9-13, 9-17
GTD-5 switch
office file entry format, 5-44
special calculations for, 5-52

H
Hierarchical chain, 3-8
Hierarchy
logical network, 3-8
High usage, 3-19
How Record Base Files Affect Network Data Views, 3-3
HTR File, 11-2

I
Independent Files, 9-15
Information
data type, 5-49
packet, 5-49
Initial File Entry Formats, 5-44
INMS (Inter-NMS) file, 5-31
INMS File, 5-31
Input commands
notation used in, 1-7
Interface
DCOS, 4-2
EADAS, 4-2
FEP, 4-2
TDMS, 4-2
Internal Network Element, RSPTE Entry, 5-72
International Code File, 5-33
Invalid Machine and Trunk Group Data, 7-16

K
Keys and Their Functions, vi Text Editor, 6-11

L
Logical operators, 5-26

M
Machine data
invalid, 7-16
Machine Data/Invalid Trunk Group Data, Valid, 7-15
Machine Exceptions, Specifying, 3-13
Mapping Domain Acronyms, 3-30
Mathematical signs, 5-26
Maximum Number of Subnetworks and Partitions, 2-2
Merged - see Shared Files, 9-19
Modifying Database Records, 7-6

N

Name-Defined Format, 6-2

Name-defined syntax
REQUIRED, 5-103

NANP, 5-53, 5-55

Network Bandwidth, 10-11

Network elements
add a DCC, 10-13

remove a 1A *ESS*, *5ESS*, *DMS* 100, *EWSD*, LSSGR, or *GTD5* switch, 10-33

Non-hierarchical digital network, 3-8

North American Numbering Plan, 5-53, 5-55

Numbering of Offices in the Example Network and a Real RSPTE File, 3-10

Numbering, RSPTE, 3-10

O

ofcset and tgset Commands
Checking Sets Files, 3-6

ofcset command, 3-6

Office Domain File, 5-53

Office File, 5-40

Office file
DCC entry format, 5-44

entry format, *GTD-5* switch, 5-44

initial entry format, 1A *ESS* switch, 5-44

Office File — Format 1, 5-41

Office File — Format 2, 5-41, 5-42, 5-43

Office File — Format 3, 5-41

Office File — Format 4, 5-41

Office File — Format 5, 5-42

Office list
DCC, 10-16

Office Sets, 5-73

Office-Related Files, 9-17

Operating System Checks, 10-10

options=sched, 5-90

Overview of the TCP/IP Interface to DCC, 10-6

P

Packet Information, 5-49

Packet value(s), 5-46

parent, 3-8

parent or child, 3-8

Partitioning
BDR, 9-1, 9-3

Partitioning, Using the INMS File to Define, 9-5

Partitions
Architecture for Subnetwork, 2-4

backup, 9-3

primary, 9-3

RSPTE, 2-6

defining NTM names, 9-5

three hosts, 9-3

thresh files, 2-6

Partitions, Maximum Number of Subnetworks and, 2-2

Password File, 5-65

Pathnames, 1-4

Personnel Tasks, Record Base, 1-3

Pooled Trunk Groups, Using, 3-21

Position-Defined Format, 6-2

POTS domain, 5-53, 5-55

Problems, Troubleshooting 1A ESS Switches with Data Alignment, 7-15

Procedure

Build Database for Feature 264, “DMS 100/200 Switch Surveillance of 1024 Trunk Groups Via TDM”, 7-22

Changing Default Domain for a Control, 7-19

Creating the Record Base Files, 10-34

Delete/Add RSPTE CLLI Changes, 7-20

Editing a Record Base File with rbed, 6-9

Full create and installdb, 8-3

Modifying Record Base Files for Subnetworks, 7-13

Realigning Registers, 7-17

Record Base Administration Tasks, 9-7

Removing a DCC, 10-23

Removing the Record Base Files, 10-24, 10-36, 10-39

Setting Up Trunk Group Threshold Data, 7-10

Single File create and installdb, 8-6

Single Office create, 8-9

Treatment of Error Messages, 9-6

Updating the System after Removing a Network Element, 10-25, 10-37

Procedures to be Performed on NTM, 10-20

Procedures to be Performed on the EADAS, 10-21

Procedures, General Flow of Update, 8-1

Process
create, 8-5

Removing a 1A ESS, 5ESS, DMS, EWSD, LSSGR, or GTD-5 Switch, 10-33

Processing, Rule, 5-99

R

Ranks, 3-8

Raw counts and calculations
GTD-5, 5-51

rbed
abnormal exit, 6-7
unlocked file(s), 6-7

rbed Command, 6-5, 7-6

rbed command, 6-5

rbed command
defining text editor for, 6-7
file locking, 6-7
procedure, 6-9
recovering an edited file, 6-8

Record base
administration process, 7-3
command sequence, 7-3
create files, 10-34
editing the, 6-5
remove *4ESS* switch files, 10-24
remove files, 10-36
subnetwork administration, 7-12

Record Base Administration for BDR, 9-1

Record Base Administration Process, 7-3

Record Base CIC Requirement Matrix, 5-91

Record base editor
introduction to the, 6-5

Record Base File Format, 6-2

Record Base File Symbols, 6-3

Record base files
Editing, 6-9

Record Base Files and Pathnames, 1-4

Record Base Personnel Tasks, 1-3

Record Format, 6-4

Recovering an Edited File, 6-8

Recovering lost files, 6-8

recreate Command, 7-7

Remove
4ESS switch record base files, 10-24
DCC, 10-23

Remove a 1A *ESS*, *5ESS*, *DMS* 100 *EWSD*, or LSSGR, *GTD-5* switch, 10-33

Required Entries in the "/etc/hosts" File, 10-6

Restrictions
data collection, 5-71

Routing Table Changes, 10-11

RSPTE Concepts, 3-8

RSPTE Entries, 5-71

RSPTE Entry — BDR Host, 5-72

RSPTE Entry — DCC, 5-72

RSPTE Entry — External Network Element, 5-72

RSPTE Entry — Internal Network Element, 5-72

RSPTE File, 5-67, 9-19

RSPTE file
definition, 5-67

RSPTE File, Using, 3-11

RSPTE Numbering, 3-10

Rule Processing, 5-99

Rules
datatypes and switch types, 5-26

Rules, Combinations in, 5-26

S

Scheduling Threshold Tables, 3-23

Security
Changing Record Base File, 6-7

Sets
Defining, 3-4

Sets File, 5-73

Sets Files
checking — ofcset and tgset Commands, 3-6

Sets, Office, 5-73

Setting Up the TCIP/IP Link Between the Host and Switch, 10-30

Setting Up Trunk Group Files, 3-19

Shared file(s)
backup host, 9-19
noxfer, 9-19

Shared Files, 9-19

Signaling Link Threshold File, 5-77

Signaling Type/Switch Cross Reference, 5-93

Single file create
list of files, 7-7

Single Office and Single File create, 7-6

snm, 2-6

Specifying Machine Exceptions, 3-13

srb, 2-6

Structure
DCC Office List, 10-16

Subnetwork, 2-2
administration, 7-12

Subnetwork Characteristics, 2-5

Subnetwork Partitions
Architecture for, 2-4

Subnetworks
Administering, 7-12
Domain Acronym File, 5-20, 5-56

Subnetworks and Partitions, Maximum Number of, 2-2

Surveillance of 1024 trunk groups, 7-22

Switch
add a DCC, 10-13

remove a 1A *ESS*, *5ESS*, *DMS* 100, *EWSD*, LSSGR or *GTD-5*, 10-33

T

Tasks, Record Base Personnel, 1-3

TCP/IP Interface to Data Collector, Requirements for Direct Connect, 10-7

TCP/IP Interface to DCC, 10-5

TDMS, 4-2

Text Editor(s), 6-8
Defining, 6-7

tgset command, 3-6

Threshold
Trunk group file, 5-96

Threshold Data
Defining, 7-9

Threshold data
defining, 7-9

trunk group, set up, 7-10

Threshold Table Schedule File, 5-82

Threshold Tables, Scheduling, 3-23

Thresholding, Trunk Group Exception, 3-15

Traditional Thresholding
without NTM Feature 189, 5-25, 5-27, 5-97, 5-100

Traffic Data Management System, 4-2

Transmitter Timeout (TTO) Thresholds File, 5-84

Troubleshooting, 10-33

Troubleshooting 1A ESS Switches with Data Alignment Problems, 7-15

Trunk group
Threshold File, 5-96

threshold file, 5-96

Trunk Group Data
invalid, 7-16

Trunk Group Data, Valid Machine Data/Invalid, 7-15

Trunk Group Exception Thresholding, 3-15

Trunk Group File, 5-86

Trunk Group File Entries, 5-93
1A ESS, 5-94

4ESS, 5-93

5ESS, 5-94

GTD-5, 5-94

Trunk Group Files, Setting Up, 3-19

Trunk Group Sets, 5-73, 5-74

Trunk Group Suffix
invalid, 5-86

"-tgn", 5-86

"-to", 5-86

Trunk Group Threshold Entries without Feature 189, 5-100, 5-102

Trunk Group Threshold File, 5-96, 9-20

Trunk Group Threshold Files
Defining, 3-21

Trunk groups
Final, 3-19

TTO
Transmitter Timeout Thresholds File, 5-84

TYPXREF (Type Cross-Reference) file, 5-103

TYPXREF File, 5-103

U

UNIX System vi Text Editor
adding text, 6-12

cursor movement, 6-12

deleting text, 6-12

general guidelines, 6-11

keys and functions, 6-11

miscellaneous functions, 6-12

moving text, 6-12

replacing text, 6-12

searching through text, 6-12

Update system
after removing *4ESS* switch, 10-15, 10-44, 10-53

after removing network element, 10-37

Using and Testing TCP/IP Connections, 10-10

Using Flags, 3-21

Using Pooled Trunk Groups, 3-21

Using the INMS File to Define Partitioning, 9-5

Using the RSPTE File, 3-11

V

Valid Machine Data/Invalid Trunk Group Data, 7-15

vi Text Editor - see *UNIX* System vi Text Editor, 6-11

vi Text Editor Keys and Their Functions, 6-11

vi, Working with, 6-11

Viewing data, 3-3

W

Working With Discretes, 3-13

Working with vi, 6-11