Network Traffic Management

8920 Network Traffic Management software

User Guide
Release 17.3

190-406-816
Issue 1.0
October 2012

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:

ACP50 and ACP550 are products of NetKit Solutions LLC.

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

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

[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.

Contents

1 Getting Started with the Browser-based GUI

The graphic user interface (GUI) and browsers 3
Skin Appearances 5
Pages in the GUI 7
Launch page 9
Search pages 10
Container pages 12
Details pages 14
Trend pages 18
GUI form elements 20
Output element types 21
Hiding/showing an area 23
Toolbar area 24
Error presentation 26
Host user ID selection 28
Manual/automatic update 29
Detached execution 31
Comma separated value formatting 33
Online Documentation 34
Using the search function 35

2 Network Elements

Network element data types 4
Network Elements data search page 5
Network Elements container page 8
Network Element Details page 11

Network Elements Trend Analysis page 15
Background 20
Audits search page 21
Audit request page 23
Audit details page 24

3 Network Connections

Trunk Groups search page 4
Trunk Groups container page 7
Trunk Group Details page 8
Trunk Groups trend page 15
Signaling Links and Link Sets search page 20
Signaling Links and Link Sets container page 21
Signaling Link and Linkset Measurement - Search Pages 24
Signaling Link and Linkset Measurements - Container pages 27
Packet Link search page 30
Packet Link container page 33

4 Network Views

Network Views search/container page 2
Network View detail page 5
Network Views display options 8
Nodes on a Network View 11
Text on a Network View 14
Timestamp on a Network View 15
Mouse menu options 16
Network View Legend 17
SS7 Historical Alerts 27
Network Event Alerting 29
Adding a node 32
Modifying a node 33
Deleting a node 34
Adding a link to a Network View 35
Deleting a link from a Network View 36
Adding a timestamp or text 37

Modifying a timestamp or text 39
Deleting a timestamp or text 40

5 **Controls**

Background 2
Parameter area 6
Code Controls search page 8
Code Controls container page 11
Code Control Request page 13
Code Controls trend page 16
Protective TG Controls search page 20
Protective TG Controls container page 22
Protective TG Control Request page 24
Background 28
Expansive TG Controls search page 30
Single Trunk Group search 32
Active Controls search 33
Active Via Trunk Groups search 34
Active Expansive TG Controls container page 35
Expansive TG Control Details page 36
Expansive TG Control Request page 37
Expansive TG Control Trend page 46
Other Controls Search Page 5-50
Other Controls Container Page 5-52
Other Controls Request Page 5-53
Control Summary page 55
Viewing existing controls 58
Setting protective trunk group controls 59
Setting code (CG) controls 60
Setting expansive trunk group controls 61
Deleting controls 63

6 **Destinations**

Destination Codes search page 4
Destination Codes container page 6

Destination Code Details page 7
Manual HTR Assignments 10
Automatic HTR Parameter Set Definitions (4ESS) 13
Automatic HTR Parameter Set Assignments 15
Retrieving destination data 20
Retrieving destination assignment data 21
Adding and modifying manual hard-to-reach assignments 22
Modifying automatic hard-to-reach parameter sets 23
Adding/modifying automatic HTR parameter set assignments 24

7 Other Functions

Error Log search page 4
Error Log container page 5
Control Log search page 8
Control Log detail page 9
Broadcast Messages 11
Sending a Broadcast Message 13
Audible Alarms page 16
Audible Alarms search result 18
Examples 19
Exception Status and Mark Assignments search page 23
Exception Status and Mark Assignments container page 25
Exception Status and Mark Assignment details page 26
Filtering alerts 30
ISA system alert filters 32
ISA system filter messages 34
Alert data field contents 36
Customized Command page 50
GUI Who page 51

8 Link Status

Link Status Table search page 4
Link Status Table container page 5
Link Status Schematic search page 8
Link Status Schematic container page 9

Changing the Link Status Schematic time difference 13
STM Periodic Status 16
Current Link Status 18
Recent Data Collection Status 20
Periodic Data Browser search page 24
Periodic Data Browser container page 27
Periodic Data Browser Details page 29

9 GUI Administration

Web User administration 3
Password administration 7
Table Layouts search page 14
Table Layouts container page 15
New Table Layout 16
Historical Session search and container pages 20
Historical Session playback toolbar icons 22
Historical Playback Information page 23
Network View Administration 26
Network View Style Administration 30
Network View Alert Group Administration 33
Network View Shape Facet Administration 36
Parameter Sets container page 40
Parameter Sets detail pages 41
Link Status Shape Facet Administration 43
Client Downloads 44
Feature Listing 45
Changing user defaults 48
Changing skins 49
Changing user permissions 50
Changing passwords 51
Restarting the network view server 52
Starting and stopping the web server 53
Starting and stopping the LDAP server 54
Adding users 55

Deleting users 57
Changing a table layout 58
Creating a table layout 59
Creating a network view style 60
Creating a historical session 61
Making a historical session active 63
Changing a parameter set 65
Creating a parameter set 66

10 Searching using Modifiers and Regular Expressions

Modifiers and Regular expressions 2
Modifiers 3
Examples of Modifiers 4
Additional Examples of Regular Expressions 6
Regular expression reference for NTM 7

11 Training Objectives and Exercises

GL Glossary

IN Index

List of figures

1 Getting Started with the Browser-based GUI

1 Initial Login Screen 4
2 Original Skin 6
3 8920 NTM Tab Skin 6
4 Example of page flows in the NTM graphic user interface 8
5 NTM Launch page (Original skin) 9
6 Search area in advanced search mode 11
7 Trunk Groups container page 13
8 Trunk Group Details page 15
9 Network Element Details page 16
10 Arrow indicator: area is shown and may be hidden 23
11 Arrow indicator: area is revealed 23
12 New period indicator 30
13 Detached execution response page 31

2 Network Elements

1 Network Elements data search page 5
2 Network Elements container page: Data table view 8
3 Network Elements container page: Data table view for discrete data 9
4 Network Element container page: exception list view 9
5 Network Element Details page 12
6 Trend links on a Network Element Details page 14
7 Network Elements — Trend Analysis page 16
8 Audits search page 21
9 Audits request page 23
10 Audits details page 24

3 Network Connections

1 Trunk Groups container page 7
2 Trunk Group Details page 9
3 High-usage trunk group 13
4 Final trunk group 13
5 Full trunk group 13
6 Trunk Groups trend page 16
7 Signalling Links/Link Sets search page in advanced search mode 20
8 Signaling Links and Link Sets container page 21
9 Link Measurement page in Simple search mode 24
10 Linkset Measurement search page 25
11 Link Measurements container page 27
12 Linksets Measurements container page 27
13 Packet Links search page in simple search mode 31
14 Packet Links (ATM Trend) container page 34

4 Network Views

1 Network Views search/container page (Original skin view) 3
2 Network View detail page 5
3 Link expansion indicator 7
4 New period indicator 7
5 Map background menu 9
6 Background menu “New” option 11
7 Node dialog menu 12
8 “New” Text dialog window 14
9 Timestamp dialog window 15
10 Portion of Network View Legend 18
11 Alerts table search page 20
12 Default alerts 23
13 Link Status alerts 24
14 Network Elements alerts 25
15 Trunk Group alerts 25
16 SS7 Historical Alerts search page 27
17 SS7 Historical Alerts container page 28

18 Code Control events alerts page 29
19 SCP Control events alerts page 29

5 Controls

1 Control icon 2
2 Code control request page: Validation request result 4
3 Code Control Request page: Failed control request 5
4 Code Controls container page 11
5 Code Control Request page: Preset parameter mode 13
6 Code Control Request page: Manual parameter mode 14
7 Code Controls trend page 17
8 Protective TG Controls container page 22
9 Protective TG Control Request page: Preset parameter mode 25
10 Protective TG Control Request page: Manual parameter mode, ESS5 office 26
11 Single Trunk Group search 32
12 Active Controls search 33
13 Active Via Trunk Groups search 34
14 Active Expansive TG Controls container page 35
15 Expansive TG Control Details page 36
16 Via Analysis area 38
17 Expansive TG Control Request page 41
18 Via Analysis Results Table 43
19 VB Suffix finalization 44
20 Expansive TG Control Trend page 47
21 Other Controls Search Page 50
22 Other Controls Container Page 52
23 Other Controls request page - preset mode 53
24 Other Controls request page - manual mode 53
25 Control Summary page 55

6 Destinations

1 Destination Codes Advanced search page 4
2 Destination Codes container page 6
3 Destination Code Details page 7
4 Manual HTR Assignments search page 10

5 Manual HTR Assignments container page 12
6 Automatic HTR Parameter Set Definitions search page 13
7 Automatic HTR Parameter Set Definitions page 14
8 Automatic HTR Parameter Set Assignments search page 15
9 Automatic HTR Parameter Set Assignments — NANP All NPA 16
10 Automatic HTR Parameter Set Assignments — NANP Home or Designated NPA 16
11 Automatic HTR Parameter Set Assignments container page 17

7 Other Functions

1 Error Log container page 5
2 Control Log detail page 10
3 Broadcast Message window 11
4 Audible Alarms page 16
5 Audible Alarms search result 18
6 NE Exception Status and Mark Assignments search page 23
7 NE Exception Status and Mark Assignment container page 25
8 TG Exception Status and Mark Assignment Request page 26
9 NE Exception Status and Mark Assignment Request page 27
10 Network Element Details page showing links to Mark Assignment Status page 28
11 Filter message 30

8 Link Status

1 Link Status Table container page 5
2 Link Status Schematic container page 10
3 STM Periodic Status search page 16
4 STM Periodic Status container page 17
5 Current link status search page 18
6 Current link status container page 19
7 Recent data collection status search page 20
8 Recent Data Collection Status container page 21
9 Periodic Data Browser search page 24
10 Periodic Data Browser container page: Data table view 27
11 Periodic Data Browser Details page 29

9 GUI Administration

1 Administration launch page 4

2 Web User Information page 5
3 Web User Administration page 6
4 /nm/web/sup_soft/http/conf/pwa.conf file 10
5 Table Layout search 14
6 Table Layouts container page 15
7 New Table Layout page 16
8 New Table Layout page for Alert Page 17
9 Historical Session container page 20
10 New Historical Playback Information page 23
11 Network View Administration page 27
12 Network View Details 28
13 Add Network Views page 29
14 Network View Style Administration page 31
15 Add Network View Style page 32
16 Network View Alert Group Administration container page 34
17 Add Network View Alert Group 35
18 Network View Alert Group Details Page 35
19 Network View Shape Facet Administration 36
20 Parameter Sets page — Code controls 40
21 Parameter Sets detail page: Call gap control, New mode 42
22 Link Status Shape Facet Administration 43
23 Network View Server Administration 52

10 Searching using Modifiers and Regular Expressions

11 Training Objectives and Exercises

List of tables

1 Getting Started with the Browser-based GUI

1 Areas on the Launch page 9
2 Form elements and descriptions 20
3 Threshold and discrete alert/alarm level visual indicators 21
4 Overall exception level output element 22
5 Toolbar icons 24

2 Network Elements

1 Search criteria for network elements 5
2 Search criteria for Network Element trend displays 17
3 Search criteria for Audits 21

3 Network Connections

1 Search criteria on the Trunk Groups search page 4
2 Search criteria for Trunk Groups trend page 16
3 Search criteria on the Link and Link Measurements Simple search pages 25
4 Search criteria for Packet Links search page 31

4 Network Views

1 Search criteria on the Network Views search page 4
2 Standard threshold/alert levels 6
3 Search criteria on the Alerts Table search page 20

5 Controls

1 Parameter set attributes 6
2 Code Controls search criteria 8
3 Search criteria for Code Controls trend pages 18
4 Protective TG Controls search criteria 20
5 Expansive TG Controls search criteria 30

6 Fields in the Via Analysis area 38
7 Search criteria for Expansive TG Control Trend page 47
8 Other Controls search criteria 50

6 Destinations

1 Destination Codes search criteria 4
2 Manual HTR Assignments search criteria 10
3 Automatic HTR Parameter Set Definitions search criteria 13
4 Automatic HTR Parameter Set Assignments search criteria 15

7 Other Functions

1 Search criteria in the Error Log 4
2 Search criteria for the Control Log 8
3 Search criteria in the Audible Alarms 17
4 Exception Status and Mark Assignments search criteria 24
5 Alerts using the Discrete alert (minimal attributes) 32
6 Alert using the Trunk Group Data alert (many attributes) 33
7 Alert Attribute Reference Table 37

8 Link Status

1 Search criteria — Link Status Table 4
2 Facets shapes and alert information 11
3 Search criteria — STM Periodic Status Table 16
4 Search criteria — Current link status Table 18
5 Search criteria — Recent data collection status search page 20
6 Search criteria for the Periodic Data Browser 25
7 Search criteria for the Periodic Data Browser Details 29

9 GUI Administration

1 Toolbar icons 22

10 Searching using Modifiers and Regular Expressions

1 Regular expression reference 7

11 Training Objectives and Exercises

List of procedures

1 Getting Started with the Browser-based GUI

Using the search function 35

2 Network Elements

3 Network Connections

4 Network Views

Adding a node 32

Modifying a node 33

Deleting a node 34

Adding a link to a Network View 35

Deleting a link from a Network View 36

Adding a timestamp or text 37

Modifying a timestamp or text 39

Deleting a timestamp or text 40

5 Controls

Viewing existing controls 58

Setting protective trunk group controls 59

Setting code (CG) controls 60

Setting expansive trunk group controls 61

Deleting controls 63

6 Destinations

Retrieving destination data 20

Retrieving destination assignment data 21

Adding and modifying manual hard-to-reach assignments 22

Modifying automatic hard-to-reach parameter sets 23

Adding/modifying automatic HTR parameter set assignments 24

7 Other Functions

Sending a Broadcast Message 13

8 Link Status

Changing the Link Status Schematic time difference 13

9 GUI Administration

Changing user defaults 48
Changing skins 49
Changing user permissions 50
Changing passwords 51
Restarting the network view server 52
Starting and stopping the web server 53
Starting and stopping the LDAP server 54
Adding users 55
Deleting users 57
Changing a table layout 58
Creating a table layout 59
Creating a network view style 60
Creating a historical session 61
Making a historical session active 63
Changing a parameter set 65
Creating a parameter set 66

10 Searching using Modifiers and Regular Expressions

11 Training Objectives and Exercises

1 Getting Started with the Browser-based GUI

Overview

Purpose

This chapter describes the elements used to request and display network management data with the 8920 Network Traffic Management software (8920 NTM) browser-based Graphical User Interface (GUI). Data is requested and displayed for network elements, trunk groups, controls, and other items of interest.

Important! The screens shown in this guide are examples taken from test machines; they may not match the screens shown for your system.

Contents

This chapter discusses the following topics:

The graphic user interface (GUI) and browsers	1-3
Skin Appearances	1-5
Pages in the GUI	1-7
Launch page	1-9
Search pages	1-10
Container pages	1-12
Details pages	1-14
Trend pages	1-18
GUI form elements	1-20
Output element types	1-21
Hiding/showing an area	1-23
Toolbar area	1-24
Error presentation	1-26
Host user ID selection	1-28
Manual/automatic update	1-29
Detached execution	1-31
Comma separated value formatting	1-33
Online Documentation	1-34
Using the search function	1-35

The graphic user interface (GUI) and browsers

Recommended browser user preferences

In order to recognize links on a page, we recommend that the user:

- set visited and unvisited links to a color other than black or white
- select the Underline links option

These options will allow the user to easily see links on the GUI pages.

Using the GUI on various platforms and browsers

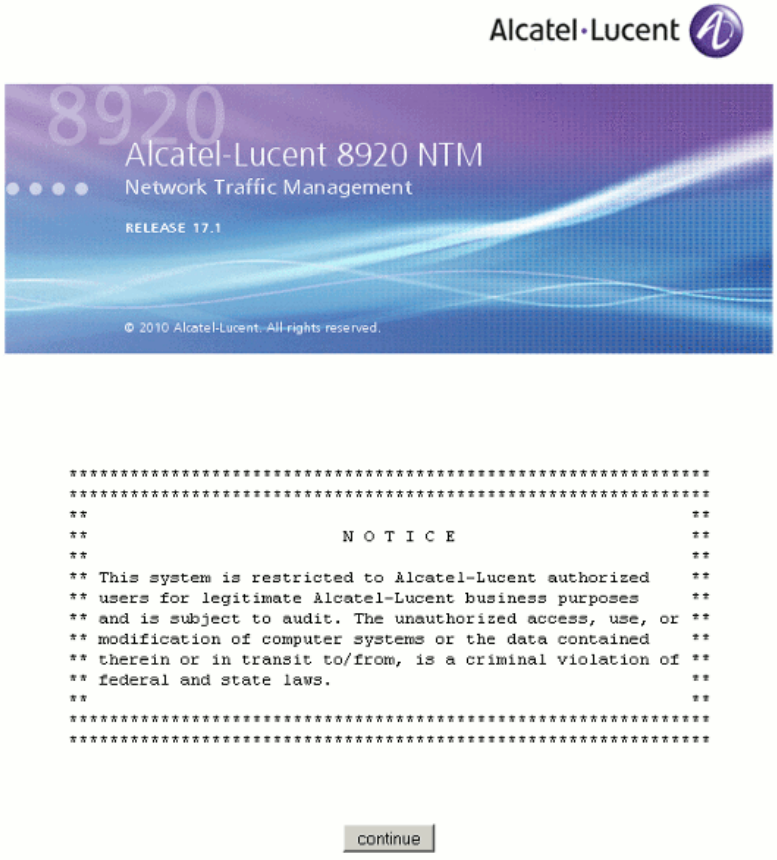
When running the NTM browser-based Graphical User Interface (GUI), certain functions like selection and sorting may work differently on PCs than on workstations even using the same browser. These are browser or platform variances. An example is selecting items from a list. On a workstation using Netscape 4 the user can select items by single clicking on each item from a list, on a PC using Netscape 4 the user can choose a range by single clicking the first item and holding the shift and selecting a range of items. To select random items on a PC using Netscape 4 from the same list the user must select the first item and then hold the ctrl key while selecting additional items.

Important! Some uses of the “Back” button within a browser can cause the browser session to stop responding. This is especially true if the “Back” option is selected while a Java window, such as Discretes or the Alerts Table is initiating.

Initial Login Screen

The initial login notice is displayed upon first access of Web Pages associated with resources requiring authorization. The GUI user must press the continue button to proceed.

Figure 1 Initial Login Screen



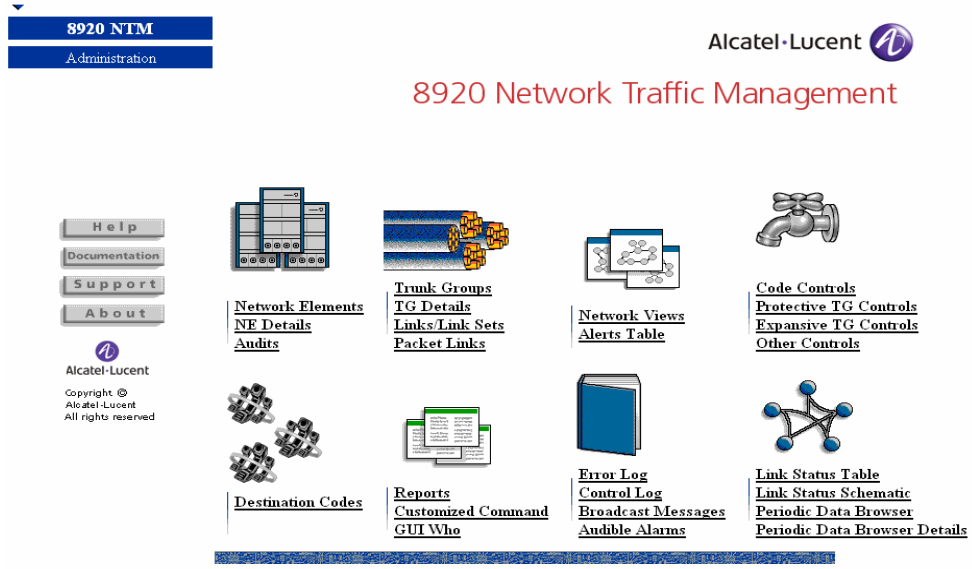
Skin Appearances

Overview

Beginning with NTM release 15, there are two skins available for NTM. The original skin (Figure 2) is the GUI interface used in NTM releases 9 through 14. The 8920 NTM Tabs skin (Figure 3) reflects a top menu driven appearance and is available in release 15 and later. Screens shown in most places in this guide reflect the original skin design.

Original

Figure 2 Original Skin



8920 NTM Tabs

Figure 3 8920 NTM Tab Skin

Pages in the GUI

Overview

Six basic types of pages are used in the GUI:

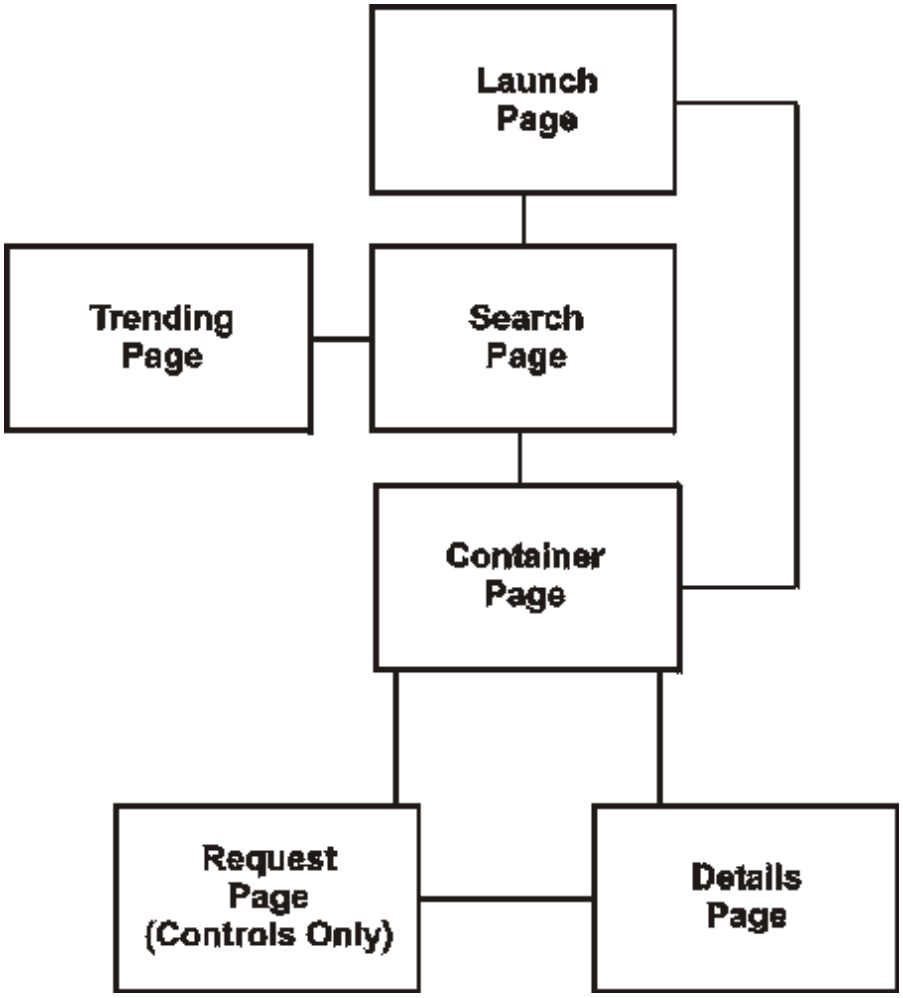
- The Launch page is used to select high-level data types to monitor. Data types include Elements (e.g., circuit switches), Connections (e.g. trunk groups and signaling links), and controls. This page is where the user can access the NTM system through icons and menus.
- Search pages are used to request data on network elements, network connections, and controls. Search pages may have one or more modes. On any search page, clicking the "Search" button without restrictions retrieves all available data.
- Container pages display the results of a search.
- Details pages provide information (such as reference data) on specific network elements or network connections. Access details pages by clicking on specific items on; a container page, on the "Details" link on the launch page, or in the navigation frame. These may also be the result of a search.
- Request pages are used to execute controls and display control parameters before controls are applied. Request pages are available only on Control pages.

  Reference: Chapter 5, "Controls"
- Trend pages graphically displays measurements for a specific set of controls, network elements, or trunk groups, and how they varied during a particular time interval.

Figure

These page types are discussed in the following sections. The following graphic illustrates an example of page flows between these page types. This is only an example. There are many possible ways to access each page through bookmarking, hyperlinks, and search options.

Figure 4 Example of page flows in the NTM graphic user interface



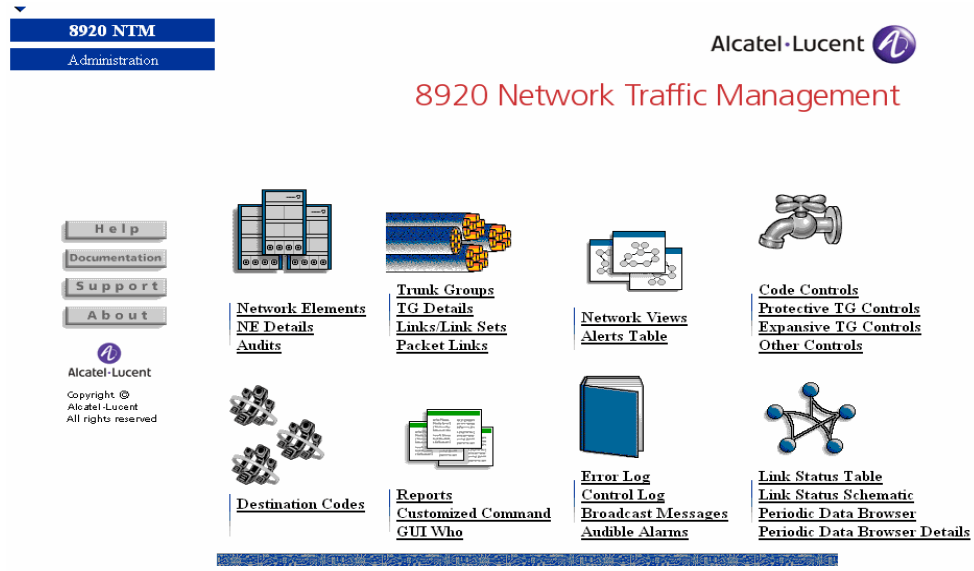
Launch page

Purpose

The original NTM Launch page contains three major areas that are common to all pages.

Reference: Table 1

Figure 5 NTM Launch page (Original skin)



Important! For information pertaining to the icons and menus found on the GUI, refer to various chapters in this guide. For more detailed information regarding the Reports icon, please refer to the *Report Writer Guide*.

Table

Table 1 describes the different areas on the Launch page.

Table 1 Areas on the Launch page

Area	Location	Contents/Function
Navigation link area	upper left	Contains boxes with underlined navigation links. These links vary from page to page.
Common area	lower left	Contains gray boxes that link to online help, online documentation, support, and information about NTM. These links appear on every page.
View area	rest of the page	This area displays the forms, data tables maps, and other elements of the system interface. All the objects shown on the launch page link to the corresponding search page for that object.

Search pages

Purpose

Search pages allow you to enter parameter values and request data from the system. Once a search has been completed, the search option is often available from the container or details page that results from the search. Additional searches can be done from the Details pages.

Search pages can have just a simple search, or both simple and advanced search options. A typical search page (for a trunk group search, in this case) is shown in Figure 6.

Selecting data

Data is requested by selecting options from menus or inputting text in text fields. If all search fields are blank then all link information is retrieved. Some search pages have required fields that must be populated before a search can be executed. These fields are usually indicated with an asterisk (*).

Refine buttons

Some fields on the Search pages have associated Refine buttons. There are two ways to use these fields:

1. Typing the first few characters of a network element or set name and tabbing out of the field will cause NTM to complete the string you typed with the first alphabetical match for a set name, or the highest-ranking switch in your RSPTE File that provides an alphabetical match.
2. Entering a regular expression in the field and clicking the associated Refine button matches patterns of character strings (e.g. enter "/." and click the Refine button to list all available network elements).

   Important! If you enter a regular expression in a search field and tab without completely identifying a network element the system will not complete the name.

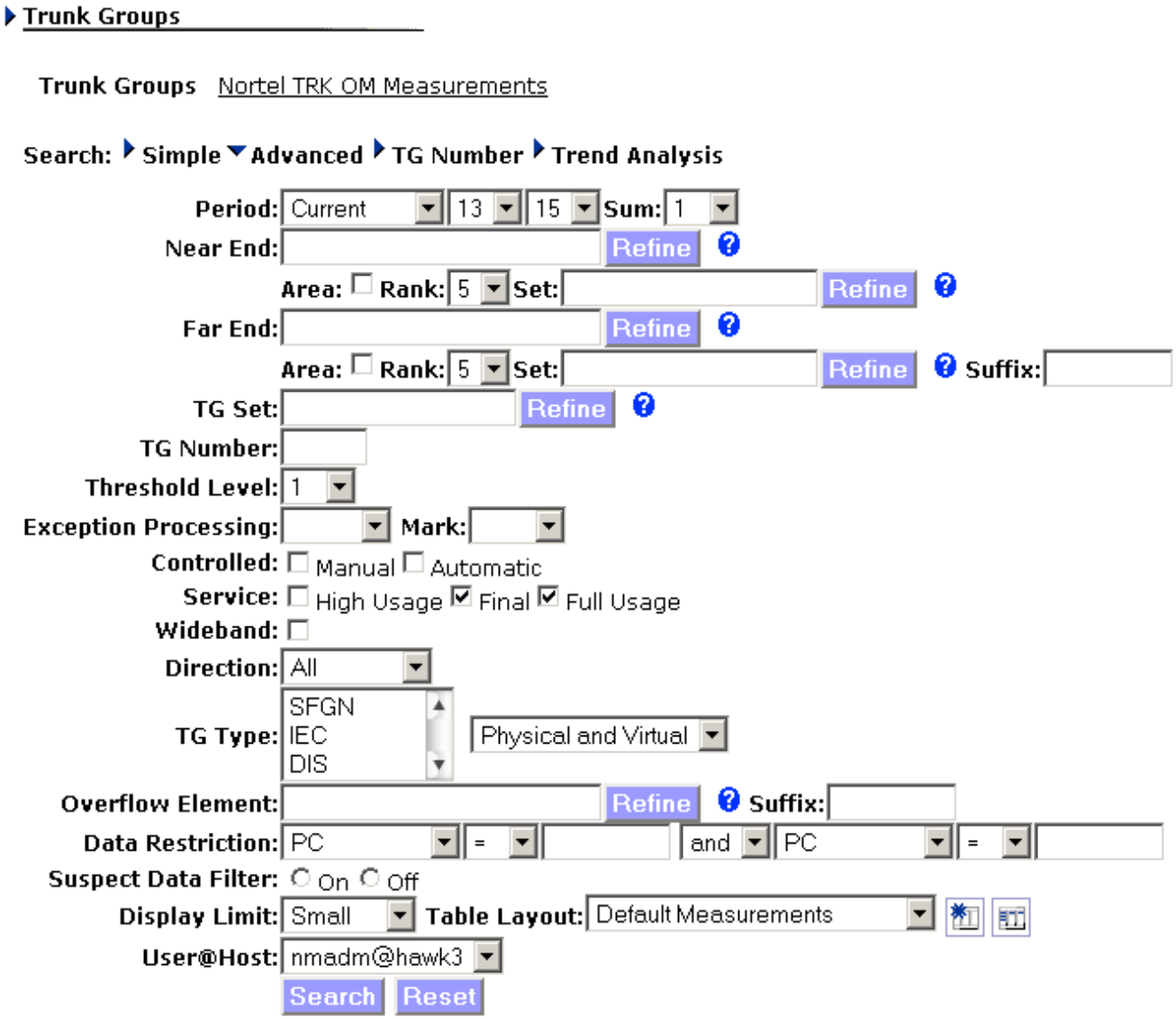
   Important! If you leave a blank search field and click the Refine button the system will not provide any information or reply with an empty list of network elements.

   Reference: Appendix 10, "Searching using Modifiers and Regular Expressions"

Figure

Figure 6 shows an example of a search page in advanced mode.

Figure 6 Search area in advanced search mode



Container pages

Overview

Search results are displayed in container pages, such as the trunk group container page shown in Figure 7.

- Each underlined item on the container page is a link to another page, that displays details for that item.
- The "?" contextual help icon at the head of each column links to the field help file for that data type.

  Important! The "?" contextual help icon can be toggled on or off.

  Reference: "Web User administration" (p. 3)
- The underlined arrows at the left of the names of internal network elements on trunk group container pages will link to another container page showing trunk group counts for all trunk groups having that network element as a near end or far end, depending on the column in which that network element appears.

Row ranking

Rows on the container page are ranked in order of how they are defined in the RSPTE File. Clicking on the column headings sorts the display in descending order on that column. Clicking the same column heading again resorts the display in ascending order on that column.

The title of the table indicates the:

- number of trunk groups displayed on the screen
- total number of trunk groups that were retrieved by your search
- data collection period
- set file name (if populated on the search page)

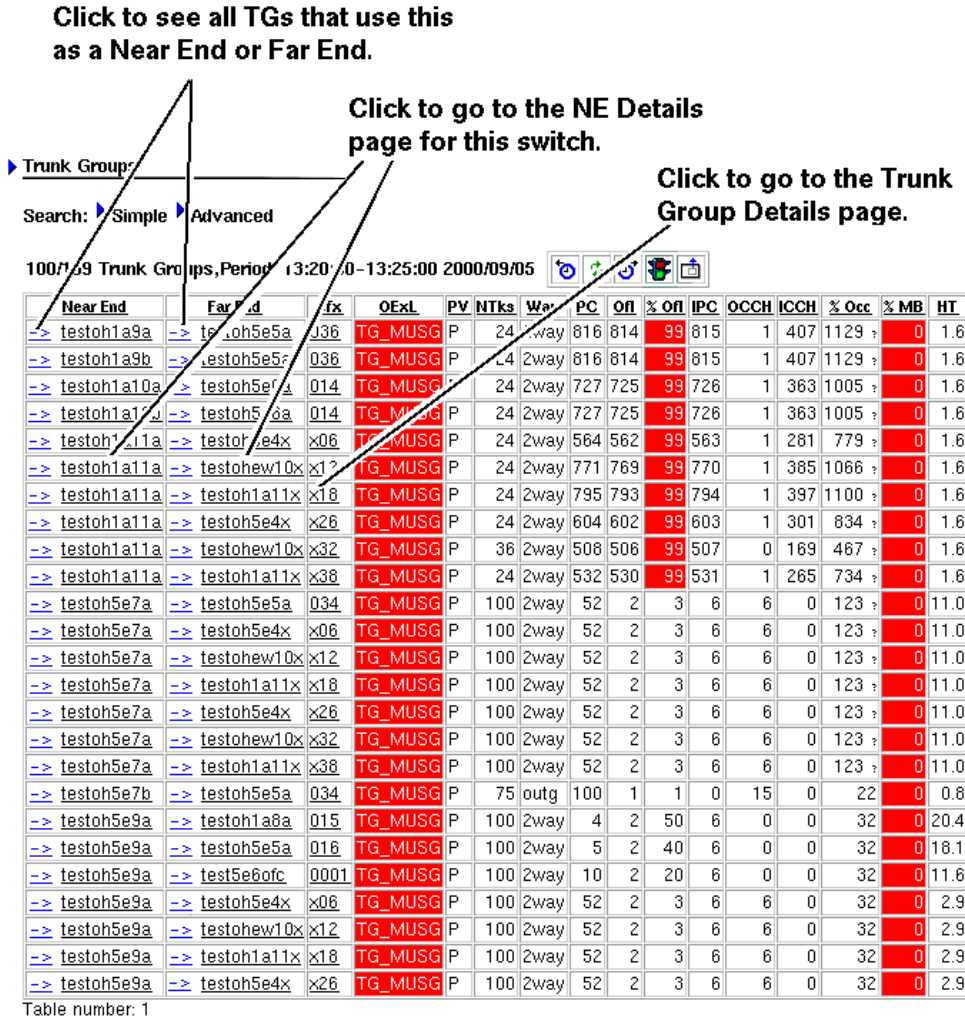
The toolbar symbols to the right of the title provide access to functions such as refresh and auto-update. The severity level of exceptions is indicated by the colored graphic in the table cells.

Reference: Table 4, "Overall exception level output element" (p. 22)

Figure

Figure 7 shows an example container page:

Figure 7 Trunk Groups container page



Near End	Far End	fx	OExL	PV	NTks	Way	PC	Ofl	% Ofl	IPC	OCCH	ICCH	% Occ	% MB	HT	Ctrl	% MFTO	WB	Excp	Mark
-> testoh1a9a	-> testoh5e5a	036	TG_MUSG	P	24	2way	816	814	99	815	1	407	1129	0	1.6	ptg etg		0	0	
-> testoh1a9b	-> testoh5e5a	036	TG_MUSG	P	24	2way	816	814	99	815	1	407	1129	0	1.6	ptg etg		0	0	
-> testoh1a10a	-> testoh5e6a	014	TG_MUSG	P	24	2way	727	725	99	726	1	363	1005	0	1.6	ptg etg		0	0	
-> testoh1a10a	-> testoh5e6a	014	TG_MUSG	P	24	2way	727	725	99	726	1	363	1005	0	1.6	ptg etg		0	0	
-> testoh1a11a	-> testoh5e4x	x06	TG_MUSG	P	24	2way	564	562	99	563	1	281	779	0	1.6	ptg etg		0	0	
-> testoh1a11a	-> testohew10x	x12	TG_MUSG	P	24	2way	771	769	99	770	1	385	1066	0	1.6	ptg etg		0	0	
-> testoh1a11a	-> testoh1a11x	x18	TG_MUSG	P	24	2way	795	793	99	794	1	397	1100	0	1.6	ptg etg		0	0	
-> testoh1a11a	-> testoh5e4x	x26	TG_MUSG	P	24	2way	604	602	99	603	1	301	834	0	1.6	ptg etg		0	0	
-> testoh1a11a	-> testohew10x	x32	TG_MUSG	P	36	2way	508	506	99	507	0	169	467	0	1.6	ptg etg		0	0	
-> testoh1a11a	-> testoh1a11x	x38	TG_MUSG	P	24	2way	532	530	99	531	1	265	734	0	1.6	ptg etg		0	0	
-> testoh5e7a	-> testoh5e5a	034	TG_MUSG	P	100	2way	52	2	3	6	6	0	123	0	11.0	rr via ptg		0	0	
-> testoh5e7a	-> testoh5e4x	x06	TG_MUSG	P	100	2way	52	2	3	6	6	0	123	0	11.0	ptg etg		0	0	
-> testoh5e7a	-> testohew10x	x12	TG_MUSG	P	100	2way	52	2	3	6	6	0	123	0	11.0	ptg etg		0	0	
-> testoh5e7a	-> testoh1a11x	x18	TG_MUSG	P	100	2way	52	2	3	6	6	0	123	0	11.0	ptg etg		0	0	
-> testoh5e7a	-> testoh5e4x	x26	TG_MUSG	P	100	2way	52	2	3	6	6	0	123	0	11.0	ptg etg		0	0	
-> testoh5e7a	-> testohew10x	x32	TG_MUSG	P	100	2way	52	2	3	6	6	0	123	0	11.0	ptg etg		0	0	
-> testoh5e7a	-> testoh1a11x	x38	TG_MUSG	P	100	2way	52	2	3	6	6	0	123	0	11.0	ptg etg		0	0	
-> testoh5e7b	-> testoh5e5a	034	TG_MUSG	P	75	outg	100	1	1	0	15	0	22	0	0.8	rr via ptg		0	0	
-> testoh5e9a	-> testoh1a8a	015	TG_MUSG	P	100	2way	4	2	50	6	0	0	32	0	20.4	ptg etg	50	0	0	
-> testoh5e9a	-> testoh5e5a	016	TG_MUSG	P	100	2way	5	2	40	6	0	0	32	0	18.1	ptg etg	33	0	0	
-> testoh5e9a	-> test5e6ofc	0001	TG_MUSG	P	100	2way	10	2	20	6	0	0	32	0	11.6	ptg etg	12	0	0	
-> testoh5e9a	-> testoh5e4x	x06	TG_MUSG	P	100	2way	52	2	3	6	6	0	32	0	2.9	ptg etg	2	0	0	
-> testoh5e9a	-> testohew10x	x12	TG_MUSG	P	100	2way	52	2	3	6	6	0	32	0	2.9	ptg etg	2	0	0	
-> testoh5e9a	-> testoh1a11x	x18	TG_MUSG	P	100	2way	52	2	3	6	6	0	32	0	2.9	ptg etg	2	0	0	
-> testoh5e9a	-> testoh5e4x	x26	TG_MUSG	P	100	2way	52	2	3	6	6	0	32	0	2.9	ptg etg	2	0	0	

Table number: 1

Details pages

Overview

Selecting any of the underlined items in a container page often returns a details page for that item.

- If you click on a near end or far end element name, you will get a details page for that network element.
- If you click on a trunk group suffix, you will get a details page for that trunk group.

You may also access details pages by clicking on the appropriate launch page or navigation link.

Details pages show reference data for the network element or trunk group, together with trend data for previous data collection periods.

> **Reference:** See "Web User administration" (p. 3) for more information about setting data collection trend periods.

Figures

Figure 8 shows a trunk group details page, and Figure 9 shows a network element details page.

Figure 8 Trunk Group Details page

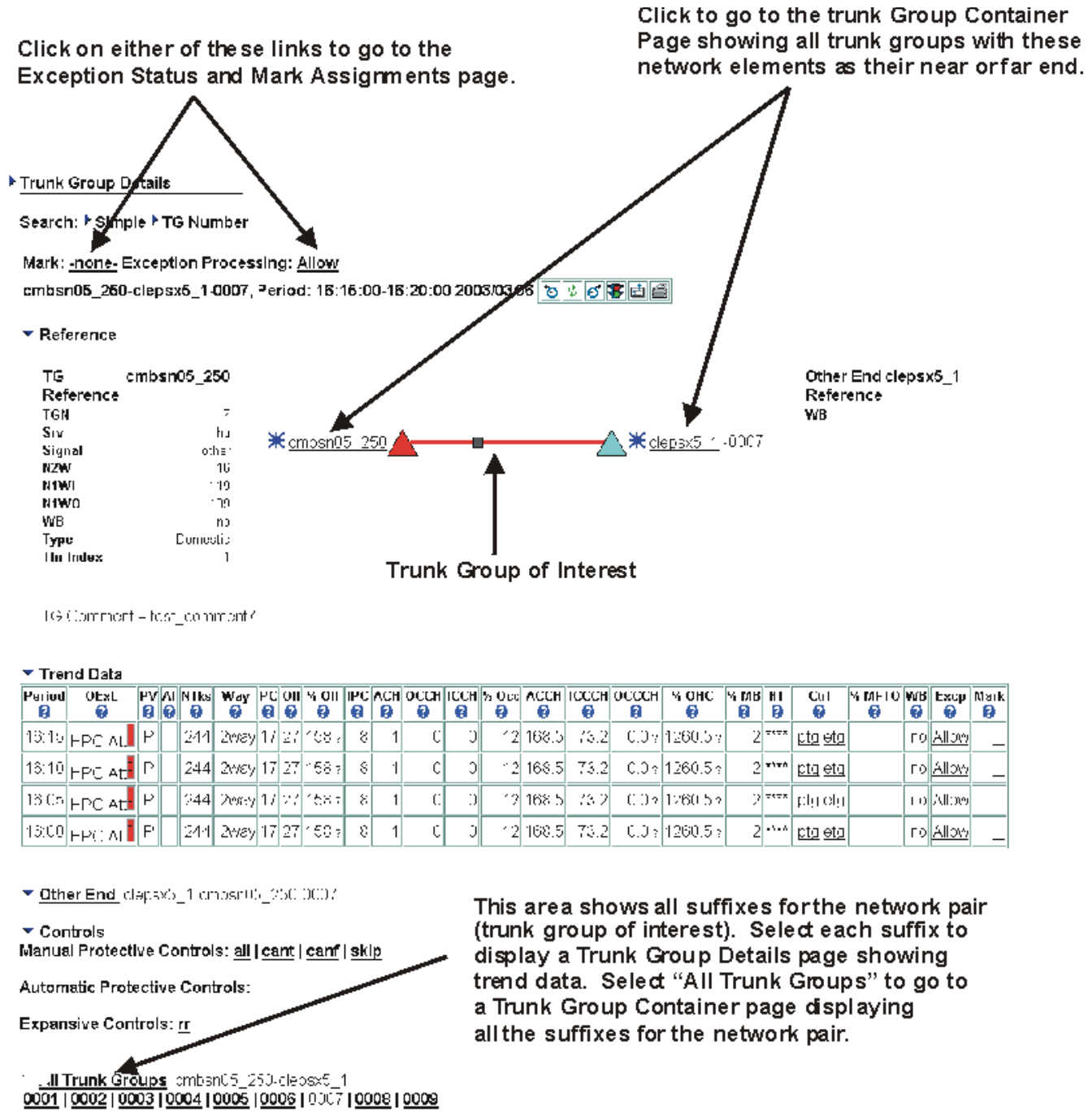
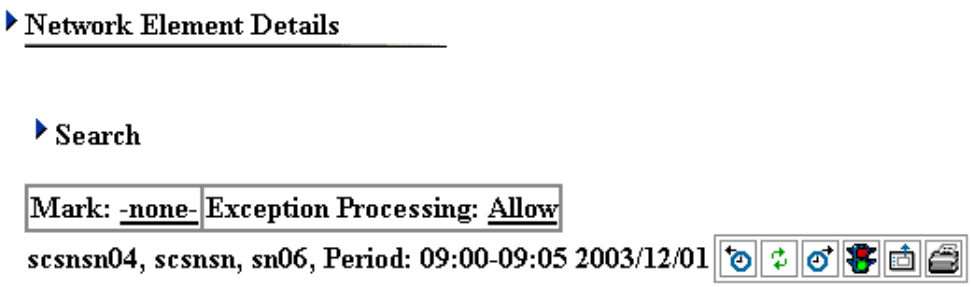


Figure 9 Network Element Details page



Network Element Details

Search

Mark: -none- Exception Processing: Allow

scsnsn04, scsnsn, sn06, Period: 09:00-09:05 2003/12/01

Reference:

Discretes:

Control Counts:

Period	Code Canc	MTG Skip	MTG Canc	RR Att	Fail To RR	RR Succ	DPTPRI Canc	DPTRES Canc
09:00	60	20	50	45	40	5	196609	1
08:55	60	20	50	45	40	5	196609	1
08:50	60	20	50	45	40	5	196609	1
08:45	60	20	50	45	40	5	196609	1

Machine Activity:

Delayed Readiness:

Machine Congestion:

Ineffective Machine Attempts:

% Occupancy:

Service Switching Point:

Traffic Load:

GET Service:

Multi-Service Gateway MNATM:

Multi-Service Gateway MNATMA1:

Multi-Service Gateway MNATMVC:

Multi-Service Gateway MNATMA5:

DPT Reservation:

DPT Max TID:

Related Links:

Hidden areas

The hidden areas on the Network Element Details page (indicated by the right-pointing arrows) hold trend data tables relating to the types of information listed. For example, if you click on “Control Counts”, you will get a data table showing control counts for this switch for the last four data collection periods.

Trend pages

Overview

Trend pages are available if you have purchased Feature 385, “Trend Analysis” This Feature provides a means to graph certain data over a defined period of time. This allows the network manager to graphically see measurements for a specific set of controls, network elements, or trunk groups, and how they varied during a particular time interval. Also, the user can see a graph for a specific measurement compared among network elements or trunk groups. These capabilities enable the network manager to monitor an event and follow its progress in order to more fully understand the effects of controls and know how to take corrective action.

This feature retrieves current or historical data for a specific period of time, and presents the data graphically and in summary tables. If the period of time (trend window) includes the current data collection period, the page can automatically update every five minutes.

Important! The pages will fail to retrieve data correctly if the database boundary is crossed in the trend window.

CAUTION

Large unrestricted trend searches, such as open ended trunk group trend searches, can result in a degradation in system performance. These searches can take several minutes to complete and may prevent other searches performed during the trend search from completing, or may result in blank GUI retrievals.

Trend displays

The user can define the number of trend rows for certain pages. Values can vary between 3 and 40. Some trend pages however have a predetermined number of rows.

Important! A detailed data table, resulting from a trend search, displays 25 rows of data, although the graph reflects the complete individual data, or aggregated data requested from a trend request.

Page elements

The Trunk Group Trending display shows a:

- Graph
- Maximum Data Table

- Summary Data Table
- Detailed Data Table

All of the tables can be sorted by a particular column by clicking on that column heading.

GUI displays having trending include:

- Packet Links
- Code Control Page (Call Gap)
- Network Element (Measurements)
- Reroute Expansive Trunk Group Controls (Reroute).
- Trunk Group

Important! For trending purposes, calculation shown as percentages will be averaged not summed.

GUI form elements

Overview

This section describes the elements that may appear within a form on a web page. Form objects consist of a label and one or more fields when they are used outside a table.

Required fields are indicated by an asterisk (*) to the left of the label.

All the forms in the NTM GUI are built from some combination of these objects.

Table 2 Form elements and descriptions

Element	Description
Menus	A single item may be selected at a time
Lists	Depending on the list, one or more items may be selected at a time
Text Fields	A text field consists of a box into which values such as *CLLI* codes or network element names may be entered.
Range Fields	The range field is similar to the text field, but it allows only numeric input. Valid input for a range field is limited to numbers and the decimal character (.)
Refine Button	Allows use of regular expressions to find network elements or set names. **Reference: Reference:** Appendix 10, "Searching using Modifiers and Regular Expressions"
Checkboxes	Clicking the box to the right of the label selects that option. For objects offering multiple options, multiple checkbox choices appear to the right of the label. Each choice has an additional label to its right.
Radio Buttons	Multiple radio button choices appear to the right of the label. Each choice has an additional label to its right. The choices are mutually exclusive; only one may be selected.
Submit Button Execute Button Search Button	Used to submit requests to the web server.
Reset Button	Used to reset the form objects back to the values they contained when the web page was last loaded. It is always labeled "Reset".
Composite Elements	Other form elements are a composite of the basic elements described above. For example, the Period field consists of four menus, and the Data Restriction field is made up of two menus and a range field.

Output element types

Overview

An output object consists of some combination of text and graphics. A label may also appear with the object when it is used outside a table. Inside a table, the column header serves as the label and the objects appear directly within the cells. Output elements also include Alarm/discrete indicator and Overall exception level indicator.

Alarm/discrete indicator

A square is used to indicate that an alarm is active or a discrete is on. The color of the square indicates the level associated with the alarm or discrete. Table 3 shows the colors that correspond to various alert/alarm and discrete levels

Table 3 Threshold and discrete alert/alarm level visual indicators

Threshold Level	Visual Indication
0	None
1, 2, 3	**(Cyan)**
4, 5, 6, 7	**(Yellow)**
8, 9, 10	**(Red)**

A user preference setting allows an alternate visual indication of the threshold level mapping for tabular displays. The alternate method colors the background of the corresponding table cell according to the threshold level mapping described above.

Active discrete indicator

The number 5 inside a circle is displayed, next to the discrete level indicator, to indicate when a discrete has been active within the last five minutes. This indicator is not shown when the trend option is selected.

Overall exception level indicator

The overall exception level (OEXL) object (Table 4) displays the data field that has the highest exception level for the data type being displayed and a threshold level indication.

When the OEXL object appears in a tabular format, sorting is performed according to the highest OEXL in exception fields.

The indicators shown in Table 4 display the exception level by using incremental values defined in Table 3. For example, if a data count has an exception with a value of 5, the indicator will be yellow and will be expanded to the second indicator level.

Table 4 Overall exception level output element

OEXL
 OFL
 %OFL
 PC

Hiding/showing an area

Overview

To save screen space, you may hide an area of a display (e.g., the Search area or Navigation area). The area may be shown again to access the data or functionality contained within it. The user can select whether to show or hide the navigation links by default.

Reference: "Web User administration" (p. 3)

A down-pointing arrow (Figure 10) indicates an area is shown and may be hidden. Selecting the down-pointing arrow will hide the area (remove it from the display). All display content below the area is shifted up or to the left to fill the space that is freed.

Figure 10 Arrow indicator: area is shown and may be hidden

A right-pointing arrow (Figure 11) indicates an area is hidden and may be shown. Selecting the right-pointing arrow will show the area, allowing you access to all the information and functionality contained within it. All display content below the area is shifted down or to the right.

Figure 11 Arrow indicator: area is revealed

Toolbar area

Overview

A toolbar (Table 5) is shown on several web pages. It can be associated with a specific table or with the entire frame. The toolbar consists of several symbols. Each toolbar may not contain every symbol; it will contain only the symbols relevant to the page.

A toolbar is:

- a horizontal group of one or more symbols
- usually located to the right of a table title, or to the right of the text that identifies the instance object and the data collection period

You can perform an action for each of the symbols in the toolbar.

Tooltips

For any toolbar symbol, holding the cursor on the symbol for a few moments will display a “tooltip” help message that tells you what the toolbar item does.

Toolbar functions

The toolbar can consist of various combinations of the following items in Table 5.

Table 5 Toolbar icons (Sheet 1 of 2)

Icon name	Icon	Description
New		Allows for addition of information. On network views nodes, text and timestamps can be added.
Previous Period		Changes current page to show previous data collection period.
Current Period		Changes to current period.
Next Period		Changes current page to show the next data collection period. When a page is retrieved using the “current” period, the next button merely refreshes the current period.
Auto-update		By selecting this icon, the user enters Auto-update mode. The Previous Period and Next Period icons will no longer be displayed. By selecting this icon a second time, the user leaves Auto-update mode. The Previous Period and Next Period icons will again be displayed.

Table 5 Toolbar icons (Sheet 2 of 2)

Icon name	Icon	Description
Select All		Selects all choices in a list.
Clear All		Clears all choices selected in a list.
Projection Mode		Clicking this icon opens another browser window showing only the display without any of the browser buttons.
Save		Saves all modifications to map and node reference data and selections from the Settings toolbar function.
Show Alerts		Launches the Network View Alerts window restricted to all alerts for this Network View.
Settings		This toolbar icon has the following sub-options: • Show All Nodes: Toggle to show all nodes or only nodes with alerting information. • Node Size: The selected size is indicated by a check mark. The default is 0. • Font Size: The selected size is indicated by a check mark. The default is 0. • Line Size: The selected size is indicated by a check mark. The default is 0. • Line Angle: The selected size is indicated by a check mark. The default is 0.
CSV Display		This toolbar icon presents the data on the page in Comma Separated Value (CSV) format. The output can be saved in this format and used in other applications that allow the use of CSV formatting.
Format to Print		Launches a browser window without any titles or search parameters to allow the maximum printing area.
New Table Layout		This button opens the New Table Layout page in a new window. Every changes will be applied for the page it was executed.
Edit Table Layout		This button opens the Table Layout page in a new window. You can edit the selected Table Layout and after submitting apply it on the page it was executed.

Error presentation

Overview

The NTM GUI presents error messages in response to conditions such as improper permission, execution errors, etc.

In some instances, if a user does not have permission to execute a function the system may appear to allow access to that function; however, the system will not perform the requested operation. For example, if a user does not have permission to assign controls, control options still may be visible but controls will not be applied.

If initiating a map or page exceeds either the user limits or the system limits described in Chapter 5, "Thresholds" in the *System Overview*, an error message is displayed indicating the capacity that was exceeded.

> **Reference:** See the limitthr command (5-37) in the *Input Commands Guide* for more information regarding system constraints on the system.

System errors

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.

- The layout includes the Navigation frame, Common frame, and Viewer Frame.
- The Navigation frame contains the standard set of links and a link to the Error Log display.
- System errors are displayed in the viewer frame.

Execution errors

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). These errors are handled in such a way that you can recover and attempt the request again. The following indicates the occurrence of an execution error:

- A graphical failure indicator (red X) appears on the page.
- The error message appears at the bottom of the web page Viewer frame, separated from the rest of the page content by a horizontal bar.

> **Reference:** Figure 3, "Code Control Request page: Failed control request" (p. 5)

Other errors

Capacity errors, display limit errors, and form validation errors are presented in the same way as System errors.

Host user ID selection

Overview

A browser-based GUI user ID may map to multiple user IDs on an NTM host. Allowing multiple user IDs on the host for a single GUI user ID allows you to access different capabilities and different views of the network, depending on your job function. A default host user ID can be set through your Web User Administration display, and the default may be overridden on displays that provide a Search capability.

Examples

For example, you may override the default host user ID setting on an execute or per-retrieval (Search) basis by selecting from a list of host user IDs in the Search area. This list is limited to the host user IDs that apply to the NTM host from which the page was served.

□

Manual/automatic update

Overview

There are some differences between the manual and auto-update modes for periodic data access.

Toolbar area

The Previous Period, Next Period, and Auto-update icons appear only in manual update mode. The Stop Auto-update icon appears only in auto-update mode. When switching between modes, the toolbar is reconfigured to display the appropriate icons.

Search area

The search criteria may be changed only in manual update mode. In auto-update mode, the search criteria are displayed as output only.

In auto-update mode, all changes to the page display mode (e.g., hide/show areas, hide/show navigation frame) and data presentation (e.g., sort order) are maintained across the updates.

A web page in auto-update mode continues to update automatically if it is restarted or reloaded by the browser (e.g., using the reload button). If the user chooses to move to another page and returns to the page that was running auto-update, the page will need to be reloaded in order for auto-update to resume. In this case, the user could choose to view the related page by opening it in another window.

Auto/Manual update mode status is not passed on links between web pages.

A web page that is bookmarked in auto-update mode will automatically begin to update when it is loaded.

New data indicator

When a page is in auto-update mode, a new data indicator appears on the page at the beginning of a new data collection period.

If you are in auto-update mode, and a stop/start is performed on the system, you must use Shift-Reload to refresh the page. The indicator changes from green to yellow after about 2 minutes.

Figure 12 New period indicator

Detached execution

Overview

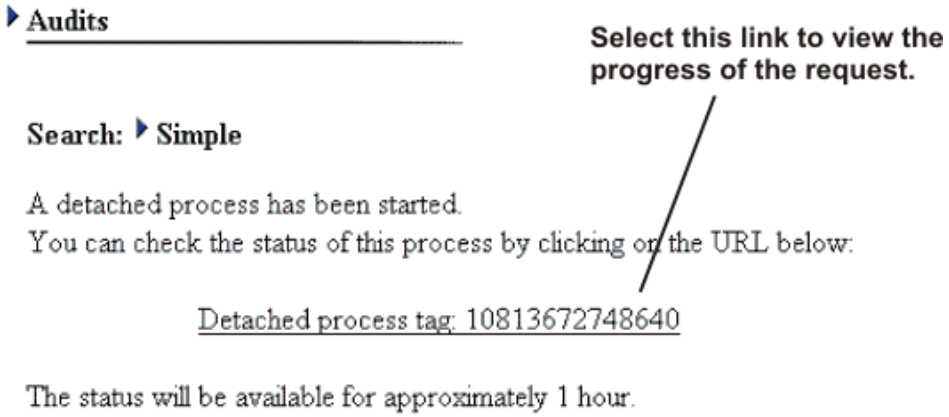
When using certain functions of the GUI, such as audits, it is better to perform them in a detached execution mode. Detached execution mode allows you to perform other tasks in the browser session while a long running operation runs “in the background” on the NTM host.

The user has the option to execute controls in the current window or in the detached mode by selecting the associated button. Audits must always executed in detached mode.

View the progress of a detached function

After a detached execution request has been issued a response page is presented indicating a detached process has been started. This page also presents a web browser link that can be selected to view the progress of the request. The link can be select repeatedly, or even stopped and started, without effecting the running operation on the NTM host. Errors from this background operation will be shown on the browser page showing the status of the request and via email as defined in the “Results of a query” (p. 32).

Figure 13 Detached execution response page



Time constraints for detached execution

The total amount of time the status of a detached operation will be allowed to run is 24 hours. Additionally after the detached operation ends, for any reason, the status output will be available for one additional hour.

Results of a query

The results of executing a request using detached execution can be emailed to one or more email addresses. To use the email function it requires email addresses be defined in the web administration section for the Web user that is running the operation.

Important! It is recommended that users define at least their own email. This will allow results from failed operations to be emailed to the person requesting the information.

Reference: See "Web User administration" (p. 3) for more information about setting user email addresses.

□

Comma separated value formatting

Overview

NTM provides the ability to present data retrieved from the GUI in Comma Separated Value format (CSV). By selecting the CSV icon on the toolbar, the results of the container page you are viewing are presented in CSV format. Normal browser behaviors apply to the icon such as “Open in new window” or “Save Link Target as”, etc....

Unlike the NTM GUI, which formats large search results into segments, the CSV value displays all the search results in a single output file. Fields with garbage data displayed by using ****, or that are empty, will have a comma separation in the output file. Although fields with textual hyper links to other GUI pages will have a comma separation, the hyper link itself will not be included in the output file. The CSV is a text file, and as would be expected, does not show exception indicators.

NTM allows you to select different ways to view data retrieved on the NTM GUI such a Exception List or Data Table. However, the CSV output will allocate a space for the fields not shown by using coma placeholders for the CSV output.

To import files into other programs that were saved in NTM using the CSV format, select “Comma Separated/Comma Delimited” as the file type.

Online Documentation

Overview

NTM provides users with the entire set of documentation online through the GUI. Select the Documentation button on the left side of the screen to view a list of documents. There is an extensive HTML search capability available to search all or specific parts of the documents for information.

Important! The documentation button is available only from the full screen view of the GUI. If users hide the links on the left (original skin) or the tabs across the top of the GUI (8920 NTM tab skin) then the Documentation button will not be seen.

Using the search function

Instructions

Follow these steps to use the search function of the browser-based GUI:

1 Select the desired search type.

2 Fill in the form objects on the Search page.

3 Retrieve data by clicking the Search button. Searches may be bookmarked for future use.

END OF STEPS

2 Network Elements

Overview

Purpose

This chapter contains information about the network elements page and its components.

Contents

This chapter contains the following topics:

Network elements	2-3
Audits	2-19

Network elements

Overview

Purpose

This section discusses the Network Elements page and its components.

Contents

This section contains the following topics:

Network element data types	2-4
Network Elements data search page	2-5
Network Elements container page	2-8
Network Element Details page	2-11
Network Elements Trend Analysis page	2-15

Network element data types

Overview

The Network Elements object represents circuit switches and packet elements. The search form changes as you move from one category to another. This chapter describes the pages that are used to retrieve and display network element data.

The data categories can vary depending upon which NTM features have been purchased:

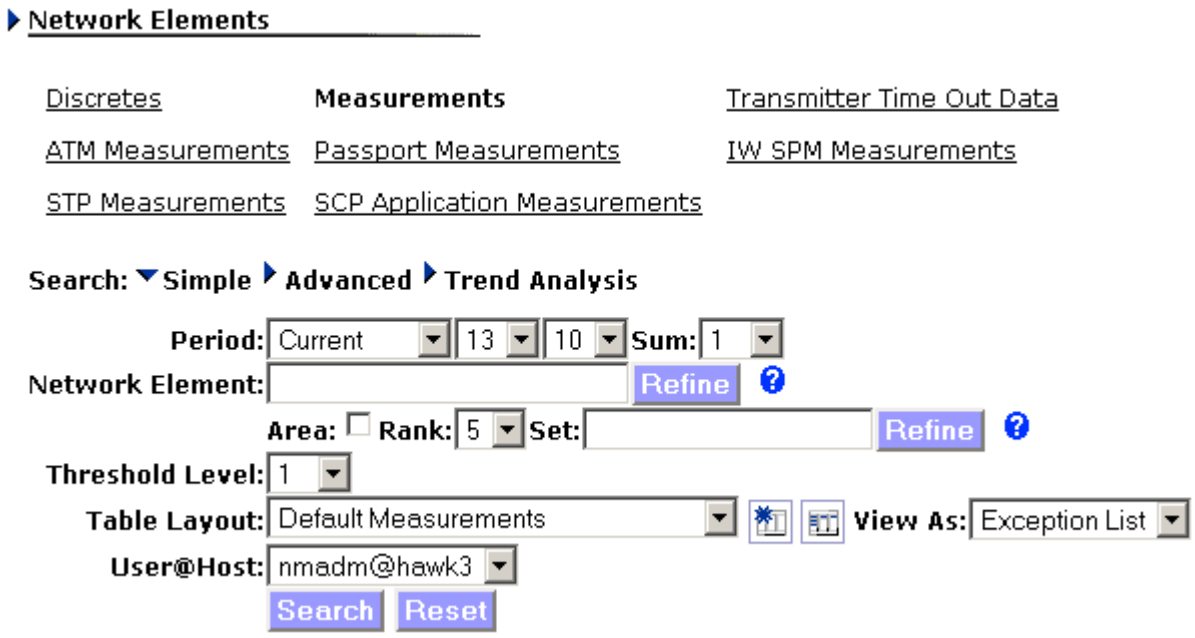
- Discretes (network element discrete data)
- Measurements (network element data counts)
- Transmitter Time Out Data (Inter-office carrier information)
- ATM Measurements
- Passport Measurements
- IWSPM Measurements
- STP Measurements
- SCP Application Measurements
- Network element trend page (shown on a separate display)

Network Elements data search page

Purpose

The Network Elements search page allows the user to restrict the retrieved data based on various attributes of a network element. Figure 1 shows a Network Elements search page for Measurements information.

Figure 1 Network Elements data search page



Search criteria

Table 1 describes the search criteria that can appear in the Search area. The first item in the list is the name of the network element. Items to the right of the network element name represent data fields in exception, with the left data field having the highest threshold level. Information cannot be sorted and data field definitions are not available from the Exception List view.

Table 1 Search criteria for network elements (Sheet 1 of 3)

Label	Description
Period	Data collection period. Includes Sum field. **Important!** When selecting period, you must select a period other than "current" to retrieve any historical data. Even though a given day may be listed in period choices, all 24 hours of data may not be available since the system may have been stopped for a time.

Table 1 Search criteria for network elements (Sheet 2 of 3)

Label	Description
Session	Historical session ID. This field is available with Feature 342, "Historical Data Playback for the Browser-based GUI"
Network Element Area Rank Set	Near end network view. Valid values include all internal network elements.
Type	In advanced search mode, allows you to select a specific type of switch on which to retrieve measurements.
OM Type	On ATM Links searches for Succession sn06+ offices, this option allows the user to select the type of office measurement data desired for a ATM4k office.
Component	On Passport Measurement searches for Succession sn07+ offices, this option allows the user to select the component type to restrict the search. The options are Shelf or Card/Fabric.
Threshold Level	Maximum threshold level. Valid values are: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10. Restriction is always >=. With Feature 415, "Browser-based Access to NetMinder Signaling Traffic Management (STM) data" the STM thresholds are (L) low, (M) Medium, (H) High.
Data Restriction	The two data restriction fields allow you to retrieve data based on values for up to two measurements. For example, you may set these fields to: For example, you may set this field to: `CALL_ATT > 20 AND %Line Busy > 50` Only those network elements having measurements matching this data restriction will be retrieved. You may use one, both, or neither of these fields.
Status	STM signaling link status
Exception Processing	NONE, ALLOW or INHIBIT
Subsystem	STM defined subsystem
Threshold Set	STM defined threshold set

Table 1 Search criteria for network elements (Sheet 3 of 3)

Label	Description
Mark	Marked Alarm status. Valid values are: • Default None • ACK • AIP • User-defined **Reference:** ***Reference:*** "Exception Status and Marked Assignments" (p. 21)
Suspect Data Filter	This field allows the user to choose to display Suspect data. **Important!** This is valid when Feature 74, "Improved Filtering and Reporting of Data" is purchased and activated. **Reference:** ***Reference:*** "Filter File" (p. 25) in the *Record Base Administration Guide*
Trend	Displays discrete trend data. Default is off.
Active Number	When this pickbox is selected a column is added showing the number of discretes per network element.
Show	In advanced search mode, for the Discretes option, the user can allow data to be displayed during the trend display. **Important!** Default is "only on now". In this mode, an office will not be listed if there are no active discretes, even if there were exceptions in the previous data collection periods.
Display Limit	Small, medium, or large limit for data retrieval. • Small: 100 rows • Medium 600 rows • Large: 1200 rows • XL: 1500 rows
Table Layout	Table layout choices. The valid choices are limited to table layouts that apply to the valid network element data types.
View As	Selection to view the data as a table or as a list of exceptions. Data Table view shows all the data fields for a given table layout whether or not the data field is currently in exception. Information can be sorted based on columns and data field definitions available. Exception List view populates only those fields currently in exception.
User@<*Host*>	Choice of user IDs on a specific host machine.

Network Elements container page

Purpose

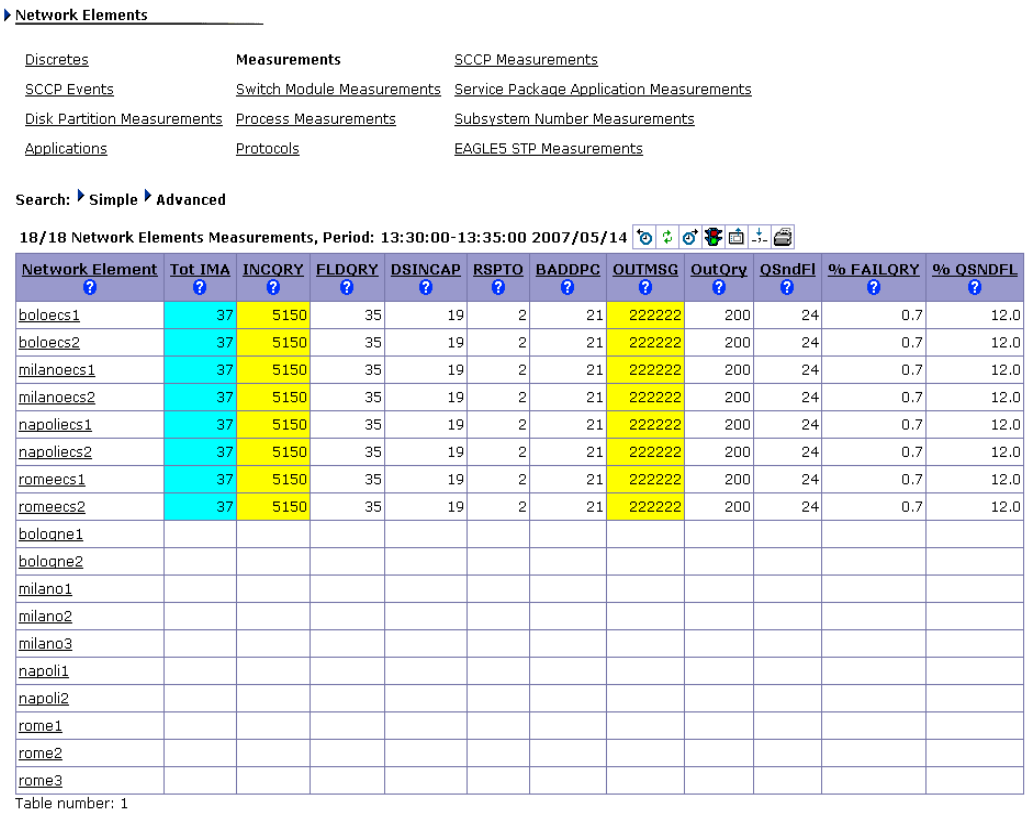
The Network Elements container page displays the results of a search in tabular format. The Network Elements container page supports manual update, automatic update, and historic access (except for Discretes). The frequency of the update is based on the data type being displayed: 5-minute or 30-second.

For the Measurements type (default), the Network Elements container page will display data in Data Table view (Figure 2) or Exception List View (Figure 4), depending on the user's choice on the Network Elements search page. Trending information is also available with the purchase of Network Elements Trend Analysis page.

Discretes are not available historically on the container page. If you select the Discrete data type, the period is always set to Current upon the execution of the search.

Reference: Figure 3, "Network Elements container page: Data table view for discrete data" (p. 9)

Figure 2 Network Elements container page: Data table view



Network Elements

Discretes	**Measurements**	SCCP Measurements
SCCP Events	Switch Module Measurements	Service Package Application Measurements
Disk Partition Measurements	Process Measurements	Subsystem Number Measurements
Applications	Protocols	EAGLE5 STP Measurements

Search: Simple Advanced

18/18 Network Elements Measurements, Period: 13:30:00-13:35:00 2007/05/14

Network Element	Tot IMA	INCQRY	FLDQRY	DSINCAP	RSPTO	BADDPC	OUTMSG	OutQry	QSndFl	% FAILQRY	% QSNDFL
boloecs1	37	5150	35	19	2	21	222222	200	24	0.7	12.0
boloecs2	37	5150	35	19	2	21	222222	200	24	0.7	12.0
milanoecs1	37	5150	35	19	2	21	222222	200	24	0.7	12.0
milanoecs2	37	5150	35	19	2	21	222222	200	24	0.7	12.0
napoliecs1	37	5150	35	19	2	21	222222	200	24	0.7	12.0
napoliecs2	37	5150	35	19	2	21	222222	200	24	0.7	12.0
romeecs1	37	5150	35	19	2	21	222222	200	24	0.7	12.0
romeecs2	37	5150	35	19	2	21	222222	200	24	0.7	12.0
bologne1											
bologne2											
milano1											
milano2											
milano3											
napoli1											
napoli2											
rome1											
rome2											
rome3											

Table number: 1

Figure 3 Network Elements container page: Data table view for discrete data

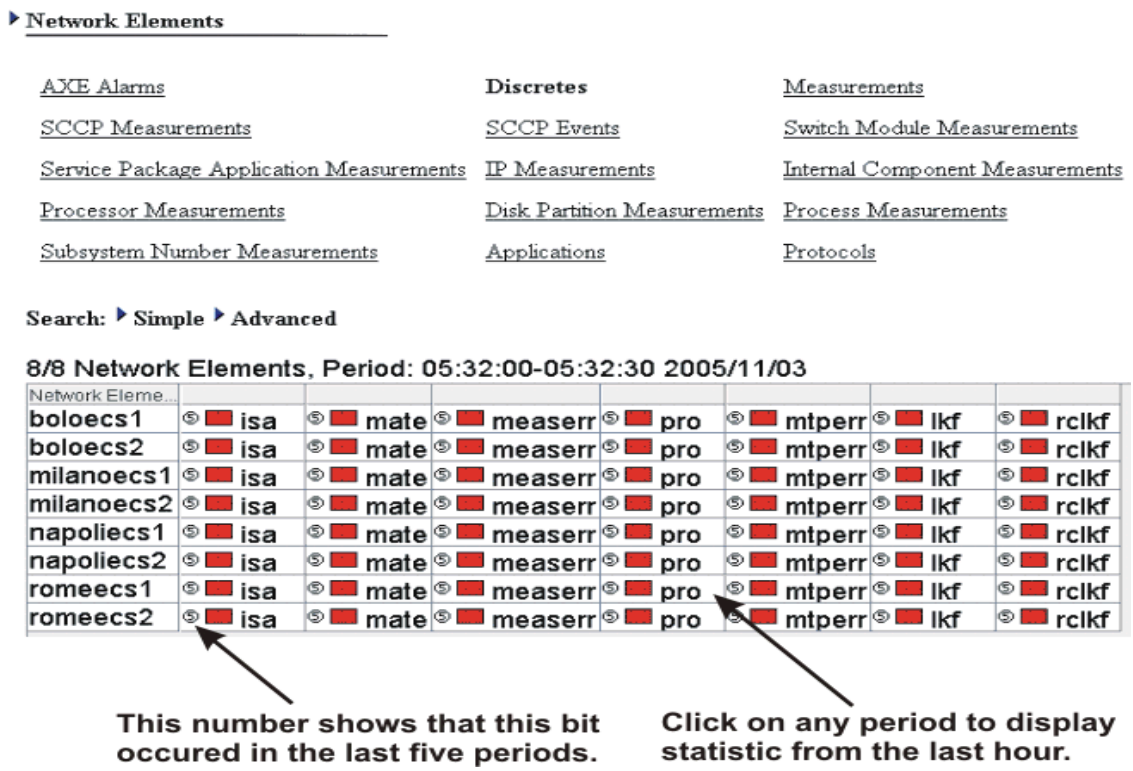
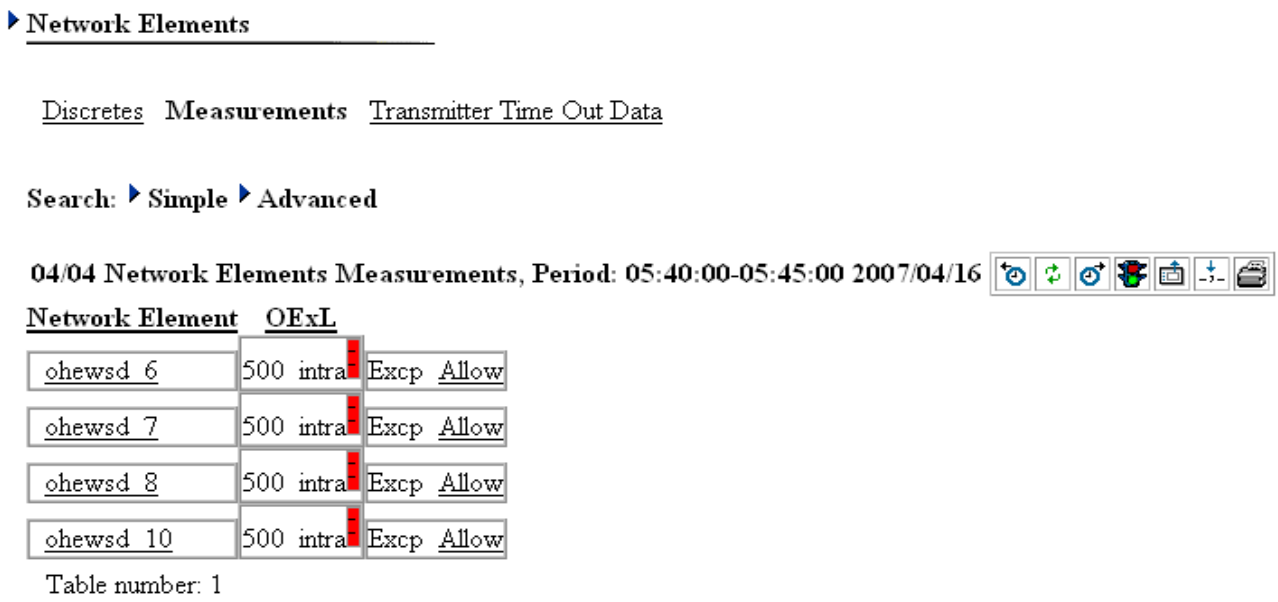


Figure 4 Network Element container page: exception list view



Page components

Column headings displayed for the Exception List view are:

- Network Element
- OEXL
- Any fields in exception

By default, the rows of the Exception List view are sorted on the OEXL column, highest to lowest.

Discretes are colored using the values:

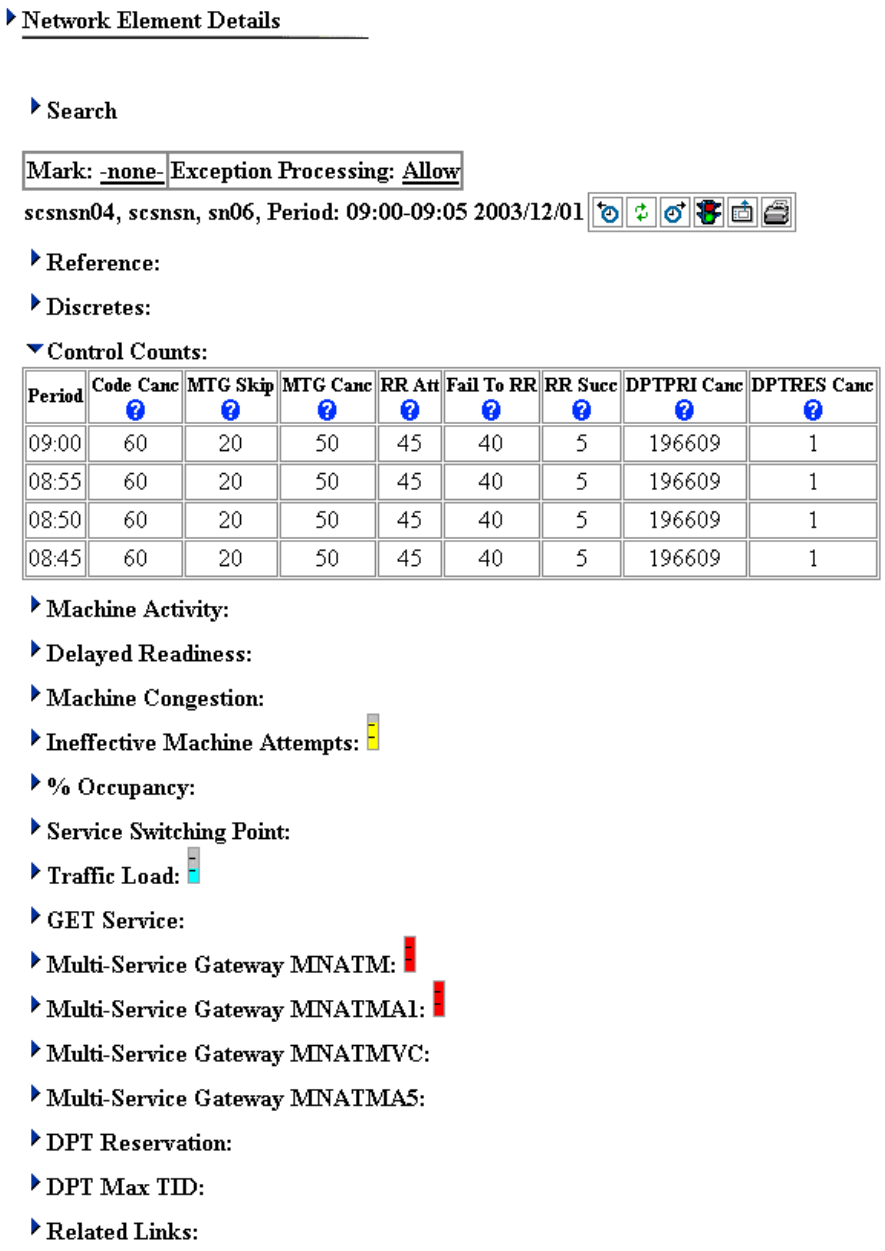
- Red — exception levels 8, 9,10
- Yellow — exception level 4, 5, 6, 7
- Cyan — exception level 1, 2, 3
- Gray — exception level 0
- Blank or empty — for previous period discretes

Network Element Details page

Purpose

The Network Element Details page displays information about a particular network element. The data shown on the page will vary depending on the type of network element. Figure 5 shows an example of the Network Element details page.

Figure 5 Network Element Details page



Network Element Details

Search

Mark: -none- Exception Processing: Allow

scsnsn04, scsnsn, sn06, Period: 09:00-09:05 2003/12/01

Reference:

Discretes:

Control Counts:

Period	Code Canc	MTG Skip	MTG Canc	RR Att	Fail To RR	RR Succ	DPTPRI Canc	DPTRES Canc
09:00	60	20	50	45	40	5	196609	1
08:55	60	20	50	45	40	5	196609	1
08:50	60	20	50	45	40	5	196609	1
08:45	60	20	50	45	40	5	196609	1

Machine Activity:

Delayed Readiness:

Machine Congestion:

Ineffective Machine Attempts:

% Occupancy:

Service Switching Point:

Traffic Load:

GET Service:

Multi-Service Gateway MNATM:

Multi-Service Gateway MNATMA1:

Multi-Service Gateway MNATMVC:

Multi-Service Gateway MNATMA5:

DPT Reservation:

DPT Max TID:

Related Links:

Page components

The page is organized into data categories. Some of the categories are:

- Reference (for reference data other than TYPE and GENERIC)
- Discretes (or Alarms)
- Controls (for control summary information)
- ATM link data

- Packet data
- Various categories for measurement data
- Other relevant data for that switch type.

A data category can be hidden and shown. Categories in exception will have OEXL indicators that are visible whether the category is hidden or shown.

Important! The OEXL indicator does not appear for the Discretes category.

The presentation of data depends on which category of data is displayed. Data can be displayed for four periods, with the retrieved period (either current period or a historical period) to the immediate right of the field labels. The next three periods worth of data are displayed to the right. Data with multiple records per network element is displayed for the retrieved period only.

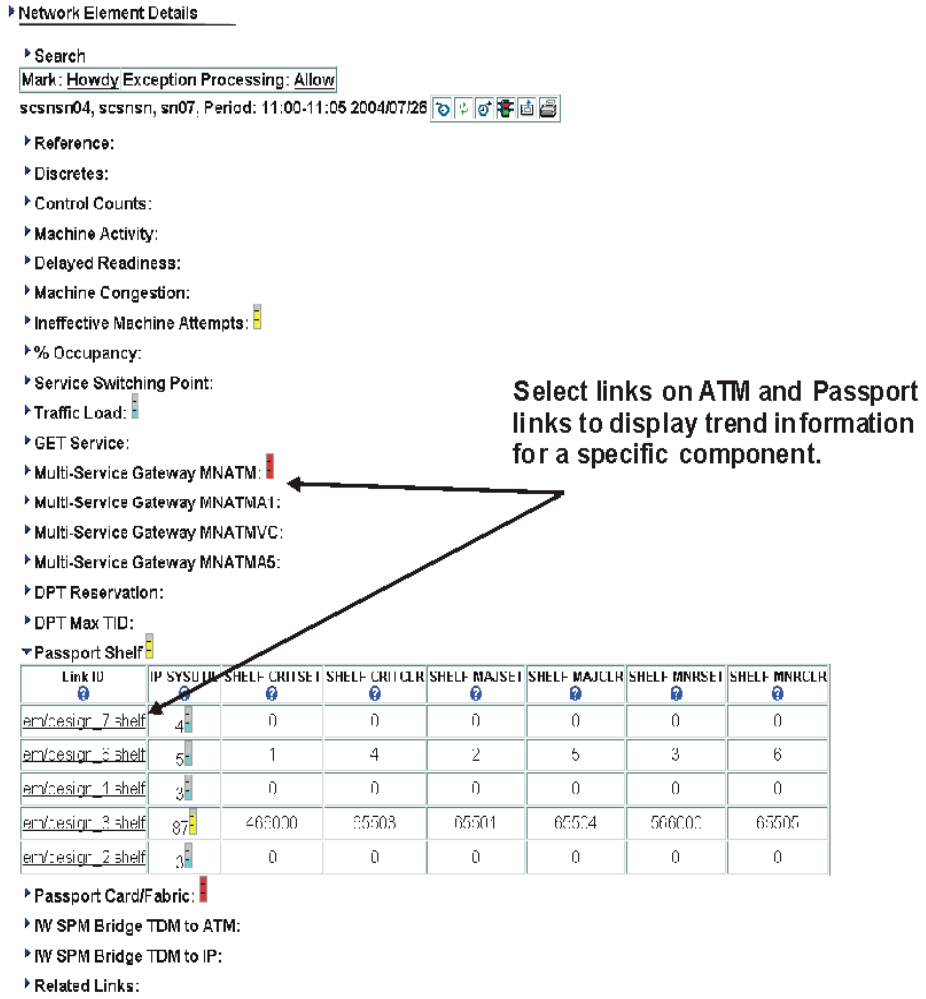
A controls category shows the number of active code controls for that network element.

Discretes are shown with the label of the discrete to the left. Indicators for ten 30-second discrete periods are displayed to the right of the retrieved period's indicator; the right indicator is the one for the "newest" 30-second period.

Component trend links

On some of the ATM and the Passport links (Figure 6), links are provided to show trending information through key information fields. These categories allow the user to view trend data for a specific item from the collection of items found on a detail page.

Figure 6 Trend links on a Network Element Details page



Changing font sizes on the discrete display

The font size is controlled using the browser preferences except when using projection mode. Displays must be removed from projection mode, then fonts can be changed and the display reinitiated in projection mode if desired.

□

Network Elements Trend Analysis page

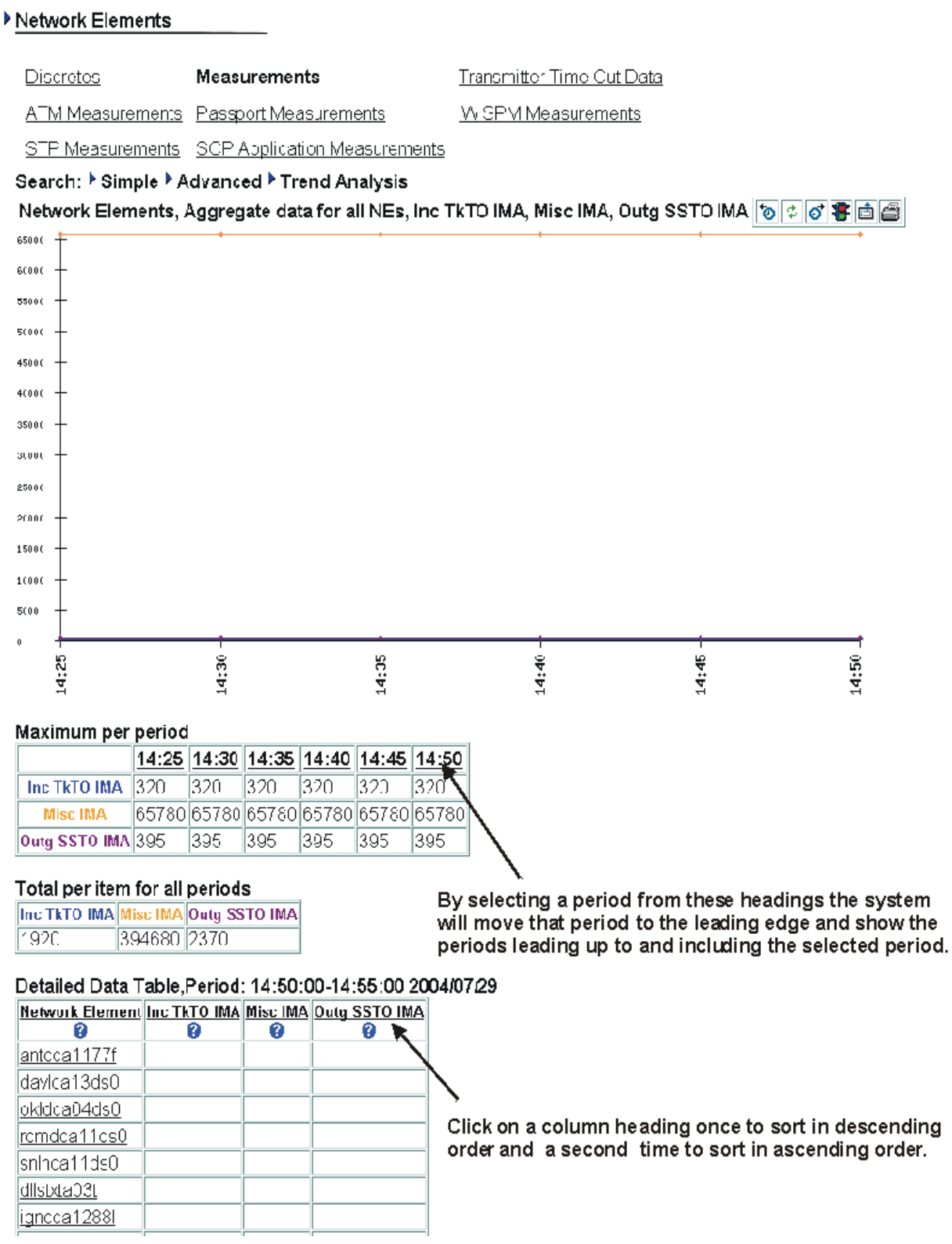
Purpose

The Network Elements trend page is available from the Network Elements — Measurements page if you have purchased Feature 385, “Trend Analysis”.

Reference: “Trend pages” (p. 18)

The Network Elements trend page allows the user to restrict the retrieved data based on various attributes of a network element. Figure 7 shows a Network Elements trend page.

Figure 7 Network Elements — Trend Analysis page



Search criteria

Table 2 describes the search criteria that can appear in the Search area.

Table 2 Search criteria for Network Element trend displays

Label	Description
Period	Data collection period. The default is Current
Network Element Area Rank Set	Near end network view. Valid values include all internal network elements.
Data Fields	**Aggregate data for all Network Elements** Items with multiple counts can be selected from the associated list. **Graph per Network Element** Items with only one data count can be selected from the associated list.
Trend Window	The number of data collection periods to be used in the trend analysis. Options are: 6, 12, 18 or 24 five-minute data collection periods (30 minutes to 2 hours).
User@<*Host*>	Choice of user IDs on a specific host machine.

Audits

Overview

Purpose

This section discusses the Audits page and its components.

Contents

This section contains the following topics:

Background	2-20
Audits search page	2-21
Audit request page	2-23
Audit details page	2-24

Background

Overview

An ***audit*** is an integrity check through which NTM searches both its own and the office's database for differences and corrects them if possible. The audits:

- synchronize the NTM database and the office database
- obtain results that may represent differences in the trunk groups or controls in the NTM and office databases

NTM maintains a database in which all the offices of the supervised network are defined, as well as the data that will be collected from each office, and the status of any controls at the office. The offices each have their own records of data to be sent to NTM and of control status. These records must always be in agreement, so that NTM can receive and process the data accurately. There are two types of audits: regular and schedule. There is a complete description of audits found in Chapter 2, “Commands for Auditing Network Elements” of the *Input Commands Guide*.

The GUI audit interface allows audits to be run more easily with the convenience of having the audit output mailed to users.

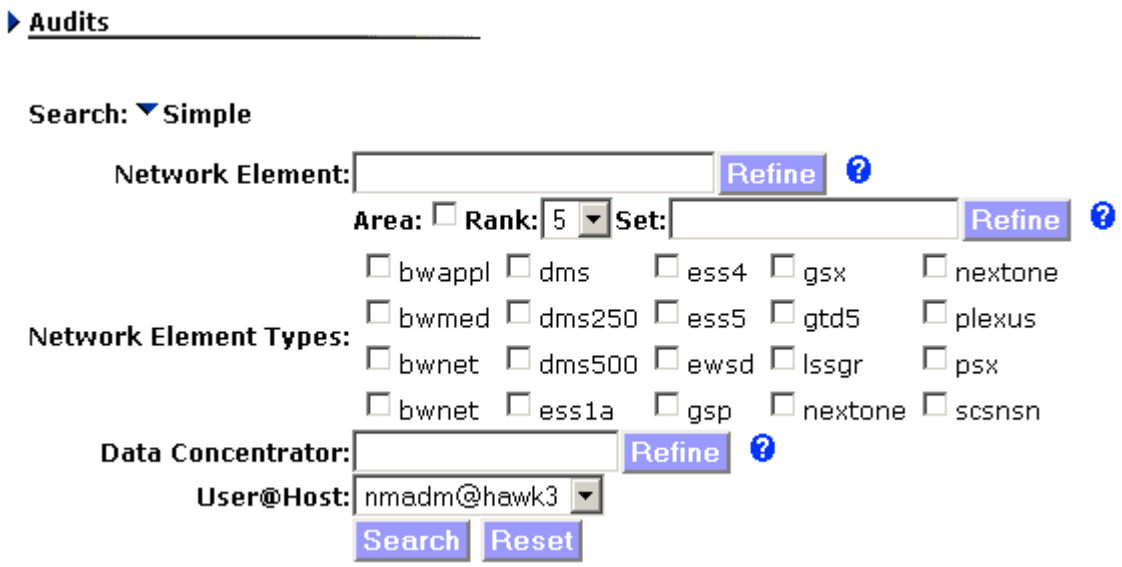
Reference: “Audit types / matrix” (p. 30) in the *Input Commands Guide*

Audits search page

Overview

The Audits search page allows the user to restrict the retrieved data based on network elements, network element types or data concentrators. Figure 8 shows an Audits search page.

Figure 8 Audits search page



Search criteria

Table 3 describes the search criteria that can appear in the search area.

Table 3 Search criteria for Audits

Label	Description
Network Element Area Rank Set	Near end network view. Valid values include all internal network elements.
Network Element Type	Allows you to select a specific type of switch on which to audit. If none is selected then all network elements will be shown.
Data Concentrator	Allows you to select a specific data concentrator and audit all connected network elements.
User@<*Host*>	Choice of user IDs on a specific host machine.

Audit request page

Purpose

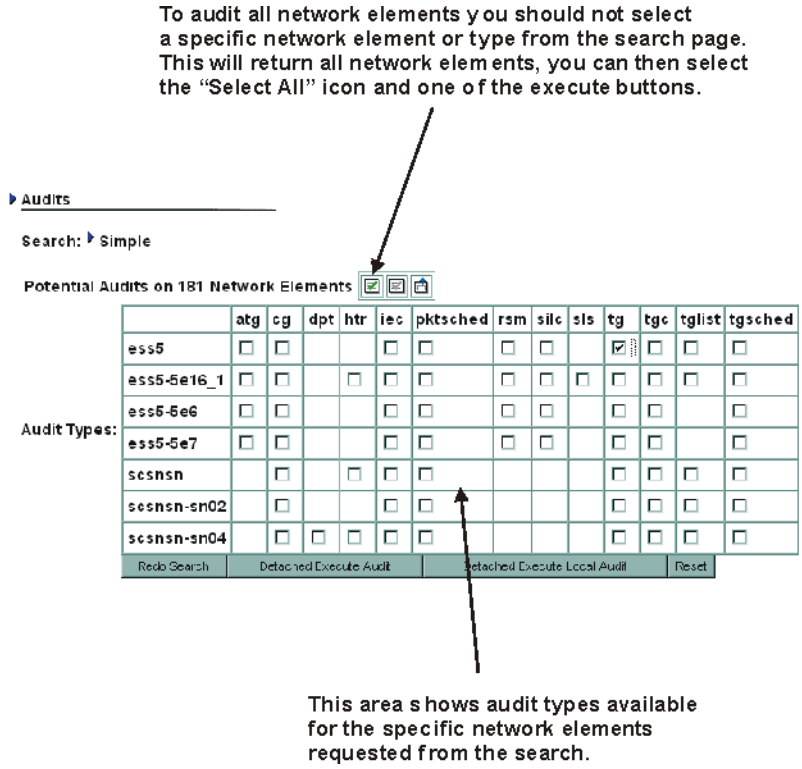
Results of a search are displayed on the Audits request page. This page displays potential audits available for the network element types and generics represented by the specific network elements retrieved in the search. The Audits request page is available on demand and does not automatically update.

The top portion of the page displays audit search request information. The bottom portion of the screen allows you to select appropriate audit types for the network element types/generics resulting from the search. You can select related audits for each network element. Audit types are associated with specific offices and generics.

> **Reference:** See Table 3, “types” (p. 30) in the *Input Commands Guide* for a complete audit list valid for each network element type.

After selecting the desired audits you can then select one of the Detached execute options to start the audit request. Buttons are also available to redo the search using the same search criteria previously defined and to reset the audit selection area of the page.

Figure 9 Audits request page



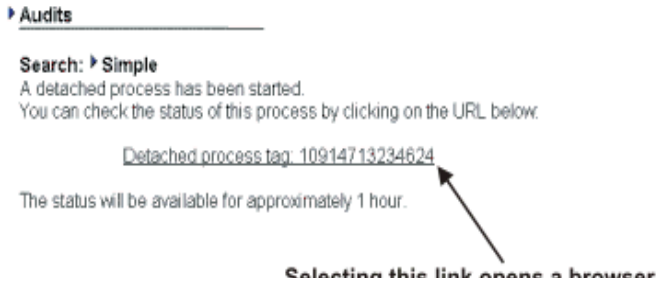
Audit details page

Purpose

The Audit details page (Figure 10) displays information about a requested audit. The data shown on the page will vary depending on the type of network element and audit requested.

Audits are executed through a Detached execution process. To view the status of the audit select the Detached Process Tag shown on the Audit details page. This will open a browser window than can be closed and reselected multiple times to show the progress without affecting the audit. Audit results will be mailed to the user-defined email addresses as described in “Results of a query” (p. 32).

Figure 10 Audits details page



3 Network Connections

Overview

Purpose

The NTM GUI allows you to retrieve data for trunk groups, signaling links, or link sets. You select the type of connection on which to retrieve data from the Launch page.

Contents

This chapter contains the following topics:

Trunk Groups	3-3
Signaling Links and Link Sets (Without Feature 415)	3-19
Signaling Links and Link Sets (With Feature 415)	3-23
Packet Links	3-29

Trunk Groups

Overview

Purpose

This section discusses the Trunk Groups pages and their components.

Contents

This section contains the following topics:

Trunk Groups search page	3-4
Trunk Groups container page	3-7
Trunk Group Details page	3-8
Trunk Groups trend page	3-15

Trunk Groups search page

Purpose

The Trunk Groups search page allows the user to restrict the retrieved data based on various attributes of a trunk group.

The Trunk Group search page contains a Search area, as described in the "Search pages" (p. 10). This Search area has a simple search mode, an advanced search mode, and a Trunk Group Number search with Feature 380, "Browser-based GUI TG Number Search Option". Trending information is available with the purchase of Feature 385, "Trend Analysis".

The results of a search are displayed in the Trunk Groups container page. An example of Trunk Group Advanced Search is shown in Figure 6, "Search area in advanced search mode" (p. 11).

Search criteria

Table 1 describes the search criteria that may appear in the Search area.

Table 1 Search criteria on the Trunk Groups search page (Sheet 1 of 3)

Label	Description
Period	Data collection period and sum length.
Session	Historical session ID. This field is available with Feature 342, "Historical Data Playback for the Browser-based GUI".
Near End Area Rank Set	Near end network element. Valid values include all internal network elements.
Far End Area Rank Set	Far end network element. Valid values include all network elements, both internal and external.
Suffix	A user-defined string (up to 5 characters long) used to identify a particular trunk group.
TG-Set	Trunk group set. Valid values include all trunk group set names.
TG Number	Trunk Group Number also called TG ID. This field is available with Feature 380, "Browser-based GUI TG Number Search Option".

Table 1 Search criteria on the Trunk Groups search page (Sheet 2 of 3)

Label	Description
Threshold Level	Minimum exception threshold level.
Exception Processing	NONE, ALLOW or INHIBIT
Mark	Marked Alarm status. Valid values are: • Default None • ACK • AIP • User-defined **Reference: Reference:** "Exception Status and Marked Assignments" (p. 21)
Controlled	Trunk group control status selection: Manual/Automatic • If neither "Manual" nor "Automatic" is selected, all TGs are displayed. • If "Manual" ***only*** is selected, only TGs with active manual controls are displayed. • If "Automatic" ***only*** is selected, only TGs with active automatic controls are displayed. • If "Manual" and "Automatic" are ***both*** selected, only TGs with active manual controls, active automatic controls, or active manual and automatic controls are displayed.
Service	Trunk group service type: • High Usage • Full • Final
Wideband	Wideband (wideband trunk group) — *5ESS* (5e9_2 and later)
Direction	Trunk group direction. Valid values are: • Incoming • Outgoing • Two Way • All (no restriction)
TG Type	Valid values are: • SFGN (Simulated Facility Group Number) — 1A *ESS* • IEC (Interexchange Carrier) — all switch types • DIS (dial-it service) — *4ESS* • DIS Mix (shared between dis and normal traffic) — *4ESS* • Domestic — all switch types • International — *4ESS*, *GTD-5,* SCSN
	Physical Only, Virtual Only or Physical and Virtual (default)

Table 1 Search criteria on the Trunk Groups search page (Sheet 3 of 3)

Label	Description
Overflow Element	Overflow entity ID. Valid values include all network elements, both internal and external.
Overflow Suffix	Overflow suffix.
Data Restriction	The two data restriction fields allow you to retrieve data based on values for up to two measurements. For example, you may set these fields to: `PC < 80 and %OFL > 5` Only those trunk groups having measurements matching this data restriction will be retrieved. You may use one, both, or neither of these fields.
Suspect Data Filter	This field allows the user to choose to display Suspect Data. his is valid when the associated feature is purchased and activated. **Reference: Reference:** Data collection and reporting — Suspect data in the *System Overview*; "Filter File" (p. 25) in the *Record Base Administration Guide*
Display Limit	Maximum number of rows to be retrieved: • Small: 100 rows • Medium: 600 rows • Large: 1200 rows • XL: 1500 rows
Table Layout	Table layout choices. Use this option to choose the measurement types you want to see.
User@Host	This displays current user ID and host information.

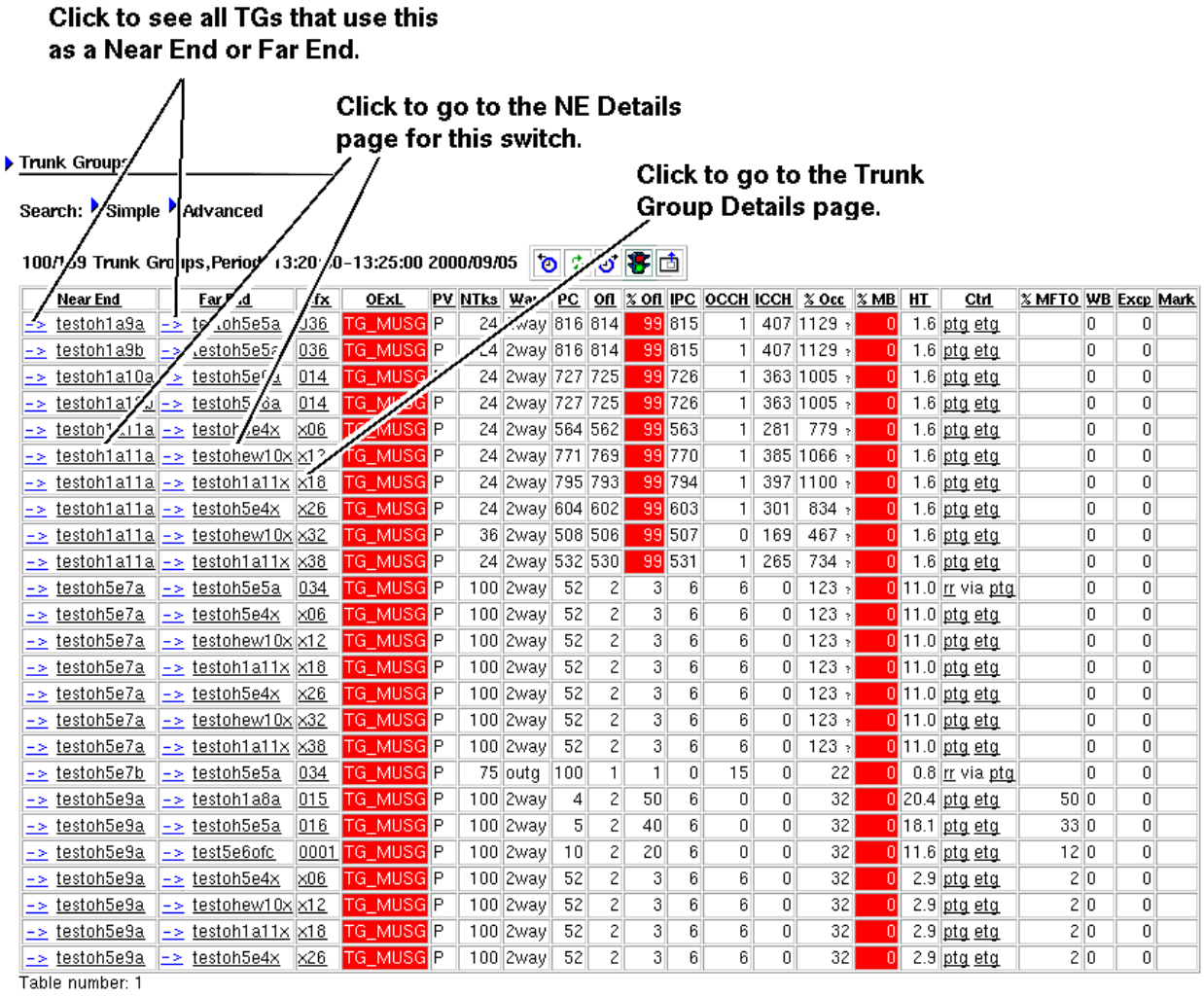
Trunk Groups container page

Purpose

The Trunk Groups container page (Figure 1) displays the results of a search in tabular format. This page supports manual update, automatic update, and historic data access. The Trunk Groups container page contains a Search area and a Toolbar area.

Reference: "Search pages" (p. 10); "Toolbar area" (p. 24)

Figure 1 Trunk Groups container page



Near End	Far End	fx	OExL	PV	NTks	Way	PC	Ofl	% Ofl	IPC	OCCH	ICCH	% Occ	% MB	HT	Ctrl	% MFTO	WB	Excp	Mark
-> testoh1a9a	-> testoh5e5a	036	TG_MUSG	P	24	2way	816	814	99	815	1	407	1129	0	1.6	ptg etg		0	0	
-> testoh1a9b	-> testoh5e5a	036	TG_MUSG	P	24	2way	816	814	99	815	1	407	1129	0	1.6	ptg etg		0	0	
-> testoh1a10a	-> testoh5e5a	014	TG_MUSG	P	24	2way	727	725	99	726	1	363	1005	0	1.6	ptg etg		0	0	
-> testoh1a10b	-> testoh5e5a	014	TG_MUSG	P	24	2way	727	725	99	726	1	363	1005	0	1.6	ptg etg		0	0	
-> testoh1a11a	-> testoh5e4x	x06	TG_MUSG	P	24	2way	564	562	99	563	1	281	779	0	1.6	ptg etg		0	0	
-> testoh1a11a	-> testohew10x	x12	TG_MUSG	P	24	2way	771	769	99	770	1	385	1066	0	1.6	ptg etg		0	0	
-> testoh1a11a	-> testoh1a11x	x18	TG_MUSG	P	24	2way	795	793	99	794	1	397	1100	0	1.6	ptg etg		0	0	
-> testoh1a11a	-> testoh5e4x	x26	TG_MUSG	P	24	2way	604	602	99	603	1	301	834	0	1.6	ptg etg		0	0	
-> testoh1a11a	-> testohew10x	x32	TG_MUSG	P	36	2way	508	506	99	507	0	169	467	0	1.6	ptg etg		0	0	
-> testoh1a11a	-> testoh1a11x	x38	TG_MUSG	P	24	2way	532	530	99	531	1	265	734	0	1.6	ptg etg		0	0	
-> testoh5e7a	-> testoh5e5a	034	TG_MUSG	P	100	2way	52	2	3	6	6	0	123	0	11.0	rr via ptg		0	0	
-> testoh5e7a	-> testoh5e4x	x06	TG_MUSG	P	100	2way	52	2	3	6	6	0	123	0	11.0	ptg etg		0	0	
-> testoh5e7a	-> testohew10x	x12	TG_MUSG	P	100	2way	52	2	3	6	6	0	123	0	11.0	ptg etg		0	0	
-> testoh5e7a	-> testoh1a11x	x18	TG_MUSG	P	100	2way	52	2	3	6	6	0	123	0	11.0	ptg etg		0	0	
-> testoh5e7a	-> testoh5e4x	x26	TG_MUSG	P	100	2way	52	2	3	6	6	0	123	0	11.0	ptg etg		0	0	
-> testoh5e7a	-> testohew10x	x32	TG_MUSG	P	100	2way	52	2	3	6	6	0	123	0	11.0	ptg etg		0	0	
-> testoh5e7a	-> testoh1a11x	x38	TG_MUSG	P	100	2way	52	2	3	6	6	0	123	0	11.0	ptg etg		0	0	
-> testoh5e7b	-> testoh5e5a	034	TG_MUSG	P	75	outg	100	1	1	0	15	0	22	0	0.8	rr via ptg		0	0	
-> testoh5e9a	-> testoh1a8a	015	TG_MUSG	P	100	2way	4	2	50	6	0	0	32	0	20.4	ptg etg	50	0	0	
-> testoh5e9a	-> testoh5e5a	016	TG_MUSG	P	100	2way	5	2	40	6	0	0	32	0	18.1	ptg etg	33	0	0	
-> testoh5e9a	-> test5e6ofc	0001	TG_MUSG	P	100	2way	10	2	20	6	0	0	32	0	11.6	ptg etg	12	0	0	
-> testoh5e9a	-> testoh5e4x	x06	TG_MUSG	P	100	2way	52	2	3	6	6	0	32	0	2.9	ptg etg	2	0	0	
-> testoh5e9a	-> testohew10x	x12	TG_MUSG	P	100	2way	52	2	3	6	6	0	32	0	2.9	ptg etg	2	0	0	
-> testoh5e9a	-> testoh1a11x	x18	TG_MUSG	P	100	2way	52	2	3	6	6	0	32	0	2.9	ptg etg	2	0	0	
-> testoh5e9a	-> testoh5e4x	x26	TG_MUSG	P	100	2way	52	2	3	6	6	0	32	0	2.9	ptg etg	2	0	0	

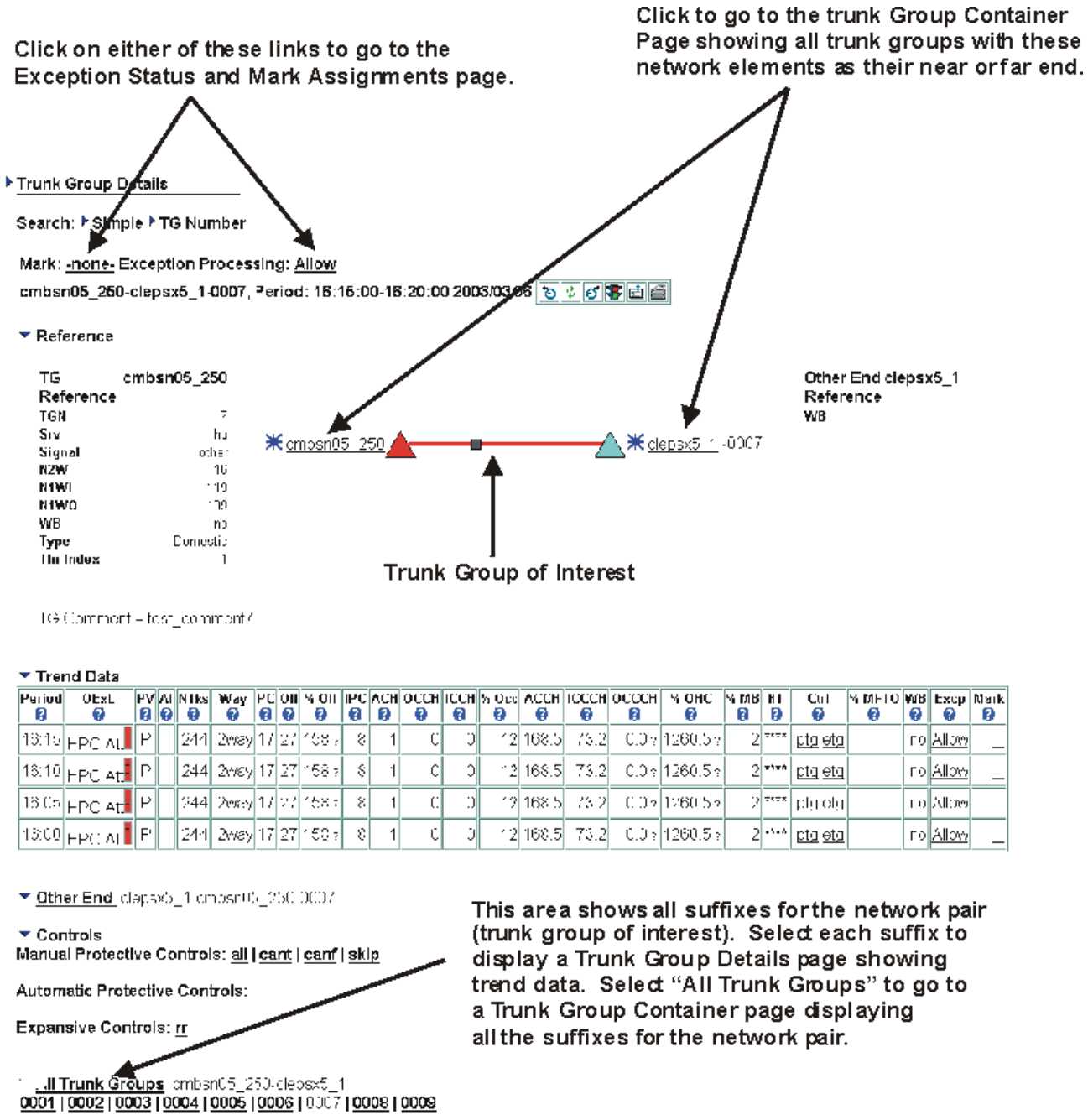
Table number: 1

Trunk Group Details page

Purpose

The Trunk Group Details page (Figure 2) displays detailed information about a particular trunk group. This page supports manual update, automatic update, and historic data access.

Figure 2 Trunk Group Details page



Page components

The page displays trunk group information under headings:

- Reference data
- Trend data

- Other end (trend data)
- Controls
- All trunk groups

All areas are displayed by default except the Reference Data section. Once the Reference area is displayed it will be displayed on all subsequent Trunk Group details pages during the browser session.

Reference data

The Trunk Group details page (Figure 2) contains an area that displays trunk group reference data. The area is arranged in four columns:

- The first column, titled “TG Reference”, contains labels of the reference data fields.
- The second column, titled with the near end network element name, contains the corresponding reference data for that network element.
- The third column, titled “Other End Reference”, contains labels of the reference data fields.
- The fourth column, titled with the far end network element name, contains the corresponding reference data for that network element. This column may be blank when the far end network element is external.
- You can add a comment of up to 80 characters that can span all four of the above columns.

Reference: “Trunk Group File” (p. 87) in the *Record Base Administration Guide*

Invalid data

If a reference data field is not valid for a particular network element, then nothing is shown. If a reference data field is not valid for both the near and the far end network elements, then it is omitted from the display.

Graphics

The Trunk Group details page contains a graphic under the Reference heading displaying high level alerting and overflow information. This graphic consists of various labels, nodes that represent network elements, and lines that represent trunk groups.

Node shapes

The possible node shapes in the graphic are a triangle and a circle. Nodes indicate the following alerting information:

- Triangle Node — (Represents a single network element.) The interior color of the node indicates the maximum threshold level of the periodic data for the single network element that it represents.

- Circle Node — (Represents a group of network elements.) The interior color of the node indicates the maximum threshold level of the periodic data across the group of network elements that it represents.

Lines and boxes

A line is drawn between two nodes and a box is shown at the midpoint. The line and box can indicate two types of alerting information:

- Line — The color of the line indicates the maximum threshold level of the periodic data for the trunk group that it represents.
- Box — The interior color of the box indicates whether or not a trunk group control is active.

If the line terminates at a circle node it may represent multiple trunk groups. In this case, the alerting information is across all of the trunk groups.

Graphic elements

The graphic display has the following elements:

- ***NearEndNE*** and the adjacent triangle shaped node represent the near end network element for the trunk group of interest. The label and node link to the Network Element Details page for the near end network element.

  Important! The blue asterisk (*) next to the near end network element is a link to a trunk group container page showing all trunk groups with the selected network element as the near end.

- ***FarEndNE-Suffix,*** the adjacent triangle shaped node, and the connected line represent the trunk group of interest. If the far end network element is internal, then the ***FarEndNE*** part of the label and the node link to the Network Element Details page for the far end network element. (The Suffix and line do not have any links.)

  Important! The blue asterisk (*) next to the far end network element is a link to a trunk group container page showing all trunk groups with the selected network element as the far end.

- ***OflToNE-Suffix,*** the adjacent triangle shaped node, and the connected line represent the trunk group to which the trunk group of interest overflows. These parts appear only if the trunk group of interest is of type high-usage and has an overflow trunk group assigned to it in the reference data.

  If ***OflToNE*** is internal, then the following links are included:

  – The ***OflToNE*** part of the label and the node link to the Network Element Details page for network element ***OflToNE***.

  - The ***Suffix*** part of the label and the line link to the Trunk Group Details page for the trunk group ***NearEndNE-OflToNE-Suffix***.

- ***Num*** Trunk Groups, the adjacent circle shaped node and the connected line represent the trunk group(s) that overflow to the trunk group of interest. These parts appear only if the trunk group of interest is assigned as the overflow trunk group of another trunk group in the reference data. ***Num*** is the number of trunk groups that overflow to the trunk group of interest. The label, node, and line link to the Trunk Group container page for the represented trunk groups, with the following additional context:
  - Near End is ***NearEndNE***
  - Overflow Element is ***FarEndNE***
  - Overflow Suffix is the ***Suffix*** associated with ***FarEndNE***
  - Default Sort Column is “OFL”

Figures

Figure 3 through Figure 5 show examples of different types of trunk group usage.

Figure 3 High-usage trunk group

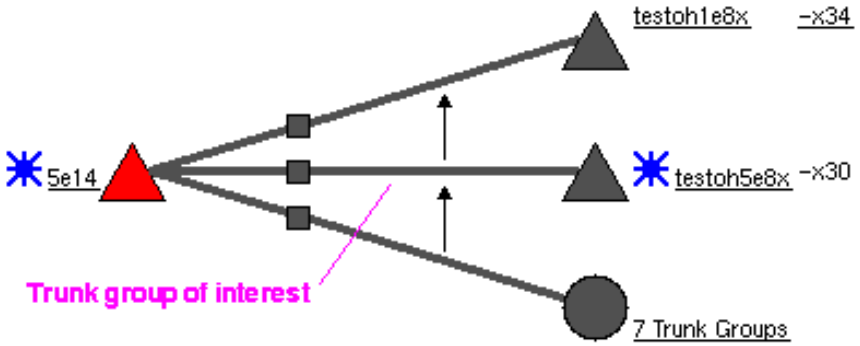


Figure 4 Final trunk group

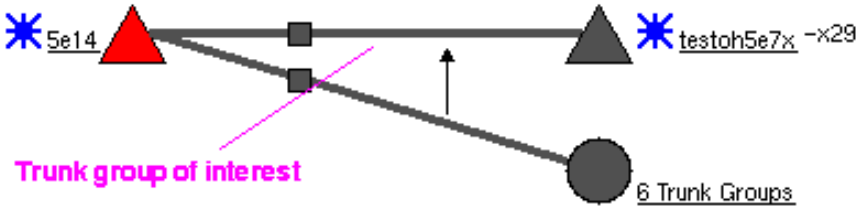


Figure 5 Full trunk group

Trend data

The Trunk Group Details page contains two Trend Data Tables. The columns of both Trend Data Tables are based on the Table Layout selection of the Search area. The first Trend Data Table (displayed when the page is loaded) displays trend data over four data collection periods for the trunk group of interest.

Other end (trend data)

A second Trend Data Table displays a single period of data for the other-end trunk group. This Trend Data Table is accessed by clicking on the underlined “Other End” link under the first data table; the second Trend Data Table is available only if the other end in an internal network element.

Controls

The Trunk Group Details page contains three areas that display trunk group control information:

- "Manual Protective Controls" lists all manual protective trunk group controls that are active for the data collection period that was searched. The manual protective trunk group control types that are valid for the trunk group are listed following the title. "All" is also an option. Each of these control types listed is a link to the protective trunk group controls container page. When the control type is selected, the control type is passed on to the control type search.
- "Automatic Protective Controls" lists all automatic protective trunk group controls that are active for the data collection period that was searched.
- "Expansive Controls" lists all the expansive trunk group controls that are active for the data collection period that was searched.

The active controls are listed with all parameters that were set when the control was applied.

All trunk groups

The lower section of the Trunk Group Details page contains an area labeled "All Trunk Groups". This section lists all suffixes between the selected near and the far end network elements. The user can select one of these to display a trunk group details page showing trend data for that trunk group or select All Trunk Groups to display a trunk group container showing all trunk groups.

□

Trunk Groups trend page

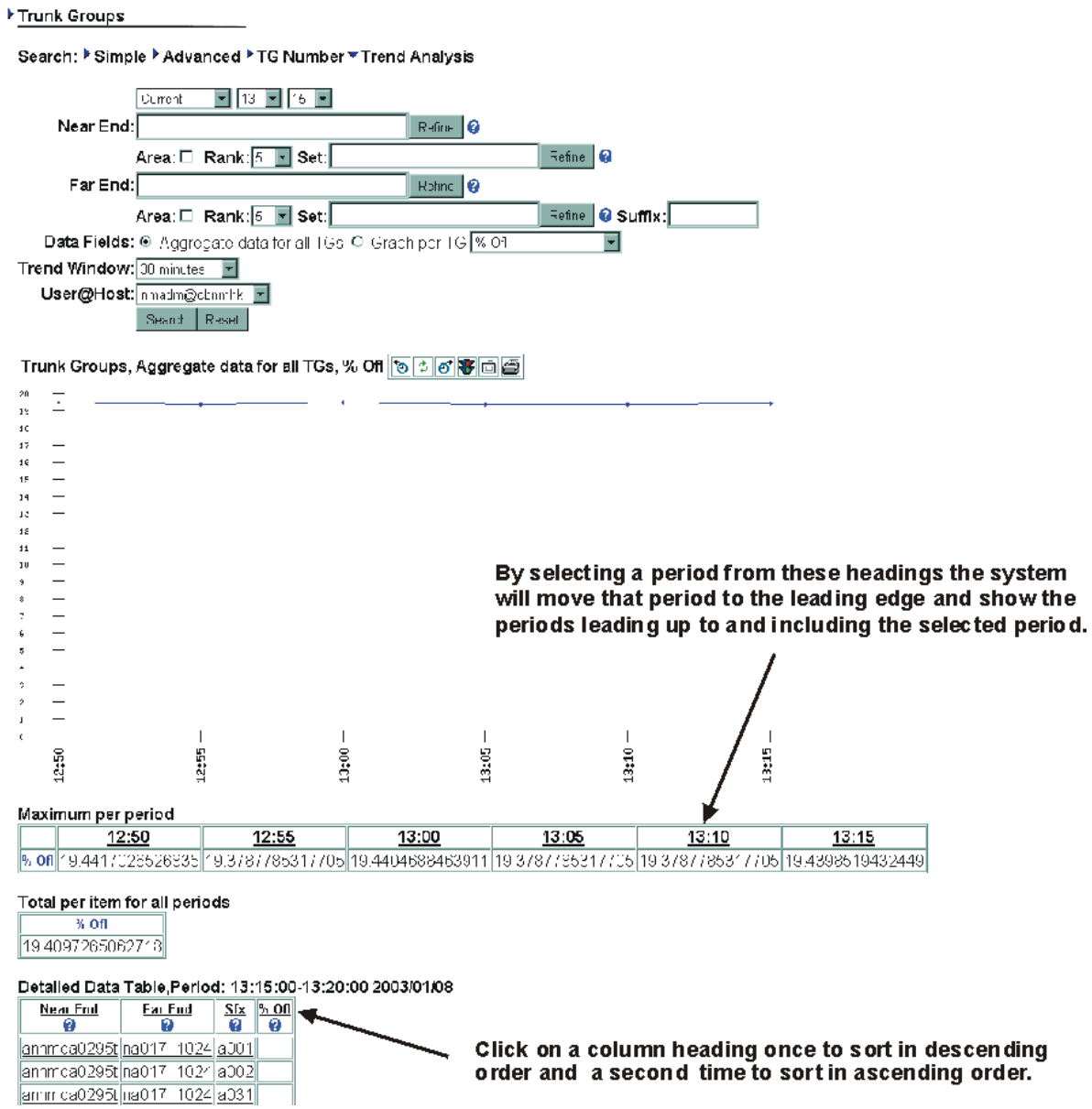
Purpose

The Trunk Groups trend page is available if you have purchased Feature 385, “Trend Analysis”.

Reference: “Trend pages” (p. 18)

The Trunk Groups trend page allows the user to restrict the retrieved data based on various trunk group attributes. Figure 6 shows a Trunk Groups trend page.

Figure 6 Trunk Groups trend page



Search criteria

Table 2 describes the search criteria that can appear in the Search area.

Table 2 Search criteria for Trunk Groups trend page

Label	Description
Period	Data collection period. The default is Current

Table 2 Search criteria for Trunk Groups trend page

Label	Description
Near End Area Rank Set	Near end network element. Valid values include all internal network elements.
Far End Area Rank Set	Far end network element. Valid values include all network elements, both internal and external.
Suffix	A user-defined string (up to 5 characters long) used to identify a particular trunk group.
TG-Set	Trunk group set. Valid values include all trunk group set names.
Data Fields	**Aggregate data for all trunk groups** Items with multiple counts can be selected from the associated list. **Graph per trunk group** Items with only one data count can be selected from the associated list.
Trend Window	The number of data collection periods to be used in the trend analysis. Options are: 6, 12, 18 or 24 five-minute data collection periods (30 minutes to 2 hours).
User@<*Host*>	Choice of user IDs on a specific host machine.

Signaling Links and Link Sets (Without Feature 415)

Overview

Purpose

This section discusses the Signaling Links and Link Sets pages and their components.

Reference: If Feature 415, “Browser-based Access to NetMinder Signaling Traffic Management (STM) data” is purchased, STM data will replace these pages. See Signaling Links and Link Sets (With Feature 415)

The Links/Link Sets object allows you to retrieve signaling link measurements, and link and linkset events. Link set measurement data is collected every 5 minutes.

Reference: “Data collection and reporting” (p. 5) in the *System Overview*

Contents

This section contains the following topics:

Signaling Links and Link Sets search page	3-20
Signaling Links and Link Sets container page	3-21

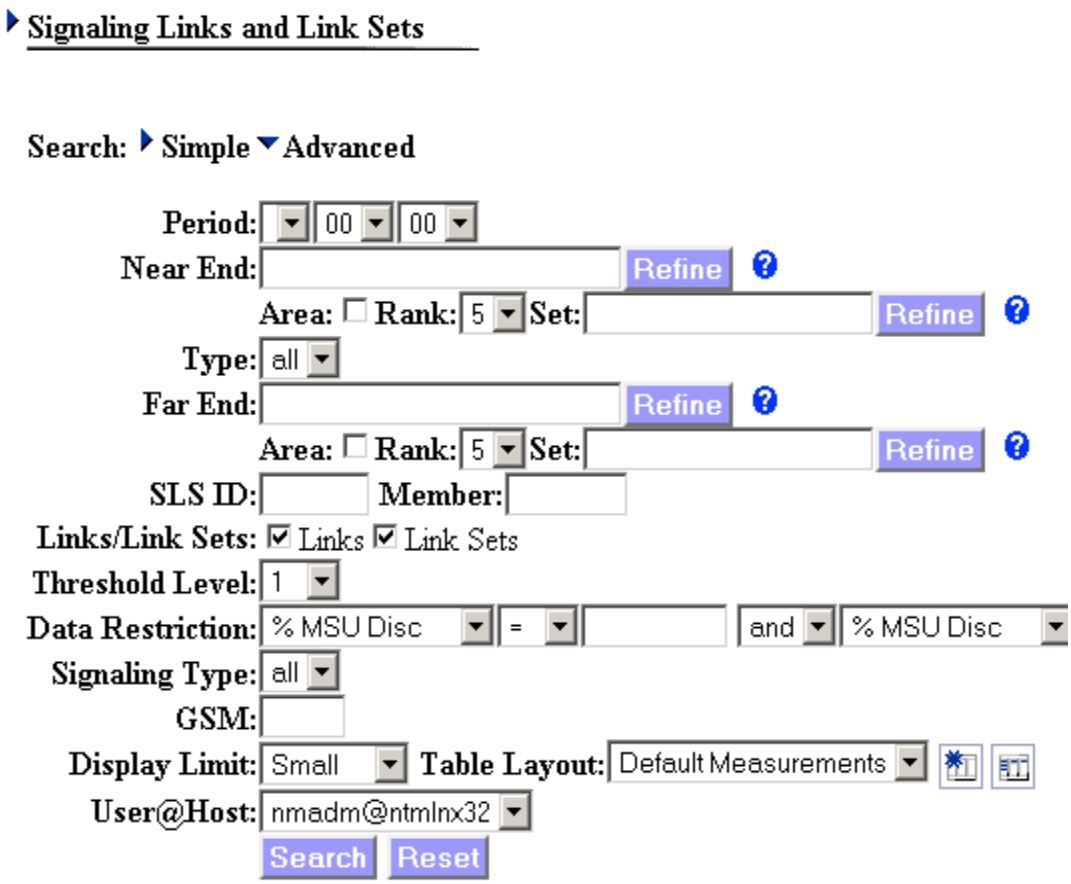
Signaling Links and Link Sets search page

Purpose

The Signaling Links and Link Sets search page allows you to retrieve signaling link measurements and link and linkset events.

Figure 7 shows the Signalling Links and Link Sets search page in advanced search mode.

Figure 7 Signalling Links/Link Sets search page in advanced search mode

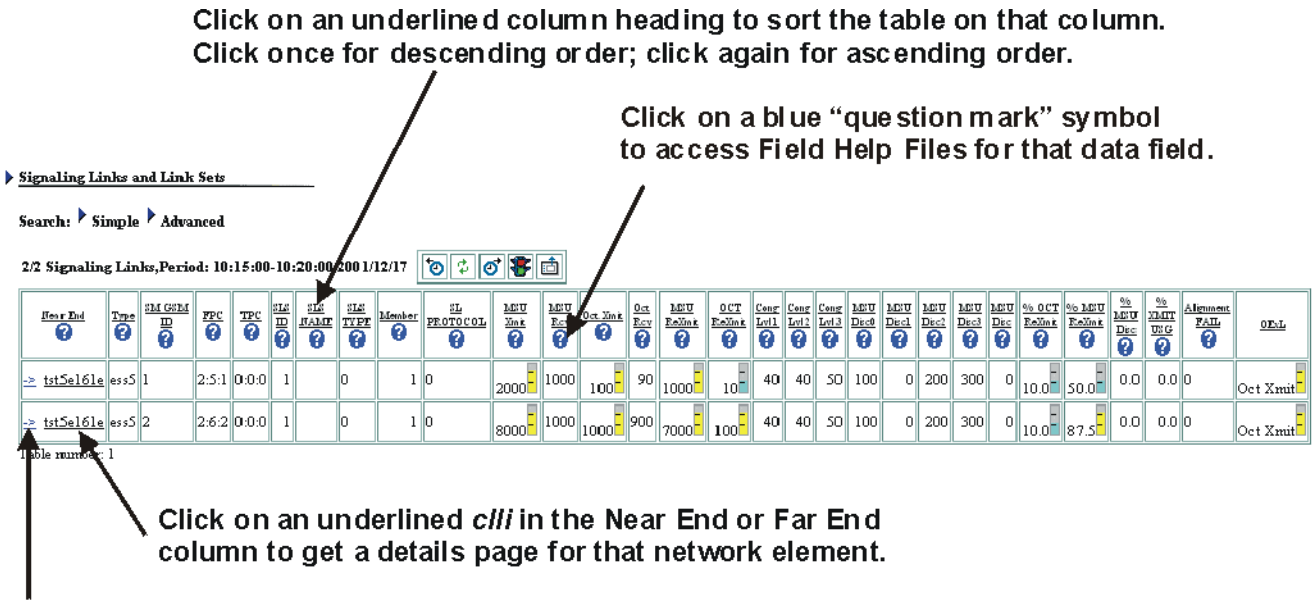


Signaling Links and Link Sets container page

Purpose

The Signaling Links and Link Sets container page (Figure 8) displays the results of your search.

Figure 8 Signaling Links and Link Sets container page



Signaling Links and Link Sets (With Feature 415)

Overview

Purpose

This section discusses the Signaling Links and Link Sets pages and their components as monitored through NetMinder STM.

Reference: If Feature 415, “Browser-based Access to NetMinder Signaling Traffic Management (STM) data” is NOT purchased, traditional NTM data will replace these pages. See Signaling Links and Link Sets (Without Feature 415)

The Links/Link Sets object allows you to retrieve signaling link measurements, and link and linkset events. Link set measurement data is collected every 5 minutes.

Reference: “Data collection and reporting” (p. 5) in the *System Overview*

Contents

This section contains the following topics:

Signaling Link and Linkset Measurement - Search Pages	3-24
Signaling Link and Linkset Measurements - Container pages	3-27

Signaling Link and Linkset Measurement - Search Pages

Purpose

The Signaling Links/Link Sets icon accesses the Link Measurements and Linkset Measurements search pages. These pages allow you to retrieve signaling link/linkset measurements via the NetMinder STM system. Two types of Signaling data can be retrieved:

- Links Measurements Figure 9
- Linkset Measurements Figure 10

Prerequisite

Feature 415, “Browser-based Access to NetMinder Signaling Traffic Management (STM) data” must be purchased and installed for the following GUI pages to appear.

Figure 9 Link Measurement page in Simple search mode

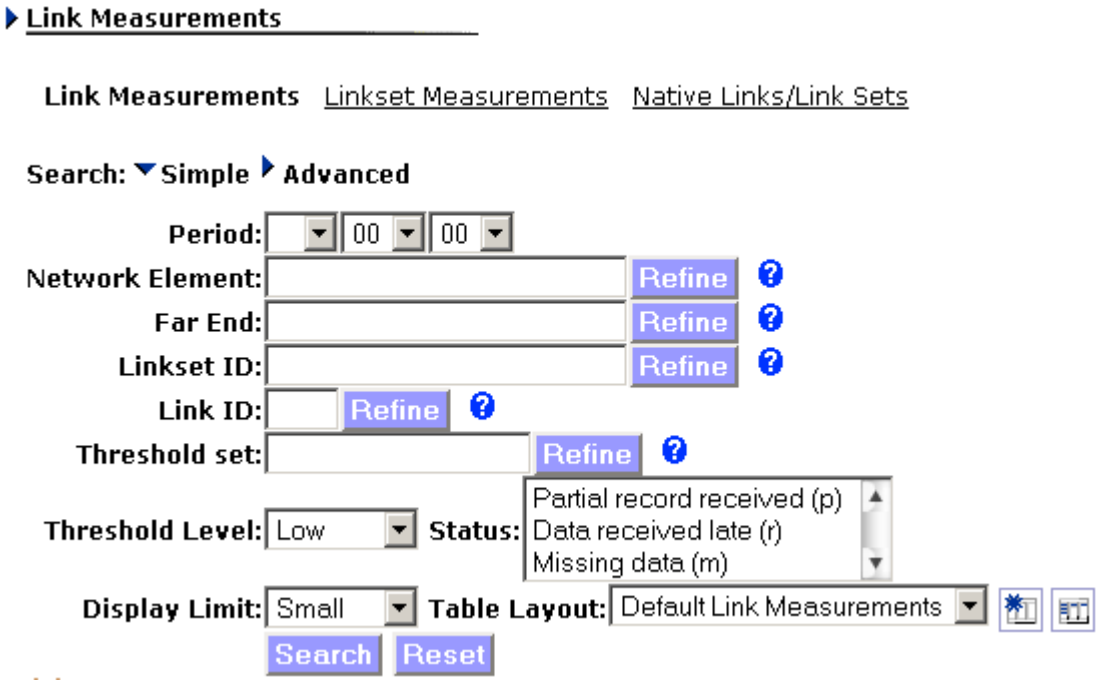
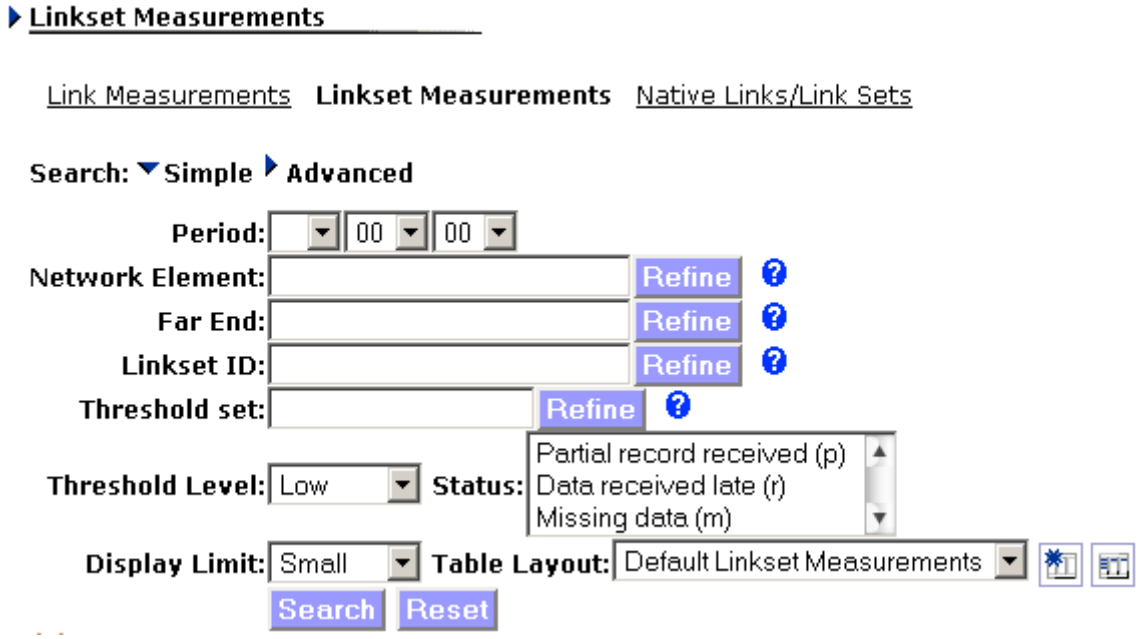


Figure 10 Linkset Measurement search page



The Link/Linkset Measurements search page allows the user to retrieve data based on various attributes of a Signaling data from STM. The simple search criteria is listed in Table 3.

Important! The advanced search criteria fields are those directly linked to STM and can be used to restrict the data displayed in the resulting container page. Please refer to your STM user documentation for more information for these fields.

Search criteria

Table 3 describes the search criteria that may appear in the Search area.

Table 3 Search criteria on the Link and Link Measurements Simple search pages (Sheet 1 of 2)

Label	Description
Period	Data collection period. The default is Current
Network Element	All monitored signaling network elements. Valid values include all internal network elements.
Far End	Far end network element. Valid values include all internal network elements.

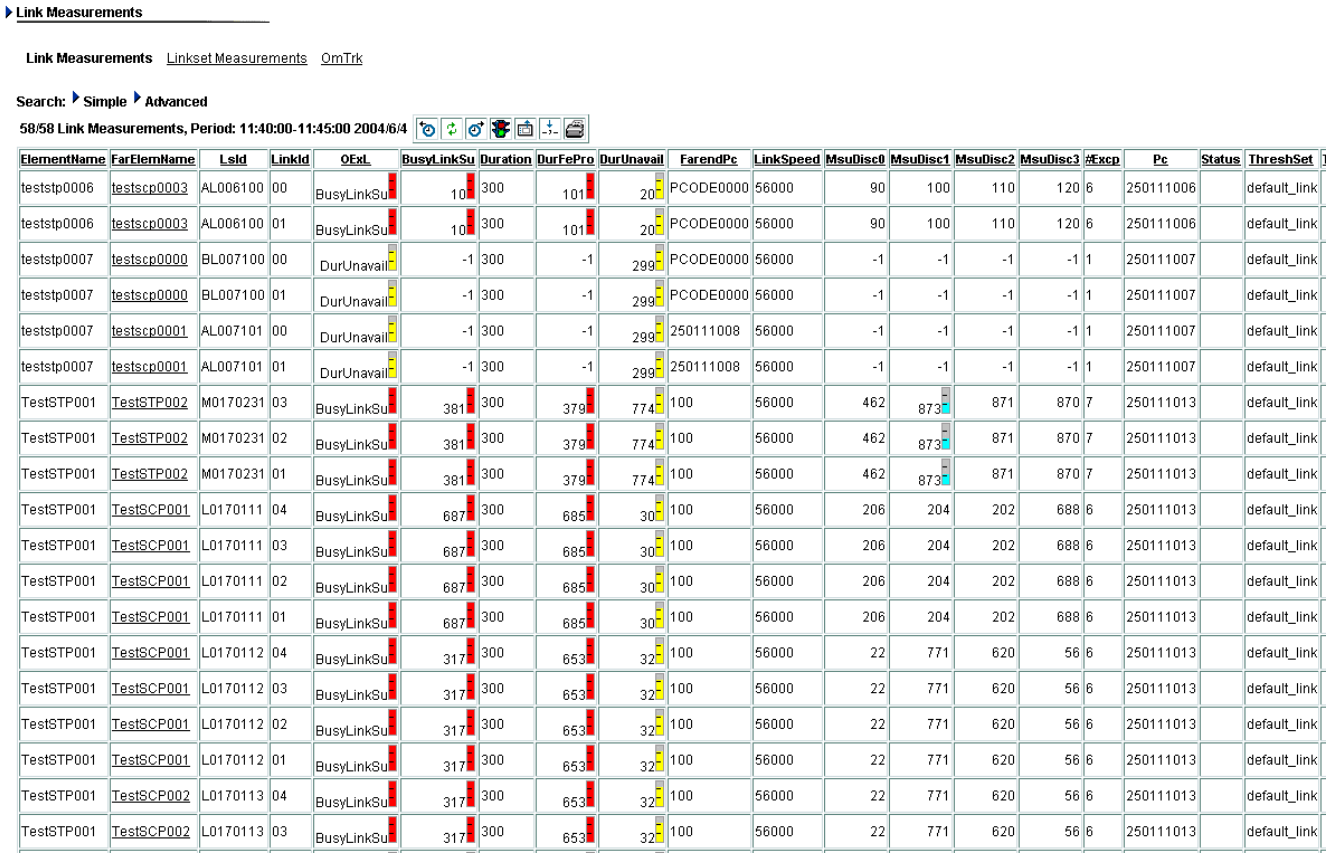
Table 3 Search criteria on the Link and Link Measurements Simple search pages (Sheet 2 of 2)

Label	Description
Linkset ID	Linkset identifier. Value of 10 characters. Provided by STM audit. Format: • *alnnnnnn* a = alphabetic • l = alphanumeric • n = numeric
Link ID (Link Measurements only)	Link identifier. Values of 0 – 15 characters. Provided by STM audit.
Threshold Set	Threshold set name. Can also be populated by an audit if supported by switch type (value = default_link).
Threshold Level	Threshold level defined in STM. Values of: (A) all, (L) low, (M) medium, (H) high.
Data Restriction	The two data restriction fields allow you to retrieve data based on values for up to two values, and an operator. For example, you may set this field to: `%SL Failed < 20 AND %MSU Disc < 75` Only those links or linksets having measurements matching these data restrictions will be retrieved.
Status	Data collection status flags.
Display Limit	Maximum number of rows to be retrieved: • Small: 100 rows • Medium: 600 rows • Large: 1200 rows
Table Layout	Table layout choices. Use this option to choose the measurement types you want to view.

Purpose

The Link and Linksets Measurements container pages (Figure 11 and Figure 12) display the results of a search.

Figure 11 Link Measurements container page



Link Measurements

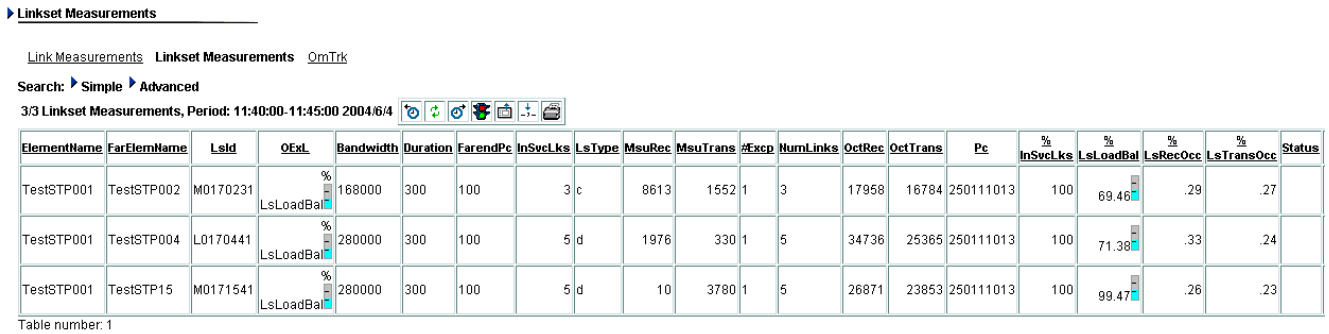
Link Measurements Linkset Measurements OmTrk

Search: Simple Advanced

58/58 Link Measurements, Period: 11:40:00-11:45:00 2004/6/4

ElementName	FarElemName	LsId	LinkId	OExL	BusyLinkSu	Duration	DurFePro	DurUnavail	FarendPc	LinkSpeed	MsuDisc0	MsuDisc1	MsuDisc2	MsuDisc3	#Excp	Pc	Status	ThreshSet
teststp0006	testscp0003	AL006100	00	BusyLinkSu	10	300	101	20	PCODE0000	56000	90	100	110	120	6	250111006		default_link
teststp0006	testscp0003	AL006100	01	BusyLinkSu	10	300	101	20	PCODE0000	56000	90	100	110	120	6	250111006		default_link
teststp0007	testscp0000	BL007100	00	DurUnavail	-1	300	-1	299	PCODE0000	56000	-1	-1	-1	-1	1	250111007		default_link
teststp0007	testscp0000	BL007100	01	DurUnavail	-1	300	-1	299	PCODE0000	56000	-1	-1	-1	-1	1	250111007		default_link
teststp0007	testscp0001	AL007101	00	DurUnavail	-1	300	-1	299	250111008	56000	-1	-1	-1	-1	1	250111007		default_link
teststp0007	testscp0001	AL007101	01	DurUnavail	-1	300	-1	299	250111008	56000	-1	-1	-1	-1	1	250111007		default_link
TestSTP001	TestSTP002	M0170231	03	BusyLinkSu	381	300	379	774	100	56000	462	873	871	870	7	250111013		default_link
TestSTP001	TestSTP002	M0170231	02	BusyLinkSu	381	300	379	774	100	56000	462	873	871	870	7	250111013		default_link
TestSTP001	TestSTP002	M0170231	01	BusyLinkSu	381	300	379	774	100	56000	462	873	871	870	7	250111013		default_link
TestSTP001	TestSCP001	L0170111	04	BusyLinkSu	687	300	685	30	100	56000	206	204	202	688	6	250111013		default_link
TestSTP001	TestSCP001	L0170111	03	BusyLinkSu	687	300	685	30	100	56000	206	204	202	688	6	250111013		default_link
TestSTP001	TestSCP001	L0170111	02	BusyLinkSu	687	300	685	30	100	56000	206	204	202	688	6	250111013		default_link
TestSTP001	TestSCP001	L0170111	01	BusyLinkSu	687	300	685	30	100	56000	206	204	202	688	6	250111013		default_link
TestSTP001	TestSCP001	L0170112	04	BusyLinkSu	317	300	653	32	100	56000	22	771	620	56	6	250111013		default_link
TestSTP001	TestSCP001	L0170112	03	BusyLinkSu	317	300	653	32	100	56000	22	771	620	56	6	250111013		default_link
TestSTP001	TestSCP001	L0170112	02	BusyLinkSu	317	300	653	32	100	56000	22	771	620	56	6	250111013		default_link
TestSTP001	TestSCP001	L0170112	01	BusyLinkSu	317	300	653	32	100	56000	22	771	620	56	6	250111013		default_link
TestSTP001	TestSCP002	L0170113	04	BusyLinkSu	317	300	653	32	100	56000	22	771	620	56	6	250111013		default_link
TestSTP001	TestSCP002	L0170113	03	BusyLinkSu	317	300	653	32	100	56000	22	771	620	56	6	250111013		default_link

Figure 12 Linksets Measurements container page



Linkset Measurements

Link Measurements Linkset Measurements OmTrk

Search: Simple Advanced

3/3 Linkset Measurements, Period: 11:40:00-11:45:00 2004/6/4

ElementName	FarElemName	LsId	OExL	Bandwidth	Duration	FarendPc	InSvcLks	LsType	MsuRec	MsuTrans	#Excp	NumLinks	OctRec	OctTrans	Pc	% InSvcLks	% LsLoadBal	% LsRecOcc	% LsTransOcc	Status
TestSTP001	TestSTP002	M0170231	% LsLoadBal	168000	300	100	3	c	8613	1552	1	3	17958	16784	250111013	100	69.46	.29	.27	
TestSTP001	TestSTP004	L0170441	% LsLoadBal	280000	300	100	5	d	1976	330	1	5	34736	25365	250111013	100	71.38	.33	.24	
TestSTP001	TestSTP15	M0171541	% LsLoadBal	280000	300	100	5	d	10	3780	1	5	26871	23853	250111013	100	99.47	.26	.23	

Table number: 1

Packet Links

Overview

Purpose

This section discusses the Packet Link pages and their components.

The Packet Link object allows you to retrieve packet measurements for:

- ATM Links
- IP Links
- PVG Links

Link measurement data is collected every 5 minutes.

Reference: “Data collection and reporting” (p. 5) in the *System Overview*

Contents

This chapter contains the following topics:

Packet Link search page	3-30
Packet Link container page	3-33

Packet Link search page

Purpose

The Packet Link search page allows you to select one of three types of packet data to retrieve:

- ATM Links
- IP Links
- PVG Links

Trending Feature

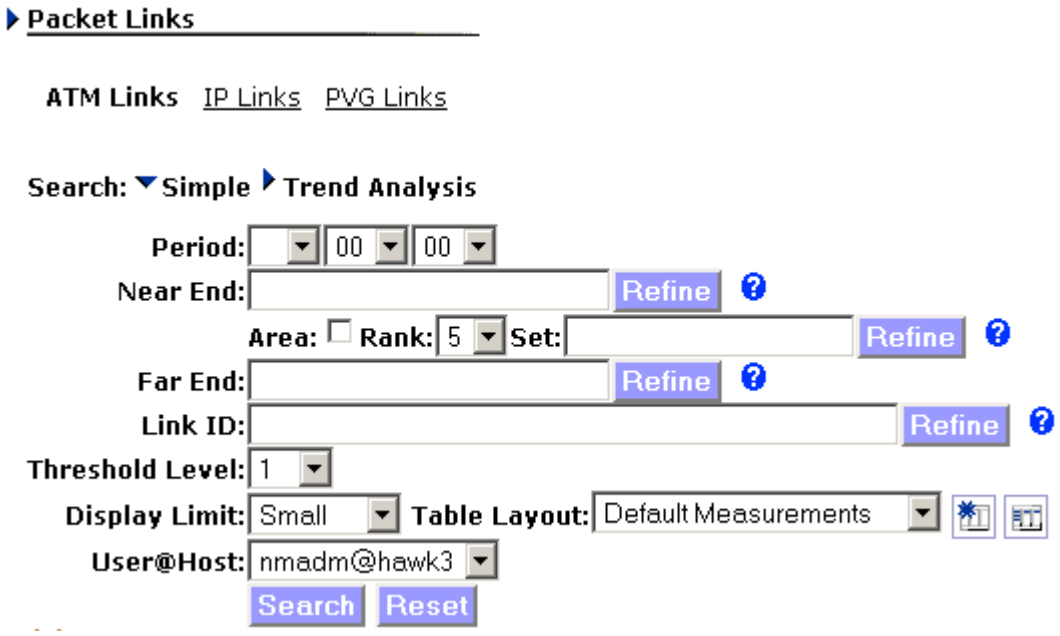
The ATM, IP, and PVG links trend pages are available if you have purchased Feature 385, "Trend Analysis".

Reference: "Trend pages" (p. 18)

The ATM/IP link trend page allows the user to restrict the retrieved data based on various ATM, PVG, or IP link attributes. Trend Analysis pages can show up to the last 24 periods of data for the passport 15k links or various counts for a specific passport link.

Figure 13 shows the Packet Links search page in ATM Links simple search mode.

Figure 13 Packet Links search page in simple search mode



Search criteria

Table 4 describes the search criteria that can appear in the Search area.

Table 4 Search criteria for Packet Links search page

Label	Description
Period	Data collection period. The default is Current
Session	Historical session ID. This field is available with Feature 342, "Historical Data Playback for the Browser-based GUI".
Near End Area Rank Set	Near end network element. Valid values include all internal network elements.
Far End	Far end network element. Valid values include all network elements, both internal and external.
Data Fields (Trend Analysis)	Users can select either; Aggregate data for all Passports or specific data types for a specific passport.
Link ID	A user-defined string (up to 30 characters long) used to identify a particular PP15k link.
Threshold Level	Minimum exception threshold level.

Table 4 Search criteria for Packet Links search page

Label	Description
Suspect Data Filter	This field allows the user to choose to display Suspect Data. This is valid when the associated feature is purchased and activated. **Reference: Reference:** Data collection and reporting — Suspect data in the *System Overview*; "Filter File" (p. 25) in the *Record Base Administration Guide*
Display Limit	Maximum number of rows to be retrieved: • Small: 100 rows • Medium: 600 rows • Large: 1200 rows
Table Layout	Table layout choices. Use this option to choose the measurement types you want to see.
User@Host	This displays current user ID and host information.

Packet Link container page

Purpose

The Packet Links container page (Figure 14) displays the results of a Links search or Trend Analysis retrieval.

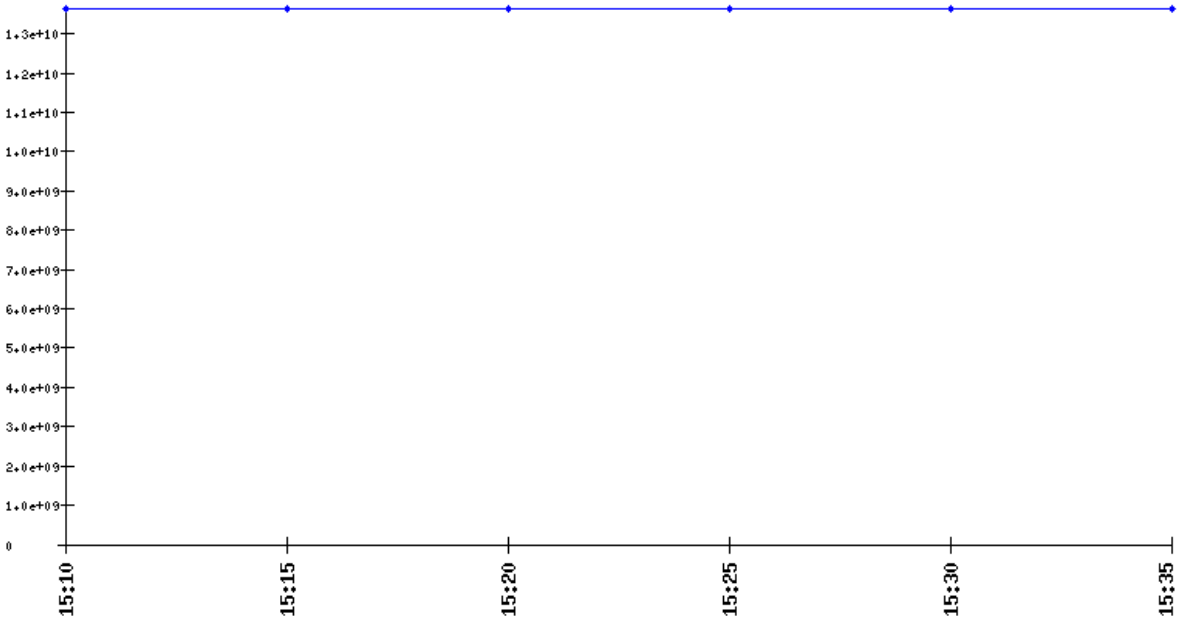
Figure 14 Packet Links (ATM Trend) container page

Packet Links

ATM Links IP Links PVG Links

Search: Simple Trend Analysis

Packet Links, Aggregate data for all Passports, ATM_LINKID, INCELLS



Maximum per period

	15:10	15:15	15:20	15:25	15:30	15:35
INCELLS	13656593338	13656593338	13656593338	13656593338	13656593338	13656593338

Total per item for all periods

INCELLS
81939560028

Detailed Data Table,Period: 15:35:00-15:40:00 2004/07/21

Near End	Far End	ATM LINKID	INCELLS
kyscsnsn_1		em/design_7 atmif/1421	0
kyscsnsn_1		em/design_7 atmif/1420	0
kyscsnsn_1		em/design_7 atmif/1422	0

4 Network Views

Overview

Purpose

The Network View pages provide you with high-level alerting information. They are generally projected onto a wallboard in the Network Management Center (NMC), but can also be used at a network manager's client workstation. Network view pages are most often geographical maps and alerts tables showing nodes (to represent network elements) and lines connecting the nodes, to represent trunk groups.

Important! Network Views require *JAVA* 2 version 1.2 plug-in to be installed.

Reference: For configuring ISA Alerts, see "ISA system alert filters" (p. 32).

Contents

This chapter contains the following topics:

Network Views display options	4-8
Nodes on a Network View	4-11
Text on a Network View	4-14
Timestamp on a Network View	4-15
Mouse menu options	4-16
Network View Legend	4-17
Alerts table	4-19
Network Event Alerting	4-29
General tasks on the Network Views pages	4-31

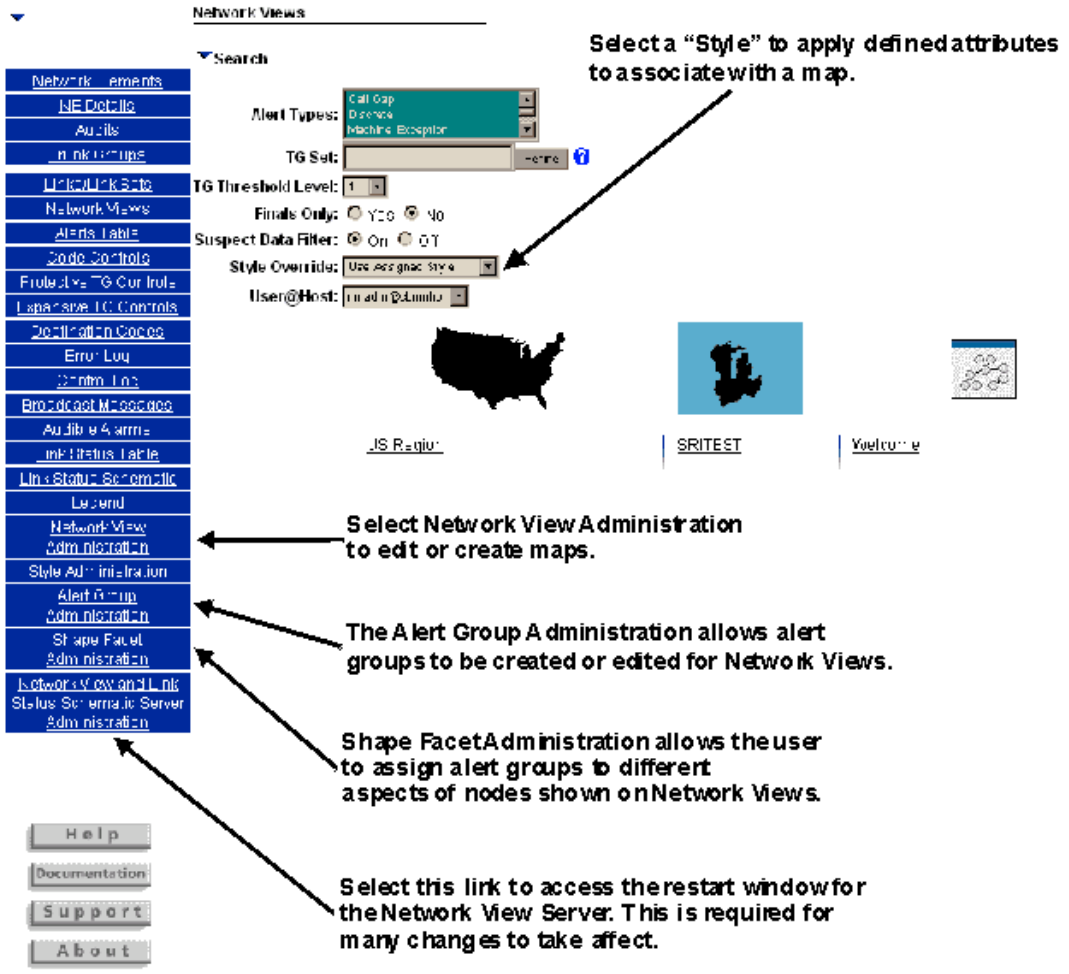
Network Views search/container page

Purpose

From the Launch page, users can select the Network Views icon to go to the Network Views search/container page (Figure 1). There is a search area at the top of the page that allows the user to restrict what data will be displayed. Select an image to link to a specific network detail page.

Important! A second authentication screen will be displayed for security reasons. Re-enter the user name and password used during initial login.

Figure 1 Network Views search/container page (Original skin view)



Errors

If initiating a map exceeds either the user limits or the system limits described in Chapter 5, "Thresholds" in the *System Overview*, an error message is displayed indicating the capacity that was exceeded.

Reference: See the limitthr command (5-37) in the *Input Commands Guide* for information about system constraints on the network views.

Search criteria

Table 1 describes the search criteria that may appear in the Search area.

Table 1 Search criteria on the Network Views search page

Label	Description
Alert Types	You can select the type of data displayed by restricting it to a specific alert type.
TG-Set	Selecting this option restricts the view to only trunk groups that belong to the selected set. Nodes defined on the network view will also be displayed.
TG Threshold Level	Minimum exception threshold level. Values are 1 – 10.
Finals Only	The restricts the trunk groups displayed to Final Trunk Groups.
Suspect Data Filter	This field allows the user to choose to display Suspect data. **Important!** This is valid when the associated feature is purchased and activated. **Reference:** **Reference:** "Filter File" (p. 25) in the *Record Base Administration Guide*
Style Override	Select a "Style" to apply defined attributes to associate with a network view.
User@Host	This displays current user ID and host information.

Network View detail page

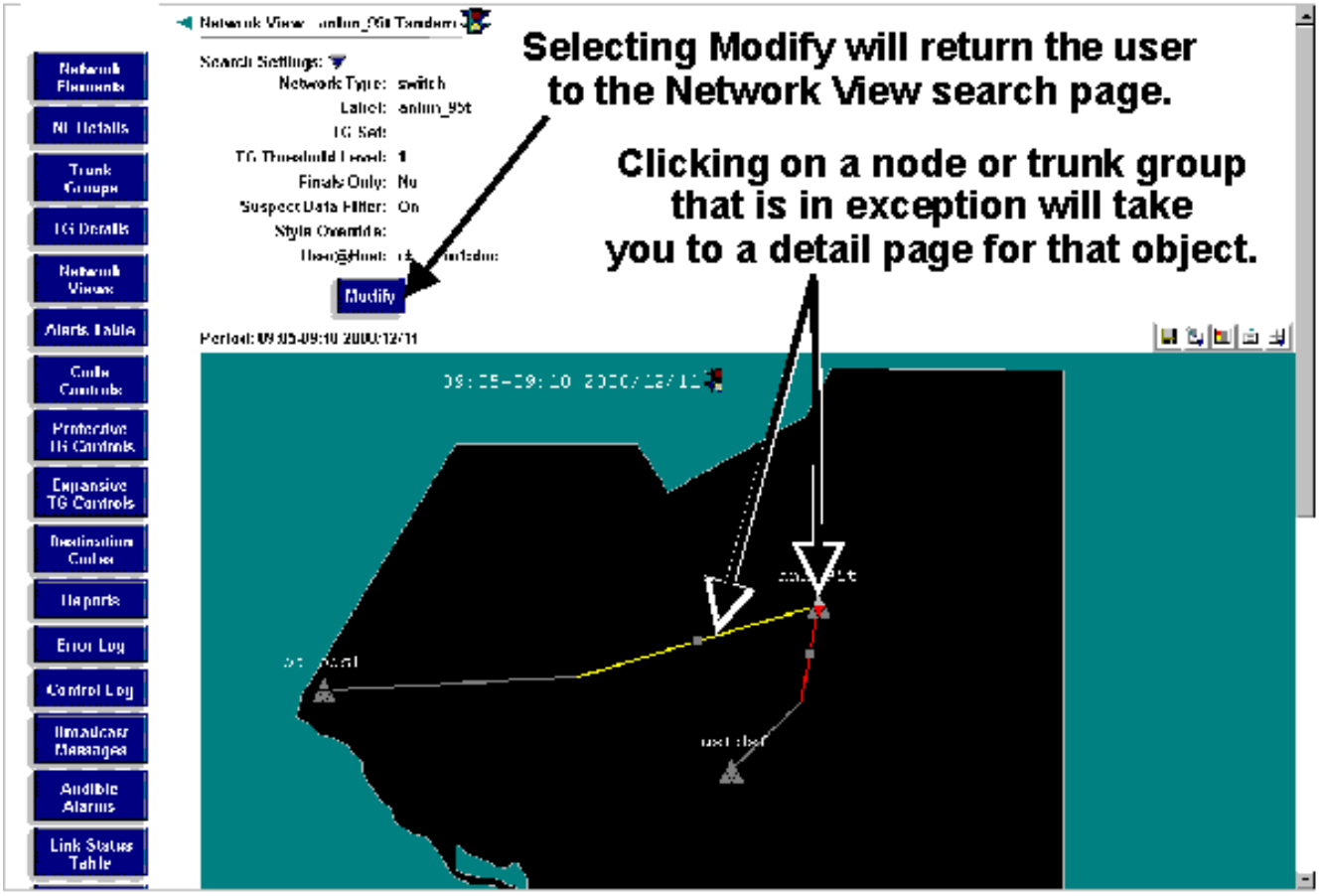
Purpose

The Network View detail page (Figure 2) shows a geographical or schematic representation of an area (this could be a country, state, province, region, city or other area) by displaying nodes and lines connecting the nodes.

Certain attributes of objects may be defined for each specific type of network display. Grouped nodes are allowed, and there is only one line between two nodes representing trunk groups. If a control is active or one of the trunk groups between grouped nodes has an exception, it is displayed as a single line.

Included with the standard displays is the Welcome display. This display can be used for public relations purposes.

Figure 2 Network View detail page



Map analysis

The data used for Map analysis is filtered based on the user who started the map, the host user group to which the user belongs, and the user's subnetwork permissions.

The data displayed on the maps depends on the preference settings, such as user name, group and subnetwork permissions. If the BDR feature is enabled, the data displayed on the map depends on the web server from which the map was run and the user name, group and subnetwork permissions.

The facets of the nodes and lines show the highest alert level for the data they represent. The threshold levels for exceptions, alarms, and discretes are converted to alert levels. The standard values are shown in Table 2.

Table 2 Standard threshold/alert levels

IF the threshold level is …	THEN the alert level is …
1 – 3	L (Low)
4 – 7	M (Medium)
8 – 10	H (High)
Control active	C (Control)

Important! If two or more alerts map to the same facet on a map, the highest alert level will be displayed.

The order of precedence for the alert levels is:

- H — high
- M — medium
- C — control
- L — low

Lines representing trunk groups are drawn only when nodes corresponding to both ends of the line appear on the map and there is an exception or control on one of the trunk groups.

Links to pages

If there are exceptions for a node or link, you can select the facet of a node or a line. When a facet is selected, the new page corresponding to the alert type with the highest level for the alert group is opened.

Facets of nodes

Nodes are divided into sections referred to as facets. Each facet can indicate various types of information depending on the type of node. For your facet assignment, refer to the legend menu item in the navigation window for details.

One possible facet is for TGDAT (Trunk Group Data). If this facet is on the node itself — not the link. It will be active when there is a trunk group exception. The facet will light up only when there is an exception on a trunk group going from the office represented by that node facet to any other switch even those not represented on the map displayed which uses that office as a near end.

Types of nodes

There are two types of nodes on the map: individual switches and grouped nodes. The identifier for individual switches comes from the name for the switch specified in the RSPTE File and the identifier for grouped nodes is the name of a set defined in the Sets File. The grouped node represents the data for all the switches that belong to that set.

Linked nodes

You can link a node on the map display to another Network View, using the Link Expansion field found by selecting the right mouse “Properties” button while over a node. When the change is applied, the node will appear with the link symbol next to the link name (Figure 3). If the link has no name, then the link will appear above the node.

Figure 3 Link expansion indicator

New period indicator

When a map is first displayed or when a new data collection period begins, a new indicator appears to the right of the timestamp. When data is first received for a new period, it appears as green. The indicator changes from green to yellow after about 2 minutes.

Figure 4 New period indicator

Network Views display options

Purpose

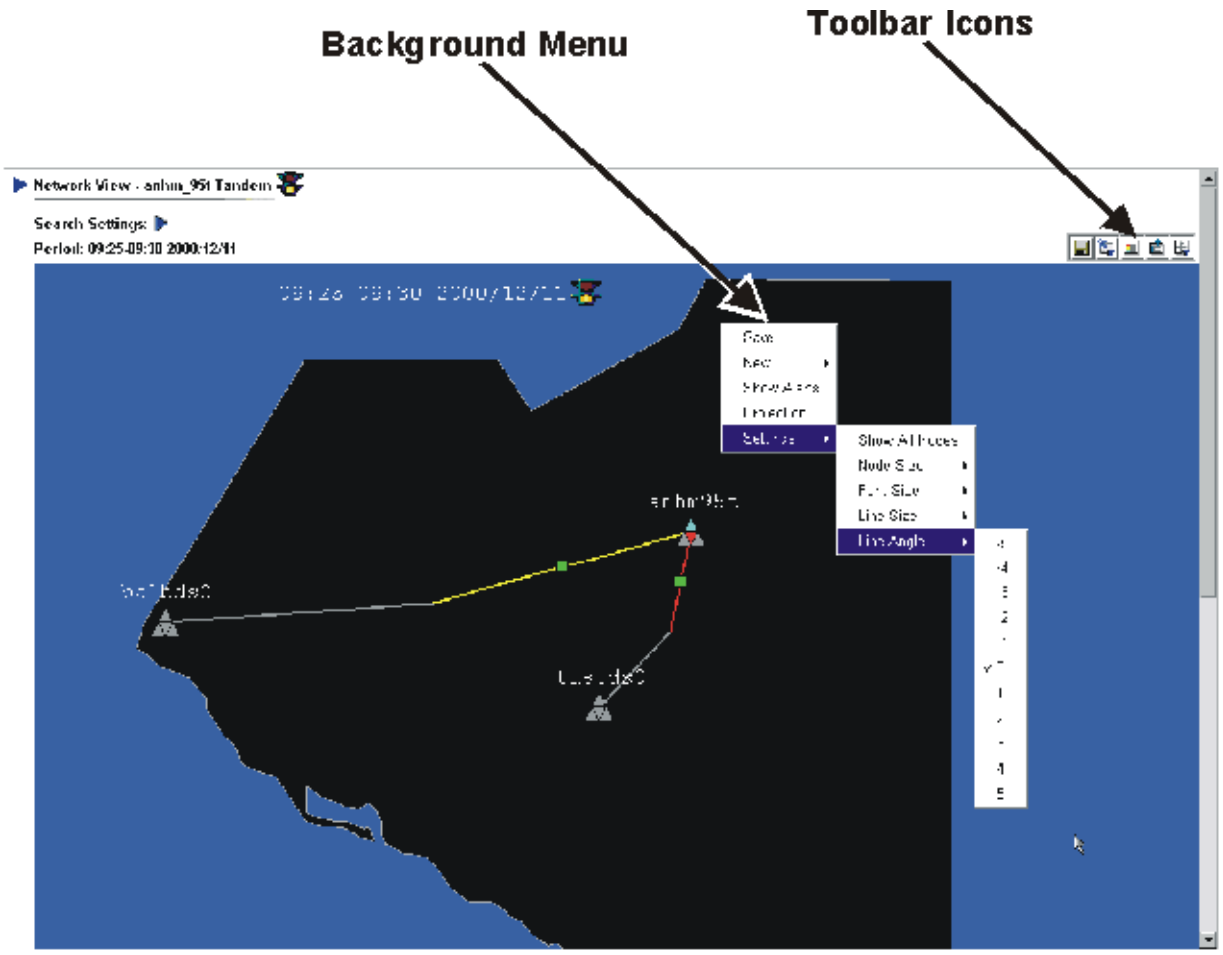
Menu mouse-clicking the background (anywhere within the map window other than on a node, line, timestamp or text) will also present a menu (Figure 5) of options that match the toolbar functions.

The user can do the following tasks:

- Saving changes (available if the user has network view administration permission)
- Creating new nodes, text or timestamp (available if the user has network view administration permission)
- Displaying the screen in projection mode
- Changing display settings

Reference: "Toolbar area" (p. 24)

Figure 5 Map background menu



Saving changes

From either the toolbar Save icon or background Save menu (Figure 5), the user can save all the changes made.

Important! The user should save after changes have been made to the Network View.

Creating new nodes, text or timestamp

From either the toolbar New icon or background New menu (Figure 5), the user can add new nodes, text or timestamp.

Displaying the screen in projection mode

From either the toolbar Projection Mode icon or background Projection Mode menu (Figure 5), the user can open another browser window showing only the display without any of the browser buttons.

Changing display settings

From either the toolbar Settings icon or background Settings menu (Figure 5), the user can change the following display properties:

- Show All Nodes: Toggle to show all nodes or only nodes with alerting information
- Node Size: The selected size is indicated by a check mark. The default is 0.
- Font Size: The selected size is indicated by a check mark. The default is 0.
- Line Size: The selected size is indicated by a check mark. The default is 0.
- Line Angle: The selected size is indicated by a check mark. The default is 0.

References

"Network View Administration" (p. 26) allows users to edit existing map preferences, add new maps, select thumbnail images, labels, background images, and more.

Using the Style Administration page ("Network View Style Administration" (p. 30)) allows users to select various attributes to be applied to network views, to search and modify a specific style or to create a new one.

□

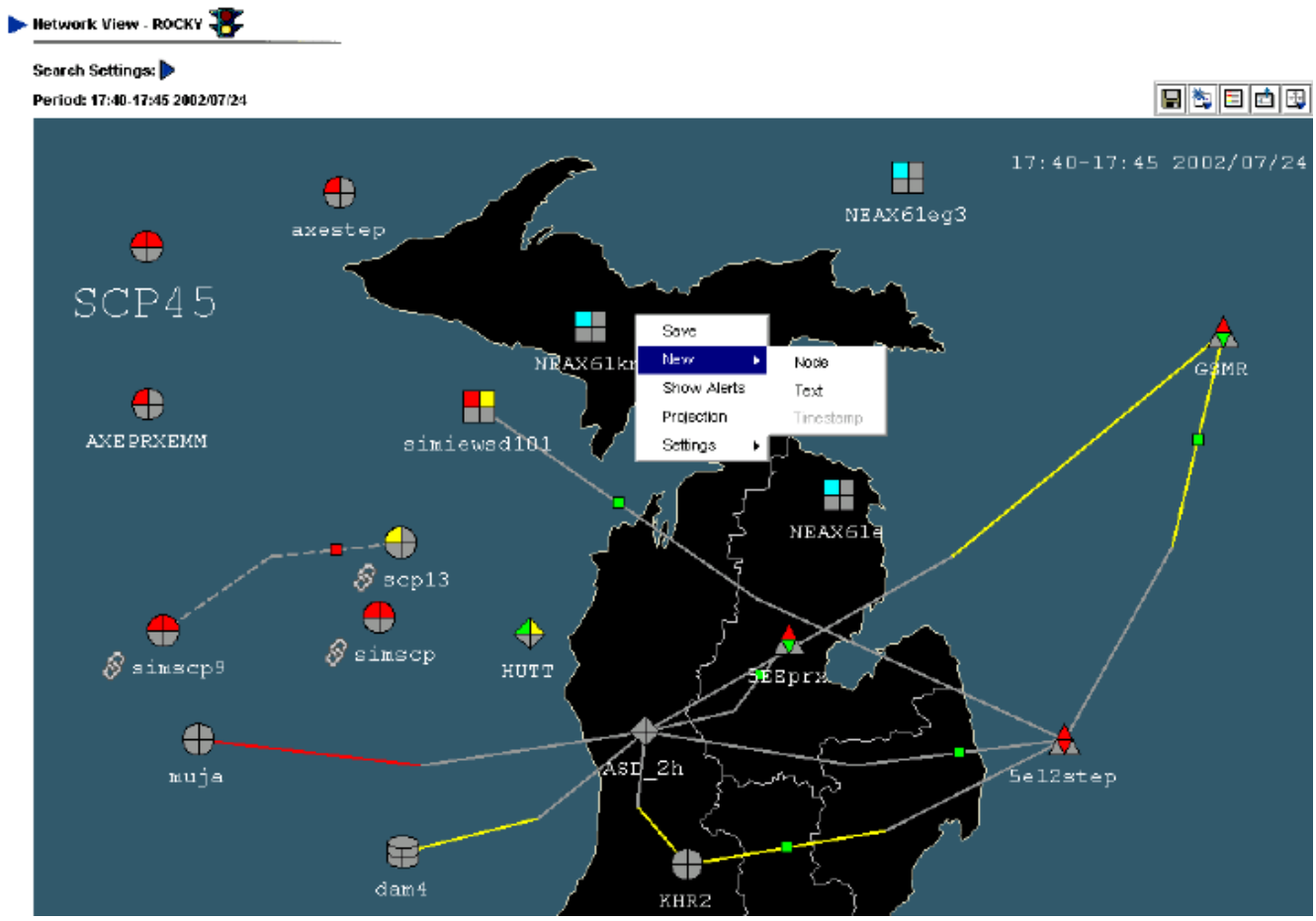
Adding a node

From either the toolbar “New” icon or the background “New” menu (Figure 6), the user can add a new node and its associated labels or text on the map display.

Important! The user should save after changes have been made to the Network View.

Reference: “Adding a node” (p. 11); “Toolbar area” (p. 24)

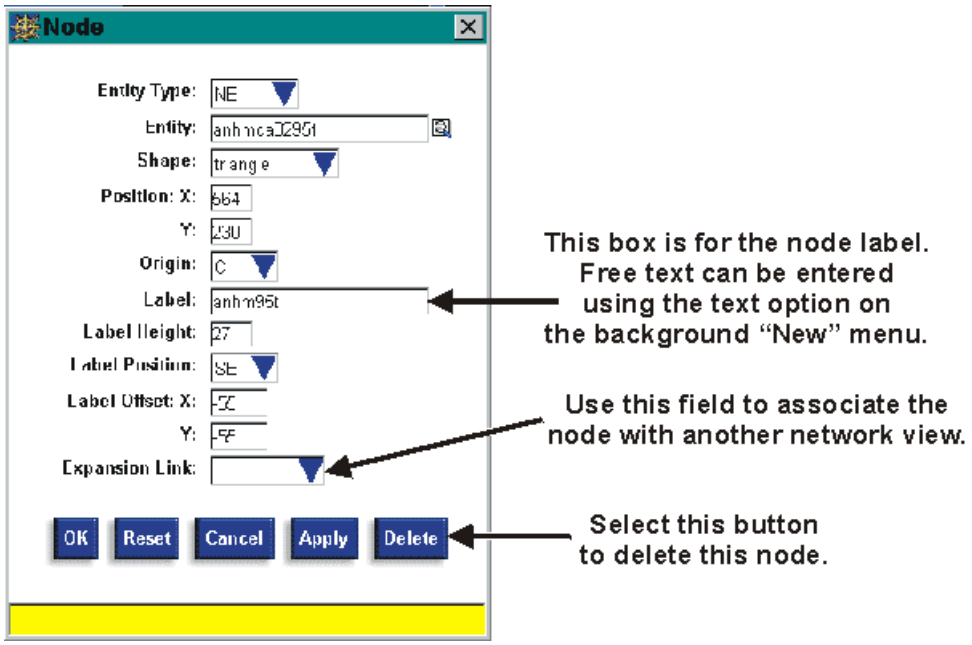
Figure 6 Background menu “New” option



Moving a node

You can move any of the nodes and their associated labels by dragging and dropping or by changing the data in the “Node” dialog window (Figure 7) accessed by clicking the menu mouse button on a node. You may locate a node anywhere in the window associated with the background (inside the background image or outside of the background image). When data is submitted, new locations of the nodes are stored.

Figure 7 Node dialog menu



Modifying a node

You can modify any of the attributes associated with Map Node found in the “Node” dialog window (Figure 6). This is accessed by clicking the menu mouse button on a node.

Important! The Network View Shape Facet Administration page allows users to assign alert groups to the facets of the various Network View and Link Status Schematic node shapes.

Reference: “Modifying a node” (p. 33)

Deleting a node

You can delete any of the nodes on the map display by menu clicking on the node you want to delete and selecting “Delete” from the Node dialog window (Figure 7). After the confirmation windows is approved the nodes are permanently removed from the map display.

Reference: “Deleting a node” (p. 34)

Text on a Network View

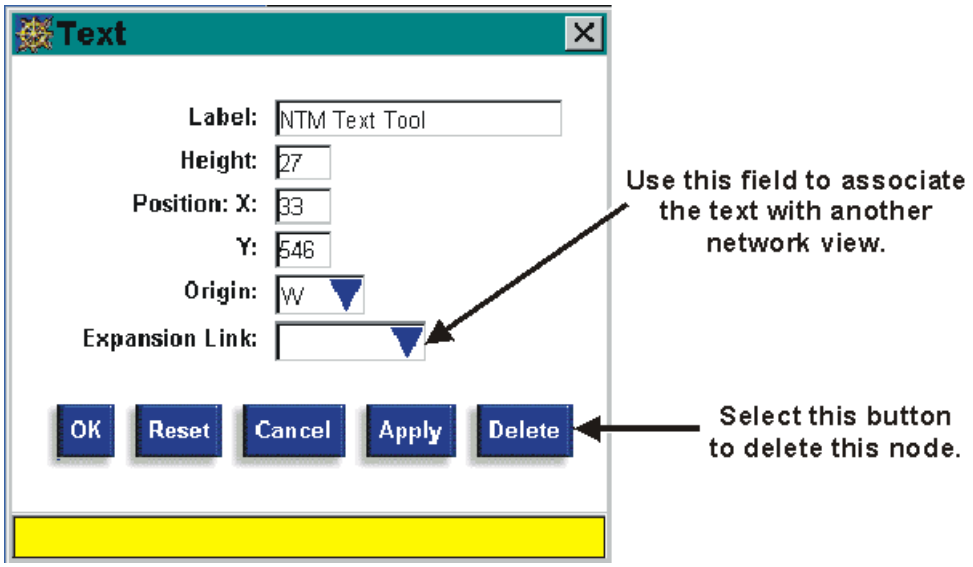
Purpose

You can add, move, modify or delete text on the map display in the same way as nodes. You can access the Text dialog window by clicking on the “New” toolbar button followed by the “Text” option, or menu mouse clicking on existing text.

Text associated with a node is often defined using the Node Label option (Figure 7).

Reference: See “Nodes on a Network View” (p. 11) for more information about adding, modifying, moving and deleting map items.

Figure 8 “New” Text dialog window



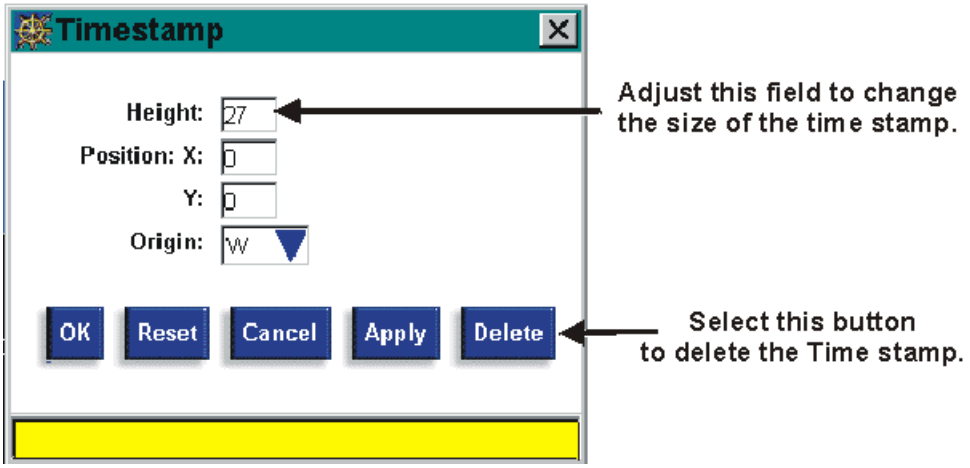
Timestamp on a Network View

Purpose

You can add, move, modify or delete a timestamp on the map display in the same way as nodes. You can access the Timestamp dialog window by clicking on the “New” toolbar button followed by the “Timestamp” option, or menu mouse clicking on existing timestamp. This option will not be available if a timestamp already exists on a Network View.

Reference: See “Nodes on a Network View” (p. 11) for more information about adding, modifying, moving and deleting map items.

Figure 9 Timestamp dialog window



Mouse menu options

Overview

Using the Menu button on the mouse and clicking on a node or a link, the following menu options are available:

- Facet Alerts — displays all alerts associated with the selected facet in the Network View Alerts Window.
- Node Alerts (From a node) — displays all alerts associated with the node containing the selected facet in the Network View Alerts Window.
- Node and Half-line Alerts (From a node) — displays all alerts associated with the node containing the selected facet. In addition, alerts are displayed for the half-lines originating at the selected node (Using the selected node as a Near End).
- Far End Half-line Alerts (From a node) — displays all alerts associated for the half-lines terminating at the selected node (Using the selected node as a Far End).
- Half-Line Alerts (From a link) — displays all alerts associated with the half-line containing the selected facet in the Network View Alerts Window (including all half-lines on the side of the line with the selected facet if multiple line styles appear between two nodes)
- Whole Line Alerts (From a link) — displays all alerts associated with the line containing the selected facet in the Network View Alerts Window (including all lines if multiple line styles appear between two nodes). When an end is a group node, it includes alerts for lines between nodes that are members of that group.
- Network Elements (From a node) — this option only appears for nodes that represent a set of network elements. It launches the Network Element details page for the set that this node represents. For nodes that aren't tied to a set, the menu item is "Network Element". Selecting it takes you to the Network Element detail page for that network element. For all nodes, either "Network Element" or "Network Elements" will be included in the menu.

  Reference: "Network Element Details page" (p. 11)
- Properties (From a node) — launches the Node Properties Dialog.

  Reference: "Nodes on a Network View" (p. 11)

Network View Legend

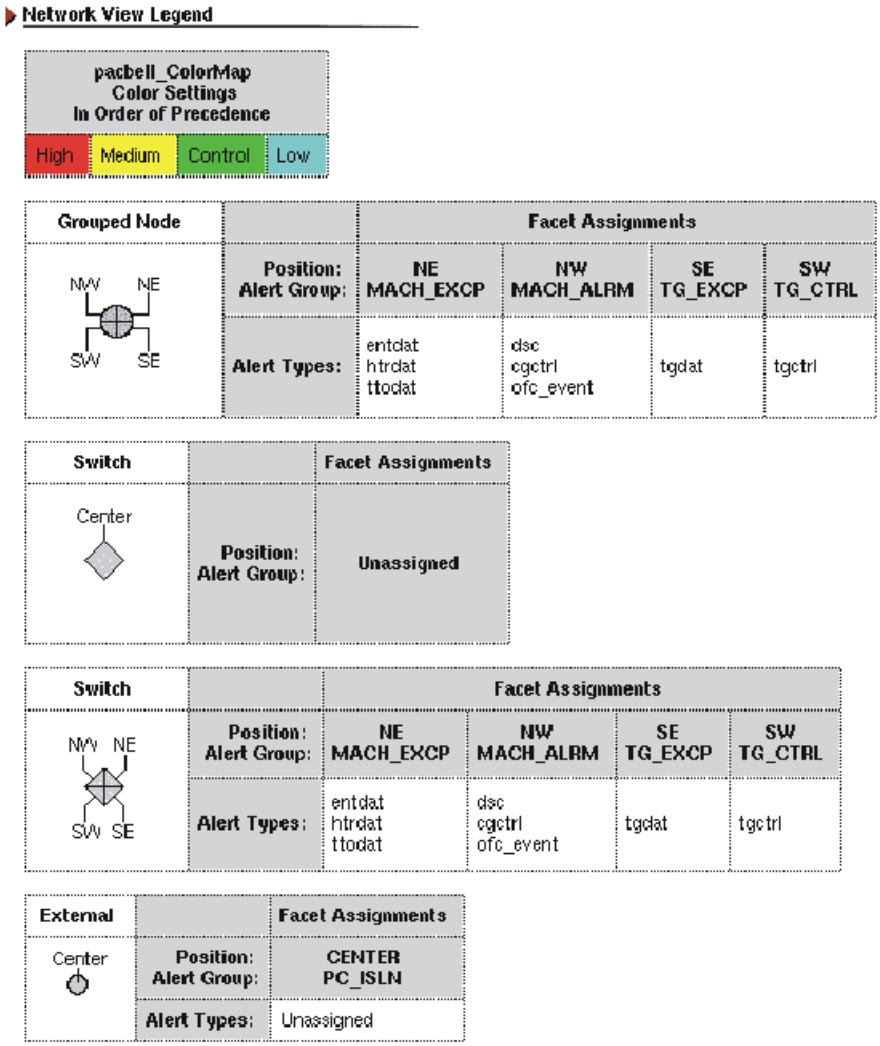
Purpose

You can view the following data:

- Node shape
- Index of colors and their associations with exception/event levels
- Alert groups with which a facet/satellite is associated
- Alert types with which an alert group is associated

To view these settings, select the “Legend” link from the Navigation area while on a map container or detail page.

Figure 10 Portion of Network View Legend



Alerts table

Overview

In alerts tables, alert data about a network element, trunk group, signaling link status, or network event is arranged in table form. The Alerts table container page supports manual and automatic updates. When first launched, the page is in manual mode by default. In auto-update mode, as data messages arrive from the host, table rows are updated internally to reflect the current state. The alerts table is updated every 30 seconds when new message data for all non-normal states is received.

Using the Alert Group Administration function users can associate alert groups with alert types to customize their alert displays.

Reference: “Network View Alert Group Administration” (p. 33)

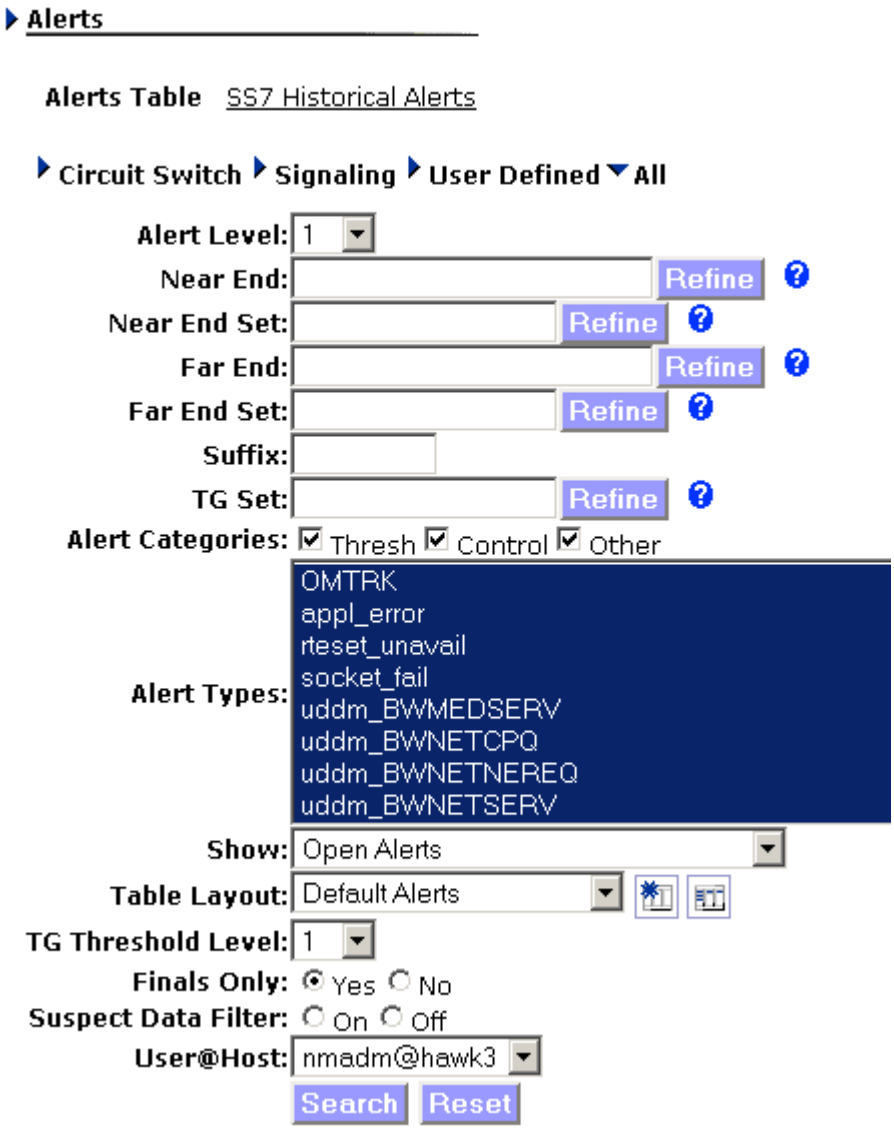
Accessing the Alerts table

You can access the Alerts table through the navigation link while viewing the Network Views container page (Figure 1), individual network views or the Alerts Table icon.

Alerts table search page

The Alerts table search page (Figure 11) allows the user to restrict the data retrieved based on various attributes of alerts or select SS7 Historical alerts (SS7 Historical alerts available with Feature 415, “Browser-based Access to NetMinder Signaling Traffic Management (STM) data”).

Figure 11 Alerts table search page



Search criteria

Table 3 describes the search criteria that may appear in the Search area.

Table 3 Search criteria on the Alerts Table search page

Label	Description
Alert Level	You can select the type of data displayed by restricting it to a specific alert type.
Near End	Near end network element. Valid values include all internal network elements.
Near End Set	The set associated with the Near End network element.
Far End	Far end network element. Valid values include all network elements, both internal and external.

Table 3 Search criteria on the Alerts Table search page (continued)

Label	Description
Far End Set	The set associated with the Far End network element.
Suffix	A user-defined string (up to 5 characters long) used to identify a particular trunk group.
Code	Controlled code. Valid codes may be up to 15 digits. If you enter a code, it will restrict the call gaps shown to just those of the number selected.
TG Set	Selecting this option restricts the view to only trunk groups that belong to the selected set.
Alert Categories	The selected categories narrows the Alert Types list. Allowed values are: Thresh, Control, Other. You can add more categories by editing the */nm/web/site/alertCategories_defs.pl* file.
Alert Types	This is a list of alerts your system will display. This list varies based on network elements supported and NTM features purchased.
Show	This list allows the user to select only Open Alerts or Open and Recently Closed Alerts.
Table Layout	Table layout choices. Use this option to choose the measurement types you want to see.
TG Threshold Level	Minimum exception threshold level. Values are 1 – 10.
Finals Only	The restricts the trunk groups displayed to Final Trunk Groups.
Suspect Data Filter	This field allows the user to choose to display Suspect data. **Important!** This is valid when the associated feature is purchased and activated. **Reference:** **Reference:** "Filter File" (p. 25) in the *Record Base Administration Guide*
User@Host	This displays current user ID and host information.

Recently Closed Alerts

Recently Closed Alert is an alert which is closed but persisted on the system for a limited duration. The system parameter "`recentLength`" controls the time of closed alert to be considered as Recently Closed Alert. The allowed values for this parameter are: 0, 5, 10, 15, 20, 25, 30. The value of "0" for the parameter `recentLength` indicate that Recently Closed Alerts would not be displayed. This parameter can be set up in the n_o_server configuration file: */nm/web/site/n_o_server_defs.pl*. The Recently Closed Alert always has a value in the End Time column and Open Alert does not. This can help distinguish Open Alerts from Recently Closed Alerts on the container page.

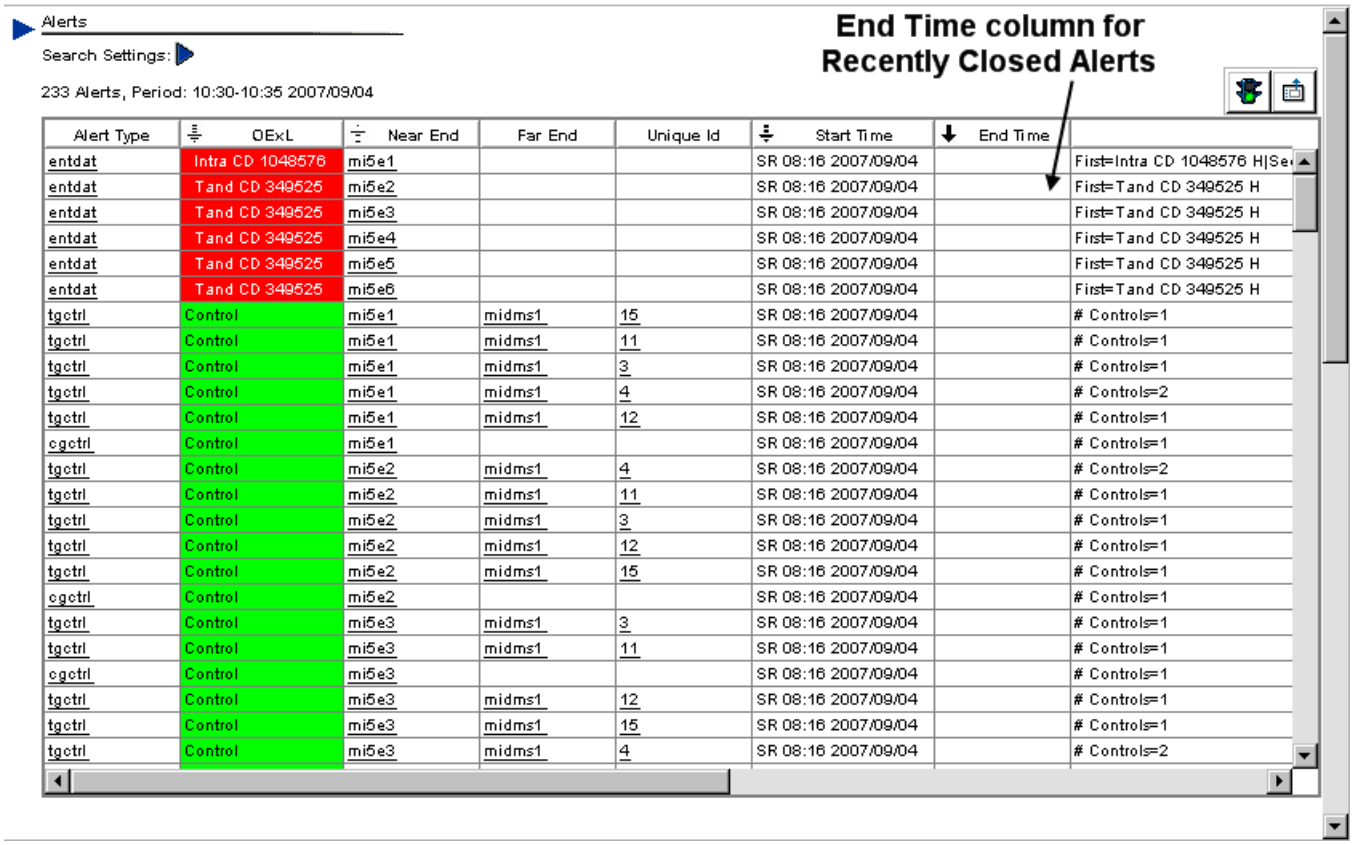
Alerts table container page

The Alerts table container page contains a data table, the layout of which depends on the table layout selected on the search page. It also contains an area below the page title that allows the user to select from the various Alert data types. It has a blue “Modify” button which navigates back to the Alerts table search page where the values displayed on the Alerts table container page are used as initial values on another Alerts table search page. The user has an option of four predefined table layouts:

- Default Alerts (Figure 12) shows network element and trunk group data in the same table.
- Link Status Alerts (Figure 13) show Signaling Link alerts.
- Network Elements Alerts (Figure 14) shows the maximum exception level, the managed object associated with the maximum exception level, and the next five highest managed object exceptions, for each network element in exception.
- Trunk Group Alerts (Figure 15) shows the maximum exception level, the managed object associated with the maximum exception level, and up to six other trunk group managed objects, whether they are in exception level or not, for each trunk group in exception.

The user can create a new table Layout by clicking the New Table Layout button. Each of the Table Layouts can be changed using Edit Table Layout button.

Figure 12 Default alerts



Alert Type	OExL	Near End	Far End	Unique Id	Start Time	End Time	
entdat	Intra CD 1048576	mi5e1			SR 08:16 2007/09/04		First=Intra CD 1048576 H|Se
entdat	Tand CD 349525	mi5e2			SR 08:16 2007/09/04		First=Tand CD 349525 H
entdat	Tand CD 349525	mi5e3			SR 08:16 2007/09/04		First=Tand CD 349525 H
entdat	Tand CD 349525	mi5e4			SR 08:16 2007/09/04		First=Tand CD 349525 H
entdat	Tand CD 349525	mi5e5			SR 08:16 2007/09/04		First=Tand CD 349525 H
entdat	Tand CD 349525	mi5e6			SR 08:16 2007/09/04		First=Tand CD 349525 H
tgctrl	Control	mi5e1	midms1	15	SR 08:16 2007/09/04		# Controls=1
tgctrl	Control	mi5e1	midms1	11	SR 08:16 2007/09/04		# Controls=1
tgctrl	Control	mi5e1	midms1	3	SR 08:16 2007/09/04		# Controls=1
tgctrl	Control	mi5e1	midms1	4	SR 08:16 2007/09/04		# Controls=2
tgctrl	Control	mi5e1	midms1	12	SR 08:16 2007/09/04		# Controls=1
cgctrl	Control	mi5e1			SR 08:16 2007/09/04		# Controls=1
tgctrl	Control	mi5e2	midms1	4	SR 08:16 2007/09/04		# Controls=2
tgctrl	Control	mi5e2	midms1	11	SR 08:16 2007/09/04		# Controls=1
tgctrl	Control	mi5e2	midms1	3	SR 08:16 2007/09/04		# Controls=1
tgctrl	Control	mi5e2	midms1	12	SR 08:16 2007/09/04		# Controls=1
tgctrl	Control	mi5e2	midms1	15	SR 08:16 2007/09/04		# Controls=1
cgctrl	Control	mi5e2			SR 08:16 2007/09/04		# Controls=1
tgctrl	Control	mi5e3	midms1	3	SR 08:16 2007/09/04		# Controls=1
tgctrl	Control	mi5e3	midms1	11	SR 08:16 2007/09/04		# Controls=1
cgctrl	Control	mi5e3			SR 08:16 2007/09/04		# Controls=1
tgctrl	Control	mi5e3	midms1	12	SR 08:16 2007/09/04		# Controls=1
tgctrl	Control	mi5e3	midms1	15	SR 08:16 2007/09/04		# Controls=1
tgctrl	Control	mi5e3	midms1	4	SR 08:16 2007/09/04		# Controls=2

Figure 13 Link Status alerts

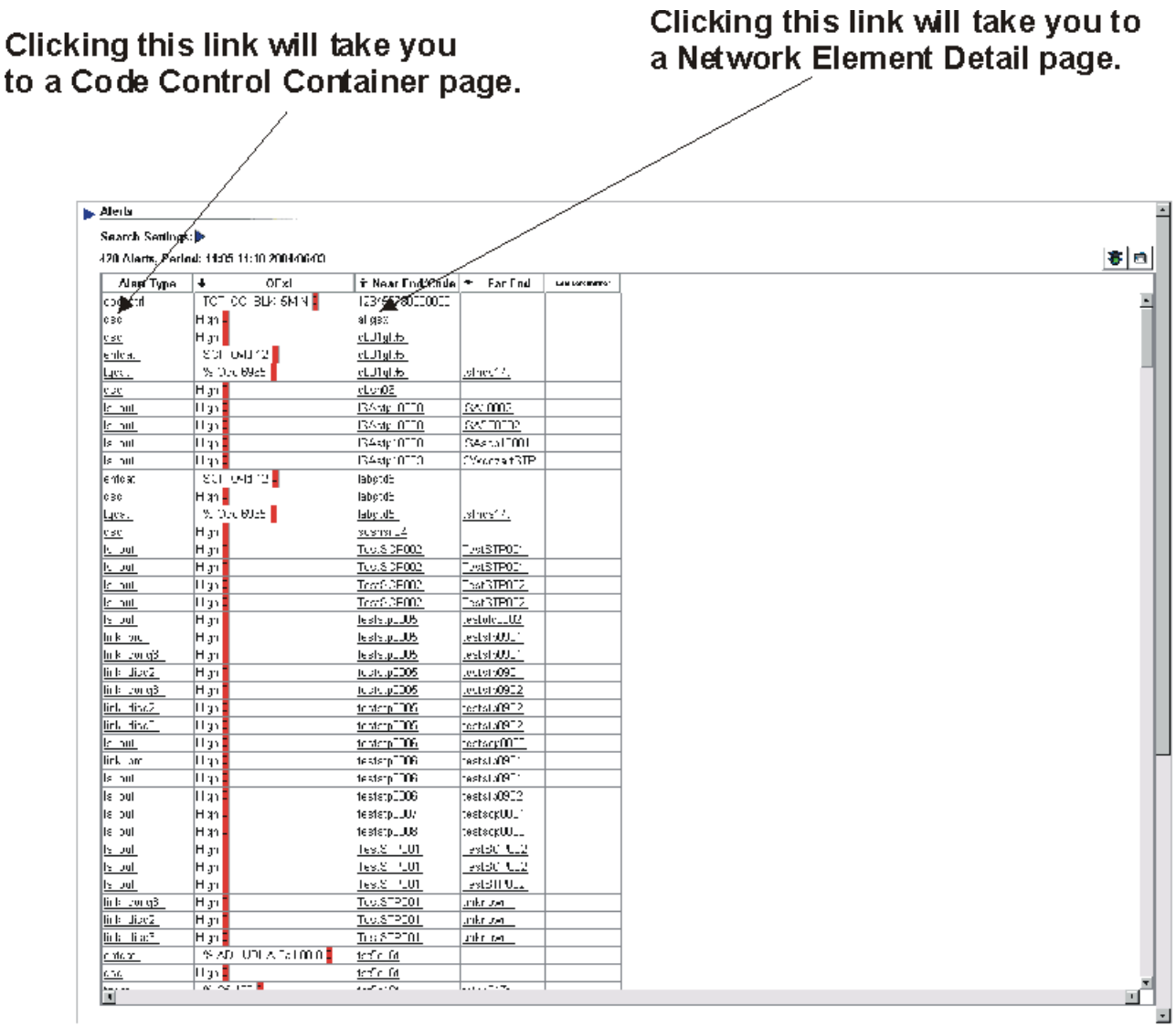


Figure 14 Network Elements alerts

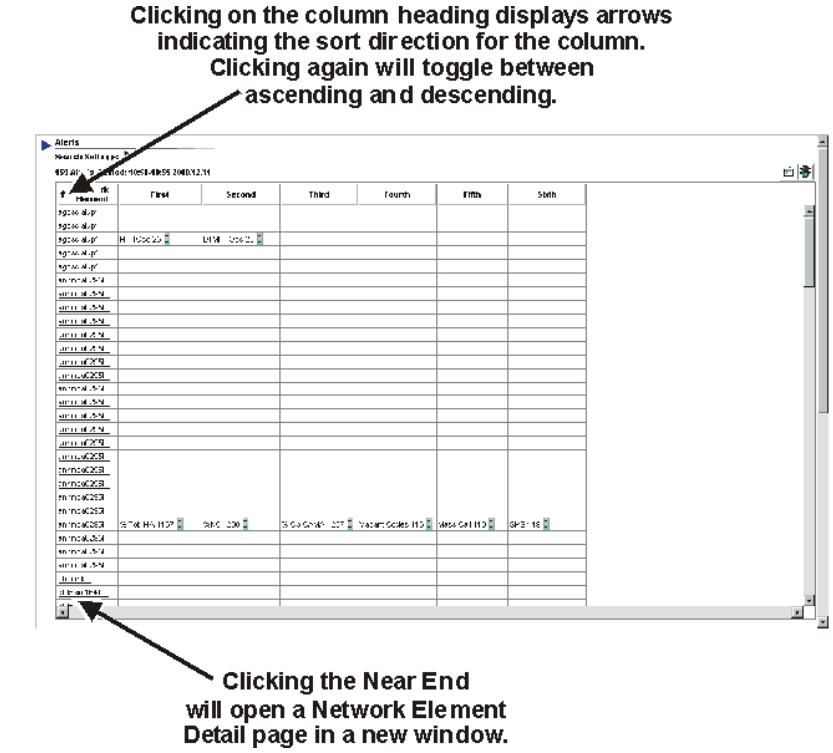
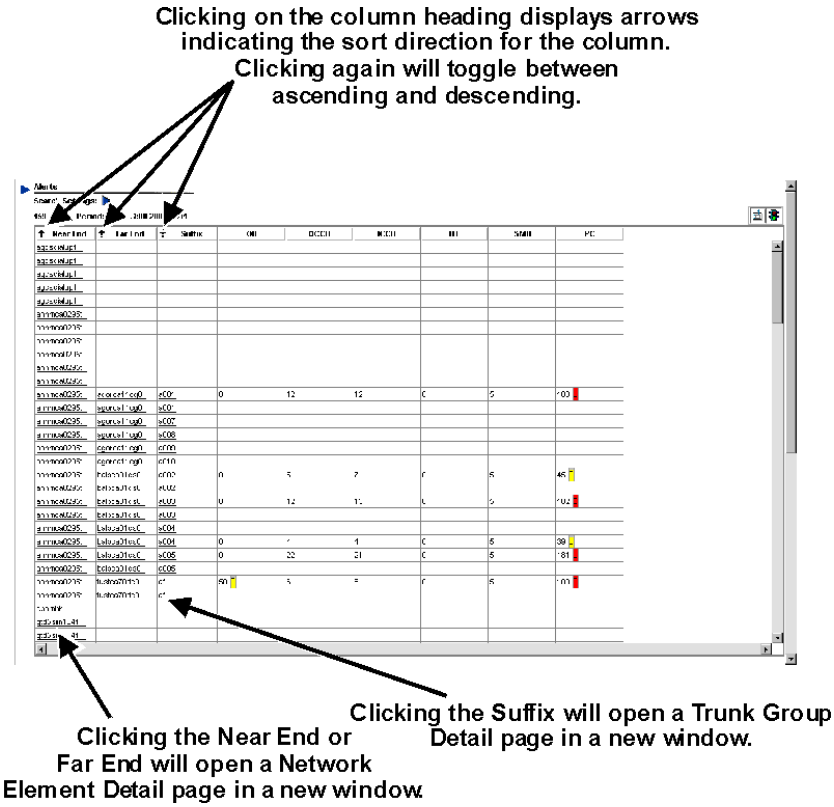


Figure 15 Trunk Group alerts



SS7 Historical Alerts

Purpose

The SS7 Historical Alerts page (Figure 16) allows users to view alerts stored in previous periods.

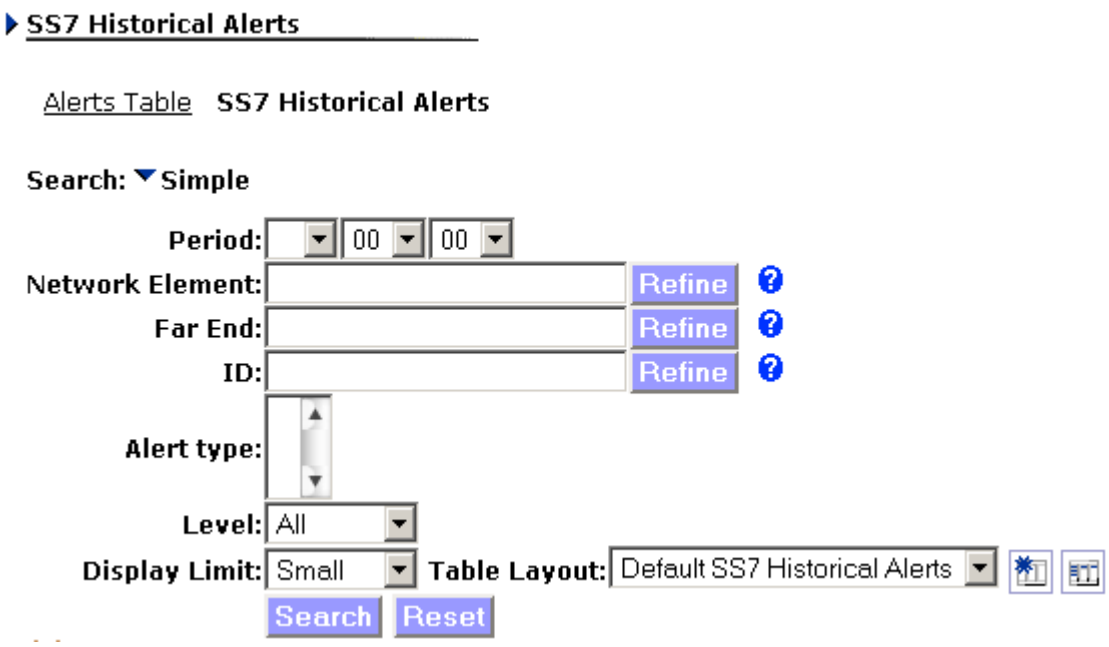
Prerequisite

SS7 historical alerts can be accessed when Feature 415, “Browser-based Access to NetMinder Signaling Traffic Management (STM) data” is purchased.

SS7 Historical Alerts Search Page

Various alert conditions can be selected for viewing using the search restriction field entitled “Alert Type”.

Figure 16 SS7 Historical Alerts search page



SS7 Historical Alerts Container Page

The SS7 Historical container page (Figure 17) displays historical data from a previous period. The data reflects alerts that were exiting alert status, entering alert status, or were in alert status throughout the entire 5-minute period.

Figure 17 SS7 Historical Alerts container page

SS7 Historical Alerts

Alerts Table **SS7 Historical Alerts**

Search: Simple

100/469 SS7 Historical Alerts, Period: 10:45:00-10:50:00 2004/6/4

ElementName	FarElemName	Id	Level	AlertType	Category	Data	Duration	ElType	NasEndTime
TestSCP002	TestSCP001		H	loc-seps_iso	system	homeSTPs=[TestSTP001-TestSTP002].	300	scp	
TestSCP001	TestSCP002		H	loc-seps_iso	system	homeSTPs=[TestSTP001-TestSTP002].	300	scp	
teststp0005	teststp0901	BL005901	M	link_short	system	1 of 2 links in service	300	ls	04-JUN-2004 10:45:02
ISAstp10000	ISAscp10001	ALISA000	M	link_short	system	1 of 2 links in service	300	ls	04-JUN-2004 10:45:30
ISAstp10000	ISAscp10001	ALISA000	M	link_short	system	1 of 2 links in service	300	ls	04-JUN-2004 10:46:32
teststp0005	teststp0901	BL005901	M	link_short	system	1 of 2 links in service	300	ls	04-JUN-2004 10:46:32
ISAstp10000	ISAscp10001	ALISA000	M	link_short	system	1 of 2 links in service	300	ls	04-JUN-2004 10:47:31
teststp0005	teststp0901	BL005901	M	link_short	system	1 of 2 links in service	300	ls	04-JUN-2004 10:47:31
teststp0005	teststp0901	BL005901	M	link_short	system	1 of 2 links in service	300	ls	04-JUN-2004 10:48:32
ISAstp10000	ISAscp10001	ALISA000	M	link_short	system	1 of 2 links in service	300	ls	04-JUN-2004 10:49:00
ISAstp10000	ISAscp10001	ALISA000	M	link_short	system	1 of 2 links in service	300	ls	
teststp0005	teststp0901	BL005901	M	link_short	system	1 of 2 links in service	300	ls	04-JUN-2004 10:49:32
teststp0005	teststp0901	BL005901	M	link_short	system	1 of 2 links in service	300	ls	
lwvlboxabba	unknown	222_2W_SS7-unknown	H	OMTRK	exception	#excp=1 PercOCC 100.00	300	UDDM_OMTRK	
lwvlboxabba	unknown	288_2W_SS7-unknown	H	OMTRK	exception	#excp=1 PercOCC 100.00	300	UDDM_OMTRK	
lwvlboxabba	unknown	CHRISJONES-unknown	H	OMTRK	exception	#excp=1 ASRIN 94.00	300	UDDM_OMTRK	
lwvlboxabba	unknown	DMS100-unknown	L	OMTRK	exception	#excp=1 ASRIN 66.00	300	UDDM_OMTRK	
lwvlboxabba	unknown	CHRISJONES5ESS-unknow	H	OMTRK	exception	#excp=1 ASRIN 100.00	300	UDDM_OMTRK	
CWcozartSTP			H	data-fail	system		300	stp	
CWcozartSTP			M	data-late	system		300	stp	
CWcozartSTP			M	Stp	exception	#excp=8 MsuDiscInvDpc 30	300	SS7_Stp	
ISAstp10003	CWcozartSTP	BLISA100	H	ls_out	alarm	pROLks=2 failLks=2 oosLks=2	300	LinkSet	04-JUN-2004 10:45:21
ISAstp10003	CWcozartSTP	BLISA100	H	ls_out	alarm	pROLks=2 failLks=2 oosLks=2	300	LinkSet	04-JUN-2004 10:46:25

Purpose

With the introduction of NTM Feature 437, “Enhanced Thresholding and Analysis”, NTM can monitor network-wide events. Users can choose to display this data for multiple periods of the event ranging from 30 minutes up to 4 hours. NTM monitors two types of network event:

- Code Events (Figure 18)
- Mass Call Events (Figure 19)
- 24-Hour Final TG Overflow Events
- Job Status

Figure 18 Code Control events alerts page

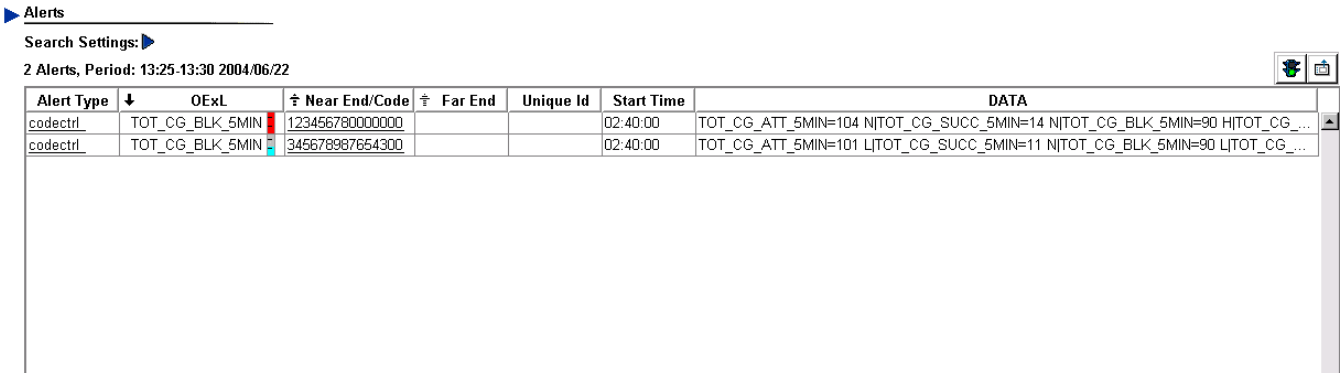
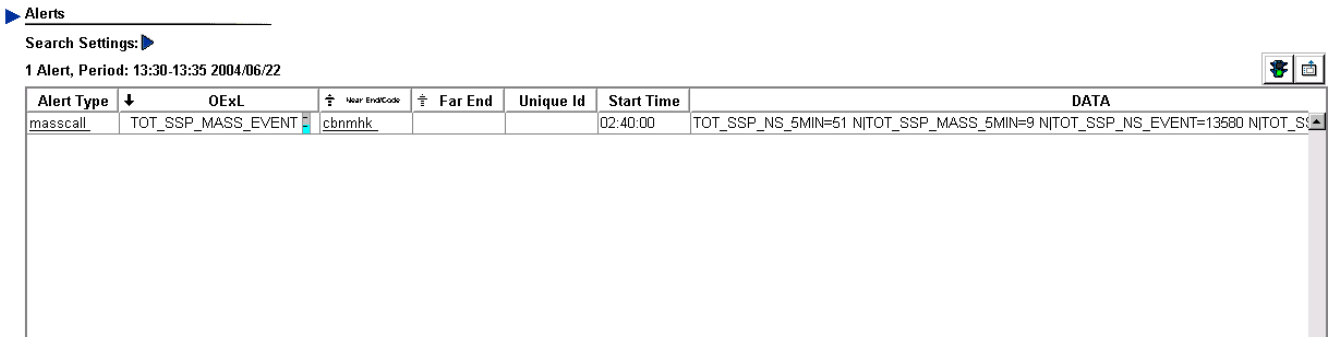


Figure 19 SCP Control events alerts page



The effect of dayend or stopping the system

Events being monitored at dayend or when the system is stopped are assumed by NTM to still be in progress when the system is restarted. If the criteria for concluding an event is met upon the system being restarted, then the event will be considered concluded.

□

General tasks on the Network Views pages

Overview

Purpose

This section provides the procedures for general tasks on the Network Views pages.

Before you begin

Before any modification can be done to nodes or labels on a map:

- The RSPTE File and the Sets File should be updated with data about the changes to be made to the node.

  Reference: Chapter 5, "Record Base Files" in the *Record Base Administration Guide*

  Important! To relocate the Node, locate the mouse arrow over the Node, click and hold the left mouse button, move the Node to a new location and release the left mouse button.

Contents

This section contains the following topics:

Adding a node	4-32
Modifying a node	4-33
Deleting a node	4-34
Adding a link to a Network View	4-35
Deleting a link from a Network View	4-36
Adding a timestamp or text	4-37
Modifying a timestamp or text	4-39
Deleting a timestamp or text	4-40

Adding a node

Instructions

Follow these steps to add a node:

1 Open the map on which you wish to add a node.

Result: The map you selected is displayed.

2 Select the New toolbar button or click the mouse menu button anywhere on the Network View except on nodes or links. Select **Node** or **New > Node** from the menu displayed.

Result: Node dialog box is displayed.

3 Enter the desired values.

Hint: You can select **Apply** *to see if the values are acceptable before selecting* **OK** *and exiting the dialog box.*

Result: Node appears on the Network View.

4 Select the Save toolbar button.

Result: Save verification box appears.

5 Click **OK** on the Save verification box.

END OF STEPS

□

Modifying a node

Instructions

Follow these steps to modify a node:

1 Open the map on which you wish to modify a node.

Result: The map you selected appears.

2 Place the cursor over the Node on the Network View and click the menu mouse button. Select the Properties box.

Result: Node dialog box is displayed.

3 Change the values desired.

Hint: You can select **Apply** *to see if the values are acceptable before selecting* **OK** *and exiting the dialog box.*

Result: Node appears on the Network View.

4 Select the Save toolbar button.

Result: Save verification box appears.

5 Click **OK** on the Save verification box.

END OF STEPS

□

Deleting a node

Instructions

Follow these steps to delete a node:

1 Open the map from which you wish to delete a node.

Result: The map you selected appears.

2 Place the cursor over the Node on the Network View and click the menu mouse button.Select the Properties box.

Result: Node dialog box is displayed.

3 Select **Delete**. Answer **Yes** to the verification dialog box.

Result: Node disappears from the Network View.

4 Select the Save toolbar button.

Result: Save verification box appears.

5 Click **OK** on the Save verification box.

6 If the entities or sets are being removed from NTM, remove the appropriate entries from the Sets File or the RSPTE File.

END OF STEPS

Adding a link to a Network View

Instructions

Follow these steps to add a link to a Network View:

1 Open the map on which you wish to add a Network View link.

Result: The map you selected appears.

2 Place the cursor over the desired node on the Network View and click the menu mouse button.

3 Select the Properties box.

Result: The Node dialog box is displayed.

4 Select the Network View name from the list in the Expansion Link menu that you wish to create a link to for this node.

5 Select **OK** to exit the Dialog window.

Result: A link appears next to the node (Figure 3).

6 Select the Save toolbar button.

Result: Save verification box appears.

7 Click **OK** on the Save verification box.

END OF STEPS

□

Deleting a link from a Network View

Instructions

Follow these steps to delete a link from a Network View:

1. Open the map from which you wish to delete a link to a Network View.

   Result: The map you selected appears.

2. Place the cursor over the Node with the link you wish to remove on the Network View and click the menu mouse button.

3. Select the Properties menu item.

   Result: Node dialog box is displayed.

4. Select the top blank option from the list in the Expansion Link menu.

5. Select **OK** to exit the Dialog window.

6. Select the Save toolbar button.

   Result: Save verification box appears.

7. Click **OK** on the Save verification box.

END OF STEPS

□

Adding a timestamp or text

Instructions

Follow these steps to add a timestamp or text:

1 Open the network view on which you wish to add a timestamp.

Result: The map you selected appears.

2 Select the New toolbar button or click the mouse menu button anywhere on the Network View except on nodes or links.

3 Select **Timestamp/Text** or **New > Timestamp/Text** from the menu displayed.

Hint: If **Timestamp** *appears "grayed-out" on the menu, this indicates the timestamp has previously been added.*

Result: Timestamp/Text dialog box is displayed.

4 Either select **OK** to accept default values or enter values in the Height; Position and Origin boxes and then select **OK**.

Hint: You can select **Apply** *to see if the values are acceptable before selecting* **OK** *and exiting the dialog box.*

Result: Timestamp/Text appears on the Network View.

Hint: To relocate the Timestamp/Text, locate the mouse arrow over the Timestamp/Text, click and hold the mouse button, move the Timestamp/Text to a new location, and release the mouse button.

5 Select the Save toolbar button.

Result: Save verification box appears.

6 Click **OK** on the Save verification box.

END OF STEPS

□

Modifying a timestamp or text

Instructions

Follow these steps to modify a timestamp or text:

1 Open the network view on which you wish to modify a timestamp/text.

Result: The map you selected appears.

2 Place the cursor over the Timestamp/Text on the Network View and click the menu mouse button. Select the Properties box.

Result: Timestamp/Text dialog box is displayed.

3 Enter values in the Height, Position, and Origin boxes and then select **OK**.

Hint: You can select **Apply** *to see if the changes are acceptable before selecting* **OK** *and exiting the dialog box.*

Result: Timestamp appears on the Network View with the new values.

Hint: To relocate the Timestamp/Text, locate the mouse arrow over the Timestamp/Text, press and hold the mouse button, move the Timestamp/Text to a new location, and release the mouse button.

4 Select the Save toolbar button.

Result: Save verification box appears.

5 Click **OK** on the Save verification box.

END OF STEPS

□

Deleting a timestamp or text

Instructions

Follow these steps to delete a timestamp or text:

1. Open the network view on which you wish to modify a timestamp/text.

   Result: The map you selected appears.

2. Place the cursor over the Timestamp/Text on the Network View and click the menu mouse button. Select the Properties box.

   Result: Timestamp/Text dialog box is displayed.

3. Select **Delete**. Answer **Yes** to the verification dialog box.

   Result: Timestamp/Text disappears from the Network View.

4. Select the Save toolbar button.

   Result: Save verification box appears.

5. Click **OK** on the Save verification box.

END OF STEPS

□

5 Controls

Overview

Purpose

This chapter contains information about the controls pages and their components.

Contents

This chapter contains the following topics:

Background	5-2
Parameter area	5-6
Code Controls	5-7
Protective TG Controls	5-19
Expansive TG Controls	5-27
Other Controls	5-49
Control Summary page	5-55
General tasks on the Control pages	5-57

Background

Purpose

The following control categories are available under the Controls icon (Figure 1) on the Launch page:

- Code Controls — Links to the Code Control search page
- Protective TG Controls — Links to the Protective TG Control search page
- Expansive TG Controls — Links to the Expansive TG Control search page
- Other Controls - Links to the Other Control search page

The following control-related functions are also available from the GUI, but are not accessible from the Launch page.

- Control Summary page

Figure 1 Control icon

Viewing controls

Controls can be viewed in the same manner as other data in the system. You can specify search criteria and retrieve matching control information by executing the search. Historic controls from the database can also be accessed.

Important! The control log can be accessed through the Control Log icon.

Reference: "Control Log" (p. 7)

In addition to active controls, a page may display potential controls. Potential controls are generated for switches and trunk groups that may have a control applied to them, but do not currently have an active control. Both active and potential controls may be selected so that you can manipulate them.

Important! Potential controls are not valid for reroute.

Adding and modifying controls

Once controls have been retrieved, you may select one or more of them on which to perform the “apply controls” action. This action transfers the selected controls to another display, called the Controls Request page, that presents the appropriate parameters for the control type, switch types and generics that have been selected. You may then specify the control parameters and execute the control requests. If all requests are successful, you are returned to the previous display for viewing controls. Request failures remain in the display with the parameter selections and may be re-executed.

A shortcut for specifying the control parameters is provided with the Parameter sets capability.

> **Important!** If you interrupt or leave the page while the execute or validate action is in progress, the requests continue execution on the host, but no further status or results are presented to you.

Validating a control request

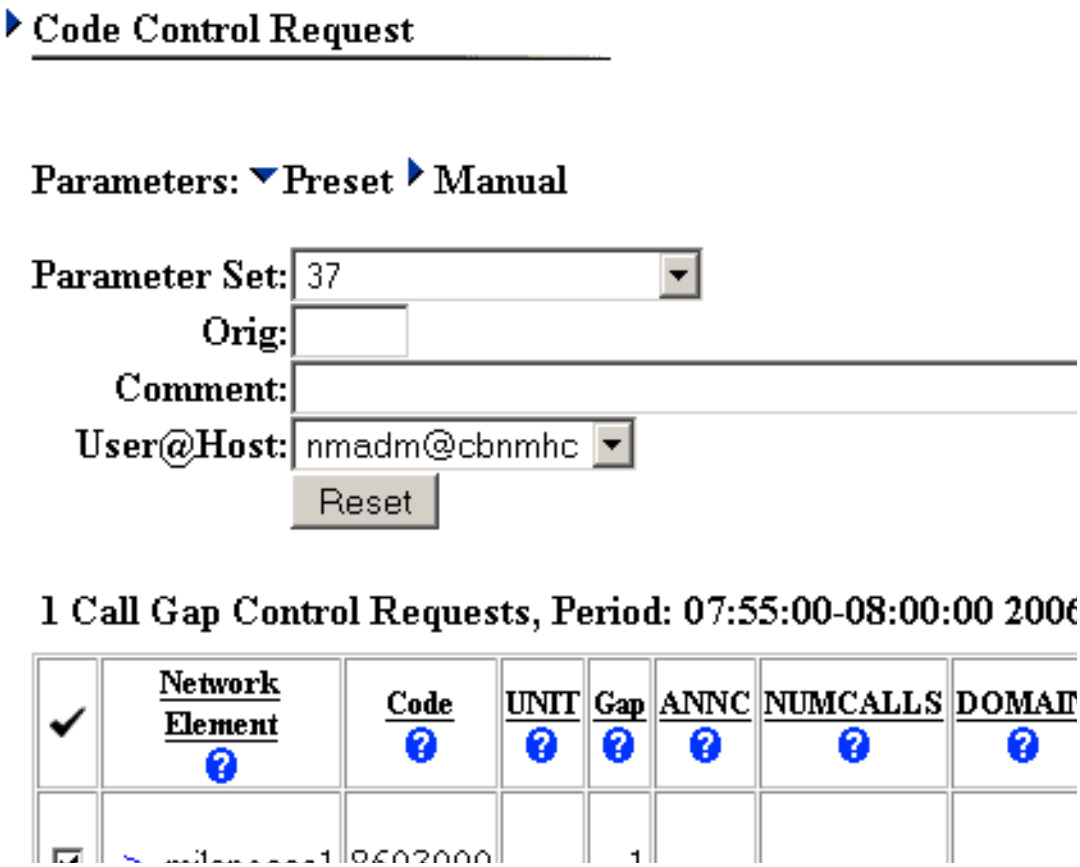
The Validate button validates the selected control requests without executing them. The Code Control Request page is displayed after the validation, with the following differences:

- Requests that were not selected are removed from the Data Table. All other requests remain selected.
- Successfully validated requests are indicated in the STATUS column by a graphical success indicator (green check).
- Failures are indicated as they are for the Execute button.

  Reference: “Executing a control request” (p. 4)
- Failures are sorted to the top of the table.

Figure 2 shows an example of the validation request result.

Figure 2 Code control request page: Validation request result



Executing a control request

The Execute button executes the selected control requests. The request action is derived from the current state of the control. If there is:

- an active control — the action is modify
- a potential control (not active) — the action is add

If all control requests complete successfully, the refreshed Code Control container page is displayed (this is the same page on which you entered the search criteria and selected the active/potential controls to execute). If the request fails, the screen will return with a red failed attempt indicator.

Reference: "Failures" (p. 5)

Deleting a control

Once controls have been retrieved, you may select one or more of them on which to select the Delete button and perform the delete action.

A confirmation window is presented to you. If you confirm the operation, then:

- Selected active controls are deleted
- Selected potential controls are ignored
- An updated Control container page is displayed if all delete requests are successful (all row selections are cleared in the updated page)
- Failed delete requests are displayed in the same manner as failed add and modify requests. Delete failures are presented in a separate display and may be re-executed.

  Reference: See "Failures" (p. 5) for information on how failed requests are presented.

Failures

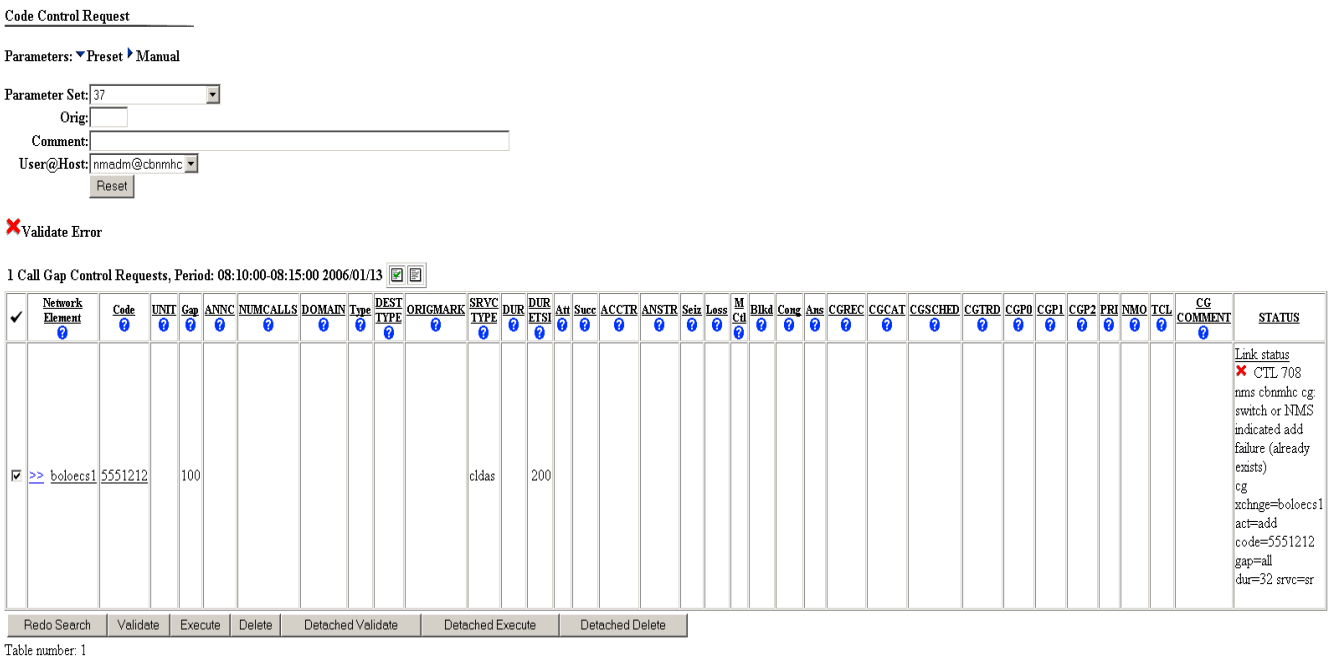
If there are any control request failures, the Code Control Request page is displayed with a graphical failure indicator (red X) above the data table title. The failed request includes:

- A graphical failure indicator (red X) at the beginning of each failure message.
- The failed control requests displayed in the Data Table with their corresponding failure message in the "STATUS" column.
- The control parameters that were attempted are reflected in the Data Table.

All rows also remain selected so that you may re-execute the requests. Successfully applied controls will reflect in the Code control container page (Figure 4).

Figure 3 shows an example of a Code Control Request failure.

Figure 3 Code Control Request page: Failed control request



Parameter area

Overview

A parameter area is the area of a control request display that contains various control parameters.

The parameter area provides two modes of operation:

- Preset parameter mode — used with Parameter sets (default)
- Manual parameter mode — used to set parameters manually at the time the control is applied

Parameter sets

A parameter set is a predefined group of control parameter values that may be used to quickly apply a control to one or more switches. A particular parameter set applies to a single control type and contains the valid parameters for all switch types/generics for that control type.

Parameter sets are supported for the Code Control and Protective Trunk Group Control displays. A set of default parameter sets is provided, or you may create your own.

A parameter set has the following attributes:

Table 1 Parameter set attributes

Name	Description	Required
Name	Name by which you can identify the set	required
Control Type	Control type to which the set applies (e.g., Call Gap)	required
Description	Description of the set	optional
Owner	User ID indicating who created or last modified the set	set by system
Parameter Values	Parameter values that apply to the given control for all switch types and generics valid for the site	optional

References

Additional information is included in the sections that describe the control pages that use Parameter Sets (“Code Controls” (p. 7) and “Protective TG Controls” (p. 19)).

For specific parameter values, see the associated command in the *Input Commands Guide*.

Code Controls

Overview

Purpose

This section describes the display for viewing and implementing code controls. The code controls that are supported are listed in the Code Controls search page section.

References

See the cg command (4-21) in the *Input Commands Guide* for more information about Call Gaps and predefined parameters used in this section.

Contents

This section contains the following topics:

Code Controls search page	5-8
Code Controls container page	5-11
Code Control Request page	5-13
Code Controls trend page	5-16

Code Controls search page

Purpose

The Code Controls search page contains a search area which has one search mode.

If the Period field is set to access a historical period (not “Current”), the controls matching the search criteria for the selected data collection period are retrieved. No potential controls are generated.

Search criteria

Table 2 describes the search criteria that can appear in the search area:

Table 2 Code Controls search criteria (Sheet 1 of 2)

Label	Description
Period	Data collection period. Options are current or a historical period.
CIC	Inter-exchange carrier prefix. Limit of 4 characters. Blank by default.
Code(s)	Code(s). User may enter multiple codes, separated by the comma character. Blank by default. You may choose to match the code(s) exactly, or search for codes greater than or less than the value(s) you entered. This is NOT a numeric greater than or less than operation. It is close to a string greater than or less than operation. Example: • If the code is 614, “Includes codes greater than” would mean all codes beginning with 614, e.g., 614,614555, 6148601212. For this application, 615, for example, is NOT greater than 614. • If the code is 6145, “Includes codes less than” would mean all codes starting with 6, 61, 614 etc., except for the exact code of 6145. **Reference: Reference:** See the cg command (4-21) in the *Input Commands Guide* for field values and restrictions.
Network Element Area Rank Set	Near end network element. Valid values include all internal network elements. By default, Near End is blank, Area is unselected, rank is 5, and set is blank.
Exclude Element	Allows specified network elements to be excluded from control search.
Exclude Set	Allows specified sets to be excluded from control search.

Table 2 Code Controls search criteria (Sheet 2 of 2)

Label	Description
Retrieve	Code control status selection. Select All, Active Only, or Potential Only
Control Type (*GTD*-5 only)	Call Gap, Routing Codes or Terminating Codes
Display Limit	Maximum number of rows to be retrieved by your search. Options are: • Small — 100 rows • Medium — 300 rows • Large — 1200 rows
User@Host	Choice of user IDs on a specific host machine.

Displaying potential and assigned controls

Depending upon which data collection period is selected, searches return assigned controls, potential controls or both. The potential controls represent possible controls that can be assigned.

IF the …	AND the …	THEN …
Period field is set to "Current"	"Retrieve" option is set to "All"	all active controls matching the search criteria are retrieved and a potential control row is generated for each item searched that does not have an active control that matches the search criteria.
Period field is set to "Current"	"Retrieve" option is set to "Active Only"	all active controls matching the search criteria are retrieved.
Period field is set to "Current"	"Retrieve" option is set to "Potential Only"	a potential control row is generated for each item searched that does not have an active control that matches the search criteria.
Period field is set to a period ***other than*** "Current"	"Retrieve" option is set to "All" or "Active Only"	No potential controls are generated for a historical period.

View-only mode

A view-only mode applies when a historic data collection period is specified in the Search area, or when you have the page operating in Auto-Update mode. In view only mode, the various form objects and controls that allow you to manipulate the controls are not available. The following display objects may not be available in view only mode:

- Select All, Clear All, Previous, and Next toolbar functions
- SELECT column in the Data Table
- Control Type menu beneath the Data Table

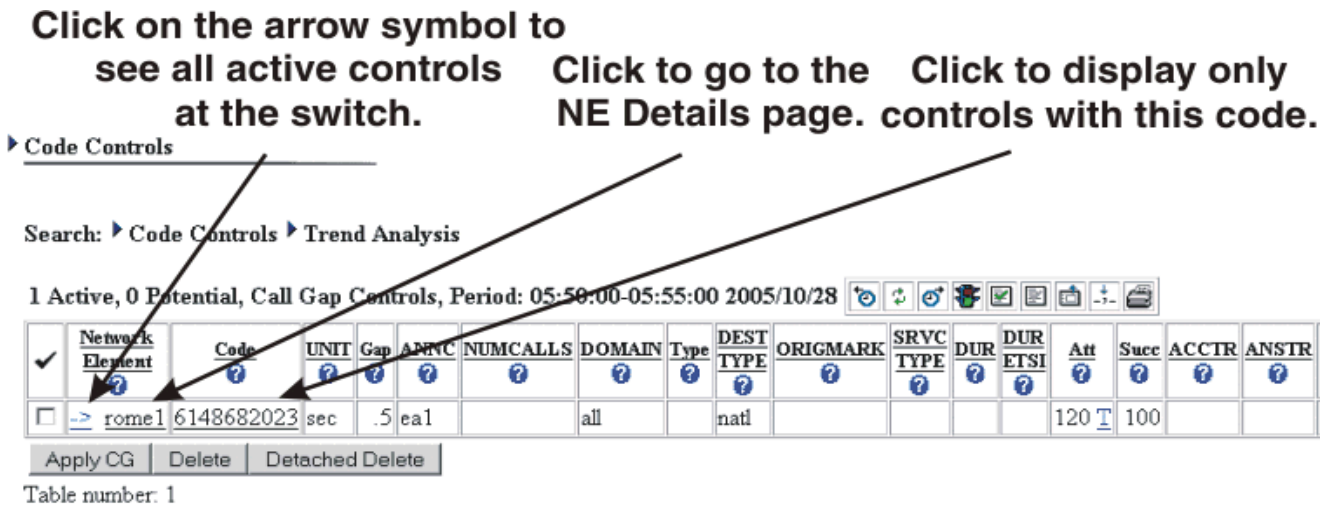
- Execute, Validate, Apply Controls, and Delete buttons

Code Controls container page

Purpose

The Code Controls container page (Figure 4) displays results of a code control search in tabular format.

Figure 4 Code Controls container page



When a historic data collection period is specified in the Search area, or when the page is in Auto-Update mode, the page is in a view-only mode.

The left column of the Data Table contains a column labeled with a checkmark. A row of the table is considered selected when the corresponding checkbox is selected. The checkmark column does not appear in view only mode.

Buttons

The Code Controls container page contains the following buttons beneath the Data Table:

- Apply CG — Selected active and potential controls are displayed in the Code Control Request page
- Delete — A confirmation window is presented to you. If you confirm the operation, then:
  - Selected active controls are deleted
  - Selected potential controls are ignored
  - An updated Code Control container page is displayed if all delete requests are successful (all row selections are cleared in the updated page)

– Failed delete requests are displayed in the same manner as failed add and modify requests, with the exception that the text, “Delete Code Controls” appears in place of the Parameter area.

Reference: See “Code Control Request page” (p. 13) for details on how failed requests are presented.

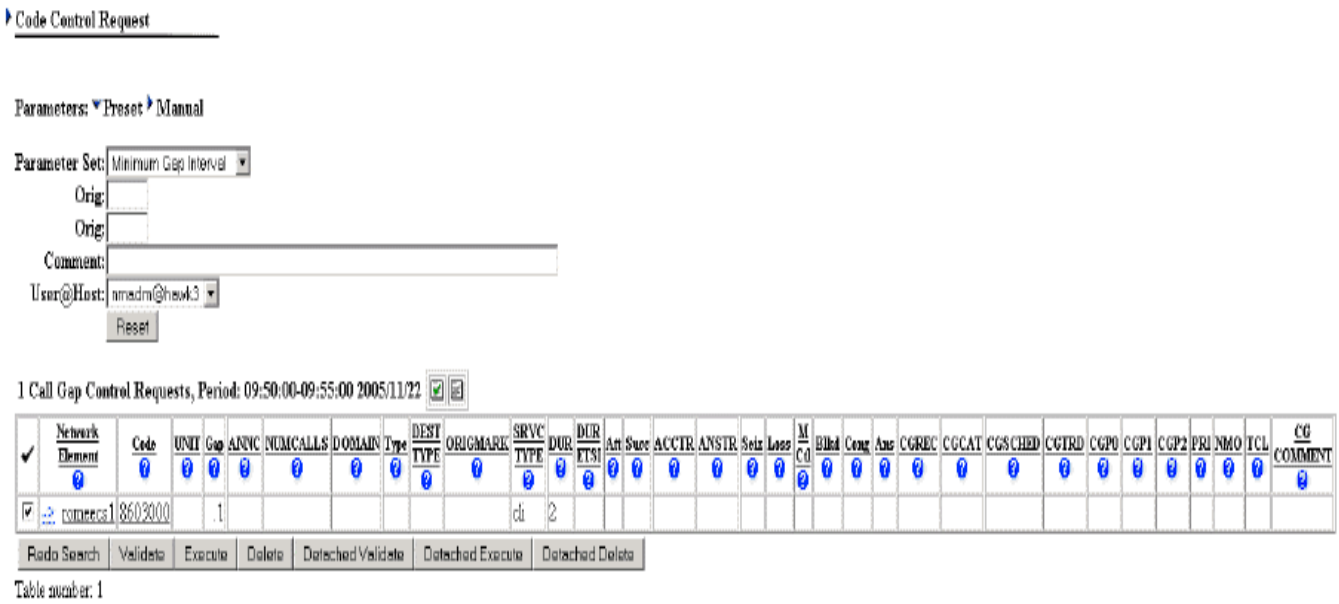
Code Control Request page

Purpose

This page allows you to select appropriate control parameters and execute the control requests. Access to this display is limited to users with permission to execute controls. If you do not have the appropriate permission, after submitting a control request, the system responds, “Permission Denied”.

Figure 5 shows an example of the Code Control Request page in preset parameter mode.

Figure 5 Code Control Request page: Preset parameter mode



Parameter area

The Code Control Request page contains a Parameter area. The Parameter area has a preset parameter mode and a manual parameter mode. The following parameter appears in the Parameter area in preset mode:

- Parameter Set: Parameter set selections for the specified code control type. The control parameters that are displayed in the Parameter Set detail page are identical to the control parameters that appear in the manual parameter mode of the Code Control Request page. The parameters for all switch types and generics that are valid for a customer’s site are displayed. The same layout, labels, and form objects are used (with the exception that the parameter fields are output only when the Parameter Set detail page is in view only mode).

Selecting a Preset parameter set will populate the control parameter form objects with the values for the parameter set.

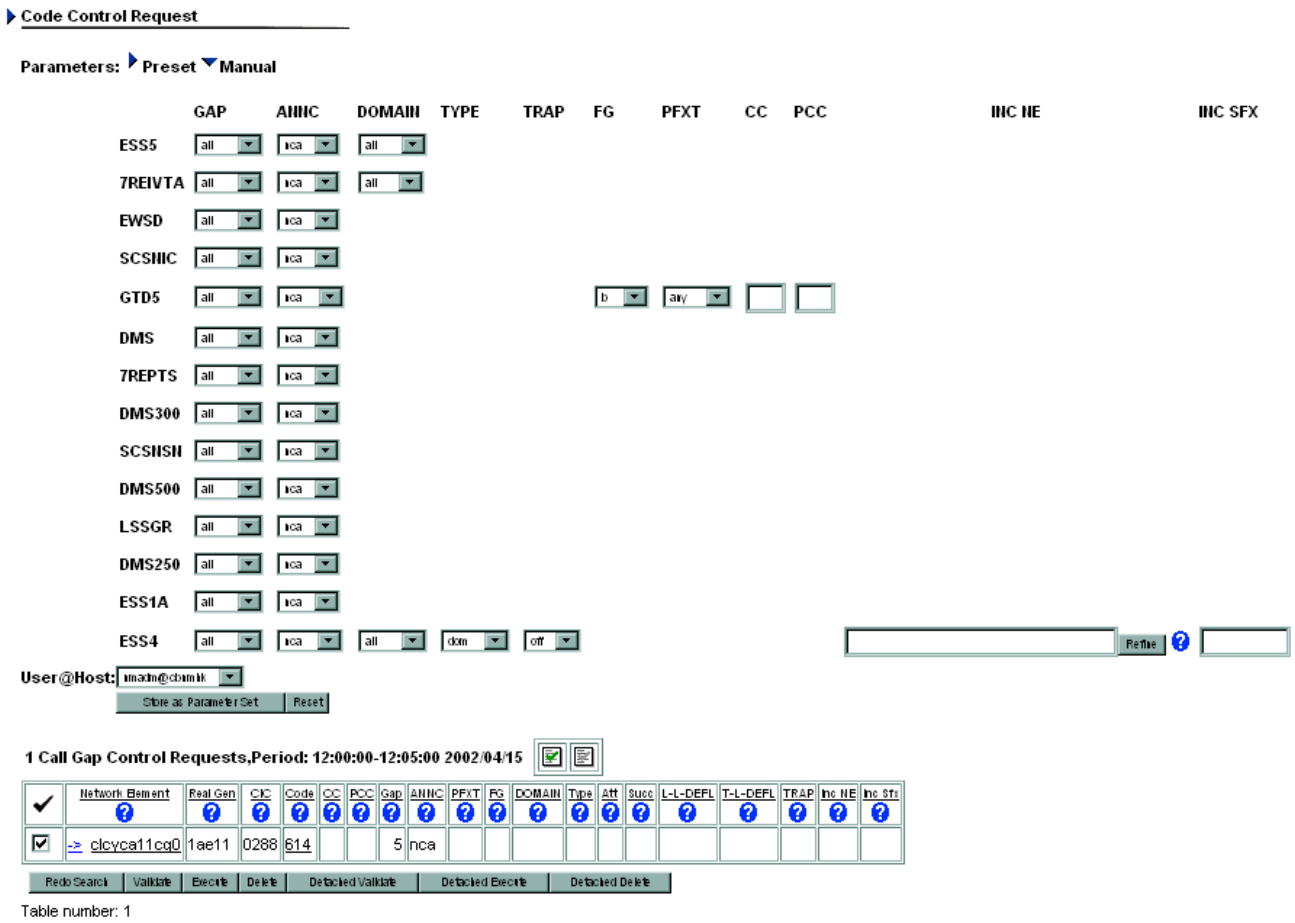
The Edit Parameter Set button provides a link to the parameter set detail page for the selected parameter set. The user can view the parameter set detail and change the defined parameters.

Reference: "Parameter sets" (p. 6)

Figure

Figure 6 shows an example of manual parameter mode for the Manual Call Gap control:

Figure 6 Code Control Request page: Manual parameter mode



Page elements

The Code Control Request page contains a Data Table in which the selected active and potential controls from the Code Controls container page are displayed.

The Gap and ANNC fields appear for all office types. Additional fields will appear depending on offices supported by your NTM system.

For *4ESS* there is a blank field labeled INC-TRUNK-SUBGROUP in which you can set different incoming trunk groups on the same code, this must be done using two or more different controls.

Important! When modifying a call gap that has an INC-TRUNK-SUBGROUP, you must re-enter the incoming trunk subgroup in the parameter area. If you do not, a new call gap control will be added.

The "STATUS" column often appears after the validate or execute buttons have been selected. It contains execution and validation status messages.

Important! Fields without default values may be required to be populated to complete the control request. To determine the value for an unpopulated field you can select the blue question mark field help icon on the table below the parameter area. This will supply you with the valid values for the field.

If you interrupt or leave the page while the execute or validate action is in progress, the requests continue execution on the host, but no further status or results are presented to you.

□

Code Controls trend page

Purpose

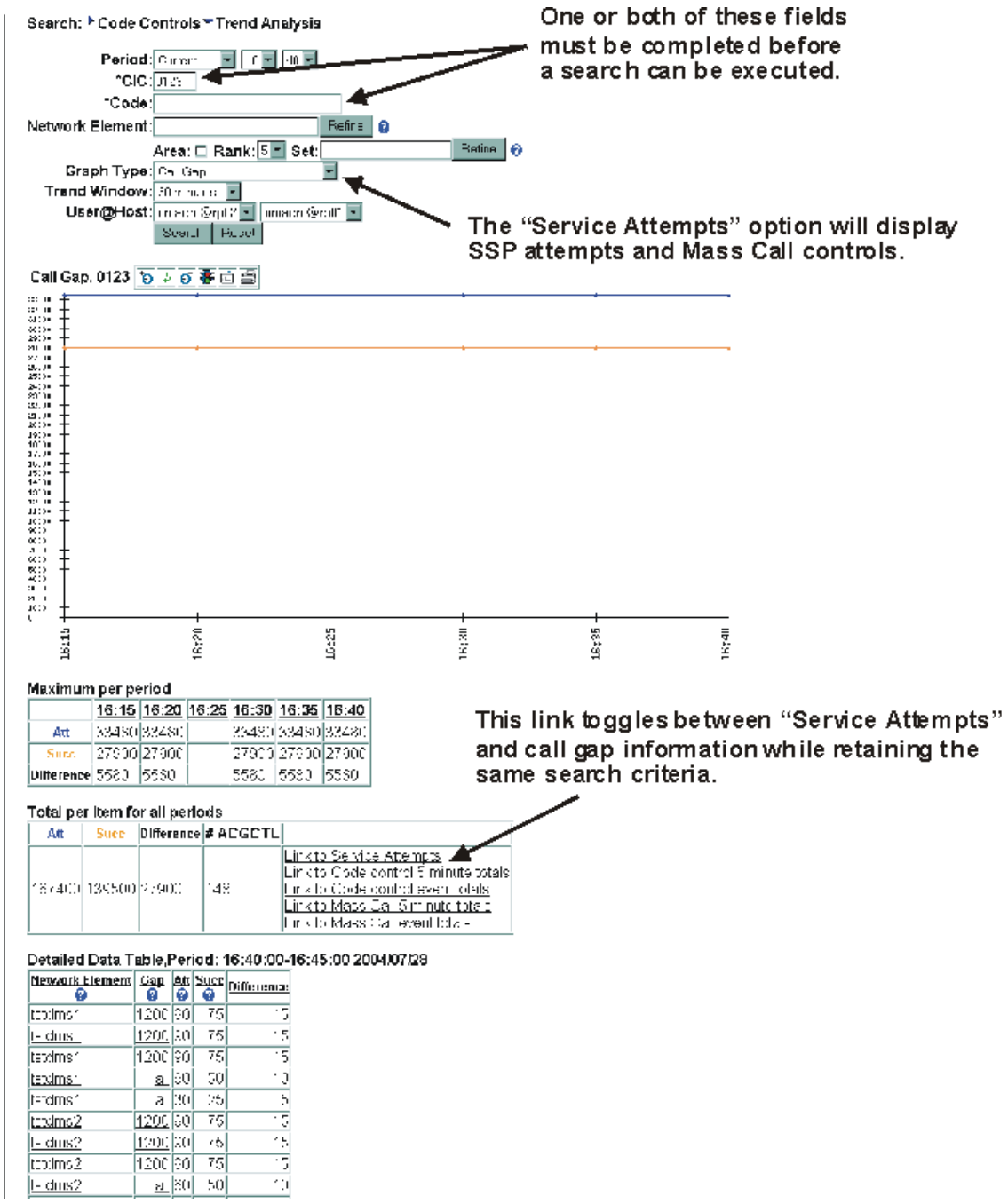
The Code Controls (Call Gap) trend page is available if you have purchased Feature 385, “Trend Analysis”.

Reference: “Trend pages” (p. 18)

The Code Controls trend page can show either Call Gap attempts and successes or SSP Service attempts and Mass Calling controls. Along with this information, the ACGCTL discrete is shown when at least one network element has automatic call gap discretes active.

The Code Controls trend page allows the user to restrict the retrieved data on various network data ***and*** either a CIC ***or*** a Code. Figure 7 shows a Code Controls trend page.

Figure 7 Code Controls trend page



Search criteria

Table 3 describes the search criteria that can appear in the Search area.

Table 3 Search criteria for Code Controls trend pages

Label	Description
Period	Data collection period. Options are current or a historical period.
CIC	Inter-exchange carrier prefix. Limit of 4 characters Blank by default.
Code(s)	Code(s). User may enter multiple codes, separated by the comma character. Blank by default. You may choose to match the code(s) exactly, or search for codes greater than or less than the value(s) you entered. This is NOT a numeric greater than or less than operation. It is close to a string greater than or less than operation. Example: • If the code is 614, “Includes codes greater than” would mean all codes beginning with 614, e.g., 614,614555, 6148601212. For this application, 615, for example, is NOT greater than 614. • If the code is 6145, “Includes codes less than” would mean all codes starting with 6, 61, 614 etc., except for the exact code of 6145. **Reference: Reference:** See the cg command (4-21) for field values and restrictions.
Network Element Area Rank Set	Near end network element. Valid values include all internal network elements. By default, Near End is blank, Area is unselected, rank is 5, and set is blank.
Graph Type	Call Gap (Network Call Gap) Service Attempts (SSP Service attempts and mass calling control information.)
Trend Window	The number of data collection periods to be used in the trend analysis.Options are: 6, 12, 18 or 24 five-minute data collection periods (30 minutes to 2 hours).
User@<*Host*>	Choice of user IDs on a specific host machine.

Protective TG Controls

Overview

Purpose

This section describes the display for viewing and implementing protective trunk group controls, such as: `cro`, `silc`, `dptpri`, `canf/cant/skip`, `acc` or `cr`.

Reference: Chapter 4, "Control Commands" in the *Input Commands Guide*

Contents

This section contains the following topics:

Protective TG Controls search page	5-20
Protective TG Controls container page	5-22
Protective TG Control Request page	5-24

Protective TG Controls search page

Purpose

The Protective TG Controls search page contains a Search area that has a simple search mode and an advanced search mode.

Search criteria

Table 4 describes the criteria that can appear on the Protective TG Controls search page.

Table 4 Protective TG Controls search criteria (Sheet 1 of 2)

Label	Description
Period	Data collection period. Options are current or a historical period. The default is “current”.
Near End Area Rank Set	Near end network element. Valid values include all internal network elements.
Far End Area Rank Set	Far end network view. Valid values include all network elements, both internal and external.
Suffix	Trunk group suffix.
TG-Set	Trunk group set. Allows multiple selections, to a maximum of 10.
Controlled	Trunk group control status selection. When selected, only active controls are displayed. When Controlled is not selected, a potential control is generated for each trunk group matching the search criteria. The default is “unselected”.
Service	Trunk group service type: High Usage, Full, Final.
TG Type	Physical Only, Virtual Only or Physical and Virtual (default)
Category	Protective TG control category. Choices are: Manual (default) or Automatic
Control Type	Protective TG control type. Manual protective TG controls include CANF, CANT, SKIP, CRO and DPTPRI. Automatic protective TG controls include CR, ACC and SILC. The default is “all”.

Table 4 Protective TG Controls search criteria (Sheet 2 of 2)

Label	Description
NCKTS Lower Bound	Lower bound for number of circuits restriction.
NCKTS Upper Bound	Upper bound for number of circuits restriction.
Display Limit	Display limit choices.The default is “small”.
User@Host	Choice of user IDs on a specific host machine.

References

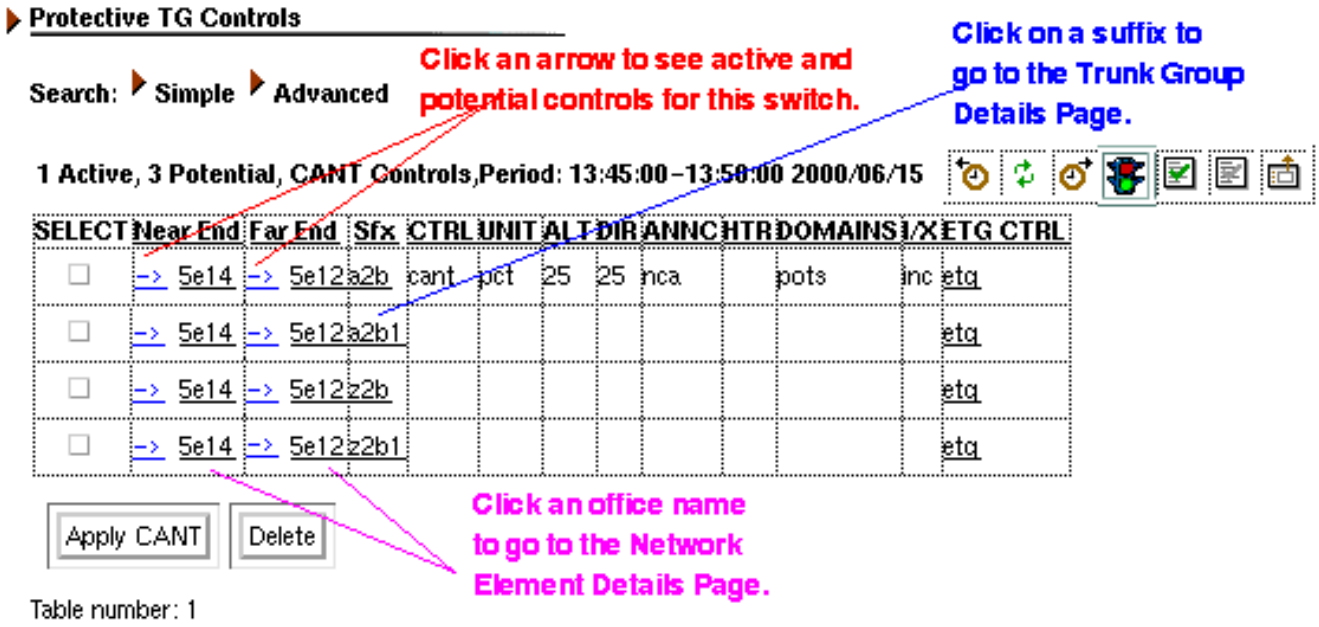
“Displaying potential and assigned controls” (p. 9); “View-only mode” (p. 9)

Protective TG Controls container page

Purpose

The Protective TG Controls container page (Figure 8) displays the results of protective TG control search in tabular format.

Figure 8 Protective TG Controls container page



Data table

The Protective TG Controls container page contains a Data Table in which the results of a search are displayed. The left column of the Data Table contains a column labeled with a checkmark. A cell in this column contains a checkbox if you have the proper subnetwork permission to apply a control to the corresponding network element. A row of the table is considered selected when the corresponding checkbox is checked. The checkmark column does not appear in view only mode.

The inclusion of a field in the Data Table is based on the protective TG control type(s) that were selected in the Search area, and on the switch types and generics that are valid for a customer's site. Only those fields that apply are displayed.

Reference: For an explanation of fields appearing in the Data Table, see the associated command in the *Input Commands Guide*.

Selecting controls

Depending on whether the category selected is manual or automatic, the user will be given an opportunity to select the desired control. The following buttons appear beneath the Control Type menu:

- Apply `cant` — Applies a “Cancel To” control
- Apply `canf` — Applies a “Cancel From” control
- Apply `skip` — Applies a “Skip” control
- Apply `cro` — Applies a “Cancel Reroute Overflow” control
- Apply `dptpri` — Applies a “Dynamic Packet Trunks Prioritization” control
- Apply `silc` — Applies a “Selective Incoming Load Control”. For the “silc” control, the action and status is “e” (enable) or “d” (disable). There is no “delete” button
- Apply `acc` — Applies a “Automatic Congestion” control
- Apply `cr` — Applies a “Circuit Reservation” control
- Delete — Deletes controls

Reference: “Deleting a control” (p. 4)

After the user selects the desired “Apply” button, the Protective TG Control Request page (Figure 9) will appear.

Important! The Control Type menu and buttons do not appear in view only mode.

References

See the *Input Commands Guide* for more information on controls.

□

Protective TG Control Request page

Purpose

This page allows you to select appropriate control parameters and execute the control requests. The Protective TG Control Request page contains a Data Table in which the selected active and potential controls from the Protective TG Controls container page are displayed. The columns of the table are the same as those displayed on the Protective TG Controls container page. Access to this display is limited to users with permission to execute controls.

Only those parameters that apply to the switch types and generics contained within the Data Table are presented in the Parameter area. The displayed parameters are also dependent on the protective TG control type that was specified on the Protective TG Controls container page.

If all control requests complete successfully, the refreshed Protective TG Control container page is displayed.

Reference: “Failures” (p. 5); “Validating a control request” (p. 3)

Preset parameter mode

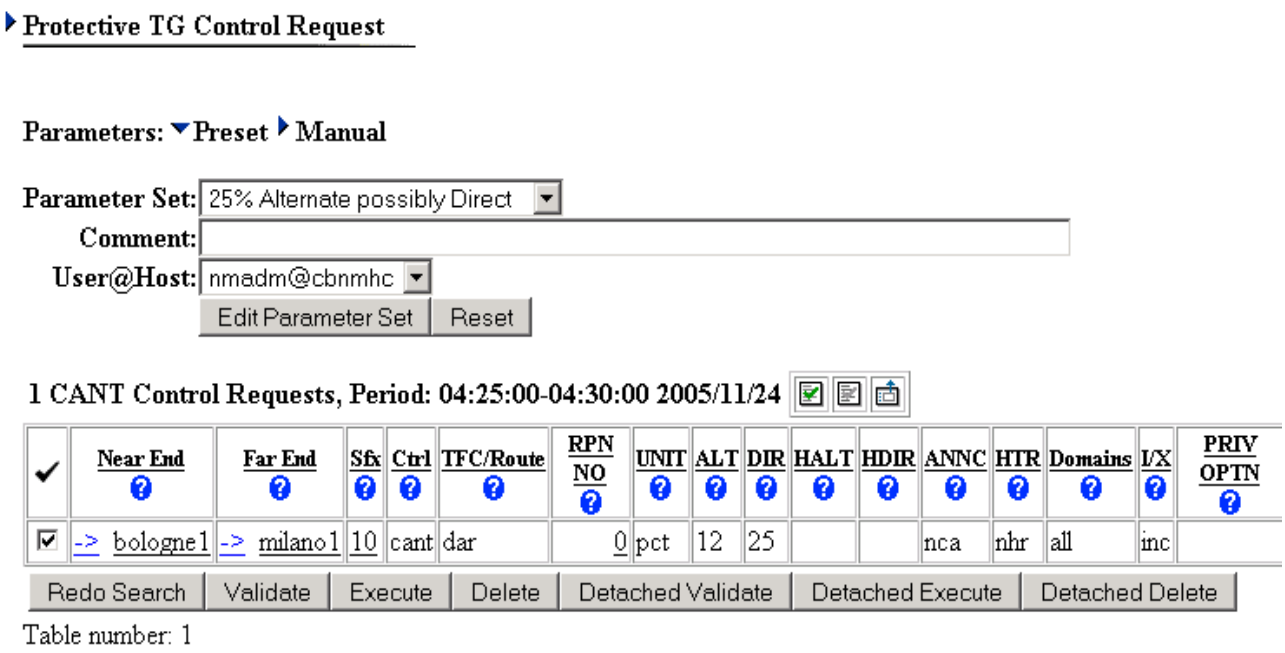
The following parameter appears in the Parameter area in preset parameter mode:

- Parameter Set: Parameter set selections for the specified protective TG control type.

  Reference: “Parameter sets” (p. 6)

Figure 9 shows an example in “Preset” parameter mode.

Figure 9 Protective TG Control Request page: Preset parameter mode



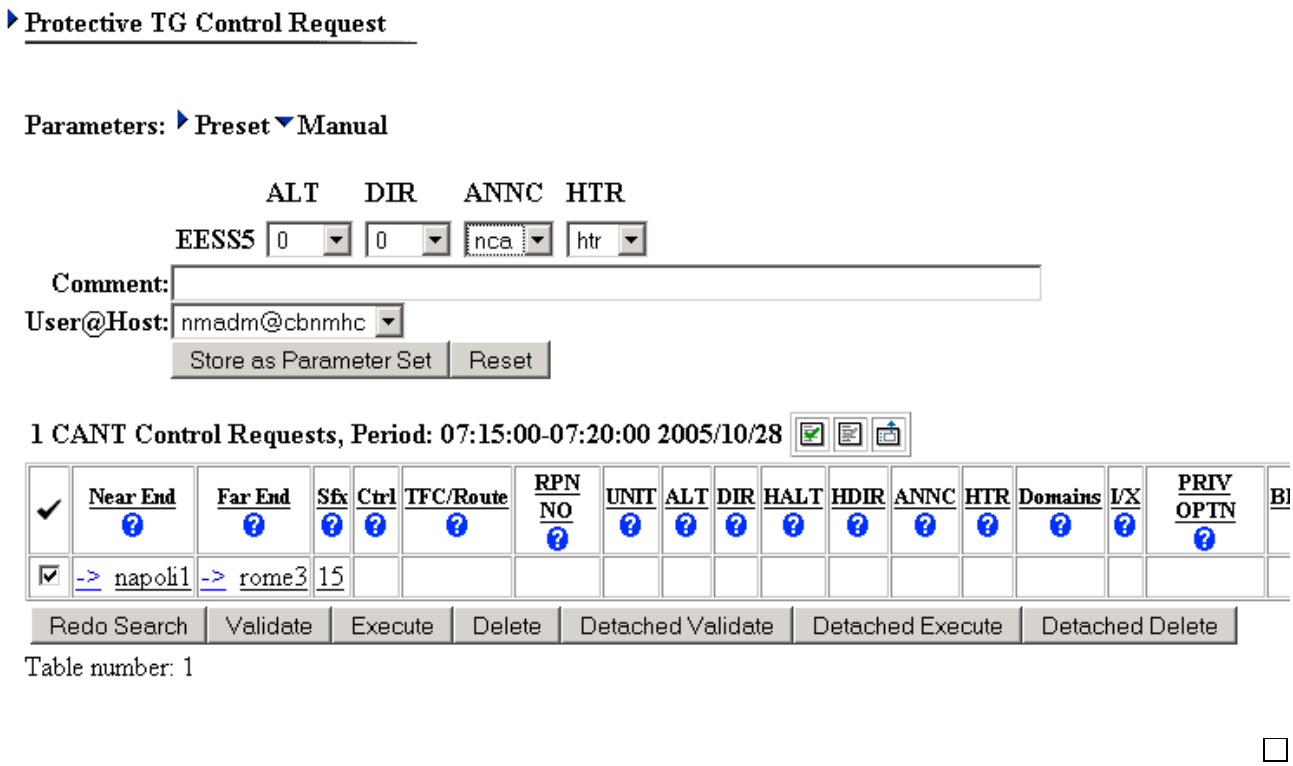
Important! For SILC, “Parameter Set” is replaced by “Action”, with valid values of “enable” or “disable”.

Manual parameter mode

The parameter appears in the Parameter area in preset parameter mode depending on which office type is selected.

Figure 10 shows an example in “Manual” parameter mode for an ESS5 office.

Figure 10 Protective TG Control Request page: Manual parameter mode, ESS5 office



Expansive TG Controls

Overview

Purpose

This section describes the displays that are used to view and implement expansive trunk group controls. Depending on the network element, there are various methods of redirecting data flow between congested network elements. Typically only those elements that process this overflow information in similar methods can be used to redirect or reroute traffic between one another. For instance calls being rerouted from Wideband trunk groups can only be rerouted to Wideband trunk groups.

Contents

This section contains the following topics:

Background	5-28
Expansive TG Controls search page	5-30
Single Trunk Group search	5-32
Active Controls search	5-33
Active Via Trunk Groups search	5-34
Active Expansive TG Controls container page	5-35
Expansive TG Control Details page	5-36
Expansive TG Control Request page	5-37
Expansive TG Control Trend page	5-46

Background

Overview

The most typical method in circuit switching is using a “via” or alternate trunk group, other methods in the network might be RDBI (*4ESS*), Indexes (*GTD-5*), and digit codes (*4ESS,* 5ESS 5e16_1 and later, DMS). For this section regarding Expansive Trunk Group Controls the term “reroute” may represent any of these methods.

The Via Analysis page displays a minimum link list of reroute via trunk groups for use in a trunk group overflow reroute control for offices that support via reroutes. The algorithm, used for identifying reroute via trunk groups, searches for direct A-B and A-V trunk groups with sufficient combined RPIC (Reroute Path Idle Capacity) to reroute all calls that overflow the “Reroute-From” trunk group, typically up to the limit of seven (7) reroute candidates.

The Via Analysis page displays all A-B candidates in descending order of RPIC, followed by all A-V candidates in descending order of RPIC. The RPIC is the lesser number of the A-V trunk group idle capacity and the combined V-B pool trunk group idle capacity. The algorithm selects potential reroute candidate trunk groups based on a number of embedded rules:

- The algorithm assumes a single via office when evaluating reroute paths through the net-work Offices that are in, or have recently been in, an overloaded state are eliminated as via office candidates. All 4ESSswitches that are in, or have recently experienced, a “phase” are eliminated as well.
- All direct A-B trunk groups are processed before any two link paths are considered. This is done to minimize the number of links a rerouted call would traverse through the network. HU (High Usage) trunk groups are processed before FU (Full) trunk groups, with FI (Final) trunk groups being processed last. This is done to protect the capacity of the Final trunk groups.
- All V-B trunk groups that pass analysis information (such as signaling type), as specified in the required and optional views, are considered as a “pool” of capacity for use by calls rerouted through that particular via switch. The V-B trunk groups are displayed by trunk group service type, HUs first, then FUs and FIs last. Any trunk group with an active reroute control is excluded from consideration. This is done to prevent calls from “looping” in the net-work.

The algorithm takes into consideration the prohibition of using specific trunk groups as A-V or V-B reroute paths based on the “av” and “vb” indications in the “options” parameter of the Record Base trunk group file for that particular trunk group. These indications use negative logic. Marking a trunk group as:

- "av" prevents it from being considered as an AV reroute candidate by the Via Analysis algorithm.
- "vb" prevents it from being considered as part of the V-B "pool" of capacity by the Via Analysis algorithm.

Normally, the algorithm uses all data that is available in the database, unless it is suspect. Customers with Feature 74, "Improved Filtering and Reporting of Data" can eliminate the display of filtered and tagged data on the page, thereby preventing the algorithm from considering all such data. This is done by selecting the "Suspect Data Filter" button on the search page.

The algorithm analyzes the latest 5-minute data collected by the NTM system.

The output of the Via analysis is where the recommended "reroute-to" via trunk groups are displayed. For each A-V reroute candidate identified, all appropriate V-B trunk groups will be displayed so that the user can view the potential effect of activating the reroute on the entire reroute path(s).

References

Chapter 4, "Control Commands" in the *Input Commands Guide*

"Filter File" (p. 25) in the *Record Base Administration Guide*

□

Expansive TG Controls search page

Purpose

The Expansive TG Controls search page has three search modes:

- Single Trunk Group search (default)
- Active Controls search
- Active Via Trunk Groups search

Search criteria

Table 5 describes the search criteria that appear in the Search area.

Table 5 Expansive TG Controls search criteria (Sheet 1 of 2)

Label	Search type(s)	Description
Period	All	Data collection period.
Session	All	Historical session ID. This field is available with Feature 342, "Historical Data Playback for the Browser-based GUI".
Near End	All	Near end network element. Valid values include all internal network elements. Multiple selections are not allowed. Enter the Near-End office name to restrict the search for active reroutes to a specific originating office.
Area (Near-End)	Active Controls	By selecting the Area box you can restrict the Near-End trunk groups used to search for active reroutes.
Rank (Near-End)	Active Controls	Select a rank value of 1 (highest) through 5 (lowest) to restrict the Near-End trunk groups used to search for active reroutes. Only those offices with the specified rank or higher that also meet all other specified criteria are considered.
Set (Near-End)	Active Controls	Enter a trunk group set name to restrict the Near-End trunk groups used to search for active reroutes. Only those trunk groups in the specified trunk group set that also meet all other specified criteria are considered.
Far End	All	Far end network view. Enter the Far-End office name to restrict the search for active reroutes to a specific terminating office. Valid values include all network elements, both internal and external.
Area (Far-End)	Active Controls	By selecting the Area box you can restrict the Far-End trunk groups used to search for active reroutes.

Table 5 Expansive TG Controls search criteria (Sheet 2 of 2)

Label	Search type(s)	Description
Rank (Far-End)	Active Controls	Select a rank value of 1 (highest) through 5 (lowest) to restrict the Far-End trunk groups used to search for active reroutes. Only those offices with the specified rank or higher that also meet all other specified criteria are considered.
Set (Far-End)	Active Controls	Enter a trunk group set name to restrict the Far-End trunk groups used to search for active reroutes. Only those trunk groups in the specified trunk group set that also meet all other specified criteria are considered.
Suffix	All	Suffix Trunk group suffix.
Via Far End	Active Via Trunk Groups	Via Far end network view. Enter the Far-End office name to restrict the search for active vias to a specific terminating office. Valid values include all network elements, both internal and external.
Via Suffix	Active Via Trunk Groups	Via Trunk group suffix.
Suspect Data Filter	All	When On is selected, no filtered or tagged items are displayed in the page output. Valid only with purchase of Feature 74, "Improved Filtering and Reporting of Data".
TG Set	Active Controls	Enter one or more trunk group set names to restrict the trunk groups used to search for active reroutes. 10 sets maximum.
Data Restriction	Active Controls	The two data restriction fields allow you to retrieve data based on values for up to two measurements. For example, you may set these fields to: `Bids < 80 and %OFL > 5` Only those trunk groups having measurements matching this data restriction will be retrieved. You may use one, both, or neither of these fields.
Display Limit	All	Sets maximum number of rows to be retrieved. Options are: • Small — 100 rows • Medium — 300 rows • Large — 1200 rows
User@Host	All	Choice of user IDs on a specific host machine.

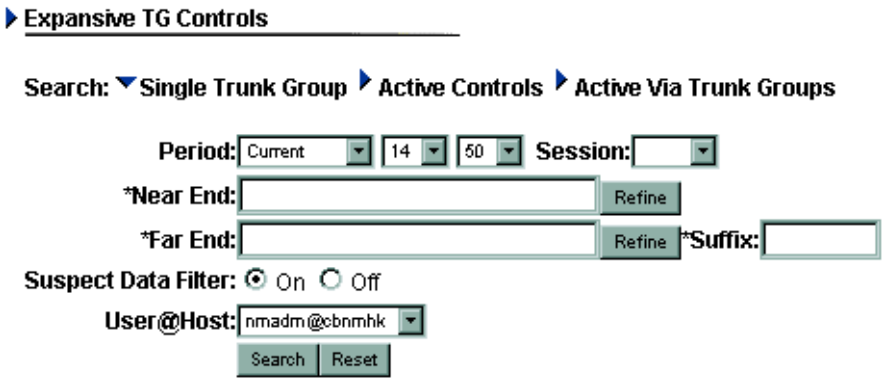
Single Trunk Group search

Purpose

The Single Trunk Group search allows you to find controls on a specific trunk group, display active controls and display trunk groups being used as vias.

Important! The required search fields are indicated by asterisks.

Figure 11 Single Trunk Group search



Search results

The Single Trunk Group search displays the following:

- If one active expansive trunk group control exists, the Expansive TG Control Details page (Figure 15) is launched to display the data for the active controls. You can:
  - analyze additional vias and apply a reroute control using the Analyze and Apply RR button
  - delete a control by selecting the Delete button
- If more than one active expansive trunk group control exists, the Expansive TG Control Container page (Figure 14) is launched to display the data for the active controls. You can select a specific trunk group and select the Ctrl Type to go to the Expansive TG Control Details page (Figure 15)
- If no active expansive trunk group control exists, the Expansive TG Control Details page is displayed. You can analyze vias and apply a reroute control using the Analyze and Apply RR button.

Important! If no expansive trunk group control existed for a historical data collection interval that was searched, the Expansive TG Control Details page is launched without the Analyze and Apply RR and the Delete buttons.

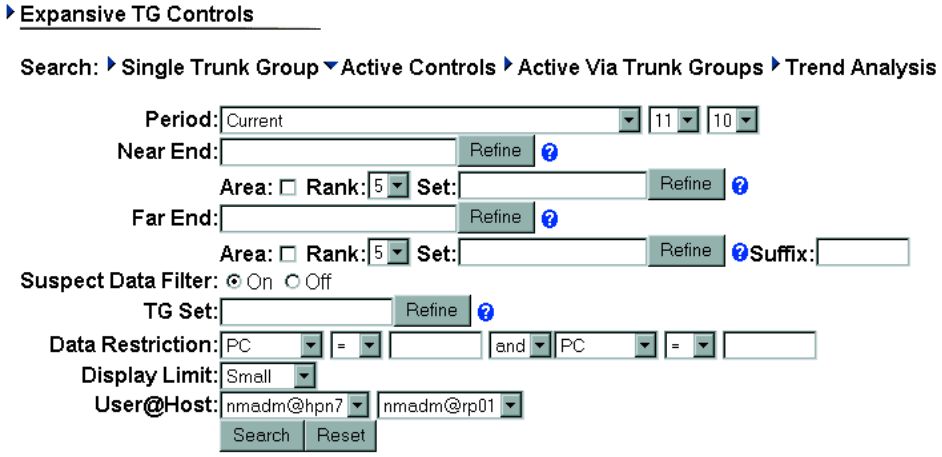
□

Active Controls search

Purpose

The Active Controls search allows you to search for all expansive controls on the network.

Figure 12 Active Controls search



Search results

The Active Controls search displays the following:

- If active expansive trunk group controls exist, the Expansive TG Controls container page (Figure 14) is launched to display the data for the active controls. You can:
  - analyze additional vias and apply a reroute control using the Analyze and Apply RR button
  - delete a control by selecting the Delete button

  Important! If an expansive trunk group control existed for a historical data collection interval that was searched, the Expansive TG Control Container page is launched without the Analyze and Apply RR and the Delete buttons.
- If no active expansive trunk group control exists, a message is returned stating “0 Active Expansive TG Controls”.

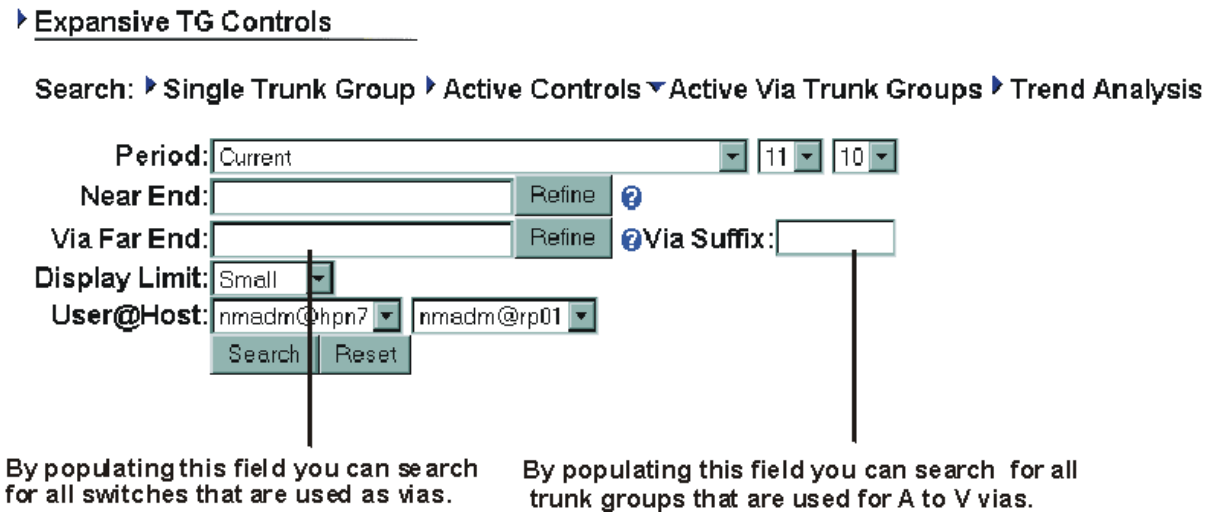
□

Active Via Trunk Groups search

Purpose

The Active Via Trunk Groups search allows you to search for all trunk groups that are used as vias on the network or you can narrow the search by selecting any or all of the input fields.

Figure 13 Active Via Trunk Groups search



Search results

The Active Via Trunk Groups search displays the following:

- If active expansive trunk groups are used as vias, the Expansive TG Control Container page (Figure 14) is launched to display the data for the active vias. You can:
  - analyze additional vias and apply a reroute control using the Analyze and Apply RR button
  - delete a control by selecting the Delete button

  Important! If an expansive trunk group control existed for a historical data collection interval that was searched, the Expansive TG Control Container page is launched without the Analyze and Apply RR and the Delete buttons.
- If no active expansive trunk group control exists, a message is returned stating “0 Active Expansive TG Controls”.

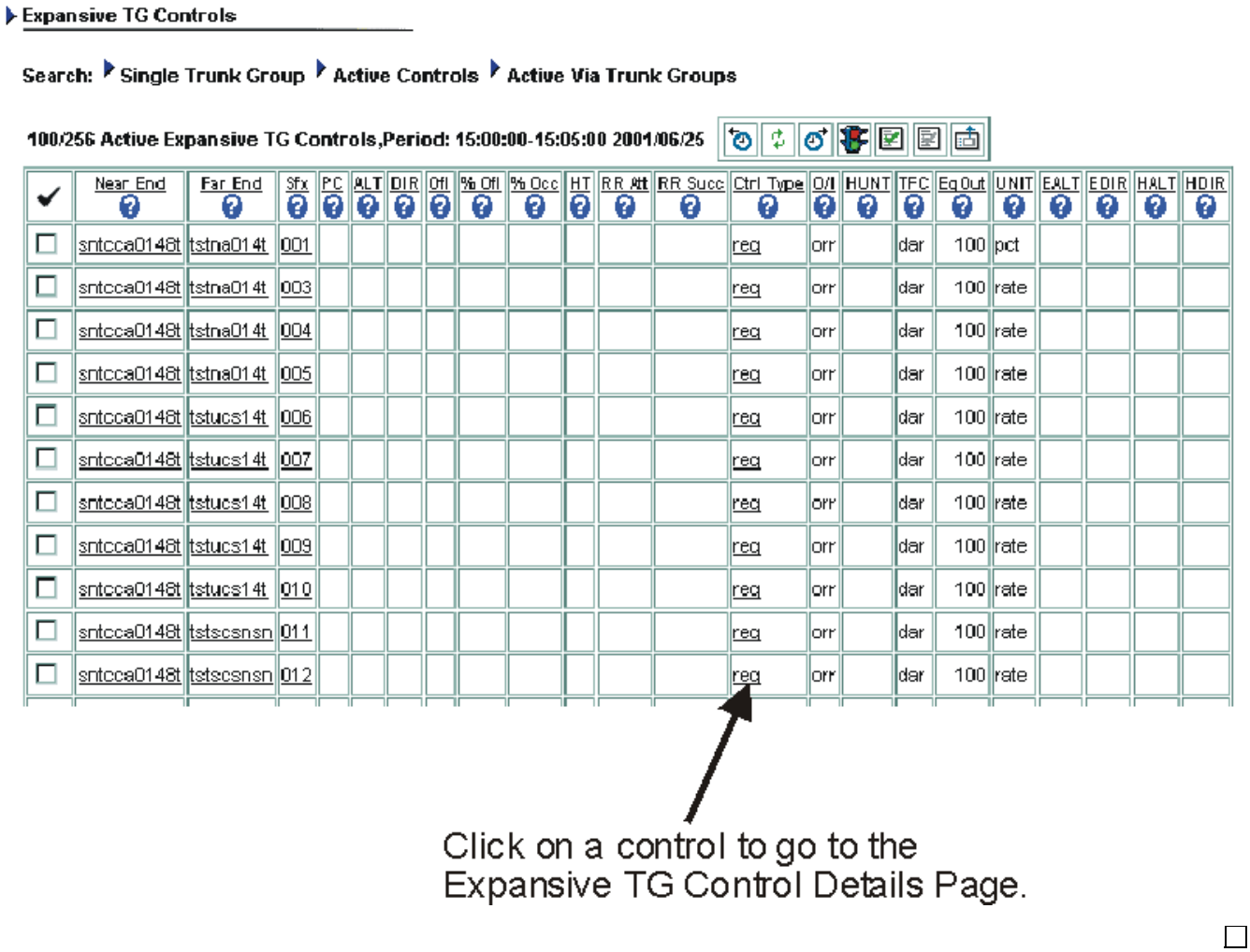
□

Active Expansive TG Controls container page

Purpose

The Active Expansive TG Controls container page displays parameters and data for active expansive trunk group controls and those that are used as vias. From this page, you may select one active control at a time to modify or delete.

Figure 14 Active Expansive TG Controls container page

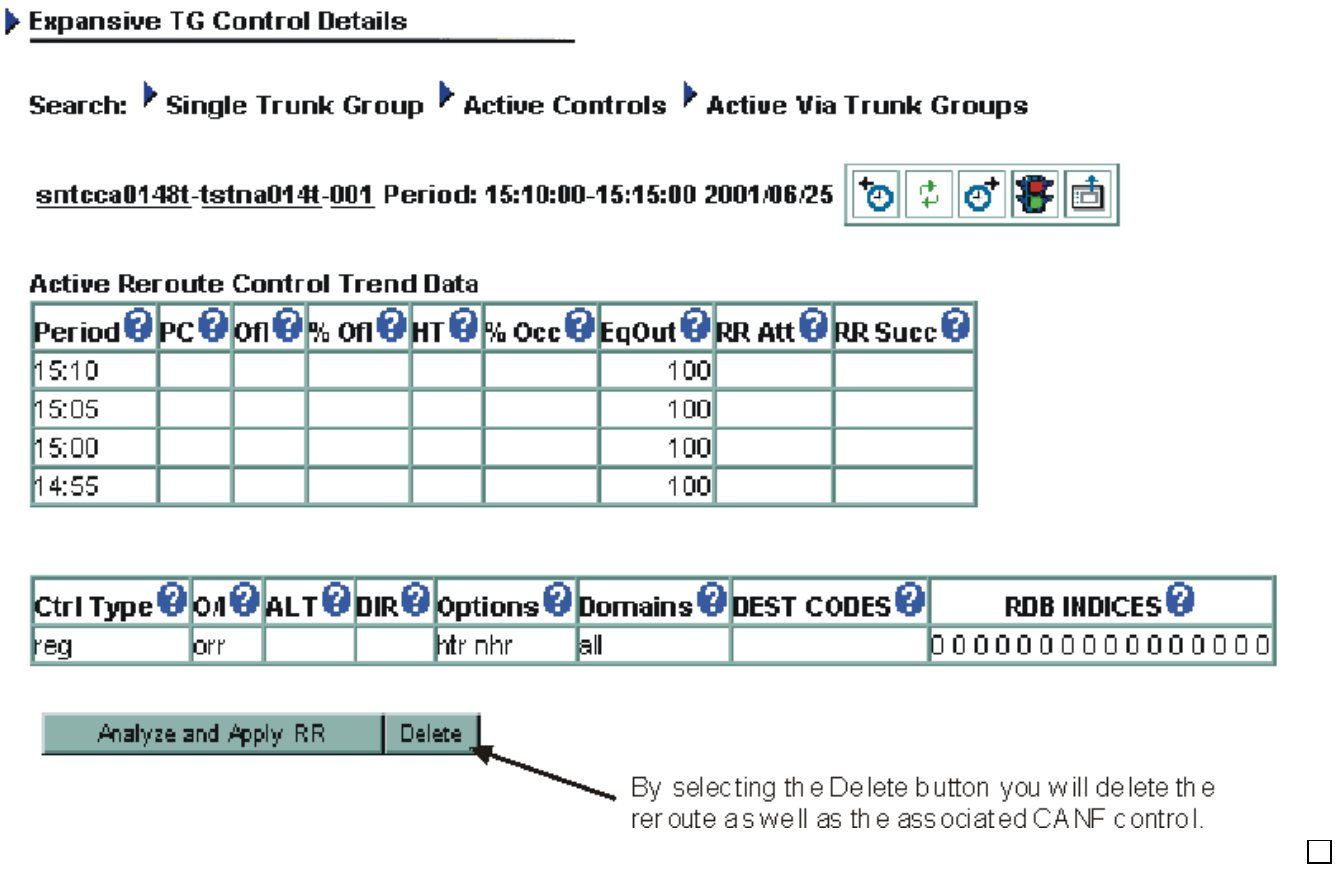


Expansive TG Control Details page

Purpose

The Expansive TG Control Details page displays trend and control data for trunk groups.

Figure 15 Expansive TG Control Details page



Expansive TG Control Request page

Purpose

The Expansive Trunk Group Controls Request page allows you to implement reroute controls on selected trunk groups.

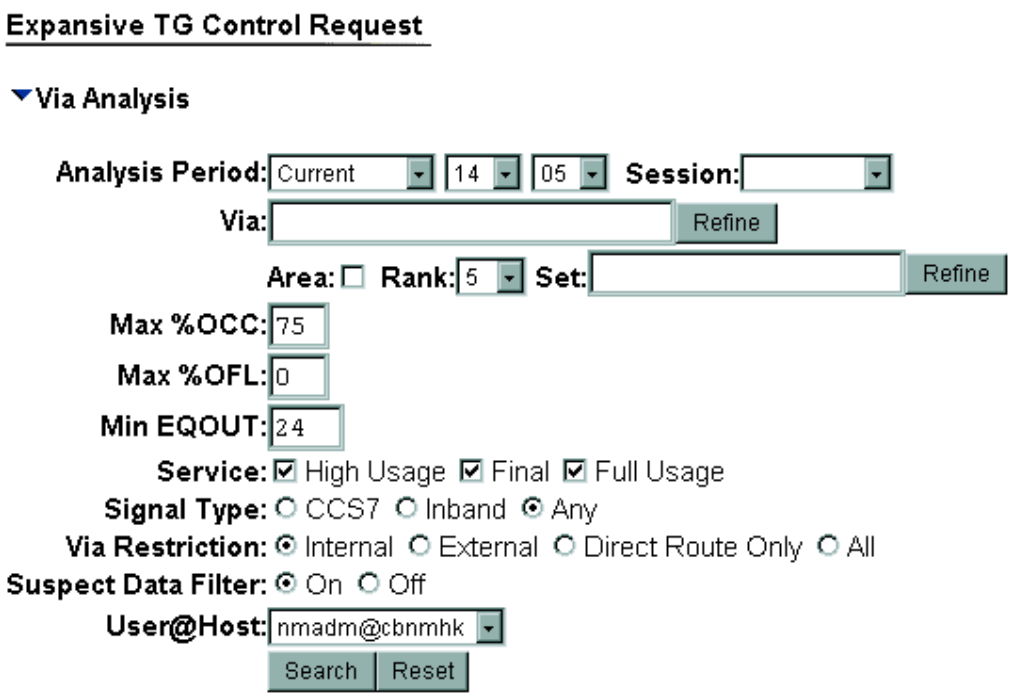
Figure 16 through Figure 19 show examples of the areas on this page.

> **Reference:** For field definitions and values for fields found in the Via Analysis area, see Chapter 1, "All Data Fields" in the *Data Tables Guide*.

The Expansive TG Control Request page contains a search area which is labeled "Via Analysis" instead of "Search", and is shown in Figure 16. This area is referred to as the Via Analysis area and allows you to search for vias with specific characteristics.

A via analysis is always automatically performed when the Expansive TG Control Request page is requested. The default analysis options are used, and the results are displayed as they are for a manually requested via analysis. The inclusion of a column of parameter fields is based on the near end network element switch type and generic. Only those fields that apply are displayed.

Figure 16 Via Analysis area



Analysis options

Table 6 describes the analysis options that appear in the Via Analysis area.

Table 6 Fields in the Via Analysis area (Sheet 1 of 3)

Label	Description
Period	Data Collection period.
Session	Historical session ID. This field is available with Feature 342, "Historical Data Playback for the Browser-based GUI"
Via	Via network element. Valid values include all internal network elements. Enter the Via office name to restrict the operation of the algorithm to a specific originating office. Multiple selections are not allowed. Blank by default.
Area	By selecting the Area box you can restrict the Via Analysis algorithm to considering a limited group of via switches. If this field is selected and the VIA field is blank, the algorithm considers all offices as potential via offices. If this field is selected and the VIA field has an entry, the algorithm considers all offices below the specified via office in the RSPTE file as potential via offices. The default is a blank (unselected) field. By selecting the Area box you can restrict the Near-End trunk groups used to search for active reroutes.

Table 6 Fields in the Via Analysis area (Sheet 2 of 3)

Label	Description
Rank	Select a rank value of 1 (highest) through 5 (lowest) to restrict the Near-End trunk groups used to search for active reroutes. Only those offices with the specified rank or higher that also meet all other specified criteria are considered.
Set	Enter a trunk group set name to restrict the algorithm to considering only those trunk groups in the specified trunk group set that also meet all other specified criteria. The default is a blank field, resulting in all trunk group sets being considered.
Max %OCC	Max %OCC Maximum percent occupancy. The algorithm will consider only those trunk groups that have a %OCC less than or equal to the entered number and that meet all other specified criteria.
Max %OFL	Max %OFL Maximum percent overflow. The algorithm will consider only those trunk groups that have a %OFL, or %CDOFL (Percent Circuit Demand Overflow) for Wideband trunk groups, less than or equal to the entered number and that meet all other specified criteria.
Min EQOUT	Min EQOUT Minimum number of outgoing circuits (was NTKO). Enter a whole number between one (1) and 1023, inclusive. The algorithm will consider only those trunk groups that have a trunk group size greater than or equal to the entered number and that meet all other specified criteria. The algorithm will consider only those trunk groups that have the specified service type(s) for the first leg (A-V) of the reroute path. Multiple selections are allowed.
Service	Trunk group service type: High Usage, Final, Full.
Signal Type	Signaling type. Enter the type of signaling to restrict the algorithm to consideration of only those trunk groups that have the specified signaling type and that meet all other specified criteria. This field allows only a single selection. The default is Any. Choose from: • CCS7 – Integrated Services Digital Network (isdn) – Primary Rate Interface (pri) • Inband – Multi-Frequency Signaling (mf) – Dial Pulse Signaling (dp) – Non-Common Channel Signaling (noncc) – Combined Dial Pulse and Dual-Tone Multifrequency (comb) – Dual Tone Multi-Frequency (dtmf) – Multi-Frequency Fast (fast) • Any – All Types

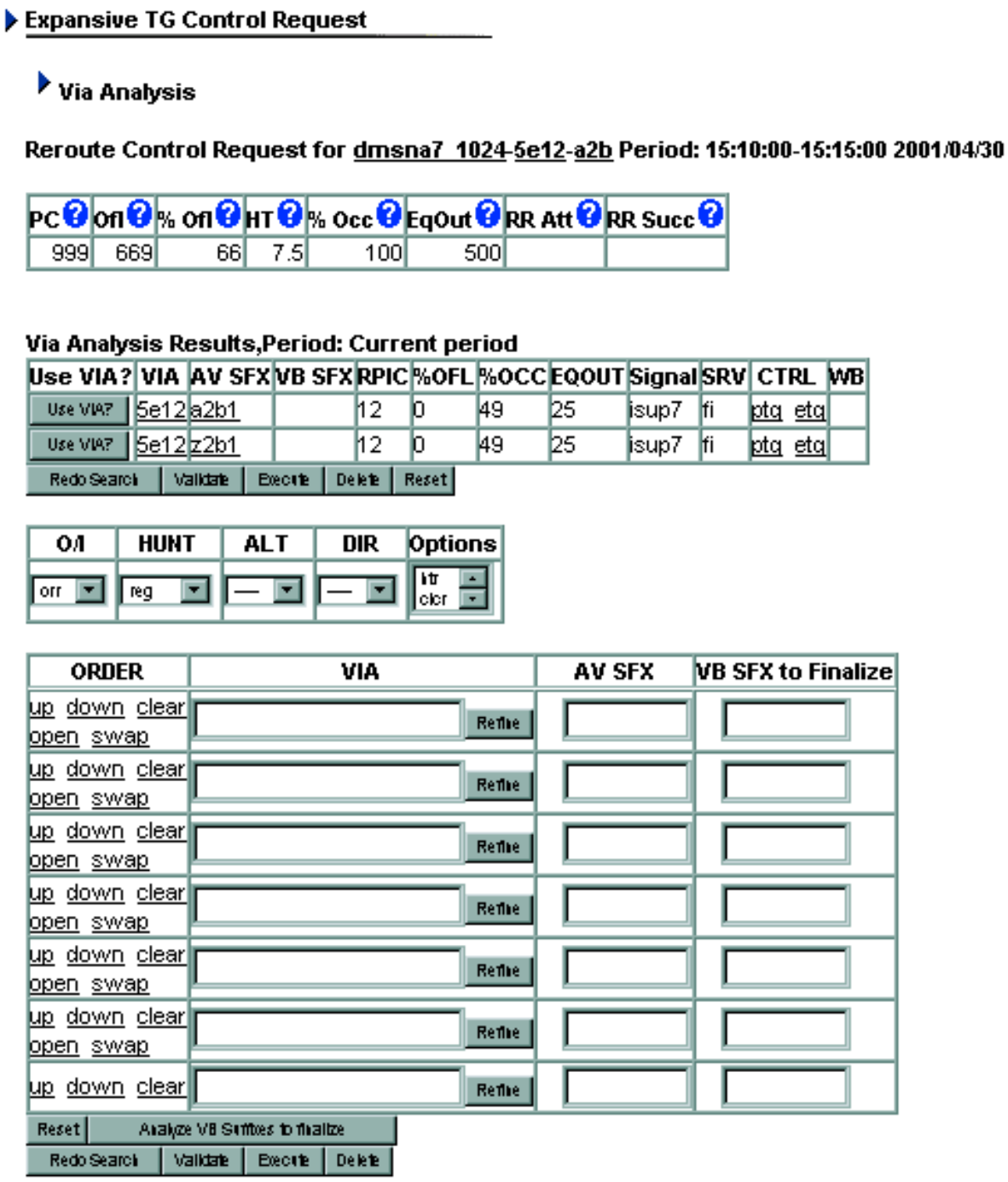
Table 6 Fields in the Via Analysis area (Sheet 3 of 3)

Label	Description
Via Restriction	Via network element restriction. Valid values include: Internal, External, Direct Route Only, and All. Default is Internal. Select Internal to restrict the algorithm to evaluating only internal offices as via office candidates. Select External to restrict the algorithm to evaluating only external offices as via office candidates. Select Direct Route Only to restrict the algorithm to considering only A-B direct routes as potential reroute candidates.
Suspect Data Filter	When On is selected, no filtered or tagged is displayed in the page output. Valid only with purchase of Feature 74, "Improved Filtering and Reporting of Data".
User@Host	Choice of user IDs on a specific host machine.

Analysis results

The results from the via analysis are displayed in the Via Analysis Results Table. Figure 17 shows an example of the control parameter area with via analysis results, and Figure 19 illustrates the links on the Via Analysis Results Table.

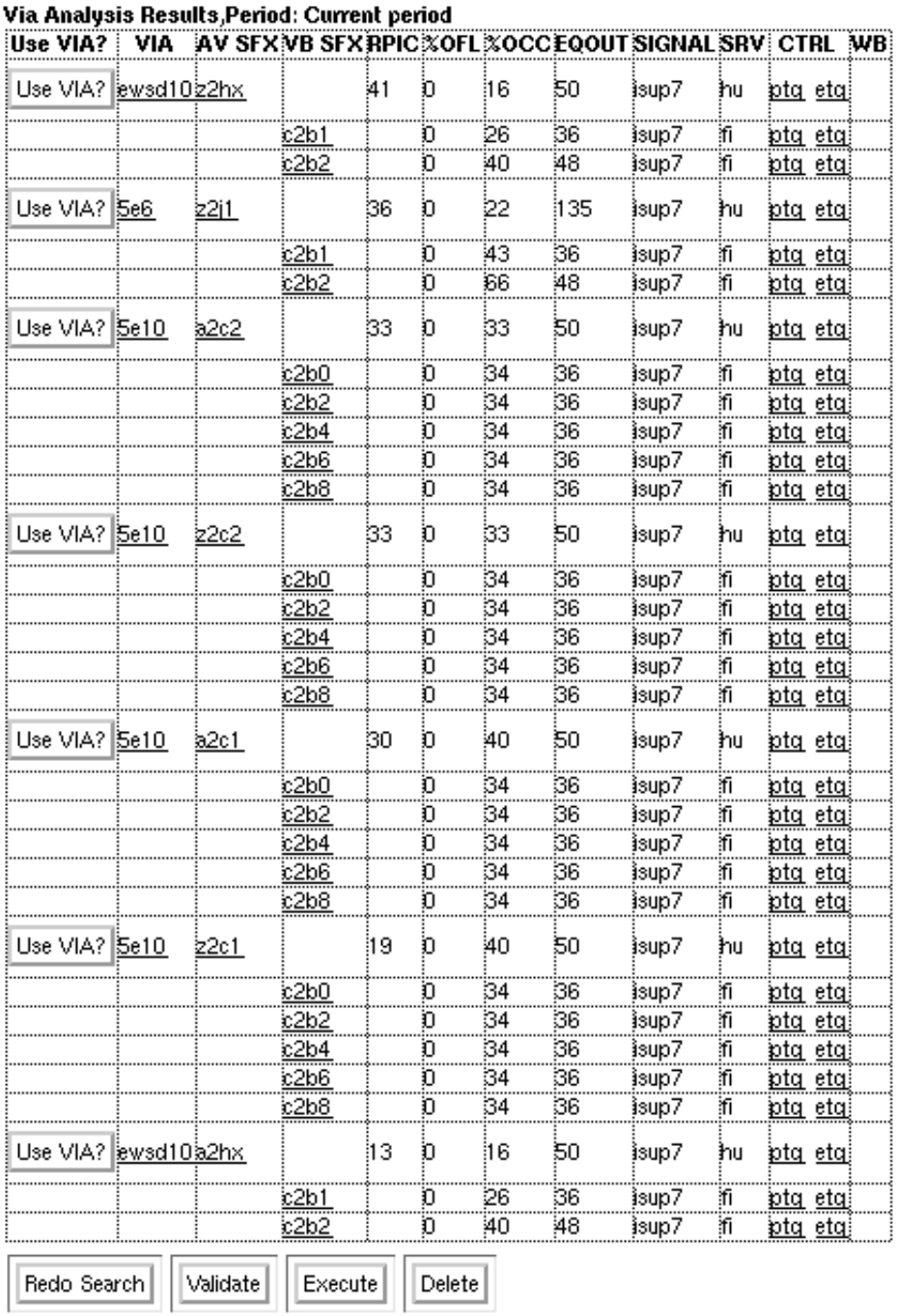
Figure 17 Expansive TG Control Request page



Vias are sorted with alternate direct A-B trunk groups at the top of the table, followed by routes that involve a via switch. To use a via route, click the button labeled “Use Via?”. The via route will be moved to the control parameter area.

Reference: For a description of the fields in the Via Analysis Results Table, see the rr command (4-44) in the *Input Commands Guide* and Chapter 1, "All Data Fields" in the *Data Tables Guide*.

Figure 18 Via Analysis Results Table



Via Analysis Results,Period: Current period

Use VIA?	VIA	AV SFX	VB SFX	RPIC	%OFL	%OCC	EQOUT	SIGNAL	SRV	CTRL	WB
Use VIA?	ewsd10	z2hx		41	0	16	50	isup7	hu	ptq etq	
			c2b1		0	26	36	isup7	fi	ptq etq	
			c2b2		0	40	48	isup7	fi	ptq etq	
Use VIA?	5e6	z2i1		36	0	22	135	isup7	hu	ptq etq	
			c2b1		0	43	36	isup7	fi	ptq etq	
			c2b2		0	66	48	isup7	fi	ptq etq	
Use VIA?	5e10	a2c2		33	0	33	50	isup7	hu	ptq etq	
			c2b0		0	34	36	isup7	fi	ptq etq	
			c2b2		0	34	36	isup7	fi	ptq etq	
			c2b4		0	34	36	isup7	fi	ptq etq	
			c2b6		0	34	36	isup7	fi	ptq etq	
			c2b8		0	34	36	isup7	fi	ptq etq	
Use VIA?	5e10	z2c2		33	0	33	50	isup7	hu	ptq etq	
			c2b0		0	34	36	isup7	fi	ptq etq	
			c2b2		0	34	36	isup7	fi	ptq etq	
			c2b4		0	34	36	isup7	fi	ptq etq	
			c2b6		0	34	36	isup7	fi	ptq etq	
			c2b8		0	34	36	isup7	fi	ptq etq	
Use VIA?	5e10	a2c1		30	0	40	50	isup7	hu	ptq etq	
			c2b0		0	34	36	isup7	fi	ptq etq	
			c2b2		0	34	36	isup7	fi	ptq etq	
			c2b4		0	34	36	isup7	fi	ptq etq	
			c2b6		0	34	36	isup7	fi	ptq etq	
			c2b8		0	34	36	isup7	fi	ptq etq	
Use VIA?	5e10	z2c1		19	0	40	50	isup7	hu	ptq etq	
			c2b0		0	34	36	isup7	fi	ptq etq	
			c2b2		0	34	36	isup7	fi	ptq etq	
			c2b4		0	34	36	isup7	fi	ptq etq	
			c2b6		0	34	36	isup7	fi	ptq etq	
			c2b8		0	34	36	isup7	fi	ptq etq	
Use VIA?	ewsd10	a2hx		13	0	16	50	isup7	hu	ptq etq	
			c2b1		0	26	36	isup7	fi	ptq etq	
			c2b2		0	40	48	isup7	fi	ptq etq	

Redo Search | Validate | Execute | Delete

Buttons

The Expansive TG Control Request page contains the following buttons:

- Reset — resets the search parameters
- Analyze VB Suffixes to Finalize — allows you to finalize trunk groups on the VB side of the reroute.

Reference: Figure 19

- Redo Search — allows you to repeat a search for vias for the trunk group you want to control.
- Execute — executes the control request

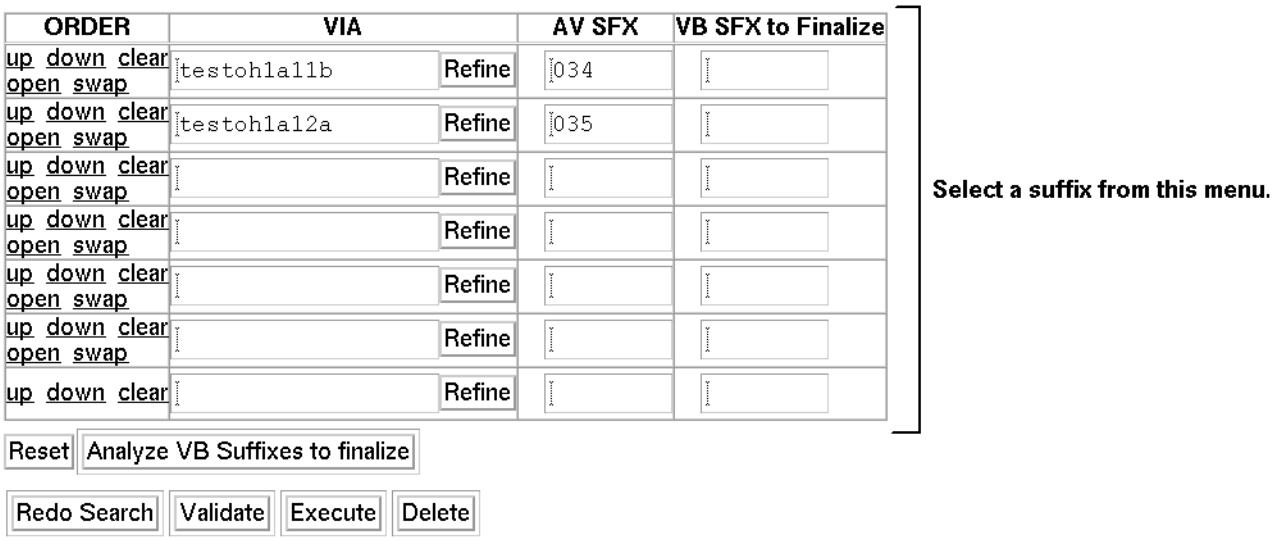
  The request action is derived from the current state of the control: if it is an active control, the action is modify; if it is a potential control (not active), the action is add. If the control request completes successfully, the Expansive TG Control Details page is displayed.

  Important! If the control request fails, the Expansive TG Control Request page is displayed with the failure displayed.

  Reference: "Failures" (p. 5)
- Validate — validates the control request
- Delete — allows you to remove selected active controls

The "Redo Search", "Execute", "Validate", and "Delete" buttons also appear below the Via Analysis Results Table.

Figure 19 VB Suffix finalization



Selecting the "Analyze VB Suffixes to finalize" button results in a display like that shown in Figure 19. For each reroute path involving a via switch, you may choose a particular trunk group (identified by its suffix) to finalize. This prevents any traffic from overflowing into another routing chain, and is accomplished by placing a CANF control at 100% DAR (direct and alternate routed traffic) on the selected trunk group.

Important! There is no way to distinguish this CANF control from other CANF controls in the network, the CANF used to finalize a V-B trunk group must be removed manually from the Protective TG Controls page when the reroute is removed. The exception to this is if a control is deleted using the Expansive TG Control Details page (Figure 15) it will delete the associated CANF control as well. This does not occur if the reroute is deleted using the Expansive TG Controls container page (Figure 14).

□

Expansive TG Control Trend page

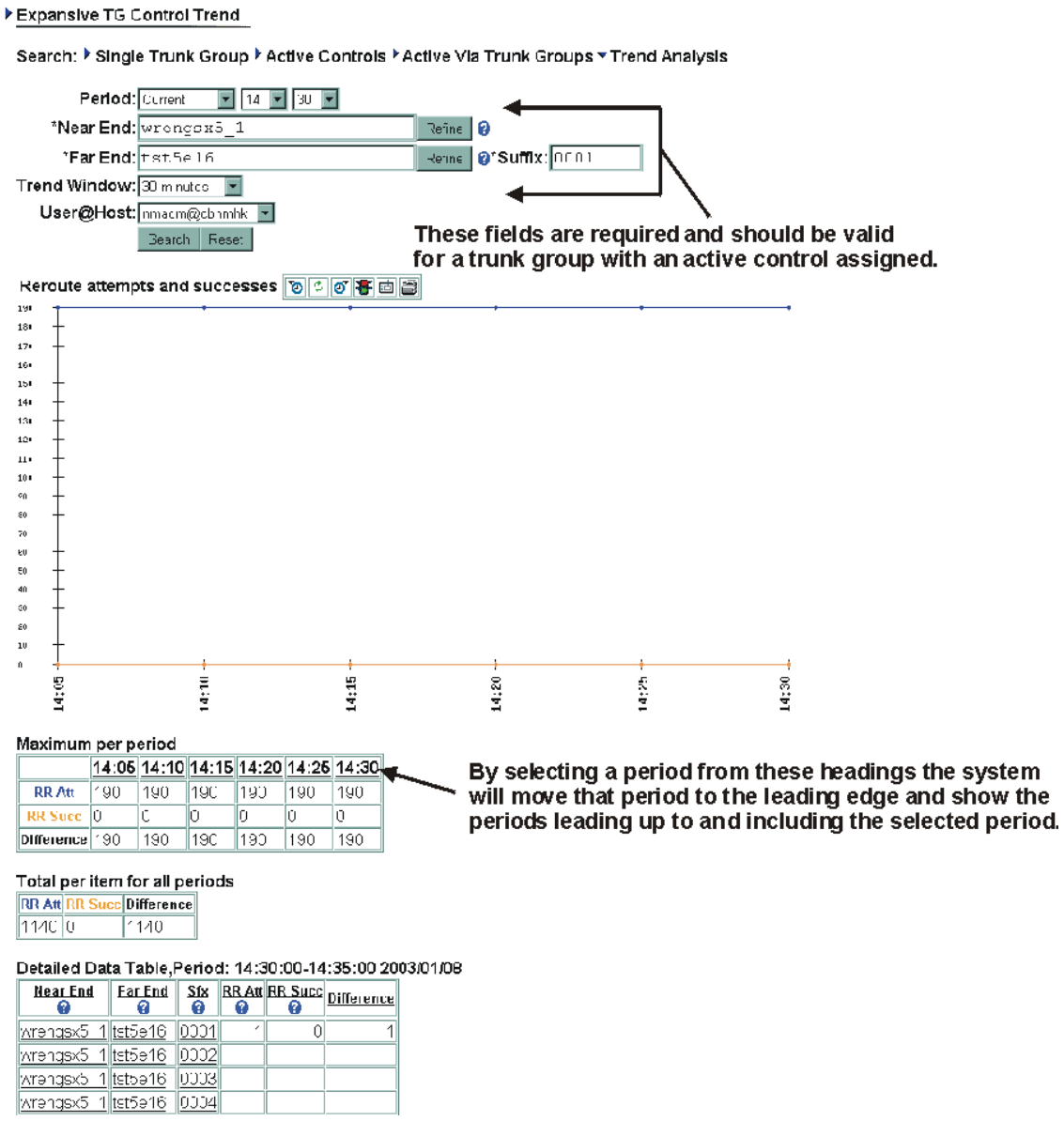
Purpose

The Expansive TG Control (Reroute) Trend page is available if you have purchased Feature 385, “Trend Analysis”.

Reference: “Trend pages” (p. 18)

The Expansive TG Control Trend page allows the user to restrict the retrieved data based on trunk groups with expansive controls active on them. Figure 20 shows an Expansive TG Controls trend page.

Figure 20 Expansive TG Control Trend page



Search criteria

Table 7 describes the search criteria that can appear in the Search area.

Table 7 Search criteria for Expansive TG Control Trend page (Sheet 1 of 2)

Label	Description
Period	Data collection period. Options are current or a historical period.

Table 7 Search criteria for Expansive TG Control Trend page (Sheet 2 of 2)

Label	Description
Near End	Near end network element. Enter the Near-End office name to restrict the search for active reroutes to a specific originating office. Valid values include all internal network elements. Multiple selections are not allowed.
Far End	Far end network view. Enter the Far-End office name to restrict the search for active reroutes to a specific terminating office. Valid values include all network elements, both internal and external.
Suffix	Trunk group suffix.
Trend Window	The number of data collection periods to be used in the trend analysis.Options are: 6, 12, 18 or 24 five-minute data collection periods (30 minutes to 2 hours).
User@<*Host*>	Choice of user IDs on a specific host machine.

Other Controls

Overview

Purpose

This section describes pages for viewing Other Controls in NTM.

Contents

This section contains the following topics:

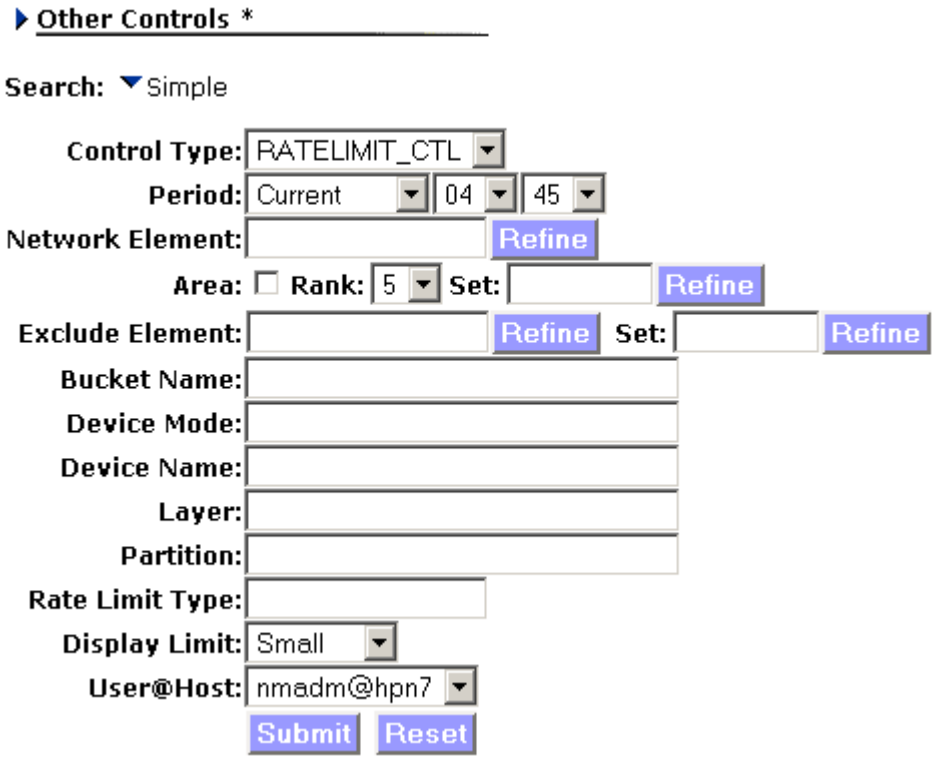
Other Controls Search Page	5-50
Other Controls Container Page	5-52
Other Controls Request Page	5-53

Other Controls Search Page

Purpose

The Other Controls search page contains a search area which has one search mode. The following is a description of Other Controls search page for “Rate Limit Controls” control type.

Figure 21 Other Controls Search Page



Other Controls Search Criteria

Table 8 describes the search criteria that can appear in the search area when default Rate Limit Controls control type is selected.

Table 8 Other Controls search criteria

Label	Description
Control type	List for available controls. The default is RATELIMIT_CTL
Period	Data collection period.
Network Element	Network Element name.

Table 8 Other Controls search criteria

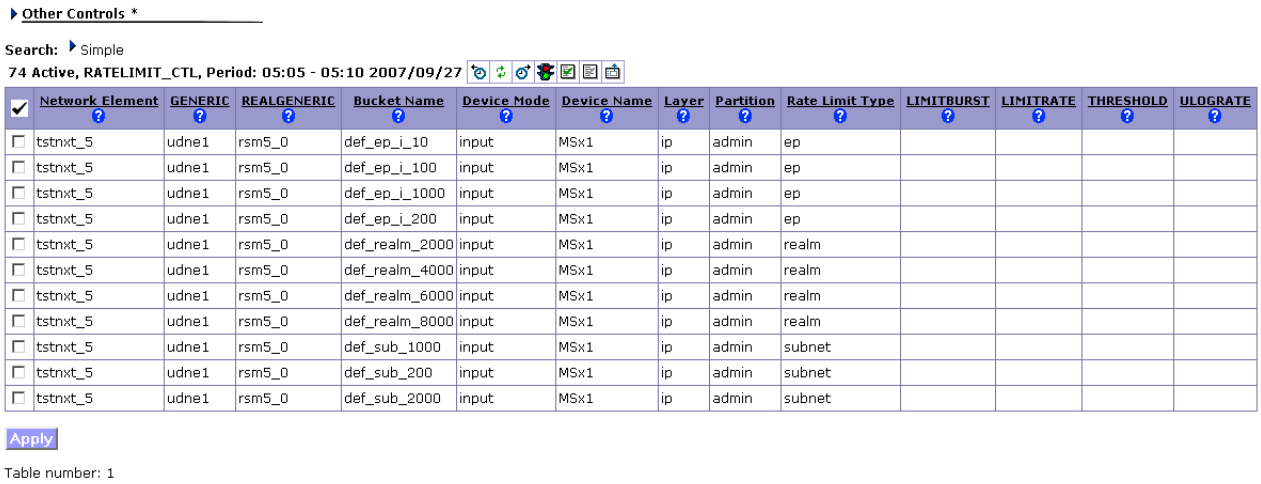
Label	Description
Area Rank Set	Network Element internal values. By default Area is unselected, rank is 5, and set is blank.
Exclude Element	Allows specified network elements to be excluded from control search.
Set	Allows specified sets to be excluded from control search.
Bucket Name	Bucket Name string value. This field is only for nextone switches.
Device Mode	This field is only for nextone switches.
Device Name	Device Name string value. This field is only for nextone switches.
Layer	This field is only for nextone switches.
Partition	This field is only for nextone switches.
Rate Limit Type	This field is only for nextone switches.
Display Limit	Small, medium, or large limit for data retrieval. • Small: 100 rows • Medium 600 rows • Large: 1200 rows • XL: 1500 rows
User@Host	Choice of user IDs on a specific host machine.

Other Controls Container Page

Purpose

The Other Controls Container Page (Figure 22) displays the results of a Other Controls search page in tabular format.

Figure 22 Other Controls Container Page



Other Controls *

Search: Simple

74 Active, RATELIMIT_CTL, Period: 05:05 - 05:10 2007/09/27

Network Element	GENERIC	REALGENERIC	Bucket Name	Device Mode	Device Name	Layer	Partition	Rate Limit Type	LIMITBURST	LIMITRATE	THRESHOLD	ULOGRATE
tstnxt_5	udne1	rsm5_0	def_ep_i_10	input	MSx1	ip	admin	ep				
tstnxt_5	udne1	rsm5_0	def_ep_i_100	input	MSx1	ip	admin	ep				
tstnxt_5	udne1	rsm5_0	def_ep_i_1000	input	MSx1	ip	admin	ep				
tstnxt_5	udne1	rsm5_0	def_ep_i_200	input	MSx1	ip	admin	ep				
tstnxt_5	udne1	rsm5_0	def_realm_2000	input	MSx1	ip	admin	realm				
tstnxt_5	udne1	rsm5_0	def_realm_4000	input	MSx1	ip	admin	realm				
tstnxt_5	udne1	rsm5_0	def_realm_6000	input	MSx1	ip	admin	realm				
tstnxt_5	udne1	rsm5_0	def_realm_8000	input	MSx1	ip	admin	realm				
tstnxt_5	udne1	rsm5_0	def_sub_1000	input	MSx1	ip	admin	subnet				
tstnxt_5	udne1	rsm5_0	def_sub_200	input	MSx1	ip	admin	subnet				
tstnxt_5	udne1	rsm5_0	def_sub_2000	input	MSx1	ip	admin	subnet				

Apply

Table number: 1

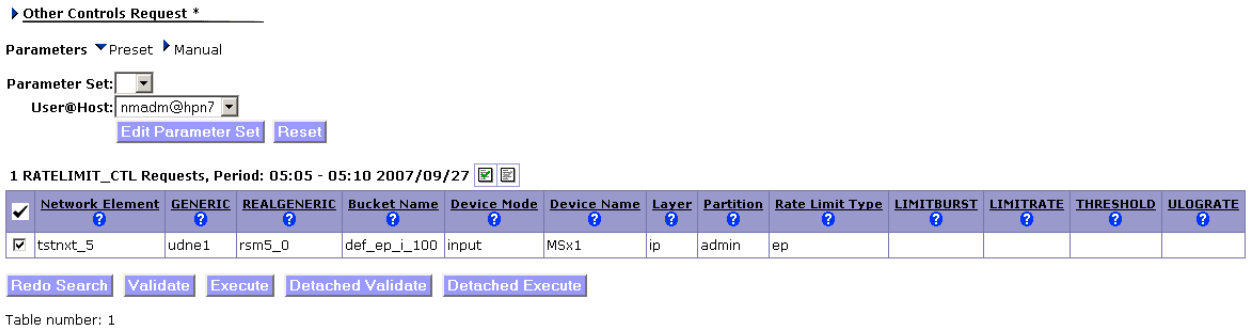
Each row of data in the container corresponds to one of the sets of control information returned by the search. The left column of the Data Table contains a column labeled with a checkmark. A row of the table is considered selected when the corresponding checkbox is selected. The Apply button will open the Other Controls Request Page for selected rows od data.

Other Controls Request Page

Purpose

The Other Controls Request Page allows you to select appropriate control parameters and execute the control requests. Access to this display is limited to users with permission to execute controls. The Other Controls Request Page has a preset parameter mode (Figure 23) and a manual parameter mode (Figure 24).

Figure 23 Other Controls request page - preset mode



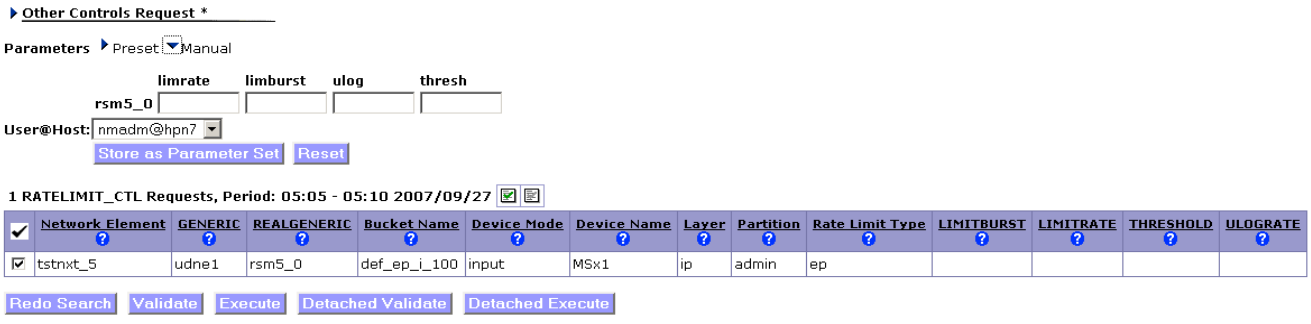
Parameter Area Preset Mode

The following parameter appears in the the Parameter area in preset mode:

- Parameter Set - For the Rate Limit control type, you can select the name of a predefined parameters

The Edit Parameter Set button provides a link to the parameter set detail page for the selected parameter set. The user can view the parameter set detail and change the defined parameters.

Figure 24 Other Controls request page - manual mode



Parameter Area Manual Mode

The following parameters can be set for Rate Limit Controls in manual mode:

- Limit Rate
- Limit Burst
- Ulog Rate
- Threshold

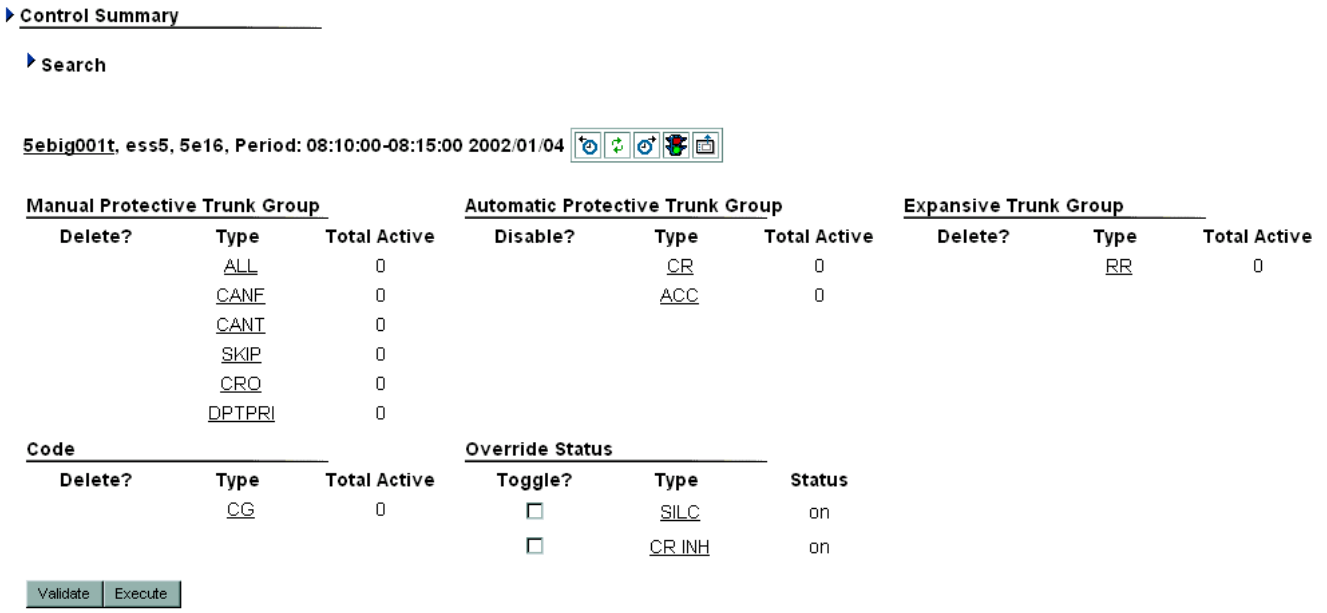
Control Summary page

Purpose

The Control Summary page (Figure 25) is available through the Navigation area of any of the control pages as well as the “Related Links” area of the Network Element Details page. This page allows the user to quickly view the active controls assigned to an individual network element.

The Control Summary search page allows you to restrict the data retrieved based on the parameters used in the `total` command.

Figure 25 Control Summary page



Page uses

The Control Summary page allows the user to:

- Display and remove each type or all Manual Protective Trunk Group Controls such as: CANF, CANT, SKIP, CRO and DPTPRI
- Display the number of active Automatic Protective Trunk Group controls, as well as disable those for SILC for a specific office. These are: SILC, CR, and ACC
- Display the total number of active Expansive Trunk Group controls, and delete them if desired, for a specific office. These are: RR (Reroute), IRR, and ORR
- Display and remove each type or all Code controls from a specific office such as: CG, RC, Term (Terminating Call Gaps), and CGX. These controls vary by office type.

- Change the override status on a specific office for SILC, and CR INH (Circuit Reservation Inhibit)
- Modify Via Reroute Turnoff Intervals (*4ESS* only)
- Display and delete Destination Codes such as HTR
- Display and delete Preprograms (1A *ESS* only)
- Delete all trunk group, code, and destination controls at one time.

References

total command (4-90) in the *Input Commands Guide*

□

General tasks on the Control pages

Overview

Purpose

This section provides the procedures for general tasks on the Control pages.

Contents

This section contains the following topics:

Viewing existing controls	5-58
Setting protective trunk group controls	5-59
Setting code (CG) controls	5-60
Setting expansive trunk group controls	5-61
Deleting controls	5-63

Viewing existing controls

Instructions

Follow these steps to view existing controls:

1 Select the control type of interest from the Controls object on the launch page.

Result: The search page for that control type appears.

2 Enter the search parameters for the controls you want to view.

3 Retrieve the data specified by your search.

Result: A container page appears with the data you retrieved.

END OF STEPS

□

Setting protective trunk group controls

Instructions

Follow these steps to set protective trunk group controls:

1. Select the Protective TG Controls subtype from the Controls object on the launch page.

   Result: The search page for that control type appears.

2. Enter the search parameters for the controls you want to view. You may use either Simple or Advanced search mode.

3. Retrieve the data specified by your search.

   Result: A container page appears with the data you retrieved. The container page displays both active and potential controls.

4. Click the Select box for the controls you wish to apply, then click on the Set Parameters button.

   Result: The Code Control Request page appears with the controls you have selected.

5. Select a Parameter Set from the menu at the top of the form, or select Manual and enter the parameters.

6. Click on the Execute button to apply the controls, or click on the Validate button to check your parameters before executing.

   Result: Controls are either applied or validated, depending on your choice.

END OF STEPS

□

Setting code (CG) controls

Instructions

Follow these steps to set code (call gap) controls:

1 Select the Code Controls subtype from the Controls object on the launch page.

Result: The search page for that control type appears.

2 Enter the search parameters for the controls you want to view.

3 Retrieve the data specified by your search.

Result: A container page appears with the data you retrieved. The container page displays both active and potential controls.

4 Click the Select box for the controls you wish to apply, then click on the Apply CG button. You may also use the Select All button to select all the potential controls in your list, or use the Delete All button to remove all the active controls in your list.

Result: The Code Control Request page appears with the controls you have selected.

5 Select a Parameter Set from the menu at the top of the form, or choose Manual Parameter mode.

6 In Manual Parameter mode, you must set the control parameters to the values you want.

7 Click on the Execute button to apply the controls, or click on the Validate button to check your parameters before executing.

Result: Controls are either applied or validated, depending on your choice.

END OF STEPS

□

Setting expansive trunk group controls

Instructions

Follow these steps to set expansive trunk group controls:

1 Select the Expansive Trunk Group Controls subtype from the Controls object on the launch page.

Result: The search page for that control type appears.

2 Using the single Trunk Group Search, enter the search parameters for the trunk group for which you wish to have a control assigned. Click on the Search button.

- If controls are active, a container page appears displaying current controls. Go to Step 3.
- If no controls are active, a details page appears giving the user the option to analyze vias and apply a reroute. Skip to Step 4.

3 If a control is active, select the control you wish to modify from the list of active controls by clicking the select box. Then click the Analyze and Apply RR button.

Result: The Expansive TG Controls Request page appears displaying possible reroute vias. Skip to Step 5.

4 If no controls exist, select Analyze VB Suffixes to finalize.

Result: The Expansive TG Controls Request page appears displaying possible reroute vias.

5 Using the via analysis available at the bottom of the page, select the desired vias. Select parameters desired from the menu at the top of the form. For some switches these parameters include codes for code specific reroutes in addition to the vias desired.

6 Click on the Validate button to check your parameters before executing, or click on the Execute button to apply the controls.

Result: Controls are either applied or validated, depending on your choice.

END OF STEPS

Deleting controls

Instructions

Follow these steps to delete controls:

1. Select the Expansive TG Controls subtype from the Controls object on the launch page.

   Result: The search page for that control type appears.

2. Using the single Trunk Group Search, enter the search parameters for the trunk group for which you wish to delete a control or, select the Active Controls button to retrieve a list of all active controls. Click on the Search button.

   Result: If there is an active control, a container page appears displaying current controls.

3. Select the control you wish to delete from the list of active controls by clicking the select box.

4. Select the Delete button.

5. Click the Select box for the controls you wish to apply, then click on the Delete button.

   Result: The control you have selected is removed from the network.

END OF STEPS

□

6 Destinations

Overview

Purpose

The Destinations object represents data for destinations (by code). This includes:

- Destination Codes — allows you to view destination data
- Destination Assignments — allows you to administer Manual HTR assignments and Automatic HTR parameter set capabilities.

Contents

This chapter contains the following topics:

Destination Codes	6-3
Destination Assignments	6-9
General tasks on the Destination pages	6-19

Destination Codes

Overview

Purpose

The Destination Codes object allows you to retrieve data based on attributes of a destination.

Contents

This section contains the following topics:

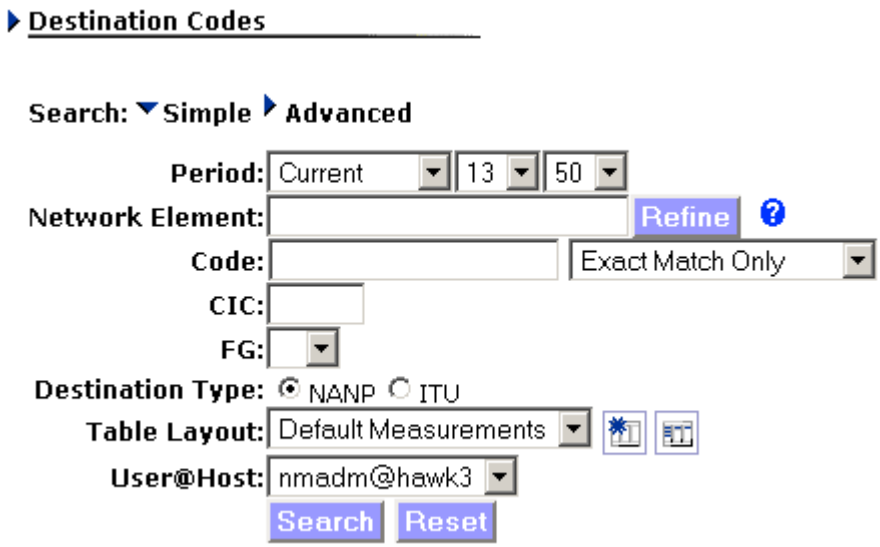
Destination Codes search page	6-4
Destination Codes container page	6-6
Destination Code Details page	6-7

Destination Codes search page

Purpose

This page contains a Search area, which has a simple search mode and an advanced search mode. Figure 1 shows an example of Destination Codes advanced search mode.

Figure 1 Destination Codes Advanced search page



Search criteria

Table 1 describes the search criteria that appear in the Search area for Destination Codes.

Table 1 Destination Codes search criteria (Sheet 1 of 2)

Label	Description
Period	Data collection period.
Session	Historical session ID. This field is available with Feature 342, "Historical Data Playback for the Browser-based GUI"
Network Element Area Rank Set	Valid values include all internal network elements and sets. Check "Area" to retrieve data on a network element area.

Table 1 Destination Codes search criteria (Sheet 2 of 2)

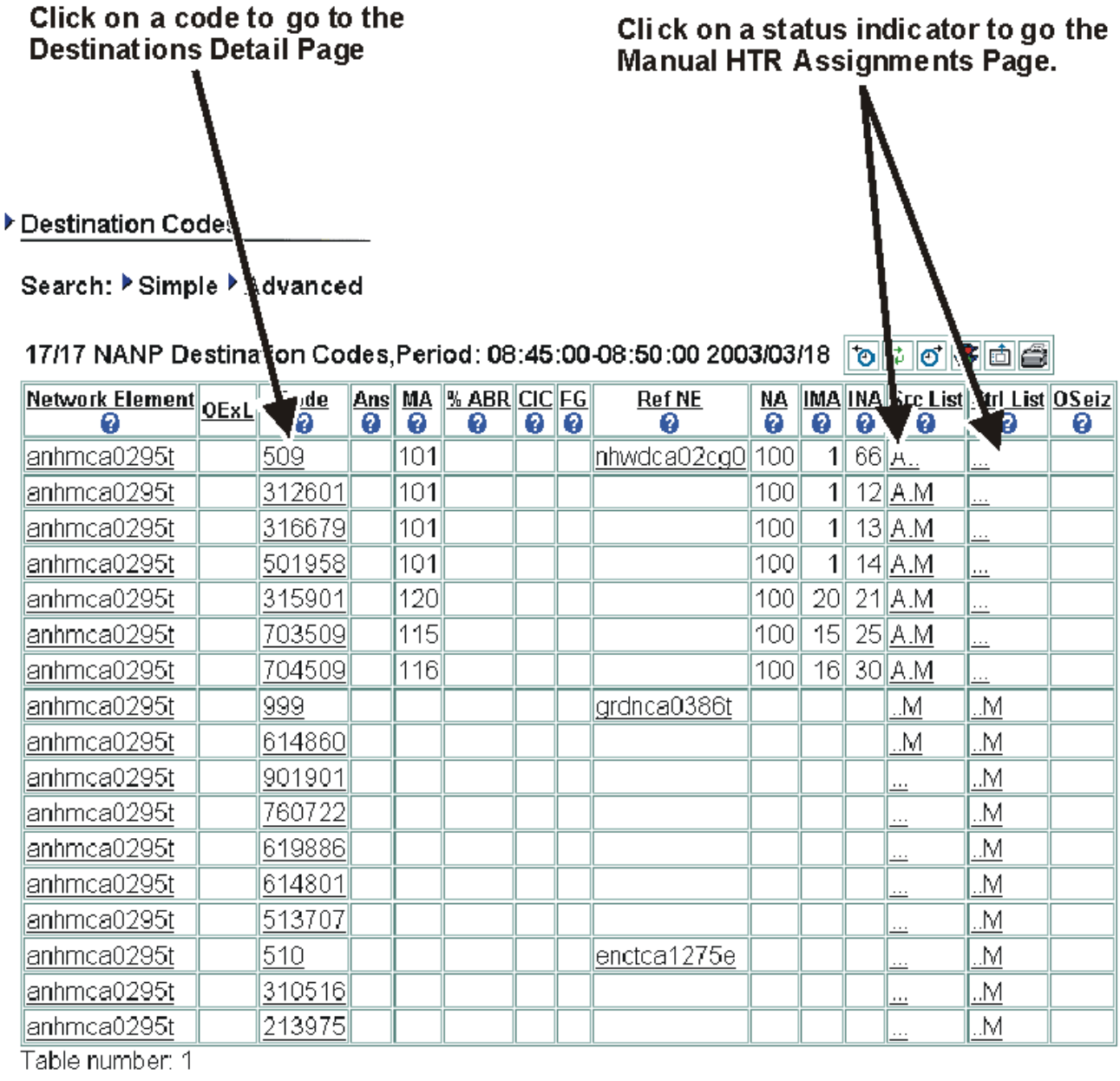
Label	Description
Code	Destination code. It can be restricted to: • Exact Match Only = exact match of given code • Include Less Than = first substrings from the given code, e.g. for "013" the matching codes are: "0", "01", and "013". • Include Greater Than = substrings starting with the given code, e.g. for "013" the matching codes are: "013", "0130", "0131", etc. • Less/Greater Than = first substrings or codes starting with the given code, but without the exact match,e.g. for "013" the matching codes are: "0", "01", "0130", "0131", "01399999", etc. Substring match = codes containing the given substring, e.g. for "013" the matching codes are: "013", "0130", "01399", "9901399", "99013", etc.
CIC	Carrier Identity Code (Blank by default) (This field ***cannot*** be selected to show *4ESS* switch data.)
FG (*GTD-5*)	Feature Group. Valid values are: blank, B, C, or D. Default is blank. (This field ***cannot*** be selected to show *4ESS* switch data.)
Destination Type	• NANP (Domestic) • ITU (International)
Data Restriction	The two data restriction fields allow you to retrieve data based on values for up to two values, and an operator. For example, you may set these fields to: `OEXL >= 75 AND PC > 300` Only those codes having measurements matching these data restrictions will be retrieved.
Display Limit	Maximum number of rows to display. Choices are: • Small — 100 rows • Medium — 600 rows • Large — 1200 rows
Table Layout	Table layout choices. The valid choices are limited to table layouts that apply to the Destination Code data tables.
User@Host	Choice of user IDs on a specific host machine.

Destination Codes container page

Purpose

The Destination Codes container page (Figure 2) displays the results of a Destination Codes search.

Figure 2 Destination Codes container page



Network Element	OExL	Code	Ans	MA	% ABR	CIC	FG	Ref NE	NA	IMA	INA	Src List	Ctrl List	OSeiz
anhmca0295t		509		101				nhwdca02cg0	100	1	66	A..	...	
anhmca0295t		312601		101					100	1	12	A.M	...	
anhmca0295t		316679		101					100	1	13	A.M	...	
anhmca0295t		501958		101					100	1	14	A.M	...	
anhmca0295t		315901		120					100	20	21	A.M	...	
anhmca0295t		703509		115					100	15	25	A.M	...	
anhmca0295t		704509		116					100	16	30	A.M	...	
anhmca0295t		999						grdnca0386t				..M	..M	
anhmca0295t		614860										..M	..M	
anhmca0295t		901901										...	..M	
anhmca0295t		760722										...	..M	
anhmca0295t		619886										...	..M	
anhmca0295t		614801										...	..M	
anhmca0295t		513707										...	..M	
anhmca0295t		510						enctca1275e				...	..M	
anhmca0295t		310516										...	..M	
anhmca0295t		213975										...	..M	

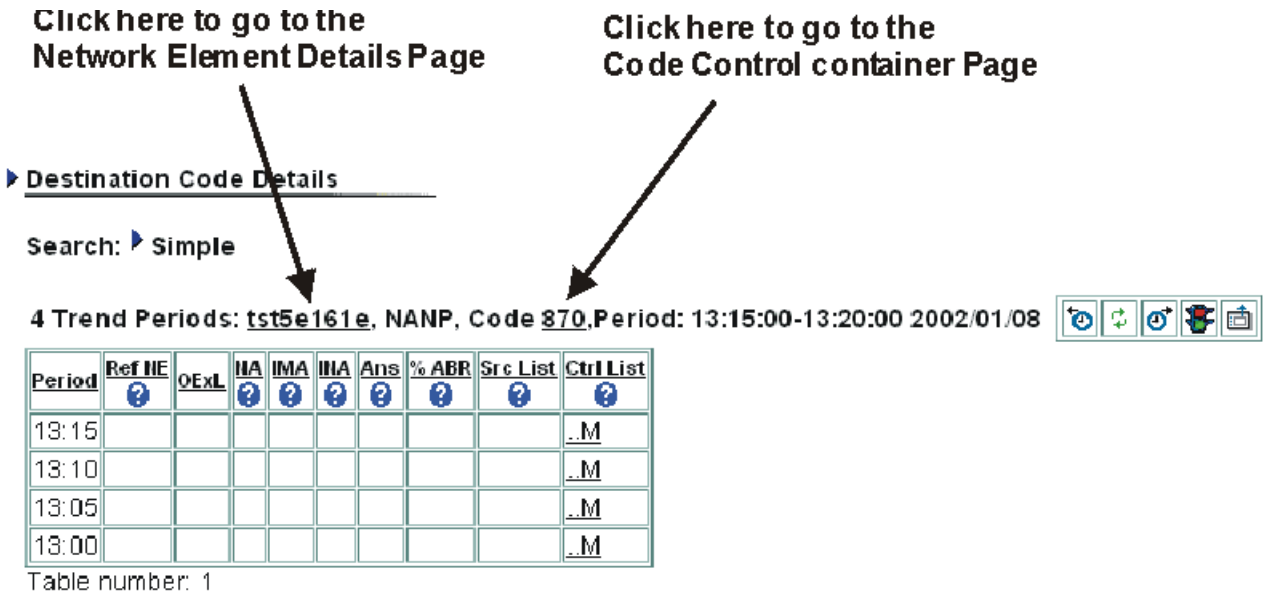
Table number: 1

Destination Code Details page

Purpose

The Destination Code Details page (Figure 3) provides destination code trend data for a network element.

Figure 3 Destination Code Details page



Destination Assignments

Overview

Purpose

Destination Assignments is available as a link in the Navigation area on the Destination Codes pages. Destination Assignments allows you to administer:

- Manual HTR Assignments (default)
- Automatic HTR Parameter Set Definitions (4ESS)
- Automatic HTR Parameter Set Assignments

Each of these options is available as a link from the top of the Destination Assignments pages.

Contents

This section contains the following topics:

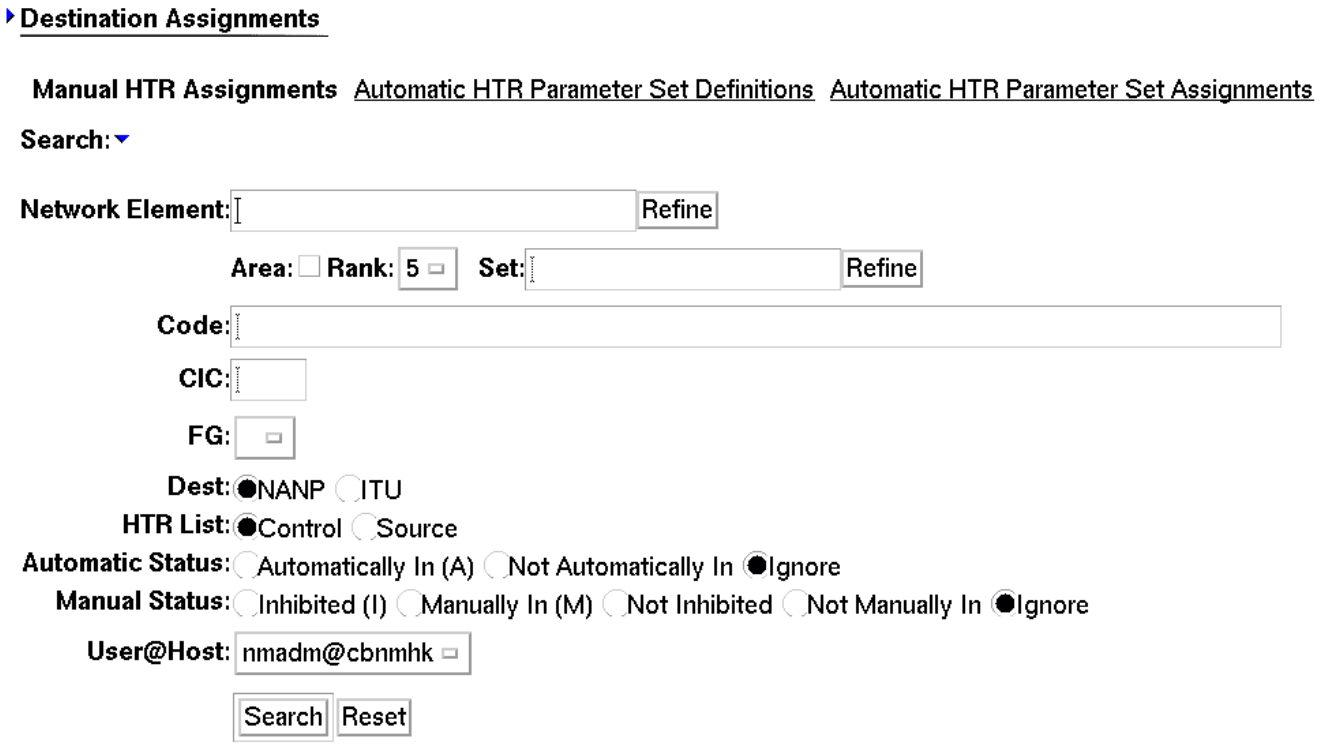
Manual HTR Assignments	6-10
Manual HTR Assignments container page	6-11
Automatic HTR Parameter Set Definitions (4ESS)	6-13
Automatic HTR Parameter Set Assignments	6-15

Manual HTR Assignments search page

The Manual HTR Assignments search page (Figure 4) contains a search area, which has only a simple search mode.

For the Manual HTR Assignments search page (Figure 4), you may search for destination assignments by network element or code. Search results are presented in a container page (Figure 5).

Figure 4 Manual HTR Assignments search page



Search criteria

Table 2 describes the search criteria that appear in the Search area for Manual HTR Assignments.

Table 2 Manual HTR Assignments search criteria (Sheet 1 of 2)

Label	Description

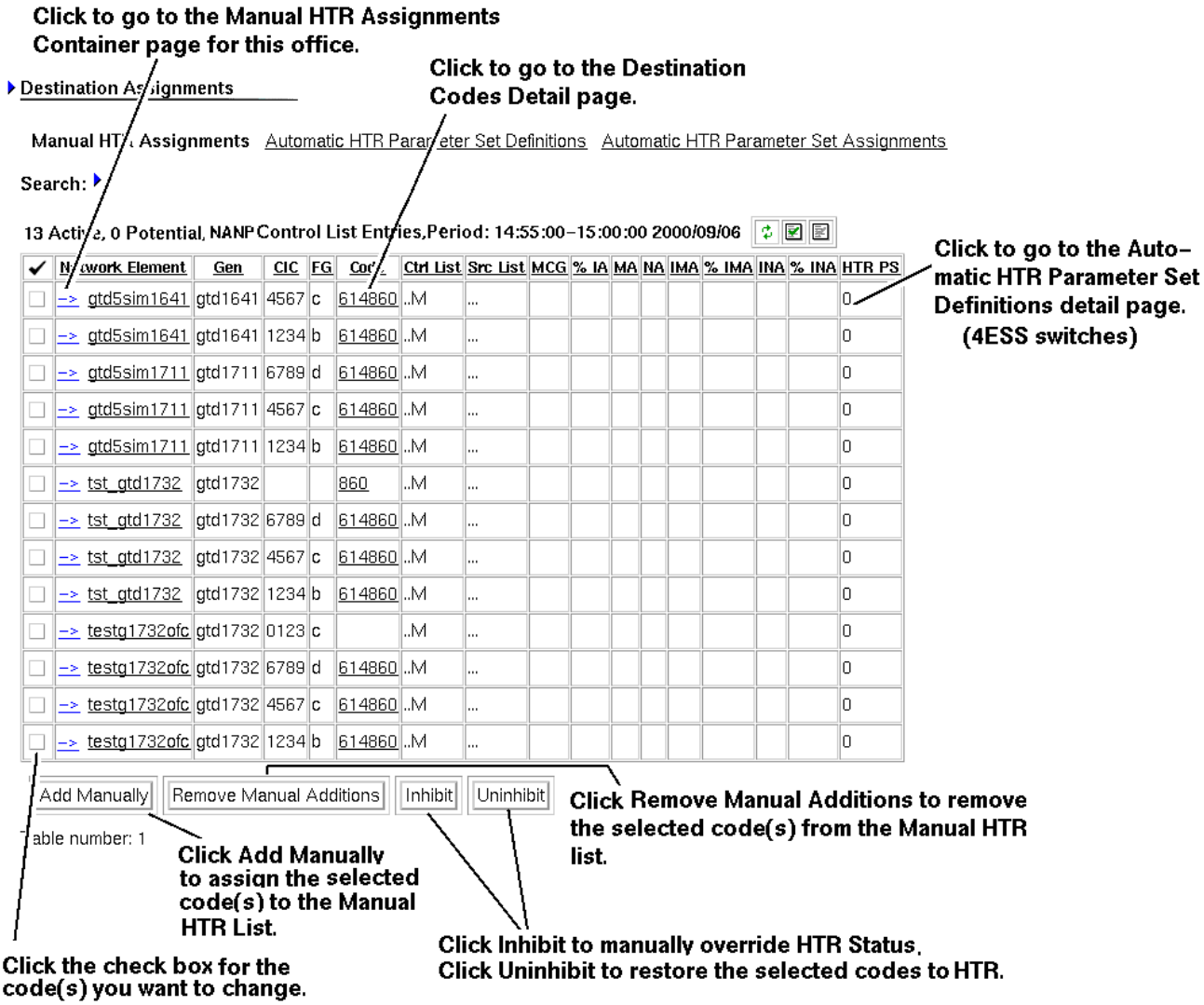
Table 2 Manual HTR Assignments search criteria (Sheet 2 of 2)

Network Element Area Rank Set	Network element name. By default, Network Element is blank, Area is unselected, rank is 5, and set is blank.
Code	Destination code. Valid codes may be up to 15 digits. Up to ten 6-digit codes can be entered, with up to 9 commas used as separators. (If left blank only active controls will be shown)
CIC	Carrier Identity Code (Blank by default) (This field ***cannot*** be selected to show *4ESS* switch data.)
FG (GTD5)	Feature Group. Valid values are: blank, B, C, or D. Default is blank. (This field ***cannot*** be selected to show *4ESS* switch data.)
Dest	• NANP (Domestic) • ITU (International)
HTR List	Valid values are: • Source (*4ESS* only) • Control (default)
Automatic Status (*4ESS*)	Valid values are: • Automatically In — Retrieves data for a list of codes placed on the HTR list by a network element. (These codes may be manually placed in HTR status or inhibited.) • Not Automatically In — Retrieves data for codes not placed on the HTR list by a network element. (These codes may be manually placed in HTR status or inhibited.) • Ignore (default) — Ignore automatic HTR status.
Manual Status (*4ESS*)	Valid values are: • Inhibited (I) — Retrieves codes that are HTR and have been manually inhibited. • Manually In (M) — Retrieves a list of codes that have been manually placed on the specified HTR list. • Not Inhibited, or Not Manually In — Retrieves a list of codes not manually placed in HTR status. (These codes may be automatically placed in HTR status or inhibited.) • Ignore (default) — Ignore manual HTR status.
User@Host	Choice of user IDs on a specific host machine.

Manual HTR Assignments container page

The Manual HTR Assignments container page (Figure 5) displays the active and potential HTR list entries for the search you requested. Potential HTR list entries are displayed only if at least one code is specified in the search.

Figure 5 Manual HTR Assignments container page

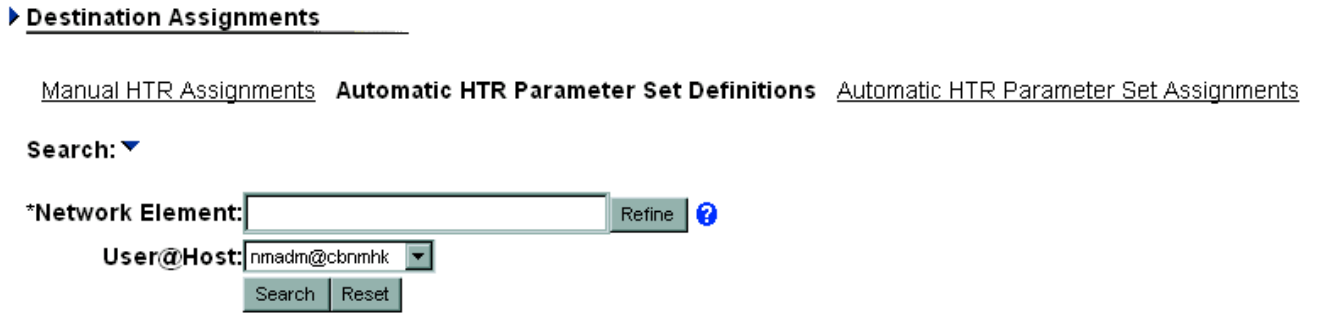


Automatic HTR Parameter Set Definitions search page

The Automatic HTR Parameter Set Definitions page contains a search area, which has only a simple search mode. Figure 6 shows an example of the Automatic HTR Parameter Set Definitions search page.

With the Automatic HTR Parameter Set Definitions option, you may set automatic HTR threshold definitions. Figure 7 shows an example of the Automatic HTR Parameter Set Definitions page.

Figure 6 Automatic HTR Parameter Set Definitions search page



Search criteria

Table 3 describes the search criteria that may appear in the Search area for Destination Assignments, depending on which option is selected.

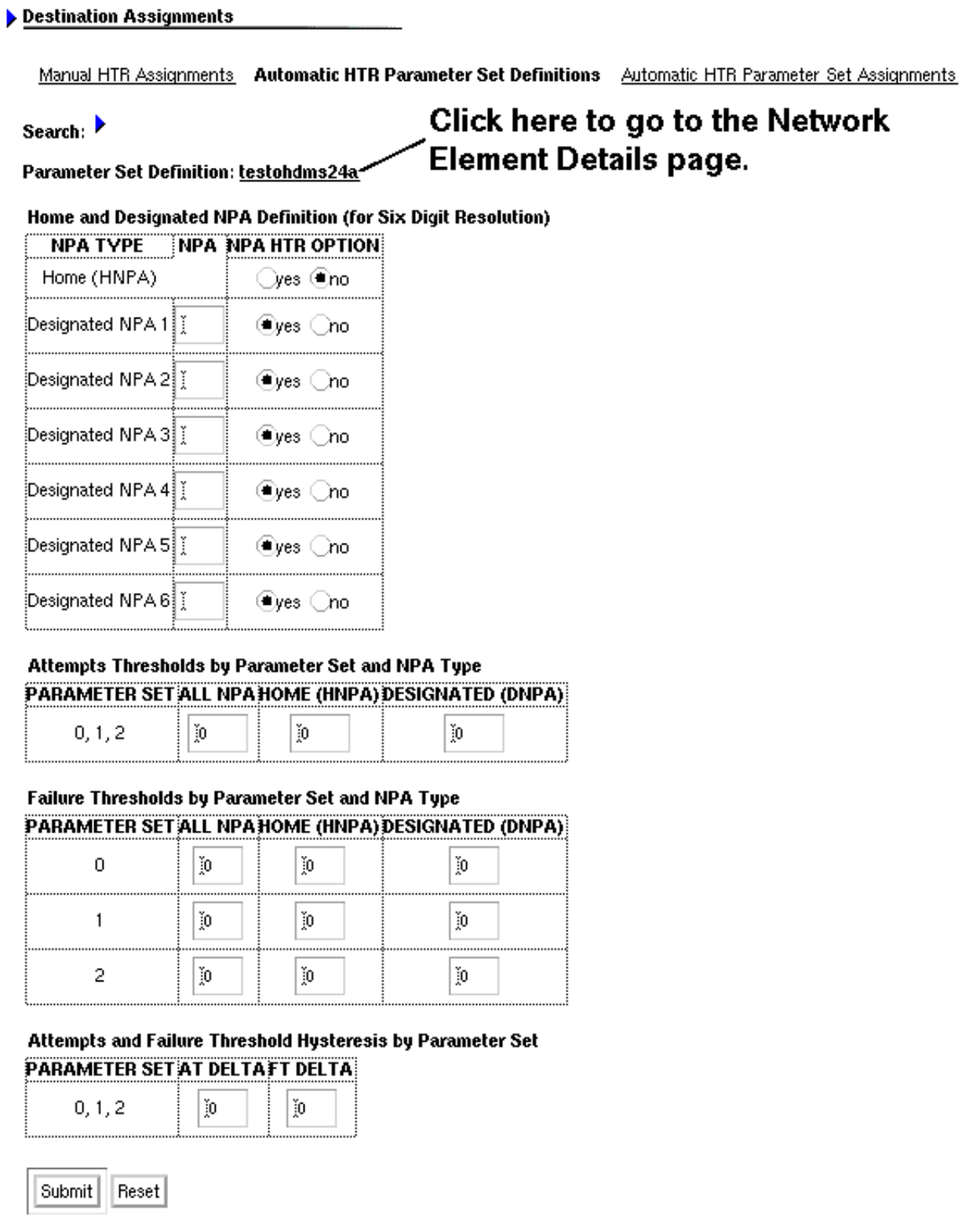
Table 3 Automatic HTR Parameter Set Definitions search criteria

Label	Description
Network Element	Network element name.
User@Host	Choice of user IDs on a specific host machine.

Automatic HTR Parameter Set Definitions page

The Automatic HTR Parameter Set Definitions page (Figure 7) displays and allows the user to change parameter set definitions.

Figure 7 Automatic HTR Parameter Set Definitions page

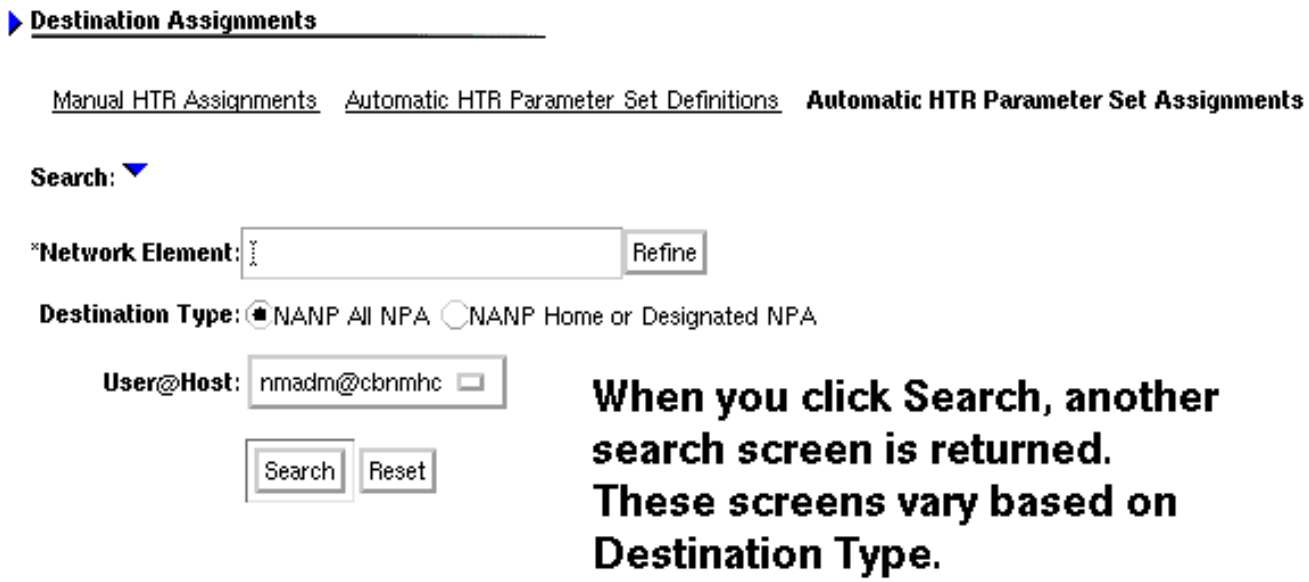


Automatic HTR Parameter Set Assignments

Automatic HTR Parameter Set Assignments search page

The Automatic HTR Parameter Set Assignments page contains a search area, that has only a simple search mode.

Figure 8 Automatic HTR Parameter Set Assignments search page



Search criteria

Table 4 describes the search criteria that appear in the Search area.

Table 4 Automatic HTR Parameter Set Assignments search criteria

Label	Description
Network Element	Network element name.
Destination Type	Valid values are: • NANP All NPA (default) • NANP Home or Designated NPA
User@Host	Choice of user IDs on a specific host machine.

For the Automatic HTR Parameter Set Assignments search option, you may search for destination assignments by Network Element and Destination Type.

The Automatic HTR Parameter Set Assignments page (Figure 8) has a two-part search. For the initial search the user must select ***one*** of the following options that result in a second part of the search parameter being displayed:

- NANP ALL NPA (Returns Figure 9 when selected)
- NANP Home or Designated NPA (Returns Figure 10 when selected)

For the ALL NPA option, you may enter up to ten NPAs in the NPA field and select a parameter set (0, 1, 2, 1 or 2) from the list. The default search includes all parameter sets.

For the Home or Designated NPA option, you may select an NPA from the NPA drop-down list, enter up to ten NXXs in the NXX field, and select a parameter set (0, 1, 2, or 1 and 2) from the parameter set list. (None of these fields are required.) The default search includes all parameter sets.

Figure 9 Automatic HTR Parameter Set Assignments — NANP All NPA

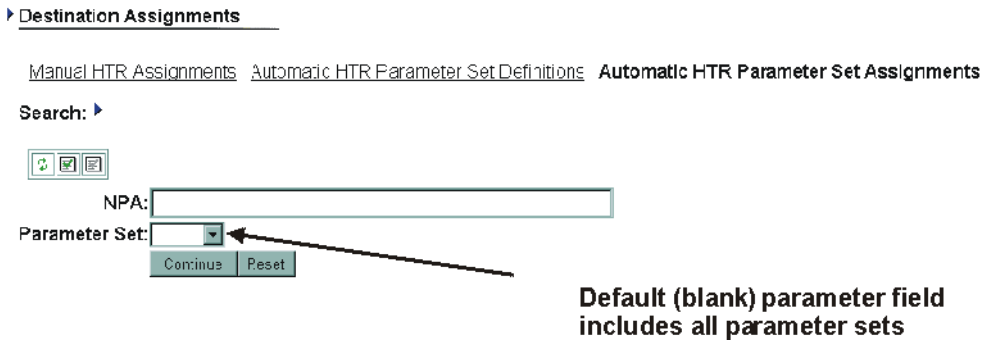
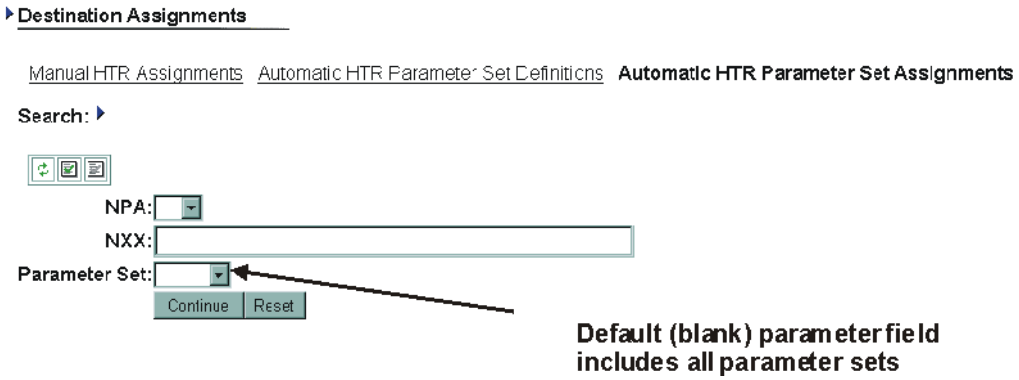


Figure 10 Automatic HTR Parameter Set Assignments — NANP Home or Designated NPA

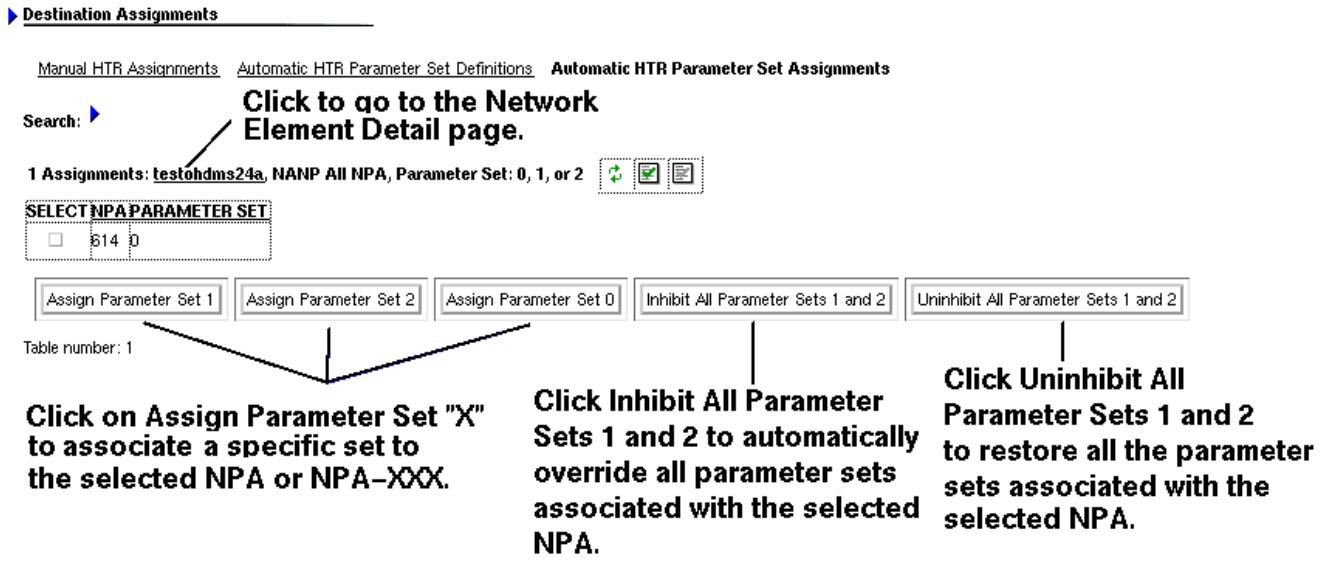


When you click “Continue”, you get a container page displaying each NPA or NPA-NXX you selected and the parameter set used to determine whether that code is Hard To Reach.

Automatic HTR Parameter Set Assignments container page

Figure 11 shows an example of the Automatic HTR Parameter Set Assignments container page. For any NPA or NPA-NXX listed in the table, you may click the select box in the left column of the row and use the buttons at the bottom of the page to assign a different parameter set or inhibit/uninhibited parameter sets 1 and/or 2.

Figure 11 Automatic HTR Parameter Set Assignments container page



General tasks on the Destination pages

Overview

Purpose

This section provides the procedures for general tasks on the Destination pages.

Contents

This section contains the following topics:

Retrieving destination data	6-20
Retrieving destination assignment data	6-21
Adding and modifying manual hard-to-reach assignments	6-22
Modifying automatic hard-to-reach parameter sets	6-23
Adding/modifying automatic HTR parameter set assignments	6-24

Retrieving destination data

Instructions

Follow these steps to retrieve destination data:

1. Select Destination Codes from the options at the top of the page.

   Result: The Search page for destination codes is displayed.

2. Fill in the form objects on the Destination Codes Search page.

3. Click on the Search button.

   Result: Data for the parameters you selected are displayed.

END OF STEPS

□

Retrieving destination assignment data

Instructions

Follow these steps to retrieve destination assignment data:

1 Select Destination Codes from the icon the launch page.

Result: The Search page for destination codes is displayed.

2 From the navigation area, select Destination Assignments.

Result: The Search page for destination assignments, in the Manual HTR Assignments mode, is displayed.

3 Fill in the form objects on the Destination Assignments Search page.

Result: Data with the parameters you selected is displayed.

Important! Depending on your search criteria, both active and/or potential controls can be displayed.

Reference: Table 2, “Manual HTR Assignments search criteria” (p. 10)

4 Click the Search button.

END OF STEPS

□

Adding and modifying manual hard-to-reach assignments

Instructions

Follow these steps to add or modify manual HTR assignments:

1 Select Destination Codes from the icon on the launch page.

Result: The Search page for destination codes is displayed.

2 From the navigation area, select Destination Assignments

Result: The Search page for destination assignments is displayed.

3 Select “Manual HTR Assignments”.

Result: A form object will appear.

4 Fill in the form objects on the search page. You may specify network element and/or code.

5 Click on the Search button.

Result: Data with the parameters you selected is displayed.

6 Select the code or codes you want to change.

7 Select the desired action button found below the selection table.

END OF STEPS

□

Modifying automatic hard-to-reach parameter sets

Instructions

Follow these steps to modify automatic HTR parameter sets:

Important! Valid characters in parameter sets include alphanumeric characters and symbols like the percent sign (%). Invalid characters include comma (,), slashes (/\), and other non-alphanumeric characters.

1 Select Destination Codes from the icon on the launch page.

Result: The Search page for destination codes is displayed.

2 From the navigation area, select Destination Assignments.

Result: The Search page for destination assignments is displayed.

3 Select the “Automatic HTR Parameter Set Definitions”.

Result: The Automatic HTR Parameter Set Definitions Search page is displayed.

4 Specify a network element.

5 Click the “Search” button.

Result: The Automatic HTR Parameter Set Definitions page is displayed.

6 Specify Home and Designated NPAs, attempts thresholds (AT) for all parameter sets, failure thresholds for each parameter set, and delta values for all parameter sets, as desired.

7 Click “Submit” to save your changes.

END OF STEPS

□

Adding/modifying automatic HTR parameter set assignments

Instructions

Follow these steps to modify automatic HTR parameter sets:

Important! Valid characters in parameter sets include alphanumeric characters and symbols like the percent sign (%). Invalid characters include comma (,), slashes (/\), and other non-alphanumeric characters.

1 Select Destination Codes from the icon the launch page.

Result: The Search page for destination codes is displayed.

2 From the navigation area, select Destination Assignments

Result: The Search page for destination assignments is displayed.

3 Select “Automatic HTR Parameter Set Assignments”.

Result: The Automatic HTR Parameter Set Assignments Search page is displayed.

4 Specify a network element and either:

- NANP All NPA.
- NANP Home or Designated NPA

5 Click the “Search” button.

Result: The Automatic HTR Parameter Set Assignments sub-search page appears.

6 Specify the desired NPA or NXX and the associated parameter set.

7 For any NPA or NPA-NXX listed in the table, you may click the select box in the left column of the row and use the buttons at the bottom of the page to assign a different parameter set or inhibit/uninhibit parameter sets 1 and/or 2.

Result: The parameter set for the selected code is changed.

END OF STEPS

7 Other Functions

Overview

Purpose

This chapter provides information about the items under the Error Log icon and additional functions of the NTM GUI.

Contents

This chapter contains the following topics:

Error Log	7-3
Control Log	7-7
Broadcast Messages	7-11
Sending a Broadcast Message	7-13
Audible Alarms	7-15
Exception Status and Marked Assignments	7-21
Filters	7-29
Additional functions of the NTM GUI	7-49

Error Log

Overview

Purpose

The Error Log icon provides GUI access to view error log files without knowing the error log file names.

Reference: errlog command (9-7) in the *Input Commands Guide*

Contents

This section contains the following topics:

Error Log search page	7-4
Error Log container page	7-5

Error Log search page

Purpose

The Error Log search page allows you to restrict the retrieved data based on various parameters. Submitting a search in the Error Log causes the system to attempt to retrieve from the last 1000 records in the error log, errors that match the search criteria you entered. For example, if “Minor” is entered as the level, the system will attempt to retrieve messages logged that have a level of Minor or greater. To view error messages exceeding the 1,000 maintained for GUI retrieval, you can use the errlog command (9-7).

Search criteria

Table 1 describes the search criteria that appear in the Error Log search.

Table 1 Search criteria in the Error Log

Label	Description
Code	Error Code. The user can enter any error code or “all”.
Number	Error Number. This will restrict the search to a specific error number or numbers. The user can enter any error number to restrict the search. Multiple error numbers are comma separated. You may enter a maximum of five 3-digit numbers, separated by commas.
Level	Valid values are “critical”, “major”, “minor”, and “information”. Those messages equal to or greater than the selected level will be retrieved. The default is “information”.
Message Text	A text field allowing the user to restrict the search to the set of error messages containing a specific string. The user can enter up to 60 characters of a message substring.
Source	If Feature 272, “NTM Report Writer” is enabled and Report Writer is installed in a stand-alone configuration, the names of the Report Writer host and the NTM host will appear here. The user may select to see errors from one or both hosts. If Feature 272, “NTM Report Writer” has not been purchased or if the Report Writer software is co-resident with NTM, this field will not appear.

References

See the “Introduction to System Responses” chapter in the *System Responses Guide*.

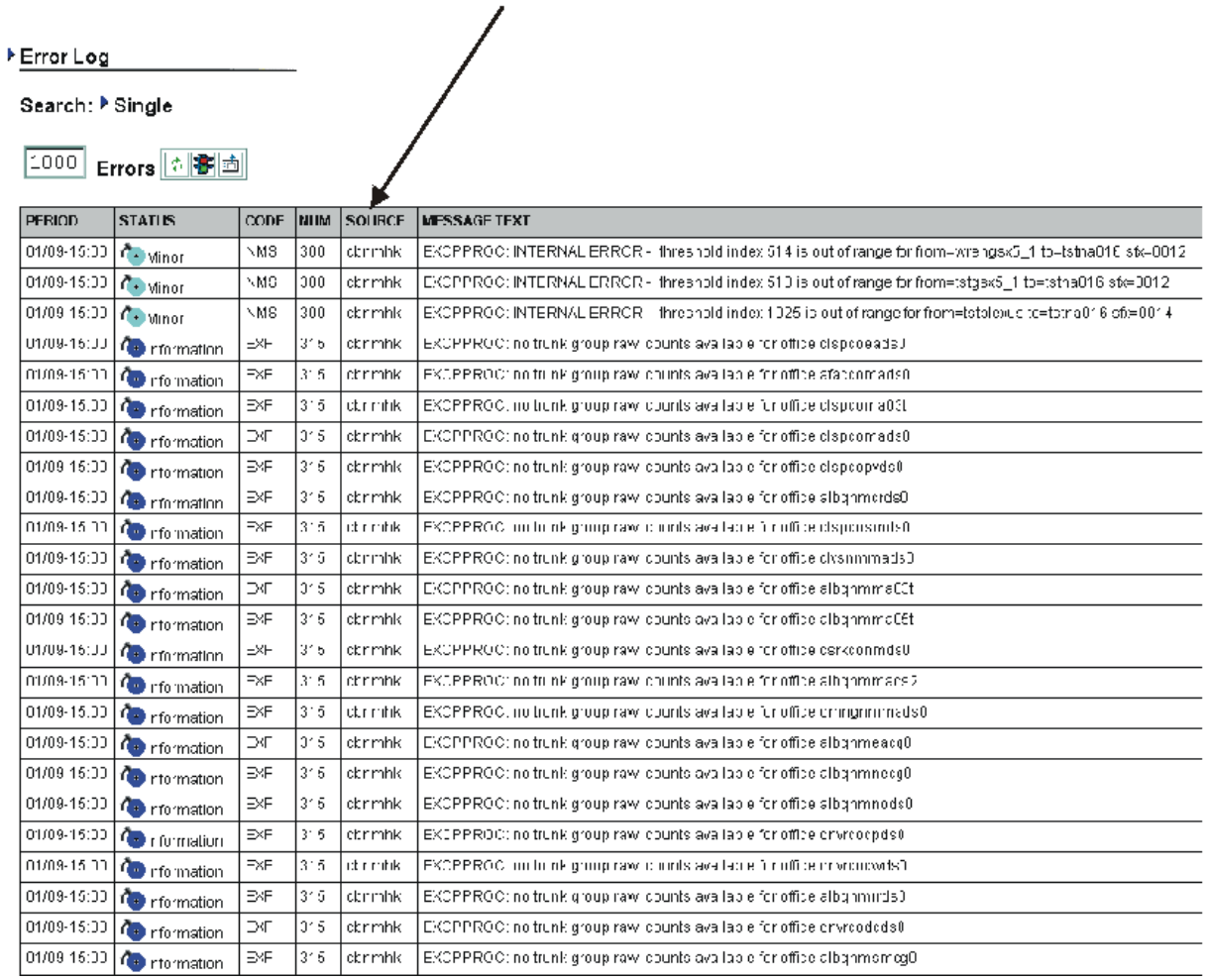
Error Log container page

Purpose

The Error Log container page (Figure 1) displays the results of a search in tabular format.

Figure 1 Error Log container page

If the optional Report Writer feature is installed in a stand-alone configuration, a "Source" column will also appear on the table. It will display the name of the NTM or Report Writer host, depending on where the error was generated. If Feature 272 has not been purchased or if Report Writer is co-resident with NTM, this column will not appear on the table.



Page characteristics

This page supports manual update and automatic update (every 30 seconds).

A graphical indicator for alarms is shown to the left of the value in the alarm level column of the display table. The following alarm indicators are used:

- Red Indicator — Critical error messages
- Yellow Indicator — Major error messages
- Cyan Indicator — Minor error messages
- Blue Indicator — Information messages

References

For an explanation of error messages, see the *System Responses Guide*.

□

Control Log

Overview

Purpose

This section provides information about the Control Log component of the NTM GUI.

Contents

This section contains the following topics:

Control Log search page	7-8
Control Log detail page	7-9

Control Log search page

Purpose

The Control Log search page allows you to restrict the data retrieved based on the parameters used in the `ctrlog` command. It allows you to view current and historic control information. It is accessed by selecting the Control Log icon on the Launch page as well as through the navigation links.

Search criteria

Table 2 describes the search criteria that appear in the Search area for the Control Log page:

Table 2 Search criteria for the Control Log

Label	Description
Network Element	Network element name. Valid values include all internal network elements. Only a single selection is allowed. Blank by default.
Type	Type of control. This field lists all control types valid for a customer, including “All”. Default is “All”.
Status	Status of control log entries (all, active, matched, summary).
By	User ID of person who applied or deleted controls or “all”. Blank by default.
Start	Start time for an interval of controls. Blank by default. The format is YY/MM/MM–HH:MM.
Stop	Stop time for an interval of controls. Blank by default. The format is YY/MM/MM–HH:MM.

Search results

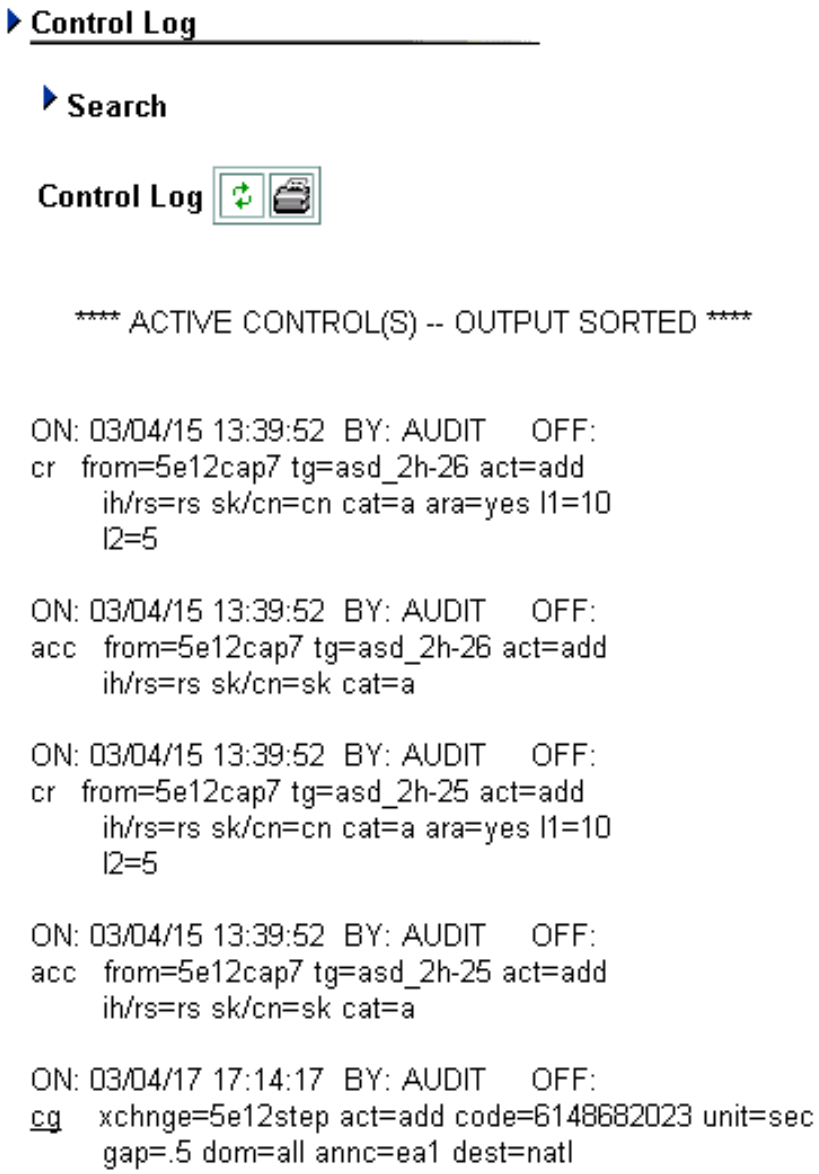
The results of a search are displayed in the Control Log detail page.

Control Log detail page

Purpose

The Control Log detail page (Figure 2) displays the results of a search for control log information. The Control Log detail page consists of the output from the `ctrlog` command, using the parameters defined in the Control Log search page.

Figure 2 Control Log detail page



References

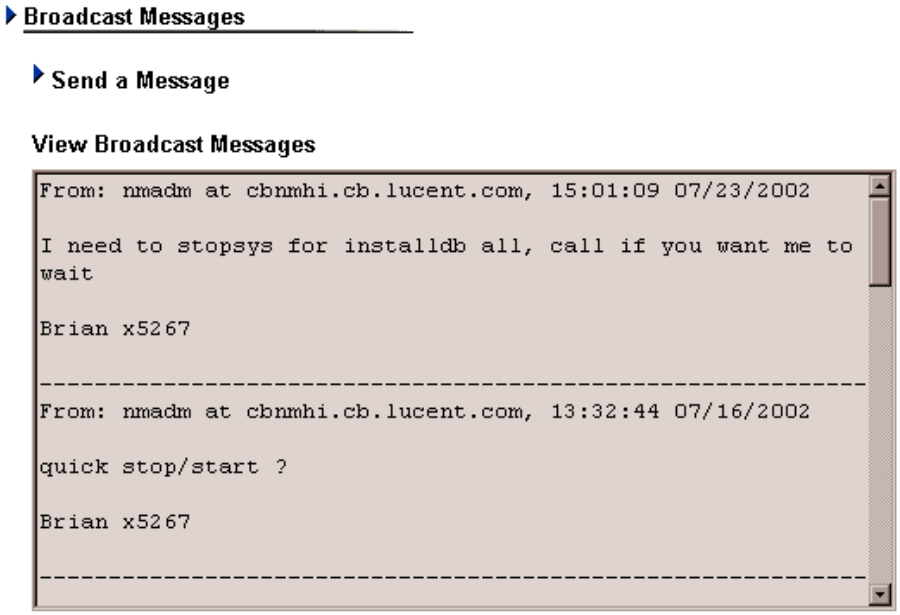
"ctrlog" (p. 59) in the *Input Commands Guide*

Broadcast Messages

Purpose

The broadcast messages page (Figure 3) provides a means to send and receive broadcast messages from other NTM users.

Figure 3 Broadcast Message window



Sending a Broadcast Message

A broadcast message can be composed in the send message portion of the Broadcast Message page (a text area in which you may enter the message). You do not need to enter return, but you can use this window as you would any other text entry box.

Submitting broadcasts the message to all NTM users currently logged on to the system with a Broadcast Message window active.

Receiving a Broadcast Message

A broadcast message is displayed in the View Broadcast Messages portion of the Broadcast Message page. “Broadcast Message Received” appears at the top of the window. This session can be minimized and still receive broadcast messages.

Important! A broadcast message page must be active in order for broadcast messages to appear.

References

To send messages to users from the host, see the `guiwall` command in the *Input Commands Guide*.

Sending a Broadcast Message

Instructions

Follow these steps to send a Broadcast Message:

Important! To get full use from the Broadcast Messages function, start and minimize a Broadcast Message window when you begin your NTM session. You will then be able to receive any messages that are sent by other users.

1 Click the Broadcast Message object on the Launch page or use the link in the Navigation Frame.

Result: The Broadcast Message window appears.

2 Enter your message in the text area at the top of the window.

3 Click on Submit to send your message.

Result: Your message will be received by all NTM users who are logged on and who have a Broadcast Message window active.

END OF STEPS

□

Audible Alarms

Overview

Purpose

Audible alarms may be assigned to various trunk group and network element conditions. These alarms are on an exception period basis. You can use this page to:

- Turn alarms on or off (only if Feature 330, "Audible Alarms for the Browser-based GUI" is purchased)
- Choose what item(s) will cause an alarm (specific network element exceptions, trunk group conditions, etc.)
- Choose at what level of exception the alarm will occur
- Choose what alarm sound to associate with the exception
- Choose a sound to indicate the end of period

CAUTION

Different users may assign the same sound to different conditions. It is recommended, however, that users coordinate on the use of audible alarms.

Before you begin

The client system must be capable of running audio basic MIME type or associated plugin before this feature will work properly.

Contents

This section contains the following topics:

Audible Alarms page	7-16
Audible Alarms search result	7-18
Examples	7-19

Audible Alarms page

Purpose

The Audible Alarm page (Figure 4) provides links to the Trunk Group and Network Element Measurements pages to view exceptions for trunk groups and network elements that meet the specified criteria. While in auto-update mode, it sounds an alarm whenever the conditions set by the user are met.

Figure 4 Audible Alarms page

Accessing the page

The Audible Alarm page is available from the Launch page and the Navigation area. After a search is made, you should choose the auto-update mode in order to cause the alarm to sound at the end of each period.

Search criteria

Table 3 describes the search criteria that appear in the Audible Alarm search.

Table 3 Search criteria in the Audible Alarms

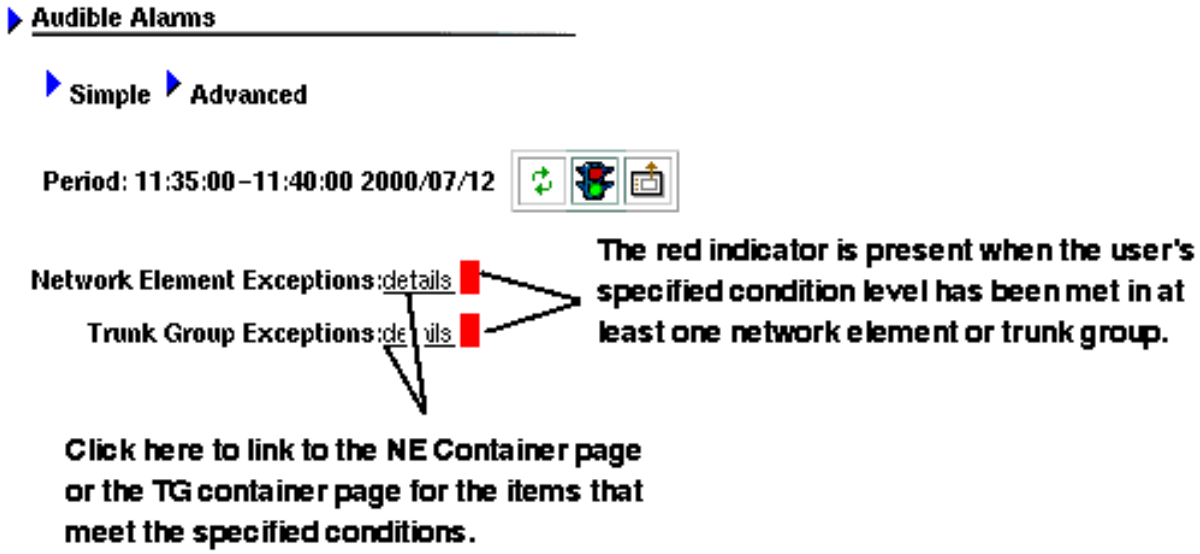
Label	Description
End of Period	On or Off. The default is Off.
EOP (End of Period) Sound URL	Valid files are in the default directory.The default is “eopsound.au”. **Important!** Other extensions like .wav can also be used instead of .au files for labels ending in URL. If you specify a sound URL, it will override the sound file in the default directory (specified using the drop-down menu).
Network Element Exception	On or Off. The default is On.
Network Element	Network element name. You can choose to specify the Area, Rank and Set. Valid values include all internal network elements.
NE Data Restriction	After specifying the switch type, you can use the 2 pop-up lists to restrict conditions which will cause the alarm to sound.
NE Threshold Level	0–10. The default is 6.
NE Sound URL	Valid files are in the default directory. The default is “nesound.au”. (Other extensions like wav can also be used.)
Trunk Group Exception	On or Off. The default is On.
Near End	Near end network element. You can choose to specify the Area, Rank and Set. Valid values include all internal network elements.
Far End	Far end network element. You can choose to specify the Area, Rank and Set. Valid values include all network elements, both internal and external.
Suffix	Trunk group suffix.
TG Set	Trunk group set. Valid values include all trunk group set names.
TG Data Restriction	You can use the 2 pop-up lists to restrict conditions which will cause the alarm to sound.
TG Threshold Level	0–10. The default is 6.
TG Sound URL	Valid files are in the default directory. The default is “tgsound.au”. (Other extensions like wav can also be used.)
User@Host	This displays the current user ID and host information.

Audible Alarms search result

Overview

When the user's specified condition level has been met, the alarm will sound and the network element or trunk group exceptions will be indicated in red. You can click on one of the links to check all the offices that meet the specified conditions from the Network Elements container page and the Trunk Groups container page.

Figure 5 Audible Alarms search result



Examples

Example 1

You may use the Audible Alarms function to alert you to the occurrence of extremely specific network conditions, as well as conditions that occur on a regular basis. (The End-of-Period alarm will sound at the end of every data collection period.)

For example, you may specify a particular trunk group in terms of near end, far end, and suffix in the Trunk Group Exception portion of the page. If you then set the Data Restriction fields for this trunk group so that %OCC >= 80 and %OASR <= 40, you will be alerted whenever this condition occurs for the specified trunk group.

Example 2

If you specify some condition you are interested in for a network element or trunk group and set Threshold Level to 0, you will be alerted to the occurrence of that condition even if it is not an exception according to the thresholds you have established for that trunk group or network element in the record base.

For example, you may specify a certain network element and set TOTLD >= 10000, %TAND >= 50, and NE Threshold Level = 0. When this condition occurs at the network element of interest you will be alerted even if this condition does not trigger an exception.

Exception Status and Marked Assignments

Overview

Purpose

This section describes a combination of Feature 316, "Marked Alarms for the Browser-based GUI" and the Exception Status GUI feature, both of which share common pages. The following section displays examples for a customer who has purchased the marked alarm feature.

- With Feature 316, "Marked Alarms for the Browser-based GUI" the user can apply a mark/flag to a trunk groups or network elements.
- With the GUI feature Inhibiting Exception processing, the user can change the status to restrict data retrieval on offices or trunk groups.
- Existing flags/status indicators can be searched for using the search function of this feature.
- Marks are also maintained across links with Feature 379, "Marked Alarm Persistence on BDR" and can be restored from the BDR machine.

Removing a mark/inhibit status

You may remove or modify a mark or inhibit status via the Exception Status and Mark Assignment page. Use the corresponding Inhibit/Mark Assignment search page to retrieve active and potential candidates. After the switch, or trunk group is retrieved, the data will be presented on a container page, where you can select the item of interest and delete the mark, or change the data collection inhibit/uninhibit status.

When a flag/status expires, the mark status and inhibit status are changed to "no mark" and "not inhibited" respectively. If a mark or an exception is assigned with the value of zero, dayend will automatically remove the mark and automatically decrease the value by one.

Reference: "What happens at dayend" (p. 21)

What happens at dayend

The `dayend` process searches the entire Marked Alarm database. Any mark that has an expiration of no greater than zero will be removed. Exceptions will be marked uninhibited and exception processing will resume.

If a trunk group is deleted (by deleting records in the record base and then running the `create` command), any marks on the trunk group will be deleted at dayend.

Contents

This section contains the following topics:

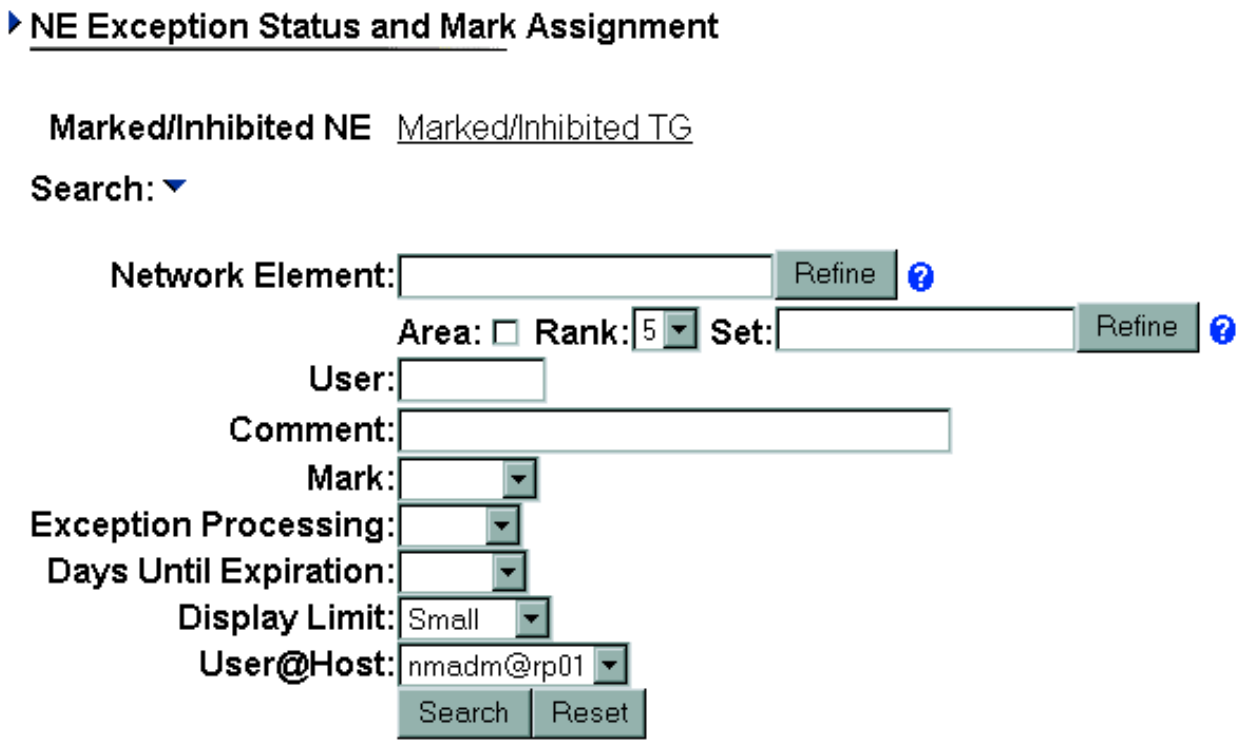
Exception Status and Mark Assignments search page	7-23
Exception Status and Mark Assignments container page	7-25
Exception Status and Mark Assignment details page	7-26

Exception Status and Mark Assignments search page

Purpose

The Exception Status and Mark Assignments search page (Figure 6) will vary slightly depending on which search category is selected; Trunk Group, or Network Element. After a search has been performed, any trunk groups, or offices with the criteria you requested will be displayed in the "Exception Status and Mark Assignments container page" (p. 25).

Figure 6 NE Exception Status and Mark Assignments search page



Accessing the page

The Exception Status and Mark Assignments search pages can be accessed by a link in the navigation area while accessing a search or container page for trunk groups or network elements.

Search criteria

Table 4 describes the search criteria in the search area:

Table 4 Exception Status and Mark Assignments search criteria

Label	Description
Near Element	Near end network element (available for the Trunk Group search page)
Far End	Far end network element (available for the Trunk Group search page)
Suffix	Trunk group suffix (available only when accessed from the Trunk Group container page)
Network Element	Network Element name (available only when accessed from the Network Element container page)
User	Specific user identification who assigned a flag or change exception status
Comment	User input field. There is a 100 character limit for the field.
Mark	Mark (mark status) may be: all (blank by default), ACK, AIP or customer defined marks. It is possible for the user to add their own mark categories by editing the "/nm/web/site/mark_inhibit.pl" file. However, it is recommended that the user work with Alcatel-Lucent field support while editing this file for the first time. **Important!** User-defined mark categories are limited to 6 characters.
Exception Processing	This field may be ALLOW (normal) or INHIBIT. When exception processing is inhibited, data is retained in the NTM database but the exception level for all exceptions is set to 0 and will not appear in searches using the exception level view.
Days Until Expiration	Length of time Mark/Exception Status was set for. Options are: 0–30 or never.

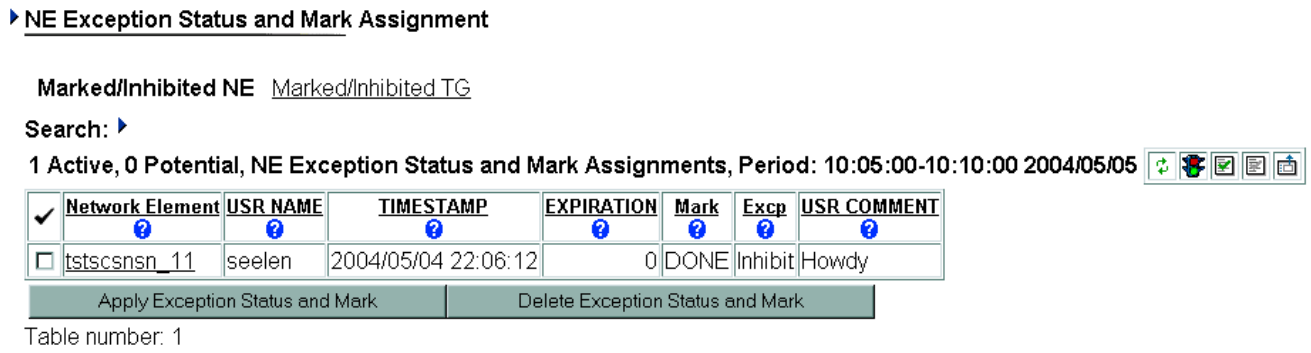
Exception Status and Mark Assignments container page

Purpose

The Exception Status and Mark Assignments container page (Figure 7) trunk groups or offices with the criteria retrieved from the search page. Selecting a checkbox next t oan active or potential candidate will take you to the “Exception Status and Mark Assignment details page” (p. 26)

.

Figure 7 NE Exception Status and Mark Assignment container page



Exception Status and Mark Assignment details page

Purpose

The Exception Status and Mark Assignment pages (Figure 8 and Figure 9) can be used to create a new mark or edit an existing mark. After a mark or status is added or changed, another search is performed automatically to reflect the new status as indicated by the “last changed” field.

After the user inhibits a network element or a trunk group, it will no longer display an exception indicator on any GUI pages. It will return the raw data counts but have an exception level of 0.

Important! Inhibiting a network element may result in the inhibited office not being shown if a network element is being viewed using the exception table view.

Figure 8 TG Exception Status and Mark Assignment Request page

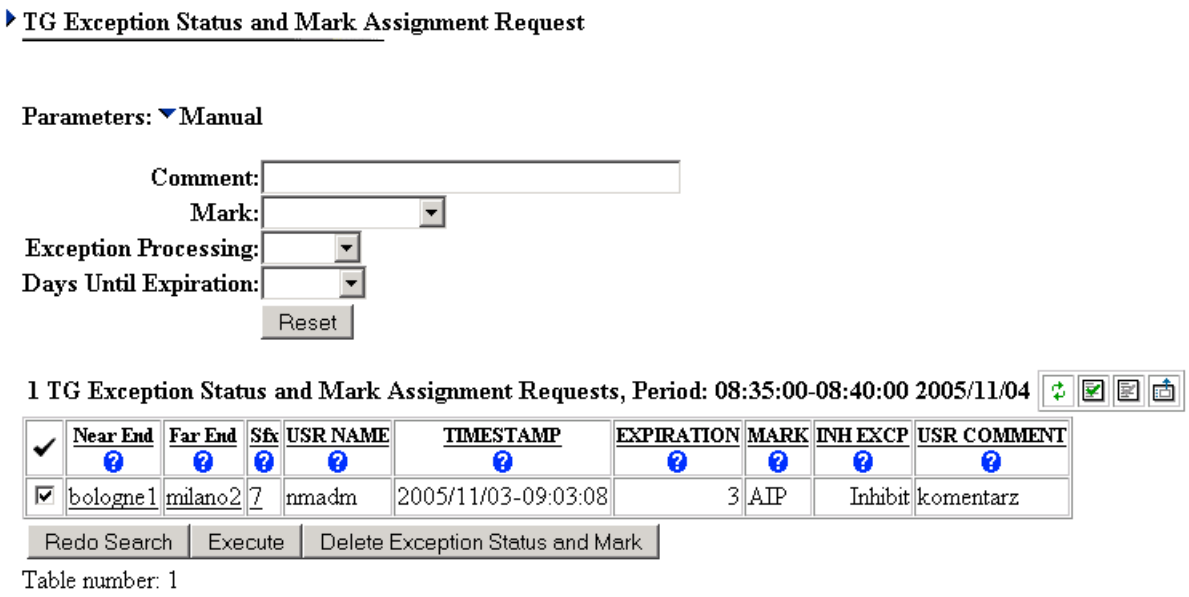
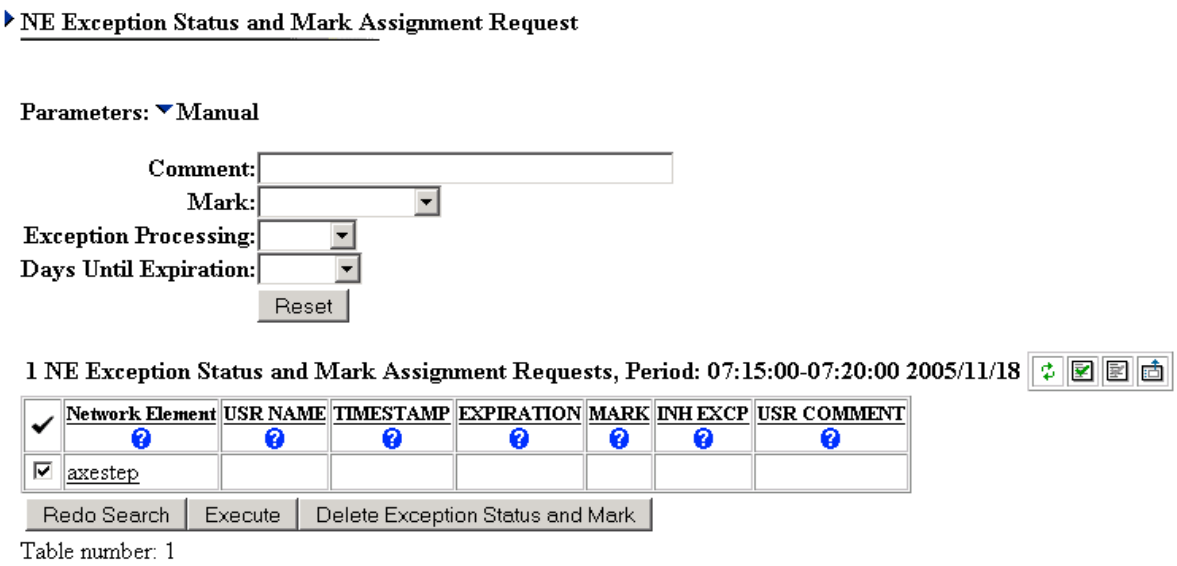


Figure 9 NE Exception Status and Mark Assignment Request page



Page elements

The information displayed on the Exception Status and Mark Assignment pages consists of:

- USR Name— The user name who last submitted a change
- USR Comment — Comment entered when the assignment was entered.
- Mark — The predefined marks are: none (blank by default), ACK or AIP.

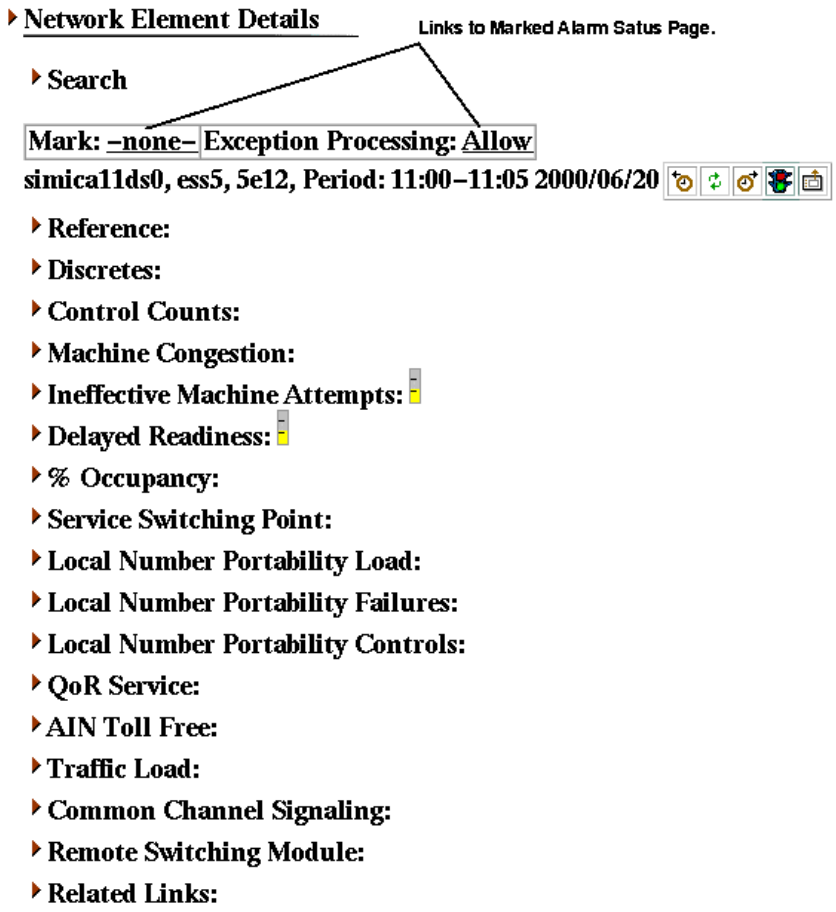
  It is possible for the user to add their own mark categories by editing the "/nm/web/site/mark_inhibit.pl" file. However, it is recommended that the user work with Alcatel-Lucent field support while editing this file for the first time.

  Important! User-defined mark categories are limited to 6 characters
- Exceptions (inhibit status). May be INHIBIT or ALLOW (normal). When exception processing is inhibited, data is retained in the NTM database but the exception level for all exceptions is set to 0.
- Days until Expiration. This may range from 0 to 30 days, or NEVER.
- Last Changed — timestamp of the last submission

Accessing the page

There are links on the Network Element and Trunk Group pages (Figure 10) that take you to the Marked Alarm Assignment/Exception Status details pages (Figure 8 and Figure 9).

Figure 10 Network Element Details page showing links to Mark Assignment Status page



References

"Network Elements data search page" (p. 5); "Overall exception level indicator" (p. 21)

Filters

Overview

Purpose

This section contains information about the different filtering options available with NTM.

Contents

This section contains the following topics:

Filtering alerts	7-30
ISA system alert filters	7-32
ISA system filter messages	7-34
Alert data field contents	7-36

Filtering alerts

Overview

The Network Overview Server (n_o_server process) on the NTM host decides which alerts to send to a client like a map, or alert table, or the ISA system. It makes these decisions based on an alert filter. The alert filter specifies what values a series of alert attributes must have. If the alert attributes of a specific alert have values that all match the allowed values, then that alert is sent to the client. If one or more of the attributes of that specific alert has a value that does not match the allowed values, then it is not sent to the client.

Figure 11 Filter message

```
type          filter
alerttype     :dsc:entdat:tgdat:tgctrl:
suspectdata   :0:
level         :8:9:10:C:0:
finalsonly    :fi:pfi:vfi:
tgset         :tgset2:tgset3:
```

Example 1

The example dsc alert shown in Table 5, “Alerts using the Discrete alert (minimal attributes)” (p. 32) would NOT make it through this filter (Figure 11). Its alert type is valid. The suspectdata, finalsonly, and tgset attributes are not applicable to the dsc alert type, so they are ignored. However, it has a level of 4. Only levels 8, 9, 10, 0, or C are allowed.

Alert Attribute Name	Value Allowed by the Filter	Value of example dsc alert	Does dsc attribute pass filter?
alerttype	dsc, entdat, tgdat, or tgctl	dsc	ok
suspectdata	0	not applicable	ok
level	level 8, 9, 10, 0 or C	4	No match
finalsonly	hu	not applicable	ok
tgset	tgset2 or tgset3	not applicable	ok
nearend	Not specified in filter, so any value is ok	xyz	ok
source	Not specified in filter, so any value is ok	host1	ok
subnet	Determined by software based on the ISA system's permissions on NTM	00001	ok

Example 2

The example tgdat alert shown in Table 6, "Alert using the Trunk Group Data alert (many attributes)" (p. 33) would also NOT make it through this filter (Figure 11). Its alert type is valid. Its level of 8 is valid. Its suspectdata status of 0 is valid. It is a member of the tgset2 trunk group set, which is one of the valid tgset values listed in the filter. However, it is a high usage (hu) trunk group, which does not match the fi, pfi, or vfi value specified for the finalsonly attribute in filter message.

Alert Attribute Name	Value Allowed by the Filter	Value of example dsc alert	Does dsc attribute pass filter?
alerttype	dsc, entdat, tgdat, or tgctl	tgdat	ok
suspectdata	0	0	ok
level	8, 9, 10, 0 or C	8	ok
finalsonly	fi, pfi, or vfi	hu	No Match
tgset	:tgset2:tgset3:	:tgset1:tgset2:	ok
nearend	Not specified in filter, so any value is ok	abc	ok
farend	Not specified in filter, so any value is ok	def	ok
uniqueid	Not specified in filter, so any value is ok	045	ok
source	Not specified in filter, so any value is ok	host1	ok
tglevel	Not specified in filter, so any value is ok	8	ok
exctype	Not specified in filter, so any value is ok	%OHC	ok
tg_datafield1	Not specified in filter, so any value is ok	Ofl=26 0	ok
tg_datafield2	Not specified in filter, so any value is ok	OCCH=14 0	ok
tg_datafield3	Not specified in filter, so any value is ok	ICCH=0 0	ok
tg_datafield4	Not specified in filter, so any value is ok	HT=0.1 4	ok
tg_datafield5	Not specified in filter, so any value is ok	%MB=40 3	ok
tg_datafield6	Not specified in filter, so any value is ok	PC=144 0	ok

ISA system alert filters

Overview

This feature works in conjunction with Feature 318, “Browser-based GUI Dual Host Support”.

An administrator can define which Alerts will be sent from an NTM Host to the Integrated Service Assurance (ISA) system by editing the “/nm/web/site/alertFilter_defs.pl” file. However, before the details of editing the file are discussed, an overview of the “alert” and “alert filter” concepts may be useful.

Tables

The NTM alert is similar to an NTM exception, except that it has additional data besides level and value associated with it. Some alerts have a small number of attributes (Table 5) while others have many (Table 6).

Table 5 Alerts using the Discrete alert (minimal attributes)

Alert Attribute Name	Alert Attribute Value (Example)	Description
alerttype	dsc	Alert Type
nearend	xyz	Office
level	4	The most severe discrete on office xyz
source	host1	The NTM host that generated the alert.
subnet	00001	The NTM subnetwork permissions a user must have to see this alert.

Table 6 Alert using the Trunk Group Data alert (many attributes)

Alert Attribute Name	Alert Attribute Value (Example)	Description
alerttype	tgdat	Alert Type
nearEnd	abc	Office
farEnd	def	Far End office
uniqueid	045	Trunk Group ID
exctype	%OHC	MAX_EXC_TYPE
level	8	The highest level exception on the office xyz (MAX_EXC_LVL)
tglevel	8	MAX_EXC_LVL
value	75	MAX_EXC_VAL
tg_datafield1	Ofl=26 0	Definable value
tg_datafield2	OCCH=14 0	Definable value
tg_datafield3	ICCH=0 0	Definable value
tg_datafield4	HT=0.1 4	Definable value
tg_datafield5	%MB=40 3	Definable value
tg_datafield6	PC=144 0	Definable value
tgset	:tgset1:tgset2:	Trunk Group Set
finalsonly	hu	Type of Trunk Group
suspectdata	0	Suspect Data level
source	host1	The NTM host that generated the alert.
subnet	00001	The NTM subnetwork permissions a user must have to see this alert.

ISA system filter messages

Purpose

The filter message applied to alerts sent to the ISA system can be customized by logging on as root and editing the file "/nm/web/site/alertFilter_defs.pl" on the NTM host.

```
$filterMessage {ISA} {fill-in alert attribute name}=:fill-in alert attribute name:
```

Important! Although knowing the Perl language is not necessary to customize this variable, some administrators may find it useful to know that filterMessage is a Perl hash variable. Perl syntax requires that the "$", "{", and "}" characters appear where they do in filterMessage.

Alert Attribute	Description
alerttype	Allows selection of alerts based on the type of alert
level	Allows selection of alerts based on the exception level of the alert. **Important!** In order for alert clears to be passed to ISA, always include "0" among the allowed levels
tglevel	Allows selection of alerts based on the exception level of alerts related to trunk groups, without affecting alerts related to network elements. **Important!** In order for alert clears to be passed to ISA, always include "0" among the allowed levels
tgset	Allows selection of alerts based on trunk group set membership
finalsonly	Allows selection of alerts based on trunk group usage type
suspectdata	Allows selection of alerts based on whether the data in the alert is suspect or not.

Alert attributes NOT used in filter messages

The following alert attributes are either used internally by the network overview server or are used primarily for Alert Table formatting purposes and should NOT be used in filterMessage:

- subnet
- oexl
- tgdat_oexl
- oexl1…oexl6
- tg_datafield1 … tg_datafield6
- vtg_datafield1 … vtg_datafield6
- linkdat_datafield … linkdat_datafield6

Syntax

Syntax for “fill-in alert attribute” value:

The alert attribute value clause must be preceded and ended with a colon (“:”). In between those two colons, one or more alert attribute values may be specified. Individual alert attribute values are separated by colons. An alert attribute value may be a regular expression.

Examples

Example 1: Default Filter Message for ISA:

```
filterMessage{ISA}{alerttype}=':dsc:entdat:tgdat:tgctrl:';
```

Example 2: Filter Message specifying more alert attributes:

```
filterMessage{ISA}{alerttype}=':dsc:entdat:tgdat:tgctrl:';
   filterMessage{ISA}{level}=':8:9:10:C:0:';
   filterMessage{ISA}{tgset}=:tgset2:tgset3:';
```

Example 3: Filter Message showing use of a regular expression:

```
filterMessage{ISA}{alerttype}=':dsc:entdat:tgdat:tgctrl:htrdat:ttodat:cgctrl:';
   filterMessage{ISA}{level}=':4:5:6:8:9:10:C:0:';
   filterMessage{ISA}{tglevel}=':9:10:0:';
   filterMessage{ISA}{tgset}=':^abc.*|^def.*:tgset2:';
   filterMessage{ISA}{finalsonly}=':.*fi.*:';
```

Explanation of Example 3

The tgset definition specifies that any tgset alert attribute starting with “abc” or any trunk group set starting with “def” or “tgset2” will pass the filter.

The finalsonly definition specifies that any finalsonly alert attribute contain the letters “fi” will pass the filter.

The use of both the level and tglevel attributes in filterMessage creates a filter that is more restrictive for trunk group related alerts than it is for machine related alerts. For example, a tgdat alert with a level and tglevel of 6 will not pass the filter. However, an entdat alert with a level of 6 will pass the filter. The tglevel attribute is not defined for the entdat alert type, so the tglevel filter definition is ignored for entdat and other machine-related alerts.

A complete listing of available alert attributes, which alert types they are applicable to, and how the value for the attribute is derived, is given in Table 7, “Alert Attribute Reference Table” (p. 37).

□

Alert data field contents

Overview

After the filter message has been changed, you can log in as "root" and view the "/nm/web/tool/field_support/testalertfilter.pl" file to see which alerts will be sent to ISA.

Data column

A "Data" column appears on the ISA alert table. The contents of this column for NTM alerts can be customized by editing the file /nm/web/site/alertFilter_defs.pl on the NTM host.

```
$formatMessage{ISA}{dataFieldAttributes}=:fill-in alert attribute(s):
```

Alert attributes clause

The alert attribute(s) clause must be preceded and ended with a colon (":"). In between those two colons, one or more alert attributes may be specified. Individual alert attributes are separated by colons. Refer to the Alert Attribute Reference Table to determine which attributes are available for which alert types.

This is an example of the default datafield contents for ISA:

```
$formatMessage{ISA}{dataFieldAttributes}=':numctrls:oexl:oexl2:oexl3:oexl4:oexl5:oex
   l6:tg_datafield1:tg_datafield2:tg_datafield3:tg_datafield4:tgdatafield5:tg_datafi
   eld6:';
```

DSC alert

If the alert server is processing a dsc alert, the only attribute from the above list that applies is oexl. Only the oexl attribute will be passed in the Data field for the dsc alert.

ENTDAT alert

If the alert server is processing an entdat alert, oexl through oexl6 attributes apply. The oexl though oexl6 attributes will be passed in the Data field for the entdat alert.

Table

Table 7 provides a complete listing of available alert attributes, which alert types they are applicable to, and how the value for the attribute is derived.

Default values supplied with NTM are marked with an asterisk (*). Values may be different if they were customized for your site.

Table 7 Alert Attribute Reference Table (Sheet 1 of 12)

Alert Type	Data Table	Alert Attributes	Attribute Value
atmmg4k	Multi-media Gateway 4000 (ATMMG4KDAT)	alerttype	"atmmg4k"
		level	MAX_EXC_LVL
		networktype	"switch"
		subnet	NTM subnetwork permissions
		suspectdata	FILTER_TAGS
		oexl	MAX_EXC_TYPE+MAX_EXC_VAL
		nearend	OFFICE
		uniqueid	ATM_KEY_INFO
		ictotal	ATM_ICTOTAL
		iclp0to	ATM_ICLP0TO
		iclp1to	ATM_ICLP1TO
		icnc	ATM_ICNC
		icclp0nc	ATM_ICCLP0NC
		icclp1nc	ATM_ICCLP1NC
		icdisc	ATM_ICDISC
		icclp0dc	ATM_ICCLP0DC
		icclp1dc	ATM_ICCLP1DC
		itagged	ATM_ITAGGED
		ogtotal	ATM_OGTOTAL
		oclp0to	ATM_OCLP0TO
		oclp1to	ATM_OCLP1TO
		p_disc_cells	%ATM_DISC_CELLS
		p_nc_cells	%ATM_NC_CELLS
		p_tag_cells	%ATM_TAG_CELLS
		p_disc_clp0	%ATM_DISC_CLP0
		p_disc_clp1	%ATM_DISC_CLP1
		p_nc_clp0	%ATM_NC_CLP0
		p_nc_clp1	%ATM_NC_CLP1
		p_in_clp0	%ATM_IN_CLP0
		p_in_clp1	%ATM_IN_CLP1
		p_out_clp0	%ATM_OUT_CLP0
		p_out_clp1	%ATM_OUT_CLP1

Table 7 Alert Attribute Reference Table (Sheet 2 of 12)

Alert Type	Data Table	Alert Attributes	Attribute Value
atmmg4ka1	Multi-media Gateway 4000 - counts per virtual channel A1 (ATMMG4KDAT)	alerttype level networktype subnet suspectdata oexl nearend uniqueid ictotal ogtotal herrcel latecel msincel lostcel p_herrcel p_latecel p_msincel p_lostcel slips oosync	“atmmg4ka1 ”MAX_EXC_LVL “switch” NTM subnetwork permissions FILTER_TAGS MAX_EXC_TYPE+MAX_EXC_VAL OFFICE ATM_KEY_INFO ATMA1_ICTOTAL ATMA1_OGTOTAL ATMA1_HERRCEL ATMA1_LATECEL ATMA1_MSINCEL ATMA1_LOSTCEL %ATMA1_HERRCEL %ATMA1_LATECEL %ATMA1_MSINCEL %ATMA1_LOSTCEL ATMA1_SLIPS ATMA1_OOSYNC
atmmg4ka5	Multi-media Gateway 4000 - counts per virtual channel A5 (ATMMG4KDAT)	alerttype level networktype subnet suspectdata oexl nearend uniqueid lenviol crc32err oversdu	“atmmg4ka5” MAX_EXC_LVL “switch” NTM subnetwork permissions FILTER_TAGS MAX_EXC_TYPE+MAX_EXC_VAL OFFICE ATM_KEY_INFO ATMA5_LENVIOL ATMA5_CRC32ERR ATMA5_OVERSDU

Table 7 Alert Attribute Reference Table (Sheet 3 of 12)

Alert Type	Data Table	Alert Attributes	Attribute Value
atmmg4kvc	Multi-media Gateway 4000 - Counts per permanent virtual channel (ATMMG4KDAT)	alerttype	"atmmg4kvc"
		level	MAX_EXC_LVL
		networktype	"switch"
		subnet	NTM subnetwork permissions
		suspectdata	FILTER_TAGS
		oexl	MAX_EXC_TYPE+MAX_EXC_VAL
		nearend	OFFICE
		uniqueid	ATM_KEY_INFO
		ictotal	ATMVC_ICTOTAL
		iclp0to	ATMVC_ICLP0TO
		iclp1to	ATMVC_ICLP1TO
		icnc	ATMVC_ICNC
		icclp0nc	ATMVC_ICCLP0NC
		icclp1nc	ATMVC_ICCLP1NC
		icdisc	ATMVC_ICDISC
		icclp0dc	ATMVC_ICCLP0DC
		icclp1dc	ATMVC_ICCLP1DC
		itagged	ATMVC_ITAGGED
		ogtotal	ATMVC_OGTOTAL
		oclp0to	ATMVC_OCLP0TO
		oclp1to	ATMVC_OCLP1TO
		p_disc_cells	%ATMVC_DISC_CELLS
		p_nc_cells	%ATMVC_NC_CELLS
		p_tag_cells	%ATMVC_TAG_CELLS
		p_disc_clp0	%ATMVC_DISC_CLP0
		p_disc_clp1	%ATMVC_DISC_CLP1
		p_nc_clp0	%ATMVC_NC_CLP0
		p_nc_clp1	%ATMVC_NC_CLP1
		p_in_clp0	%ATMVC_IN_CLP0
		p_in_clp1	%ATMVC_IN_CLP1
		p_out_clp0	%ATMVC_OUT_CLP0
		p_out_clp1	%ATMVC_OUT_CLP1

Table 7 Alert Attribute Reference Table (Sheet 4 of 12)

Alert Type	Data Table	Alert Attributes	Attribute Value
atmpp	PP15k counts (ATMPPDAT)	alerttype level networktype subnet suspectdata oexl nearend farend uniqueid inlinkocc outlinkocc atm_aht p_outcells_dis p_incells_dis p_inerrors p_outerrors sysutil linkcap sigchanstat incells outcells outcells_dis incells_dis outcbrclp0_1dis outrtvbrclp0_1dis outnrtvbrclp0_1dis outubrclp0_1dis insetup infail outsetup outfail	“atmpp” MAX_EXC_LVL “switch” NTM subnetwork permissions FILTER_TAGS MAX_EXC_TYPE+MAX_EXC_VAL OFFICE LINKED ATM_LINKID INUTIL OUTUTIL AHT %OUTDISC %INDISC %INERR %OUTERR SYSUTIL LINKCAP SIGSTAT INCELLS OUTCELLS OUTCELLS_DIS INCELLS_DIS OUTCBRCLP0_1DIS OUTRTVBRCLP0_1DIS OUTNRTVBRCLP0_1DIS OUTUBRCLP0_1DIS INSETUP IFAIL OUTSETUP OFAIL
cgctrl	Trunk Group Control (CGCTL)	alerttype level numctrls subnet networktype oexl nearend	“cgctrl” “0” or “C” # of active controls on that switch NTM subnetwork permissions “switch” “0” or “C” OFFICE

Table 7 Alert Attribute Reference Table (Sheet 5 of 12)

Alert Type	Data Table	Alert Attributes	Attribute Value
dsc	Machine Discrete (DISCRETE)	alerttype level networktype subnet oexl nearend	“dsc” MAX_DSC_LVL “switch” NTM subnetwork permissions MAX_DSC_LVL OFFICE
entdat	Machine Data (ENTDAT)	alerttype nearend level value exctype suspectdata networktype subnet oexl oexl1 oexl2 oexl3 oexl4 oexl5	“entdat” OFFICE MAX_EXC_LVL MAX_EXC_VAL MAX_EXC_TYPE FILTER_TAGS “switch” NTM subnetwork permissions MAX_EXC_TYPE + MAX_EXC_LVL MAX1_EXC_TYPE + MAX1_EXC_VAL MAX2_EXC_TYPE + MAX2_EXC_VAL MAX3_EXC_TYPE + MAX3_EXC_VAL MAX4_EXC_TYPE + MAX4_EXC_VAL MAX5_EXC_TYPE + MAX5_EXC_VAL
htrdat	Hard To Reach Exception (HTRDAT)	alerttype nearend level value exctype networktype subnet oexl	“htrdat” OFFICE MAX_EXC_LVL MAX_EXC_VAL MAX_EXC_TYPE “switch” NTM subnetwork permissions MAX_EXC_TYPE + MAX_EXC_VAL

Table 7 Alert Attribute Reference Table (Sheet 6 of 12)

Alert Type	Data Table	Alert Attributes	Attribute Value
iwbmdat	Inter-working bridge measurements (????)	alerttype level networktype subnet suspectdata oexl nearend uniqueid	“iwbmdat” MAX_EXC_LVL “switch” NTM subnetwork permissions FILTER_TAGS MAX_EXC_TYPE+MAX_EXC_VAL OFFICE IWBM_KEY_INFO
linkdat5	5 Minute Signaling Link Data (LINKDAT)	alerttype level tglevel linkdats_datafield1 linkdats_datafield2 linkdats_datafield3 linkdats_datafield4 linkdats_datafield5 linkdats_datafield6 suspectdata networktype oexl tgdat_oexl exctype value subnet nearend farend uniqueid	“linkdat5” MAX_EXC_VAL MAX_EXC_LVL SL_MSUXMIT SL_MSURCV SL_OCTXMIT SL_OCTRCV Not defined Not defined FILTER_TAGS “switch” MAX_EXC_TYPE + MAX_EXC_VAL MAX_EXC_TYPE + MAX_EXC_VAL MAX_EXC_TYPE MAX_EXC_VAL NTM subnetwork permissions OFFICE TO_OFFICE SLS_ID + SLS_MEMBER
ofc_event	Machine Status (EVENT) where EVENT = data_missing, exc_late_ofc, exc_dcolfail, no_data_event, exc_manoos, exc_more	alerttype nearend level exctype data_concentrator oexl networktype subnet	“ofc_event” OFFICE MAX_ALRM_LVL EVENT name of data concentrator or directly-connected switch type EVENT+EVENT_LVL “switch” NTM subnetwork permissions

Table 7 Alert Attribute Reference Table (Sheet 7 of 12)

Alert Type	Data Table	Alert Attributes	Attribute Value
pp15k_card	PP15k Card data (IPPPDAT)	alerttype level networktype subnet suspectdata oexl nearend uniqueid	“pp15k_card” MAX_EXC_LVL “switch” NTM subnetwork permissions FILTER_TAGS MAX_EXC_TYPE+MAX_EXC_VAL OFFICE PACKET_LINKID
pp15k_fabric	PP15k fabric data (IPPPDAT)	alerttype level networktype subnet suspectdata oexl nearend uniqueid	“pp15k_fabric” MAX_EXC_LVL “switch” NTM subnetwork permissions FILTER_TAGS MAX_EXC_TYPE+MAX_EXC_VAL OFFICE PACKET_LINKID
pp15k_ip	PP15k physical interface data (IPPPDAT)	alerttype level networktype subnet suspectdata oexl nearend uniqueid	“pp15k_ip” MAX_EXC_LVL “switch” NTM subnetwork permissions FILTER_TAGS MAX_EXC_TYPE+MAX_EXC_VAL OFFICE PACKET_LINKID
pp15k_pvg	PP15k packet voice gateway (IPPPDAT)	alerttype level networktype subnet suspectdata oexl nearend uniqueid	“pp15k_pvg” MAX_EXC_LVL “switch” NTM subnetwork permissions FILTER_TAGS MAX_EXC_TYPE+MAX_EXC_VAL OFFICE PACKET_LINKID
pp15k_shelf	PP15k shelf data (IPPPDAT)	alerttype level networktype subnet suspectdata oexl nearend uniqueid	“pp15k_shelf” MAX_EXC_LVL “switch” NTM subnetwork permissions FILTER_TAGS MAX_EXC_TYPE+MAX_EXC_VAL OFFICE PACKET_LINKID

Table 7 Alert Attribute Reference Table (Sheet 8 of 12)

Alert Type	Data Table	Alert Attributes	Attribute Value
tgctrl	Trunk Group Control (TGCTL) Where virtual = 0	alerttype level numctrls finalsonly subnet networktype oexl tgset nearend farend uniqueid	“tgctrl” “0” or “C” # of active controls on that trunk TG_SRV NTM subnetwork permissions “switch” “0” or “C” TG_SET OFFICE TO_OFFICE SUFFIX
tgdat	Trunk Group Exception (TGDAT) Where virtual = 0	alerttype level tglevel tg_datafield1 tg_datafield2 tg_datafield3 tg_datafield4 tg_datafield5 tg_datafield6 suspectdata tgset finalsonly networktype oexl tgdat_oexl exctype value subnet nearend farend uniqueid	“tgdat” MAX_EXC_LVL MAX_EXC_LVL OFL* OCCH* ICCH* HT* %MB* PC* FILTER_TAGS TG_SET TG_SRV “switch” MAX_EXC_TYPE + MAX_EXC_VAL MAX_EXC_TYPE + MAX_EXC_VAL MAX_EXC_TYPE MAX_EXC_VAL NTM subnetwork permissions OFFICE TO_OFFICE SUFFIX

Table 7 Alert Attribute Reference Table (Sheet 9 of 12)

Alert Type	Data Table	Alert Attributes	Attribute Value
ttodat	Transmitter Timeout Exception (HTRDAT)	alerttype nearend level value exctype networktype subnet oexl	“ttodat” OFFICE MAX_EXC_LVL MAX_EXC_VAL MAX_EXC_TYPE “switch” NTM subnetwork permissions MAX_EXC_TYPE + MAX_EXC_VAL
v_tgctrl	Virtual Trunk Group Control (TGCTL) Where virtual = 1	alerttype level numctrls finalsonly subnet networktype oexl tgset nearend farend uniqueid	“v_tgctrl” “0” or “C” # of active controls on that trunk TG_SRV NTM subnetwork permissions “switch” “0” or “C” TG_SET OFFICE TO_OFFICE SUFFIX

Table 7 Alert Attribute Reference Table (Sheet 10 of 12)

Alert Type	Data Table	Alert Attributes	Attribute Value
v_tgdat	Virtual Trunk Group Exception (TGDAT) Where virtual = 1	alerttype level tglevel vtg_datafield1 vtg_datafield2 vtg_datafield3 vtg_datafield4 vtg_datafield5 vtg_datafield6 suspectdata tgset finalsonly networktype oexl tgdat_oexl exctype value subnet nearend farend uniqueid	"v_tgdat" MAX_EXC_LVL MAX_EXC_LVL OFL* OCCH* ICCH* HT* %MB* PC* FILTER_TAGS TG_SET TG_SRV "switch" MAX_EXC_TYPE + MAX_EXC_VAL MAX_EXC_TYPE + MAX_EXC_VAL MAX_EXC_TYPE MAX_EXC_VAL NTM subnetwork permissions OFFICE TO_OFFICE SUFFIX
ls_dcc_failoos	Data Collector Failed Out Of Service (EVENT) where DC_STATUS=11	alerttype nearend level exctype data_concentrator oexl networktype subnet	"ls_miss" OFFICE MAX_ALRM_LVL EVENT name of data concentrator or directly-connected switch type EVENT+MAX_ALRM_LVL "lss" NTM subnetwork permissions
ls_dcc_manoos	Data Collector Failed Out Of Service (EVENT) where DC_STATUS=10	alerttype nearend level exctype data_concentrator oexl networktype subnet	"ls_miss" OFFICE MAX_ALRM_LVL EVENT name of data concentrator or directly-connected switch type EVENT+MAX_ALRM_LVL "lss" NTM subnetwork permissions

Table 7 Alert Attribute Reference Table (Sheet 11 of 12)

Alert Type	Data Table	Alert Attributes	Attribute Value
ls_failoos	Office Failed Out Of Service (EVENT) where EVENT= exc_dcolfail	alerttype nearend level exctype data_concentrator oexl networktype subnet	“ls_miss” OFFICE EVENT_LVL EVENT name of data concentrator or directly-connected switch type EVENT+ EVENT_LVL “lss” NTM subnetwork permissions
ls_late	Late Data (EVENT) where EVENT= exc_late_ofc	alerttype nearend level exctype data_concentrator oexl networktype subnet	“ls_miss” OFFICE EVENT_LVL EVENT name of data concentrator or directly-connected switch type EVENT+ EVENT_LVL “lss” NTM subnetwork permissions
ls_manoos	Office Manually Out Of Service (EVENT) where EVENT = exc_manoos	alerttype nearend level exctype data_concentrator oexl networktype subnet	“ls_miss” OFFICE EVENT_LVL EVENT name of data concentrator or directly-connected switch type EVENT+ EVENT_LVL “lss” NTM subnetwork permissions
ls_miss	Data Missing (EVENT) where EVENT = no_data_event, data_missing	alerttype nearend level exctype data_concentrator oexl networktype subnet	“ls_miss” OFFICE EVENT_LVL EVENT name of data concentrator or directly-connected switch type EVENT+ EVENT_LVL “lss” NTM subnetwork permissions

Table 7 Alert Attribute Reference Table (Sheet 12 of 12)

Alert Type	Data Table	Alert Attributes	Attribute Value
ls_sync	Time Sync Office (EVENT) where SYNC_OFC=sync	alerttype nearend level exctype data_concentrator oexl networktype subnet	“ls_miss” OFFICE EVENT_LVL2 EVENT name of data concentrator or directly-connected switch type EVENT+EVENT_LVL2 “lss” NTM subnetwork permissions
ls_timediff	Time Difference (EVENT) where EVENT=DCSTAT and TIME_DIFF > 5 or TIME_DIFF < -5	alerttype nearend level exctype data_concentrator oexl networktype subnet	“ls_timediff” OFFICE EVENT_LVL EVENT name of data concentrator or directly-connected switch type EVENT+ EVENT_LVL “lss” NTM subnetwork permissions

Additional functions of the NTM GUI

Overview

Purpose

This section provides information about items not directly linked from the NTM Launch page.

Contents

This section contains the following topics:

Customized Command page	7-50
GUI Who page	7-51

Customized Command page

Purpose

Customized Command provides a GUI interface to NTM commands previously only available through a command line interface. These commands are not part of the standard NTM GUI functionality. Some examples include:

- Report writer commands
- Linux shell scripts
- Performance reports for Linux or NTM
- Other user-defined commands

Accessing commands

When a command is built into the Customized Command page, it appears as a menu selection. When a command is selected from the menu, users may enter parameter values for the command through GUI elements like drop down menus, radio buttons, picklists, etc.

Adding commands

Commands may be added to the Customized Command page through Alcatel-Lucent consulting services. Training can be provided by Alcatel-Lucent to enable sites to build their own interfaces to custom commands.

GUI Who page

Purpose

The GUI Who page provides a method of querying the system to find who is currently or was recently using the GUI interface and what pages each user has recently accessed.

This feature is accessible directly from the Launch page. The user can select from a specified range of time to find who is or recently was accessing the GUI. This typically doesn't work across `dayend` periods if scripts remove certain user log entries.

The timestamp shown at the top of the screen reflects the most recent periodic data. Using the Auto-update mode, administrators can have an ongoing view of those accessing the NTM GUI.

8 Link Status

Overview

Purpose

This chapter provides information about the Link Status Table, Link Status Schematic, and Periodic Data Browser components of the NTM GUI.

Contents

This chapter contains the following topics:

Link Status Table	8-3
Link Status Schematic	8-7
Changing the Link Status Schematic time difference	8-13
STM Periodic Status	8-15
Periodic Data Browser	8-23
Periodic Data Browser Details page	8-29

Link Status Table

Overview

Purpose

The Link Status Table object provides GUI access to display the data collection status of NTM office(s).

Reference: linkstat command (9-9) in the *Input Commands Guide*

Contents

This section contains the following topics:

Link Status Table search page	8-4
Link Status Table container page	8-5

Link Status Table search page

Purpose

The Link Status Table search page allows the user to retrieve link status information.

Search criteria

Table 1 describes the search criteria that appear in the Search area for Link Status.

Table 1 Search criteria — Link Status Table

Label	Description
Network Element	Network element name. Valid values include all elements that are valid for the `linkstat` command.
Network Element Set	Network element set names separated by comma. Up to 20 sets and 180 characters are allowed in this field. Valid values include all defined office sets. If the set field is populated, then the system disregards the network element field and returns all members of the set as defined in the" /musr/rb/rspte/rspte" file.
Type	Network element type. Only those types that are valid for the customer's system configuration are shown. If only one choice is valid, then this field object is not displayed.
Connection Status	These options allows the user to select the network elements by their connection status to NTM.
User@Host	This displays current user ID and host information.

Link Status Table container page

Purpose

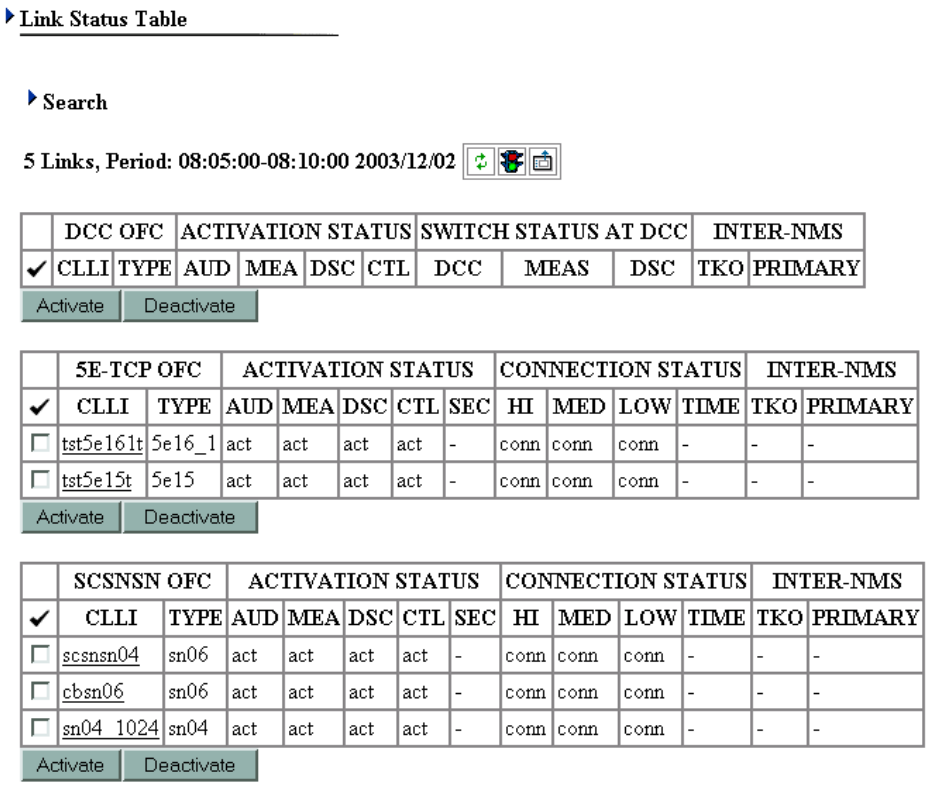
The Link Status Table container page (Figure 1) displays the results of a Link Status Table search in tabular format.

The Link Status Table container page supports both manual and auto update.

The fields in the output table for the Link Status Table match the fields that are shown as output from the `linkstat` command.

You can activate or deactivate an office by selecting the checkbox at the beginning of each line. The system will respond with either a green check if the action was successful or a system message will appear in the Status column indicating the action was unsuccessful.

Figure 1 Link Status Table container page



Link Status Table

Search

5 Links, Period: 08:05:00-08:10:00 2003/12/02

	DCC OFC		ACTIVATION STATUS				SWITCH STATUS AT DCC			INTER-NMS	
✓	CLLI	TYPE	AUD	MEA	DSC	CTL	DCC	MEAS	DSC	TKO	PRIMARY

Activate Deactivate

	5E-TCP OFC		ACTIVATION STATUS					CONNECTION STATUS				INTER-NMS	
✓	CLLI	TYPE	AUD	MEA	DSC	CTL	SEC	HI	MED	LOW	TIME	TKO	PRIMARY
☐	tst5e161t	5e16_1	act	act	act	act	-	conn	conn	conn	-	-	-
☐	tst5e15t	5e15	act	act	act	act	-	conn	conn	conn	-	-	-

Activate Deactivate

	SCSNSN OFC		ACTIVATION STATUS					CONNECTION STATUS				INTER-NMS	
✓	CLLI	TYPE	AUD	MEA	DSC	CTL	SEC	HI	MED	LOW	TIME	TKO	PRIMARY
☐	scsnsn04	sn06	act	act	act	act	-	conn	conn	conn	-	-	-
☐	cbsn06	sn06	act	act	act	act	-	conn	conn	conn	-	-	-
☐	sn04_1024	sn04	act	act	act	act	-	conn	conn	conn	-	-	-

Activate Deactivate

Link Status Schematic

Overview

Purpose

The Link Status Schematic (Figure 2) provides a network view of the communication status between the NTM host and directly connected network elements, data collection concentrators (DCC) and backup hosts if you have Feature 8, “Disaster Recovery (Duplex)”and Feature 40, “Enhanced Disaster Recovery”.

Contents

This chapter contains the following topics:

Link Status Schematic search page	8-8
Link Status Schematic container page	8-9

Link Status Schematic search page

Purpose

After selecting the Link Status Schematic icon from the NTM launch page (Figure 5). A search page appears. You can choose to view a subset of network elements by entering the name of an entity set, as defined in the Sets File, or a specific DCC. By leaving the input field blank and selecting search, the following will be displayed:

- DCC connected network elements will be shown grouped by DCC
- Directly connected network elements will be shown by network element type
- 4ESS offices connected to the NTM

Reference: "Sets File" (p. 74) in the *Record Base Administration Guide*

Link Status Schematic container page

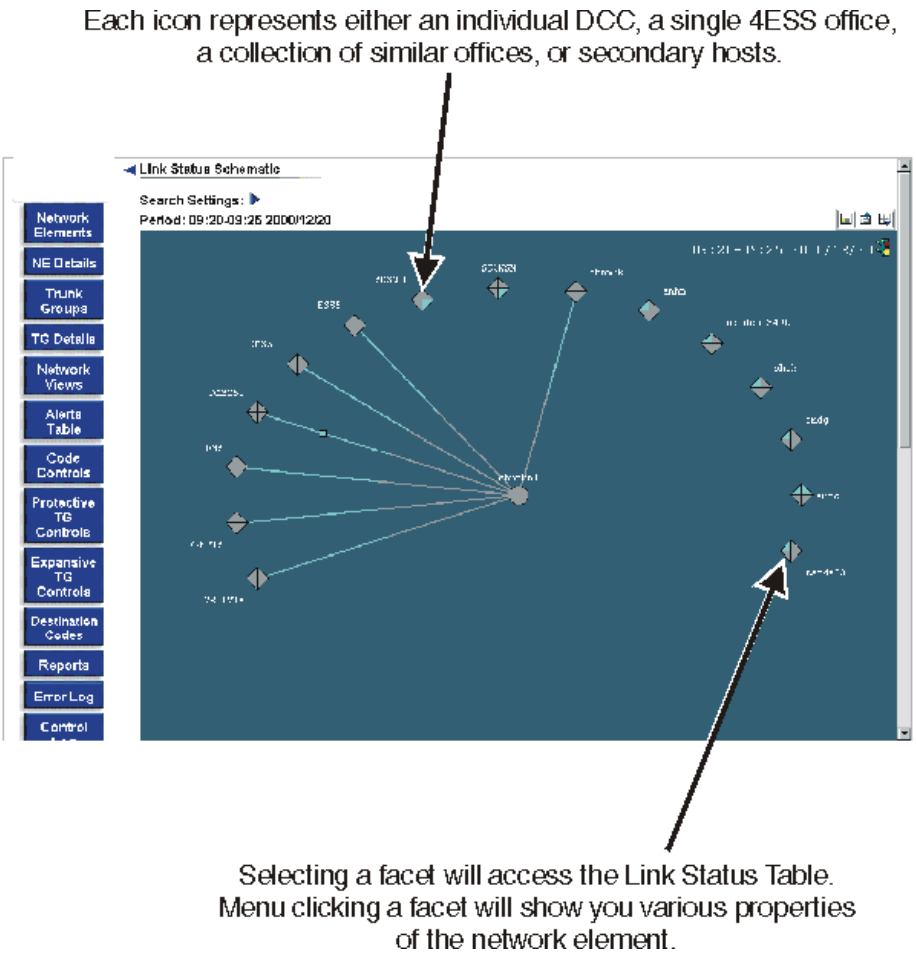
Purpose

The display presents the NTM host in the center of the display surrounded by nodes that represent the various types of network elements. The labels are either nicknames or CLLIs as defined in the RSPTE File. The Link Status Schematic Legend displays information unique to the Link Status Schematic and is available through a link in the navigation area.

This display is designed to view information only therefore, it is not possible to edit the nodes shown on this display.

Important! If you have Feature 8, “Disaster Recovery (Duplex)”and Feature 40, “Enhanced Disaster Recovery”, during takeover or switchback from a backup host, it is necessary to reload the screen to view elements added from the other host.

Figure 2 Link Status Schematic container page



Table

If you select a highlighted node facet with the menu mouse button, it will return an alert indicator as shown in Table 2, along with the name of the DCC or the group of network elements.

Important! Not all facets described in the legend may be available on your system.

Table 2 Facets shapes and alert information

Facet Shape	Location	Alert Type	Alert Group	Description
Square	NE	ls_timediff	LS_TIMEDIFF	The time difference between NTM and a DCC that the link is connected to is greater than the value defined in the n_o_server_defs.pl file. **Reference: Reference:** Chapter 10, "Time Synchronization" in the *System Administration Guide*
Square	NW	ls_late	LS_LATE	The measurement data was late for at least one office connected to the DCC.
Square	SE	ls_dcc_manoos ls_dcc_failoos	LS_DCC_OOS	DCC either failed out of service or manually out-of-service.
Square	SW	ls_miss	LS_MISS	Measurement data was not received for at least one office connected to the DCC.
Diamond	NE	ls_sync	LS_SYNC	This is the *4ESS* office that NTM is using as the synchronization office.
Diamond	NW	ls_late	LS_LATE	The measurement data was received late for a directly-connected network element for at least one office of this type.
Diamond	SE	ls_timediff	LS_TIMEDIFF	The *4ESS* office either failed out of service or manually out-of-service.
Diamond	SW	ls_miss	LS_MISS	The measurement data was not received for a directly-connected network element for at least one office of this type.
Line		ls_manoos	LS_MANOOS	A manually out-of-service condition exists between the DCC and one of the offices, or between the NTM host and a directly connected office.
Box Line		ls_failoos	LS_FAILOOS	A failed out of service condition exists between the DCC and one of the offices, or between the NTM host and a directly-connected office.

References

For information on defining alarms, see the “Event_Alarm File” (p. 23) in the *Record Base Administration Guide*.

□

Changing the Link Status Schematic time difference

Instructions

Follow these steps to change the Link Status Schematic time difference:

> **Important!** Although there is a default time difference defined for the time between the NTM host and the DCC, the user can change the default. Changing the default will change all instances of the Link Status Schematic.

1. Log in as `root`.

2. Check if the file "/nm/web/site/n_o_server_defs.pl" exists. If not, copy "n_o_server_defs.pl" from /nm/web/defs to /nm/web/site.

3. Verify file "n_o_server_defs.pl" permissions are set to 644, owner is root, and group is nsgroup.

4. Change the line "alertIfTimeDiffGreaterThanThis=5;" if the default value of 5 is not suitable. Replace "5" with the preferred value.

5. Stop the map data server using "Stopping the map data server" (p. 9).

6. Start the map data server using "Starting the map data server" (p. 8).

END OF STEPS

□

STM Periodic Status

Overview

Purpose

The STM Periodic Status table object provides GUI access to display the data collection status of STM office(s).

After selecting the STM Periodic Status icon from the NTM launch page, a search page appears. You can choose to view a subset of STM specific data collection information.

Contents

This section contains the following topics:

STM Periodic Status	8-16
Current Link Status	8-18
Recent Data Collection Status	8-20

STM Periodic Status

Purpose

This page allows the user to retrieve and view Periodic STM link status information.

STM Periodic Search Page

Figure 3 shows the STM periodic Status page. Table 3 describes the search criteria that appear in the Search area for Link Status.

Figure 3 STM Periodic Status search page

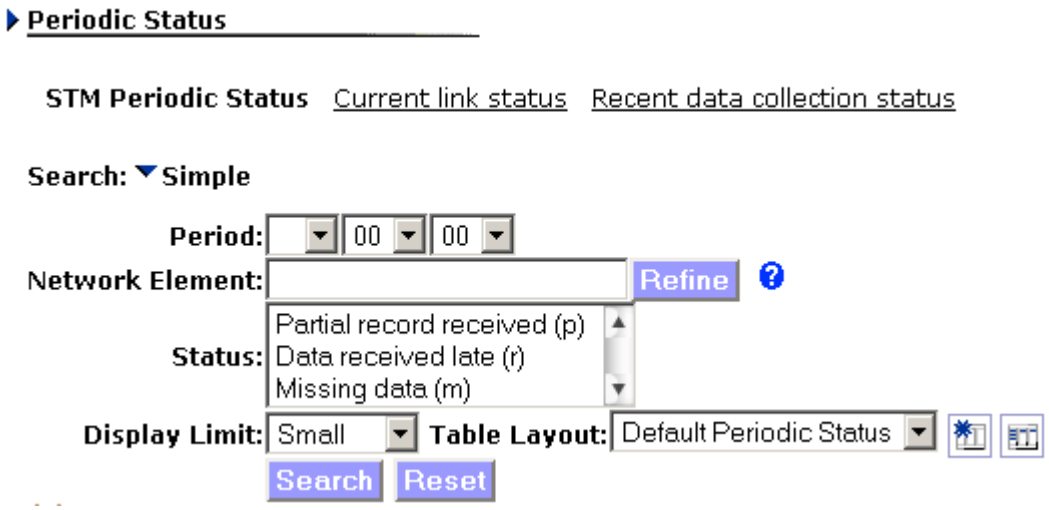


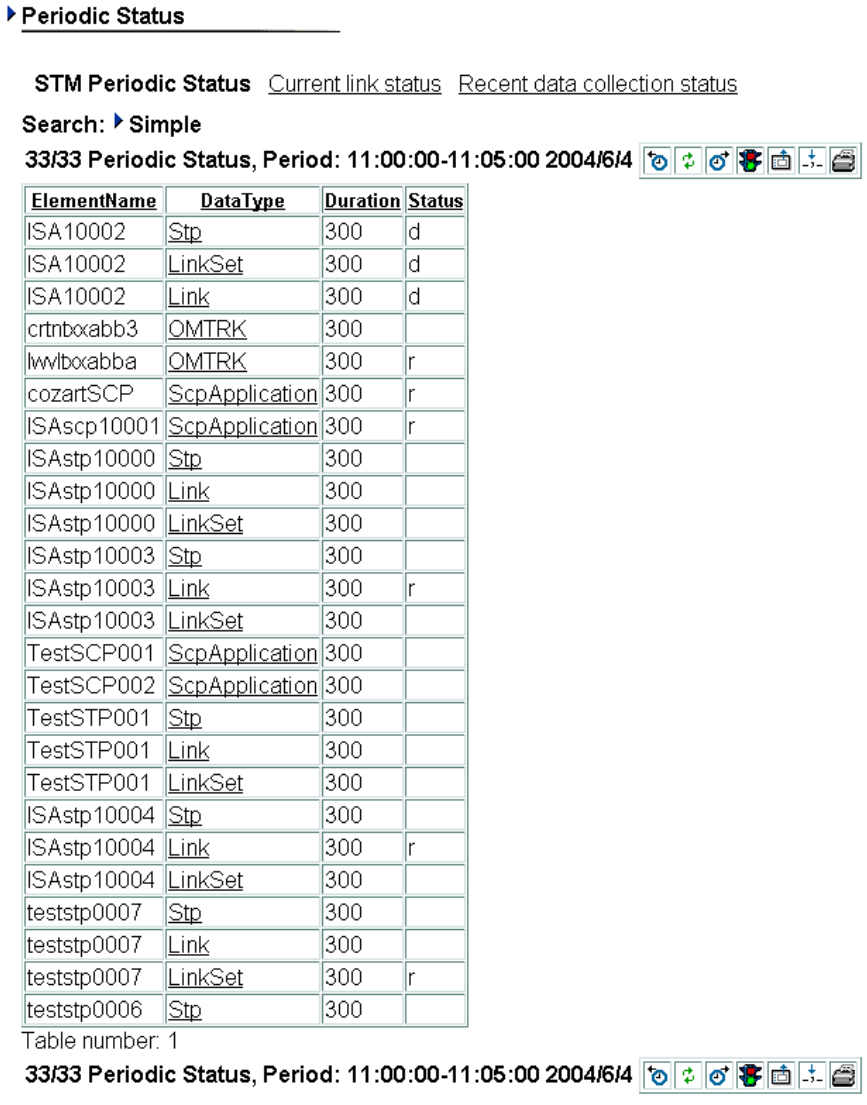
Table 3 Search criteria — STM Periodic Status Table

Label	Description
Period	Data collection period, typically current period, today, or one of the previous historical sessions.
Network Element	Network element name.
Status	These options allows the user to select the network elements by their connection status to STM.
Display Limit	Maximum number of rows to be retrieved: • Small: 100 rows • Medium: 600 rows • Large: 1200 rows
Table Layout	Table layout choices. Use this option to choose the measurement types you want to see.

STM Periodic Container Page

Figure 4 shows the STM periodic Status page. This page displays STM network elements and provides links to detail information about the network element. In addition, it displays the length of the latest data collection period and the status of the link during the period.

Figure 4 STM Periodic Status container page



Periodic Status

STM Periodic Status Current link status Recent data collection status

Search: Simple

33/33 Periodic Status, Period: 11:00:00-11:05:00 2004/6/4

ElementName	DataType	Duration	Status
ISA10002	Stp	300	d
ISA10002	LinkSet	300	d
ISA10002	Link	300	d
crtntboxabb3	OMTRK	300	
lwvlboxabba	OMTRK	300	r
cozartSCP	ScpApplication	300	r
ISAscp10001	ScpApplication	300	r
ISAstp10000	Stp	300	
ISAstp10000	Link	300	
ISAstp10000	LinkSet	300	
ISAstp10003	Stp	300	
ISAstp10003	Link	300	r
ISAstp10003	LinkSet	300	
TestSCP001	ScpApplication	300	
TestSCP002	ScpApplication	300	
TestSTP001	Stp	300	
TestSTP001	Link	300	
TestSTP001	LinkSet	300	
ISAstp10004	Stp	300	
ISAstp10004	Link	300	r
ISAstp10004	LinkSet	300	
teststp0007	Stp	300	
teststp0007	Link	300	
teststp0007	LinkSet	300	r
teststp0006	Stp	300	

Table number: 1

33/33 Periodic Status, Period: 11:00:00-11:05:00 2004/6/4

Current Link Status

Purpose

This page allows the user to retrieve and view the current STM link status information. This page presents the same information displayed using the STM “linkstat” command.

Current Link Status search page

Figure 5 shows the Current link status search page. Table 4 describes the search criteria that appear in the Search area for link status.

Figure 5 Current link status search page

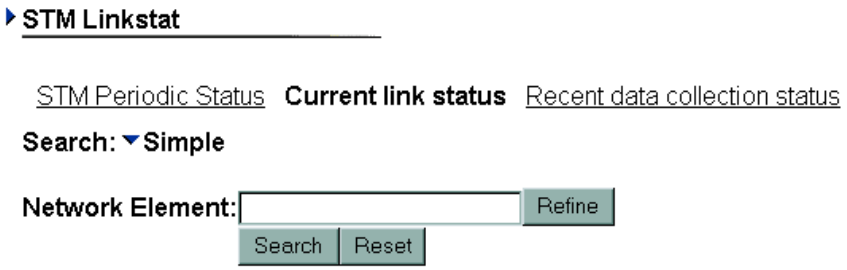


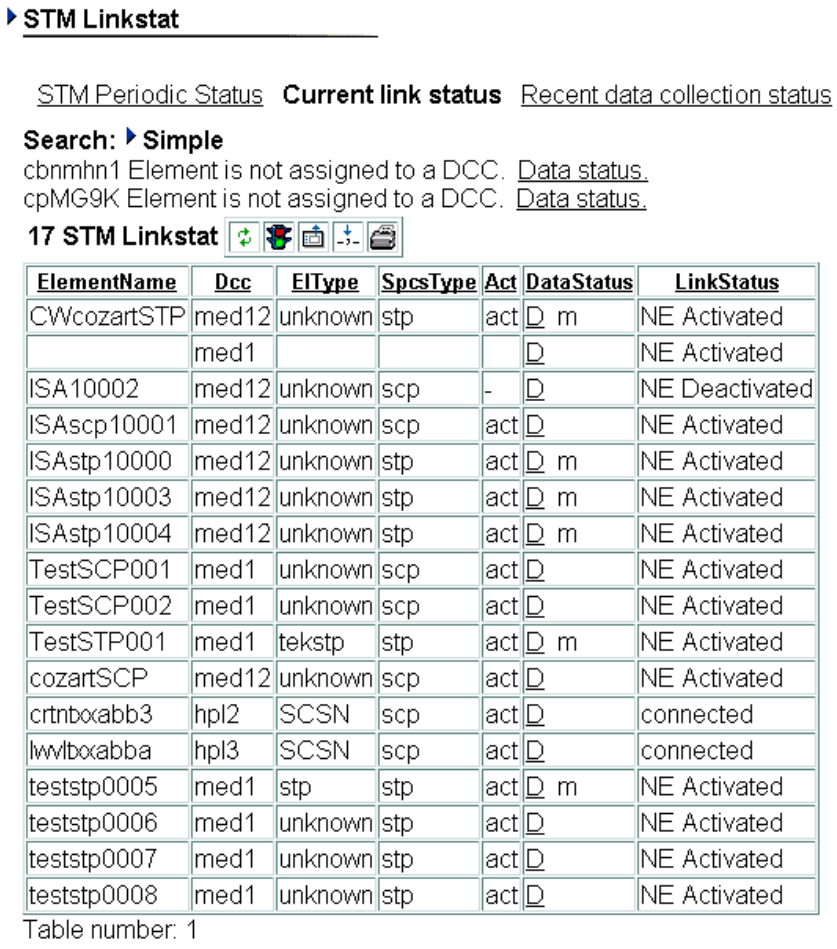
Table 4 Search criteria — Current link status Table

Label	Description
Network Element	Network element name. If this field is left blank, all signaling network elements will be retrieved.

Current Link Status container page

Figure 6 shows the Current link status search page. This page displays the current status of one, or all of the signaling elements in the network.

Figure 6 Current link status container page



STM Linkstat

STM Periodic Status **Current link status** Recent data collection status

Search: Simple

cbnmhn1 Element is not assigned to a DCC. Data status.
cpMG9K Element is not assigned to a DCC. Data status.

17 STM Linkstat

ElementName	Dcc	ElType	SpcsType	Act	DataStatus	LinkStatus
CWcozartSTP	med12	unknown	stp	act	D m	NE Activated
	med1				D	NE Activated
ISA10002	med12	unknown	scp	-	D	NE Deactivated
ISAscp10001	med12	unknown	scp	act	D	NE Activated
ISAstp10000	med12	unknown	stp	act	D m	NE Activated
ISAstp10003	med12	unknown	stp	act	D m	NE Activated
ISAstp10004	med12	unknown	stp	act	D m	NE Activated
TestSCP001	med1	unknown	scp	act	D	NE Activated
TestSCP002	med1	unknown	scp	act	D	NE Activated
TestSTP001	med1	tekstp	stp	act	D m	NE Activated
cozartSCP	med12	unknown	scp	act	D	NE Activated
crtnbxabb3	hpl2	SCSN	scp	act	D	connected
lwvlbxabba	hpl3	SCSN	scp	act	D	connected
teststp0005	med1	stp	stp	act	D m	NE Activated
teststp0006	med1	unknown	stp	act	D	NE Activated
teststp0007	med1	unknown	stp	act	D	NE Activated
teststp0008	med1	unknown	stp	act	D	NE Activated

Table number: 1

Recent Data Collection Status

Purpose

This page allows the user to retrieve and view only the most current link status information. This page presents the same information displayed using the STM “rdatastat” command.

Recent Data Collection search page

Figure 7 shows the Recent data collection status search page. Table 5 describes the search criteria that appear in the search area for link status.

Figure 7 Recent data collection status search page

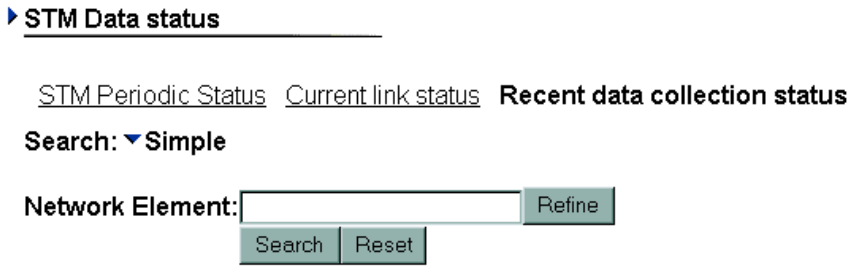


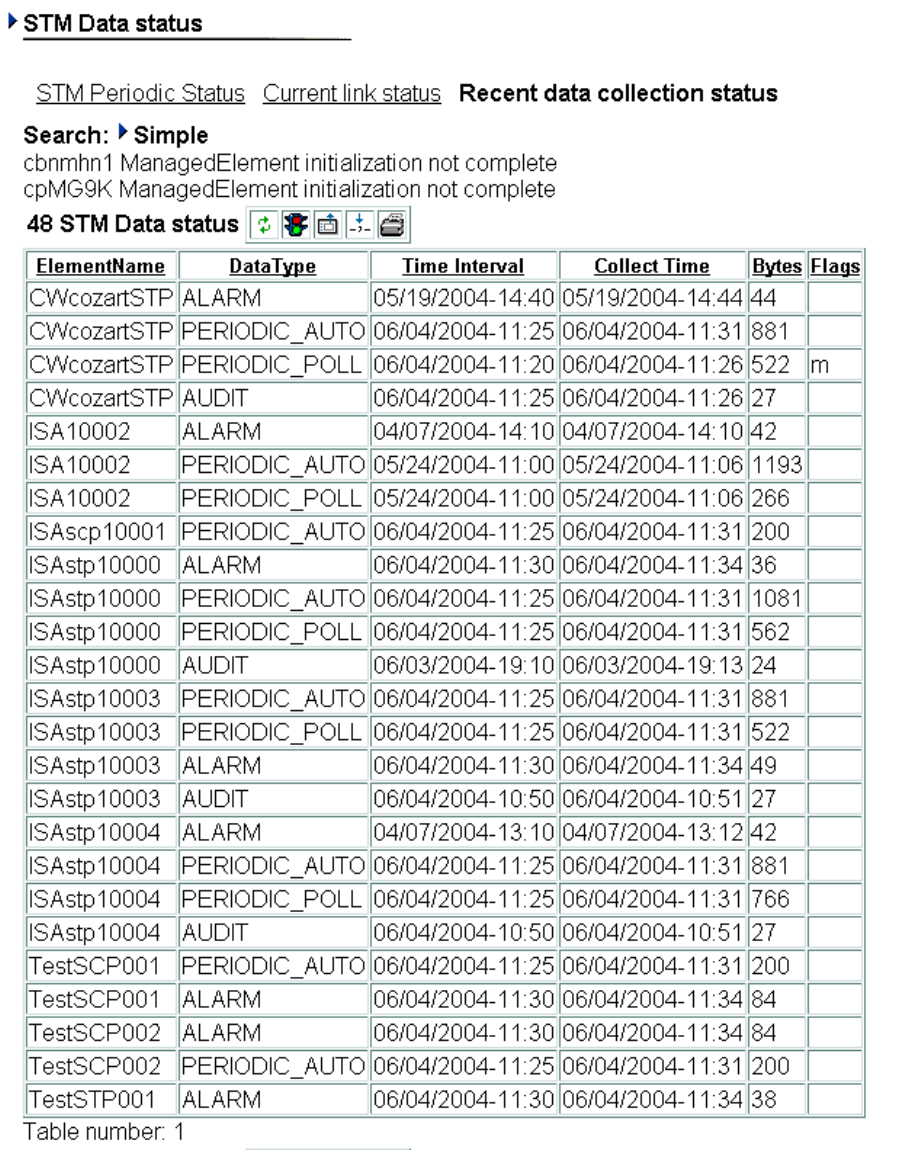
Table 5 Search criteria — Recent data collection status search page

Label	Description
Network Element	Network element name. If this field is left blank, all signaling network elements will be retrieved.

Recent Data Collection container page

Figure 8 shows the Recent data collection status container page. This page displays link details from the most recent data period.

Figure 8 Recent Data Collection Status container page



STM Data status

STM Periodic Status Current link status **Recent data collection status**

Search: Simple

cbnmhn1 ManagedElement initialization not complete
cpMG9K ManagedElement initialization not complete

48 STM Data status

ElementName	DataType	Time Interval	Collect Time	Bytes	Flags
CWcozartSTP	ALARM	05/19/2004-14:40	05/19/2004-14:44	44	
CWcozartSTP	PERIODIC_AUTO	06/04/2004-11:25	06/04/2004-11:31	881	
CWcozartSTP	PERIODIC_POLL	06/04/2004-11:20	06/04/2004-11:26	522	m
CWcozartSTP	AUDIT	06/04/2004-11:25	06/04/2004-11:26	27	
ISA10002	ALARM	04/07/2004-14:10	04/07/2004-14:10	42	
ISA10002	PERIODIC_AUTO	05/24/2004-11:00	05/24/2004-11:06	1193	
ISA10002	PERIODIC_POLL	05/24/2004-11:00	05/24/2004-11:06	266	
ISAscp10001	PERIODIC_AUTO	06/04/2004-11:25	06/04/2004-11:31	200	
ISAstp10000	ALARM	06/04/2004-11:30	06/04/2004-11:34	36	
ISAstp10000	PERIODIC_AUTO	06/04/2004-11:25	06/04/2004-11:31	1081	
ISAstp10000	PERIODIC_POLL	06/04/2004-11:25	06/04/2004-11:31	562	
ISAstp10000	AUDIT	06/03/2004-19:10	06/03/2004-19:13	24	
ISAstp10003	PERIODIC_AUTO	06/04/2004-11:25	06/04/2004-11:31	881	
ISAstp10003	PERIODIC_POLL	06/04/2004-11:25	06/04/2004-11:31	522	
ISAstp10003	ALARM	06/04/2004-11:30	06/04/2004-11:34	49	
ISAstp10003	AUDIT	06/04/2004-10:50	06/04/2004-10:51	27	
ISAstp10004	ALARM	04/07/2004-13:10	04/07/2004-13:12	42	
ISAstp10004	PERIODIC_AUTO	06/04/2004-11:25	06/04/2004-11:31	881	
ISAstp10004	PERIODIC_POLL	06/04/2004-11:25	06/04/2004-11:31	766	
ISAstp10004	AUDIT	06/04/2004-10:50	06/04/2004-10:51	27	
TestSCP001	PERIODIC_AUTO	06/04/2004-11:25	06/04/2004-11:31	200	
TestSCP001	ALARM	06/04/2004-11:30	06/04/2004-11:34	84	
TestSCP002	ALARM	06/04/2004-11:30	06/04/2004-11:34	84	
TestSCP002	PERIODIC_AUTO	06/04/2004-11:25	06/04/2004-11:31	200	
TestSTP001	ALARM	06/04/2004-11:30	06/04/2004-11:34	38	

Table number: 1

Periodic Data Browser

Overview

Purpose

The Periodic Data Browser provides GUI access to display the User-defined Data types, User-defined network elements, and status of related jobs. This pages are related to Feature 436, “UDDM/UDNEI” and Feature 437, “Enhanced Thresholding and Analysis”.

Contents

This section contains the following topics:

Periodic Data Browser search page	8-24
Periodic Data Browser container page	8-27
Periodic Data Browser Details page	8-29

Periodic Data Browser search page

Purpose

The Periodic Data Browser search page allows you to restrict the data retrieved based on the specific parameters. It allows you to view current and historic UDDM/UDNEI information. The field labels on the Periodic Data Browser search page are those defined in the UDDM metadata. This page is accessed by selecting the Periodic Data Browser icon on the Launch page as well as through the navigation links. The Trend Analysis is available to graph a particular field for individual UDDM objects only if Feature 385, "Trend Analysis" has been purchased.

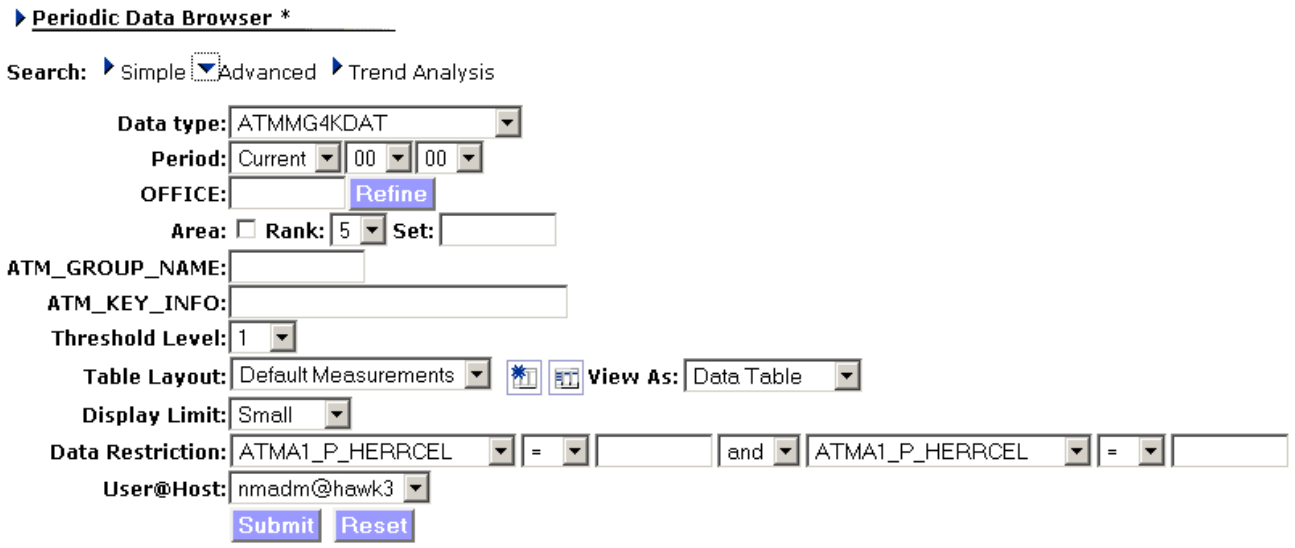
Important! Notice that the Back button in the browser moves you to the previous page and not to the previous form. After going from the launch page to the Periodic Data Browser page, performing search for a few times and then pressing Back button will move you to the launch page not to the results of the previous search.

Important! If you want to add the page with search results to favourites click the asterisk (*) near the title of Periodic Data Browser page to resolve the URL address then you can bookmark it.

Periodic Data Browser Search Page

Figure 9 shows the Periodic Data Browser search page.

Figure 9 Periodic Data Browser search page



Search Criteria

Table 6 describes the search criteria that appear in the Search area for the Periodic Data Browser page:

Table 6 Search criteria for the Periodic Data Browser

Label	Description
Data type	Available UDDM data types and UDNEI network elements.
Period	Data collection period. The deafult is current.
OFFICE Area Rank Set	Office name. Valid values include all internal network elements.
FAREND Area Rank Set	Far end network element. Valid values include all network elements, both internal and external.
Threshold Level	0–10. The default is 1.
Table Layout	Table layout choices. The valid choices are limited to table layouts that apply to the valid data types.
Display Limit	Small, medium, or large limit for data retrieval. • Small: 100 rows • Medium 600 rows • Large: 1200 rows • XL: 1500 rows
Exception Processing	NONE, ALLOW or INHIBIT
Mark	Mark (mark status) may be: all (blank by default), ACK, AIP or customer defined marks. It is possible for the user to add their own mark categories by editing the *"/nm/web/jsp/WEB-INF/classes/ntmgui_site_defs.properties"* file. However, it is recommended that the user work with Alcatel-Lucent field support while editing this file for the first time. **Important!** User-defined mark categories are limited to 6 characters.
Data Fields	You can aggregate data for all or specific objects.
Trend Window	Time window (5min to 2 hrs).
Data Restrictions	You can use the 2 pop-up lists to restrict conditions which will cause the alarm to sound.

Table 6 Search criteria for the Periodic Data Browser

User@Host	This displays the current user ID and host information.

Periodic Data Browser container page

Purpose

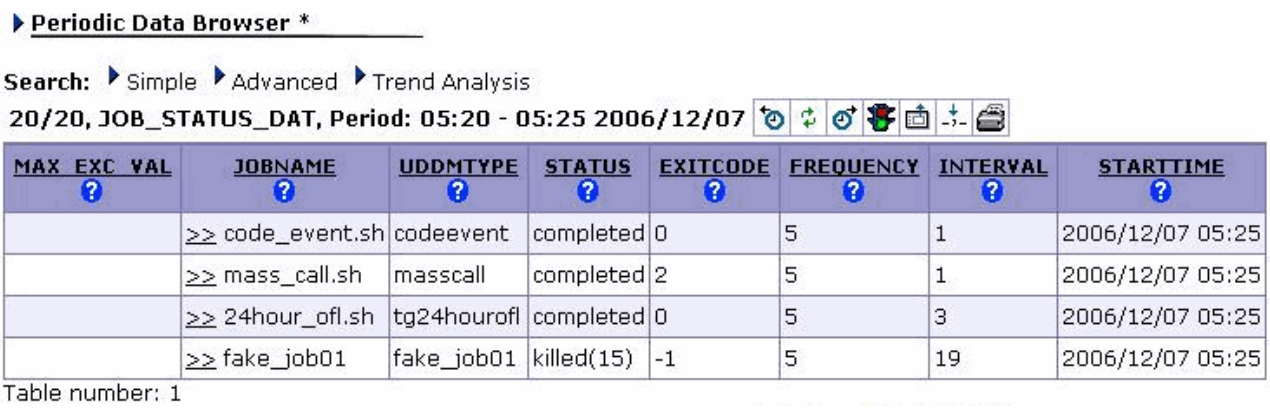
The Periodic Data Browser container page displays the results of a search in tabular format.

The Periodic Data Browser container page displays data in Data Table view (Figure 10) or Exception List View, depending on the user's choice on the Periodic Data Browser search page.

Periodic Data Browser Container Page

Figure 10 shows the Periodic Data Browser container page.

Figure 10 Periodic Data Browser container page: Data table view



MAX_EXC_VAL	JOBNAME	UDDMTYPE	STATUS	EXITCODE	FREQUENCY	INTERVAL	STARTTIME
	>> code_event.sh	codeevent	completed	0	5	1	2006/12/07 05:25
	>> mass_call.sh	masscall	completed	2	5	1	2006/12/07 05:25
	>> 24hour_ofl.sh	tg24hourofl	completed	0	5	3	2006/12/07 05:25
	>> fake_job01	fake_job01	killed(15)	-1	5	19	2006/12/07 05:25

Table number: 1

Page components

To change the label for any column edit the *"/nm/dbutil/metadata/labels.U"* file and use the `upd_meta` command.

The ">>" field is a link to Detail data for the UDDM record or an icon for each record which is a link to the Detail data.

The Mark and Inhibit fields is displayed for each record (if defined in the reference table) and it provides links to the Mark and Inhibit Assignment Page.

Suspected data is indicated with a small question mark (?) after the value in each table cell.

Column headings displayed for the Data Table view are fields regarding the Table Layout. Click on a column heading once to sort in descending order and second time to sort in ascending order.

Status Column

The following are values for status column which shows current statuses for jobs:

- Not Started – No binary file or wrong permissions,
- Killed(<signumber>) - Job killed by signal number <signumber>,
- Feature off – Job feature is disabled,
- Failed – Job could not start because of error in job executable file (e.g. syntax),
- Completed - Job finished using exit function,
- Skipped – Job has 15 or 30 or 60 Frequency value inside jobList file, and it was not 5min valid boundary to start job (e.g. for 30 min jobs valid 5 min boundaries are: 1.00, 1.30, 2.00, 2.30 and so on.)
- Not attempted- Job which has not executed and next EOP arrived.

Periodic Data Browser Details page

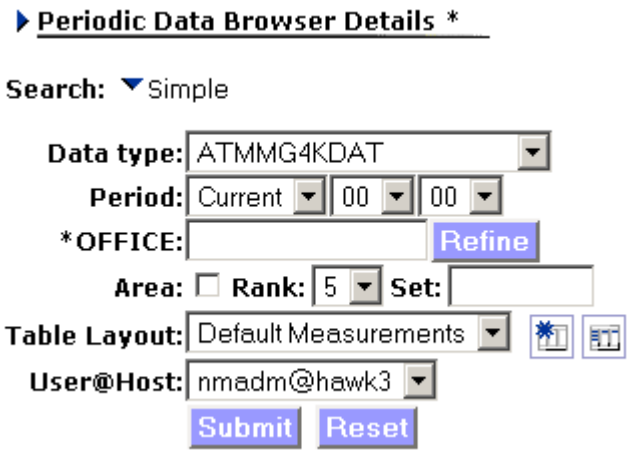
Purpose

The Periodic Data Browser Details page allows you to restrict the data retrieved based on the specific parameters of UDDM objects. This page displays the reference attributes for the UDDM object along with the trend data for the number of intervals specified in the preferences. The result is presented on the Periodic Data Browser container page. It is accessed by selecting the Periodic Data Browser Details icon on the Launch page as well as through the navigation links.

Periodic Data Browser Details Page

Figure 11 shows the Periodic Data Browser Details page.

Figure 11 Periodic Data Browser Details page



Search Criteria

Table 7 describes the search criteria that appear in the Search area for the Periodic Data Browser Details page:

Table 7 Search criteria for the Periodic Data Browser Details

Label	Description
Data type	Available UDDM data types and UDNEI network elements.
Period	Data collection period. The deafult is current.

Table 7 Search criteria for the Periodic Data Browser Details

OFFICE Area Rank Set	Office name. Valid values include all internal network elements.
FAREND Area Rank Set	Far end network element. Valid values include all network elements, both internal and external.
Table Layout	Table layout choices. The valid choices are limited to table layouts that apply to the valid data types.
User@Host	This displays the current user ID and host information.

9 GUI Administration

Overview

Purpose

This chapter describes functions of NTM GUI Administration available through the Administration Launch page (Figure 1). Using the Web Administration functions the user can:

- Perform Web User Administration (Web User administration)
- Perform Password administration
- Change default table layouts (Table Layout administration)
- Operate "Feature 342, "Historical Data Playback for the Browser-based GUI"" (p. 106) (Historical Session administration)
- Administer Network View attributes Network Views (map) administration
- Create, modify and delete parameter sets (Parameter Sets administration)
- Administer Network View attributes for Link Status Schematic (Link Status Shape Facet Administration)
- Access Browser support files through the Client Downloads link.
- Access Feature listing for your NTM system through the Feature Listing link.

Contents

This chapter contains the following topics:

Web User administration	9-3
Password administration	9-7
Table Layout administration	9-13
Historical Session administration	9-19
Network Views (map) administration	9-25
Parameter Sets administration	9-39
Link Status Shape Facet Administration	9-43
Client Downloads	9-44
Feature Listing	9-45
General tasks on the Administration pages	9-47

Web User administration

Purpose

Depending on user permissions, one of two pages will initially be displayed after the Web User link is selected from the Administration launch page (Figure 1):

- Web User Information — for users ***without*** Web Administration permission. Web users who do not have web administration permission will be shown only display preferences.

  Important! A similar page (Figure 2) with additional capabilities can be accessed from the Web User Administration page mentioned below.

- Web User Administration (Figure 3) — for Users ***with*** Web Administration permission. You can perform searches for specific users in addition to being able to administer the following functions:
  - Adding and deleting users
  - Change Password
  - Web Administration
  - Default view settings
  - Network Views
  - Table Layouts
  - Control Parameter Sets

  From the Web User Administration page you can change your own privileges as well as changing other users permissions, view preferences and administration privileges.

Related tasks

"Changing user permissions" (p. 50)
"Changing passwords" (p. 51)
"Adding users" (p. 55)
"Deleting users" (p. 57)

Figures

Figure 1 shows a sample of the Administration launch page. Figure 2 provides an example of a Web User Information page accessed from the Web User Administration page. Figure 3 provides an example of a Web User Administration page.

Figure 1 Administration launch page

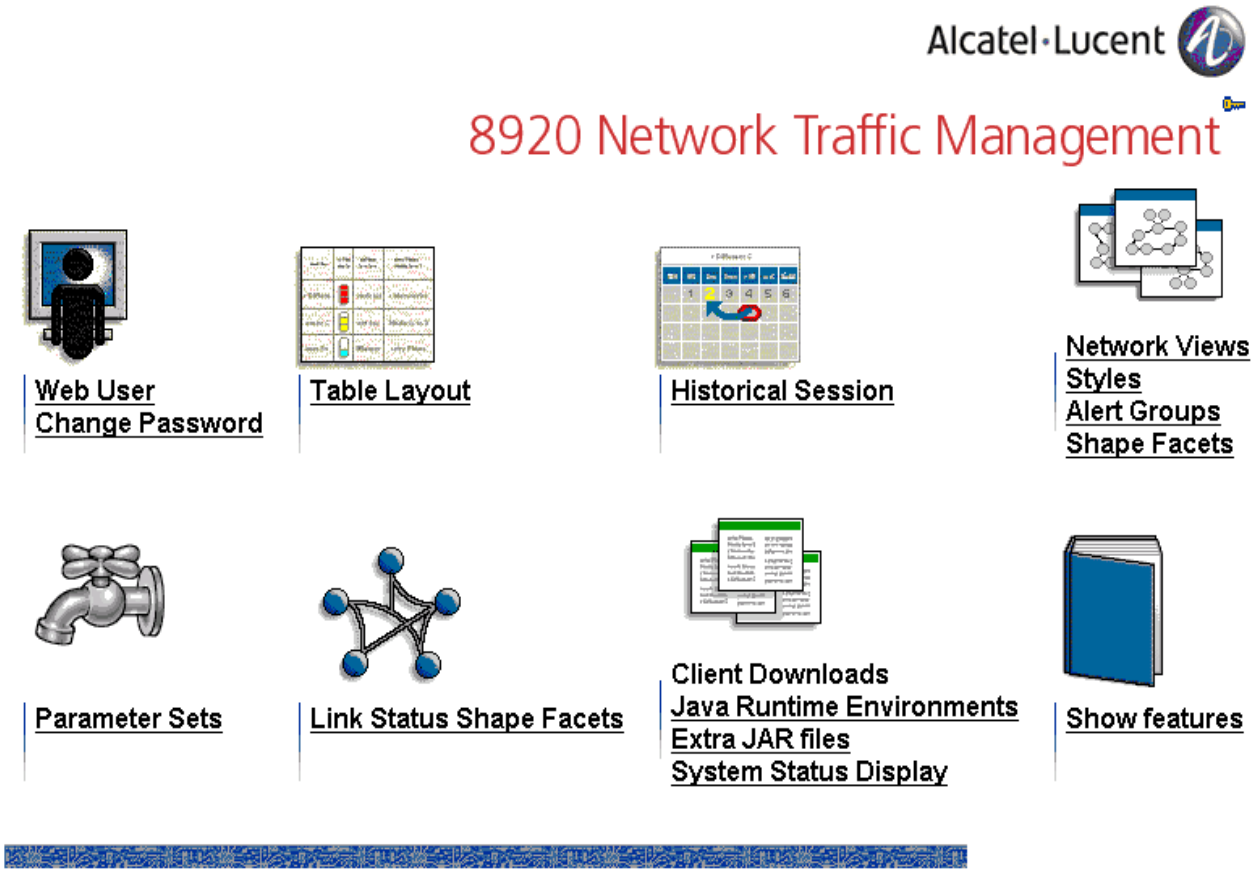


Figure 2 Web User Information page

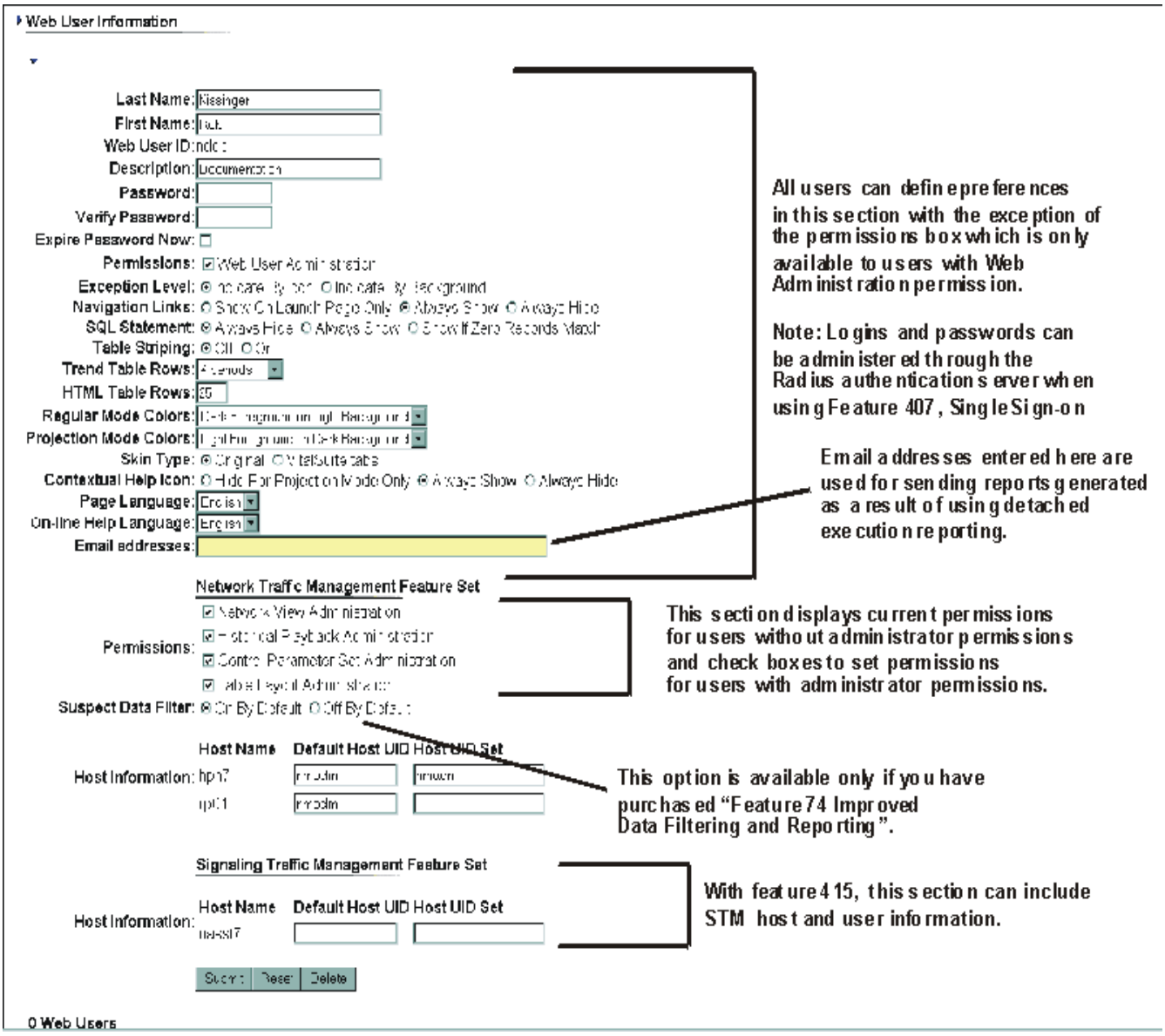
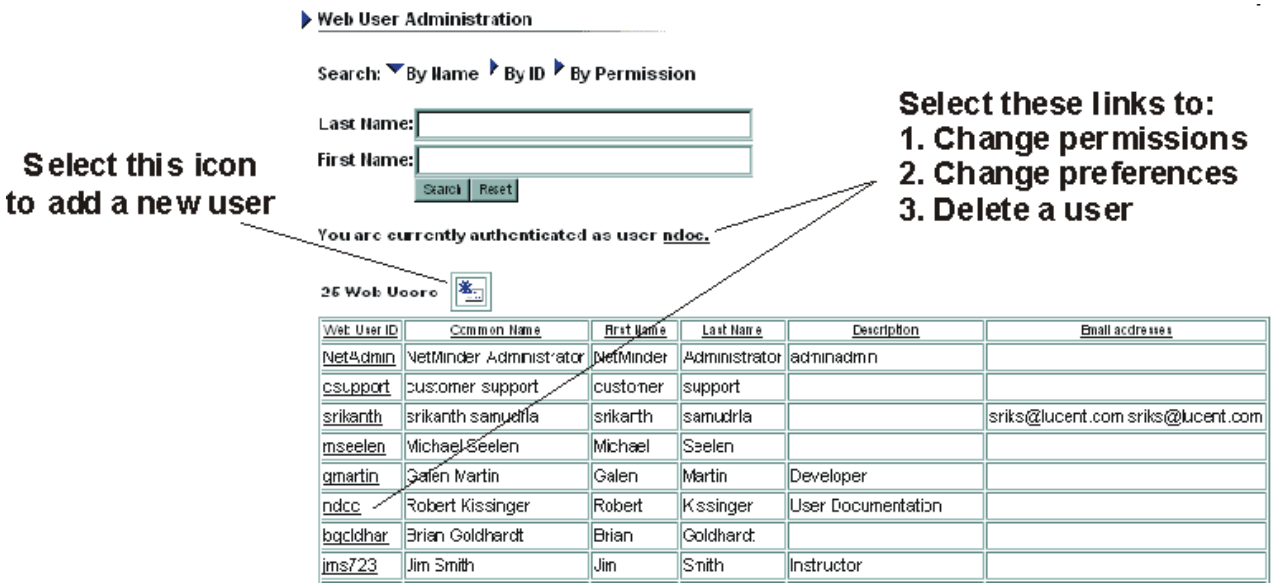


Figure 3 Web User Administration page



Password administration

Overview

Defining characteristics of Web GUI passwords can reduce exposure to unauthorized access to the system. Those with administrator/root permission can configure specific Web GUI password characteristics for users including:

- Minimum number of characters required for Web GUI user password. A new or modified password must contain at least the specified minimum number of characters to be considered valid. The minimum will be configurable.
- Password composition. This requires a user password to contain characters from specific groups (alpha-numeric, special, etc.) to be considered valid. The character groups are configurable.
- Password Aging. This requires a user password to be changed within a given number of days. When the user's password expires, the user will be redirected to a password modification page until the password has been modified. The number of days is configurable.
- Inactivity Lock. A user's entry is "locked" from Web GUI access after the specified number of consecutive inactivity days is reached.
- Ineffective authentication attempts lock. A user's entry is "locked" from Web GUI access after the specified number of consecutive failed authentication attempts is reached. The minimum value is two (2).
- Temporary password assignment. This capability allows a Web User Administrator to mark a user's entry such that it will require the user to enter a new password upon its next use.

Inactivity and password aging checks

The web user inactivity and password aging checks are performed as part of the log check (logchk) script executed through the cron. Therefore, if the cron is not available at the appropriate time or the cron tables are modified to affect the execution of the log check script, the ability to accurately perform the inactivity and password aging checks may be affected.

Feature 374

With "Feature 374, "Enhanced Password Aging"" (p. 130) additional options are:

- The ability to specify a minimum number of days that must lapse before the user's Web GUI password can be changed.
- The ability to specify the number of passwords stored per user in an effort to guard against password recycling.

Important! By default, any user marked as a web user administrator is exempt from both EPWA checks when modifying any password. The web user administrator can change any user's password whenever they like, regardless of the EPWAMINCHANGE value. Also, if a web user administrator sets a web user's password no comparison to the current or stored old passwords is made, regardless of the EPWANUMOLDPASSWORDS value, AND the list of stored passwords for that user is cleared as well.

Password composition

The password length and composition components, by default, are set to a minimum length of 3 characters and composed of characters from the following list:

```
abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890!#^&*()
-_+=|[]{};:,./<>?
```

The password length and composition components are configurable but can be complex to administer. Please contact your NTM site coordinator or field support personnel for assistance in this area.

Passwords in a multihost environment

In a NTM multi-host environment utilizing Directory Server (LDAP) replication, it is recommended that the inactivity and password aging thresholds be set to the same value on all hosts to help simplify operation and administration. If the values are different between NTM hosts, then the smallest value is effectively the threshold since it will expire first.

Password expiration

There is no notification to the user of proximity to password expiration, therefore it is recommended that the user adopt a policy of password modification before the expiration period. If a user's password does expire, the user will be redirected to a password administration screen upon his next NTM Web GUI access request. A new password must be entered at that time.

Important! If a user's password is changed while they have a browser session active that had previously authenticated through the NTM Web GUI, their next web access attempt will result in an authorization failed response. This will affect all previously authenticated browser sessions for this user on all clients including those used for wall board displays etc. When authentication fails simply retry using the new password to gain access.

Exceeding the defined thresholds

Users trying to access the system that has exceeded a threshold may be:

- prompted to refresh their password,
- denied Web GUI access,
- asked to re-enter a password that will conform to length or composition rules.

Authentication attempts that exceed the threshold will not only result in “locking” the specific web user ID but also result in a message appearing in the “/musr/log/errors file”.

Reference: See the *System Responses Guide* for specific error messages.

Excluding users from password thresholds

Individuals can be excluded from the processing for the characteristics by defining those who are not to be included on the “PWA_<characteristic>_EXCLUDE <user Ids>” line of the “/nm/web/sup_soft/http/conf/pwa.conf” file. User Ids can be a single web user Id, or a list of web user Ids separated by “|” symbols. Do not use white spaces within the “user(s)” string. Follow the comment text and examples given in the pwa.conf file. If no user is to be excluded, then this line must be commented out by using the “#” symbol at the beginning of the line referred to above.

Important! If the web user administrator is NOT excluded from the various thresholds, then you risk losing the capability to perform web user administration/recovery.

Modifying passwords

To modify the ineffective attempts, inactivity, or expiration characteristics, log in as root and edit the “/nm/web/sup_soft/http/conf/pwa.conf” file and adjust the items which are configurable by following the commented text included. After changes are made, the web server must be restarted for the changes to take effect.

Important! The NTM GUI will be unavailable to all users during the period in which the web server is stopped and is restarting for the given host.

CAUTION

It is recommended that a copy of the file be saved before editing to allow a recovery path in the event of server startup failure. After

changes are made, the web server must be restarted for the changes to take effect.

Resetting passwords

To reset the user's Web GUI password once the inactivity or ineffective attempts threshold is exceeded, the Web Administrator needs to specify a new one for the user through the Web User Information Page (Figure 2). In addition to resetting the password the administrator may also choose to use the “expire password now” option on the Web User Information Page (Figure 2) to force the user to select a new password upon his next NTM Web GUI access attempt.

Reference: “Starting and stopping the web server” (p. 53); “Starting and stopping the LDAP server” (p. 54)

Figure 4 /nm/web/sup_soft/http/conf/pwa.conf file

```
#  @(#)pwa.conf37.1.2.1
#

#
#  Copyright (c) 2002  Lucent Technologies
#
# This configuration file is used to specify the PWA feature
# related attributes. This file is to be readable only by root.


# Load the PERL scripts used for the PWA feature and checks, and specify
# the handler.

PerlRequire /nm/web/other-bin/site_perl/Apache/PWAcheck.pl

PerlLogHandler Apache::PWAcheck
# For support use only
#PerlSetEnv PWADEBUG on


##### Customer Modifiable Variables below #######

# The PWAATTLIMIT variable defines the number of invalid consecutive attempts
# threshold.  When exceed the web server will effectively "lockout" that
# Web User by replacing their Web GUI password with an unknown value.
# The value MUST be >= 2 (i.e. - 1 will cause no locking to occur).
# Default as delivered is 10.
PerlSetEnv PWAATTLIMIT 10

# The PWAMUSTCHANGE variable specifies the number of days within which a
# user "must" change their password.
```

```
SetEnv PWAMUSTCHANGE 90

# The PWAINACTIVITY variable specifies inactivity threshold in days.
# When crossed the user's web access will be locked. BE VERY CAREFUL,
# ESPECIALLY USING SMALL NUMBERS, AND CONSIDER USING THE PWA EXCLUDES
# LISTED BELOW TO AVOID UNWANTED LOCKS, ESPECIALLY FOR ADMINISTRATORS.
SetEnv PWAINACTIVITY 45

# Below are defined the lists of users to be excluded from specific categories
# of PWA processing.  The value format for each variable is a list of users
# separated by a "|" symbol delimiter.  For example to exclude "joe" and
# "jane" from inactivity processing the line would read:
#
# SetEnv PWA_INACT_EXCLUDE joe|jane
#
# The categories are:
# PWA_INACT_EXCLUDE <= The inactivity exclude list
# PWA_AGE_EXCLUDE <= The aging exclude list
# PWA_ATT_EXCLUDE <= The ineffective attempt exclude list
#
# By default the Web ID "NetAdmin" appears on all 3 lists.
#
SetEnv PWA_INACT_EXCLUDE NetAdmin
SetEnv PWA_AGE_EXCLUDE NetAdmin

# NOTE: if no users are to appear on the PWA_ATT_EXCLUDE list
# then comment the line out, else a blank exclude list will cause
# an error during server startup.

PerlSetEnv PWA_ATT_EXCLUDE NetAdmin

##### If the Enhanced Password Aging (EPWA) feature is enabled         #####
##### the following attributes (EPWAMINCHANGE and EPWANUMOLDPASSWORDS) #####
##### apply.                                                          #####

# The EPWAMINCHANGE defines the miniumum number of days that must
# lapse before the user is allowed to change their password again
# Note: this value should be greater than 0 to be effective, a value
# of 0 will disable this check.
SetEnv EPWAMINCHANGE 3

# The EPWANUMOLDPASSWORDS defines the number of old passwords to
# remember to guard against password cycling.
# Note: this value must be greater than 0 to be effective, a value
# of 0 will disable this check.
SetEnv EPWANUMOLDPASSWORDS 5
```

Table Layout administration

Overview

Purpose

Table Layout administration allows a user to determine what information is displayed after a search is performed for various types of data. The predefined selections can be viewed by accessing the link on the Administration launch page (Figure 1).

Contents

This section contains the following topics:

Table Layouts search page	9-14
Table Layouts container page	9-15
New Table Layout	9-16

Table Layouts search page

Purpose

After selecting the Table Layout link from the Administration launch page (Figure 1), a search page is returned (Figure 5). Using the search will display the default layout for each type of predefined data.

Figure 5 Table Layout search

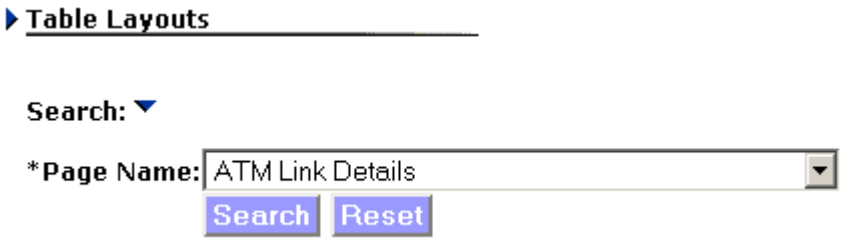


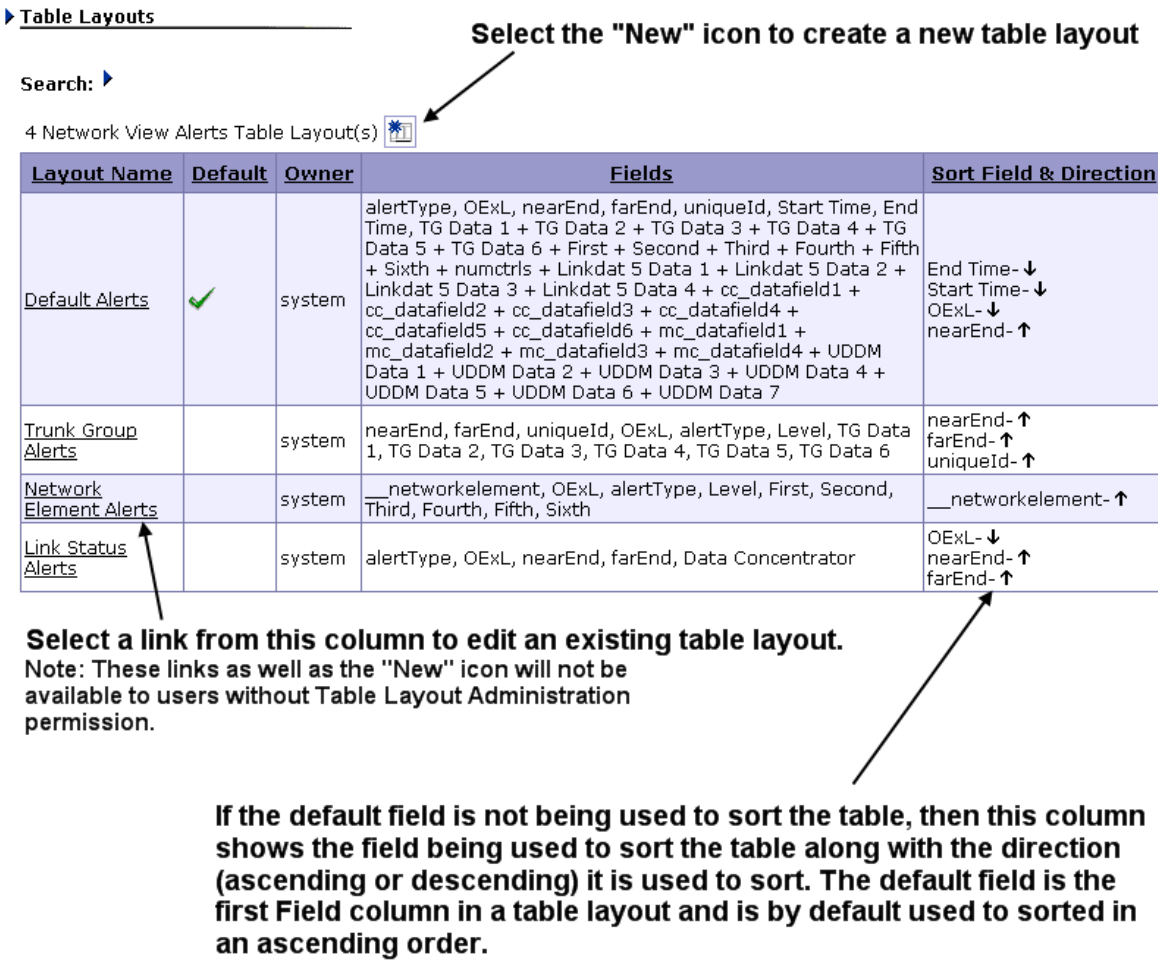
Table Layouts container page

Purpose

Depending on user permissions, one of two pages will initially be displayed after a search is performed.

- Table Layouts — for Users ***without*** Table Layout editing permission. Default fields for various data types are displayed.
- Table Layouts— for Users ***with*** Table Layout editing permission. Default fields for various data types are displayed with links to edit existing table layouts as well as the "New" toolbar button to create new table layout.

Figure 6 Table Layouts container page



□

New Table Layout

Purpose

To create a new Table Layout a user must have Table Layout administration permission, see “Web User administration” (p. 3). Selecting the “New” toolbar button from the search result container page, or any other search page where is a Table Layout choice, will access the new Table Layout page (Figure 7 and Figure 8). The fields shown on this page change depending on which page type it was accessed.

Figure 7 New Table Layout page

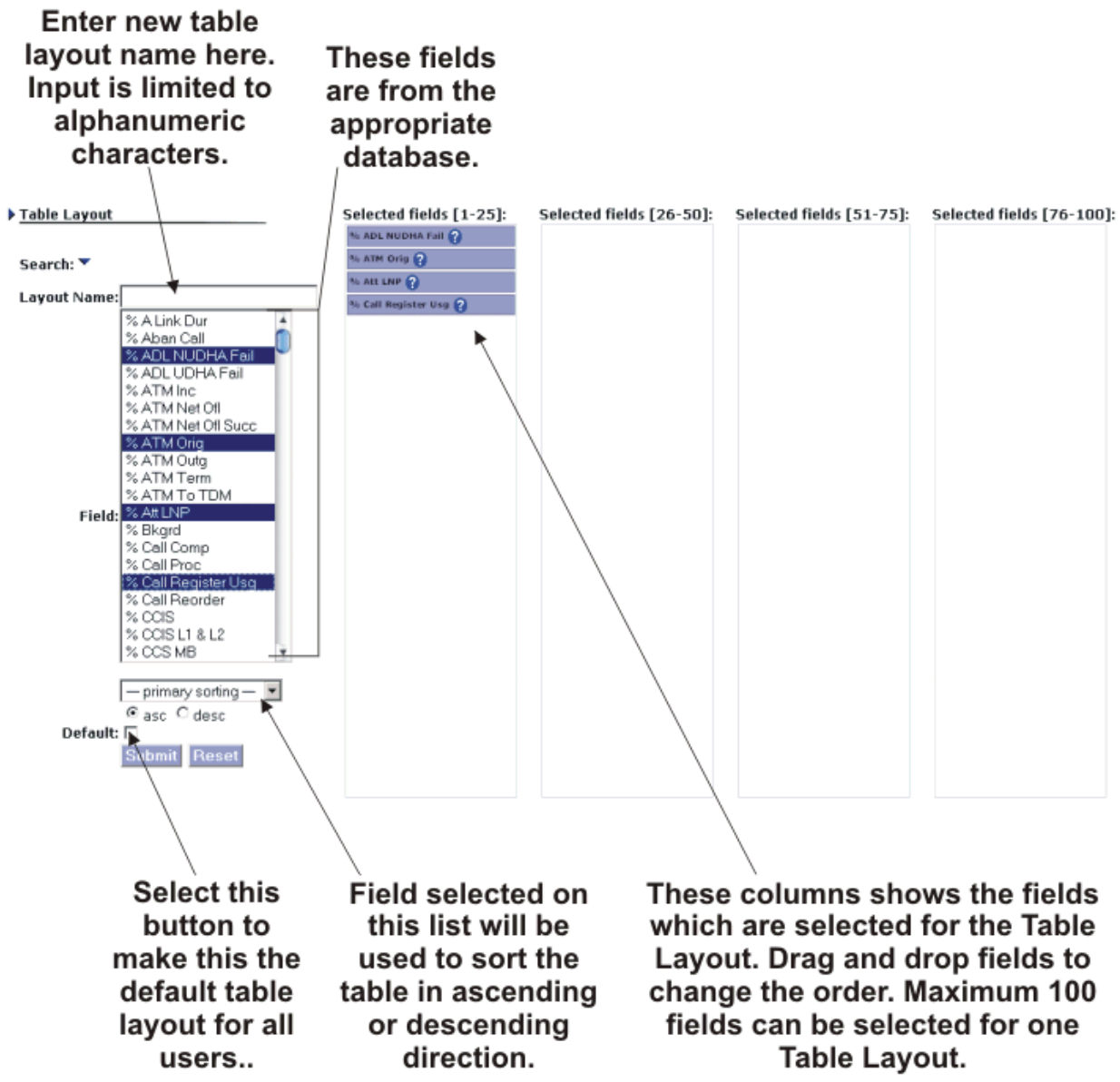
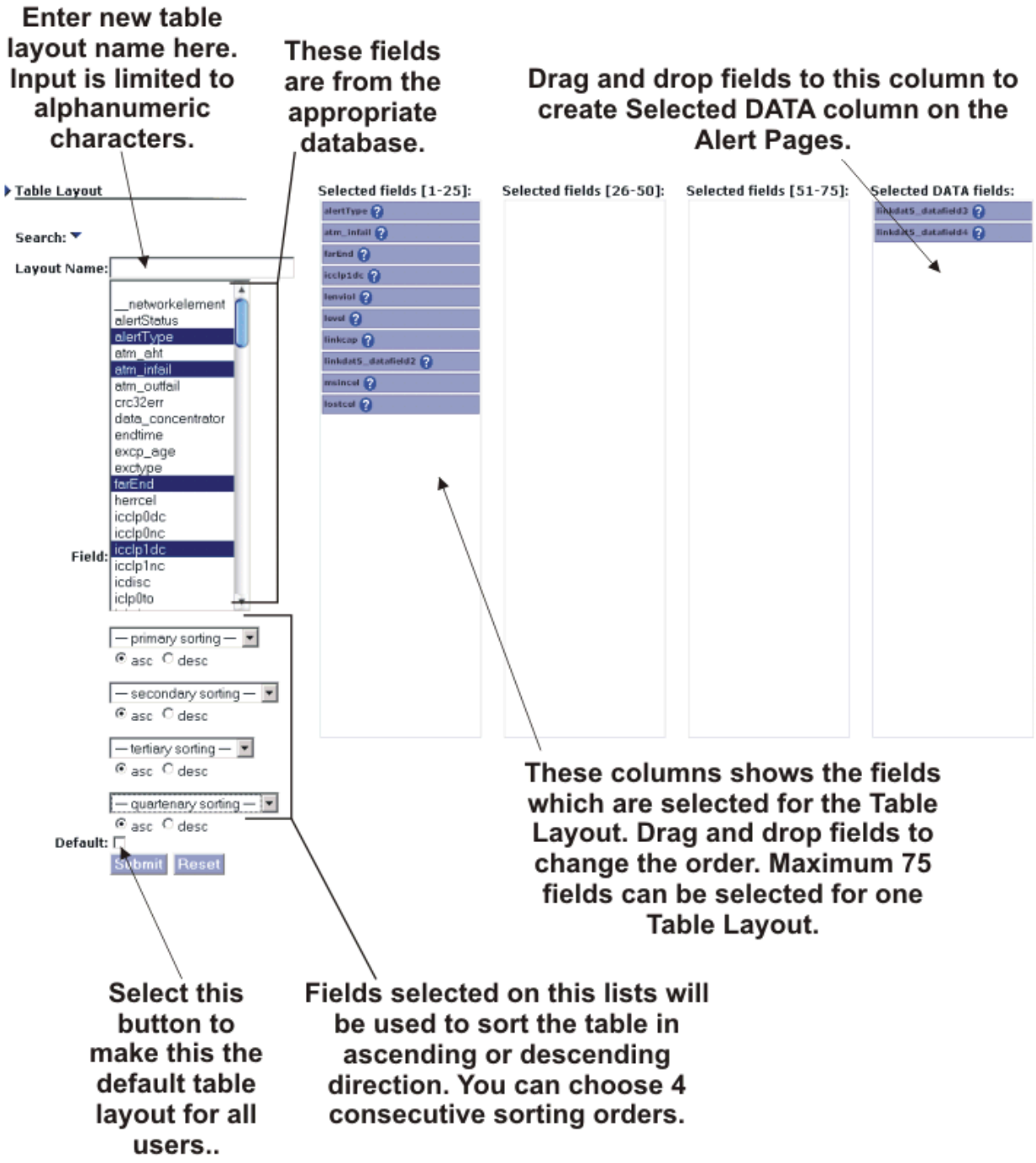


Figure 8 New Table Layout page for Alert Page



Historical Session administration

Overview

Purpose

Historical Session administration allows the user to add, delete or modify historical sessions. This function is used with “Feature 342, “Historical Data Playback for the Browser-based GUI”” (p. 106).

Only users with Historical Playback Permission as defined in the “Web User administration” (p. 3) will be able to add or modify sessions. Those without permission will only be able to view currently defined Historical Session.

The Historical Session Administration is accessed through the Historical Session icon from the Administration Launch page (Figure 1).

Contents

This chapter contains the following topics:

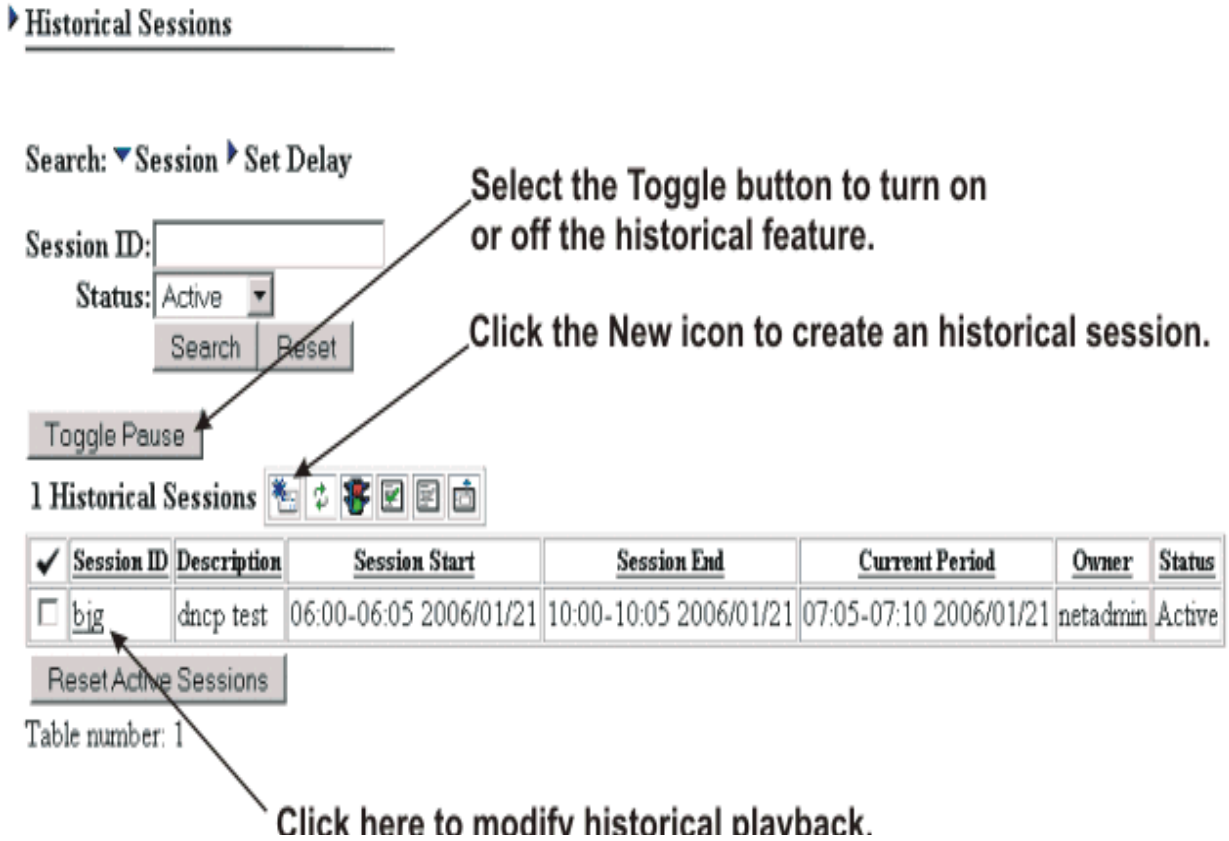
Historical Session search and container pages	9-20
Setting time delay	9-20
Historical Session playback toolbar icons	9-22
Historical Session search and container pages	9-20
Historical Playback Information page	9-23

Purpose

After selecting the Historical Session Administration link from the Administration Launch page (Figure 1) a search page is returned. The page only has a simple search option.

Using the search will display a container page (Figure 9) showing all active and inactive historical sessions available on the host.

Figure 9 Historical Session container page



Setting time delay

The time delay can be set using the Set Delay option on the Historical Session container page. This allows the user to control the time between data collection periods during automatic historical playback.

Important! Depending on the quantities of data being processed and subsequent processing time, the user may need to select a longer playback interval (60-seconds or

more) in order to allow the system to retrieve the data for all the periods defined in the historical session or for auto update mode to retrieve correctly.

Historical Session playback toolbar icons

Purpose

Some historical session playback toolbar icons vary from the standard toolbar icons as defined in Chapter 1, “Getting Started with the Browser-based GUI” “Toolbar area” (p. 24). Some that differ are found in Table 1.

Table 1 Toolbar icons

Icon Name	Icon	Description
New		Allows for the creation of a new historical session. This is only present for users with Historical Playback Administration permission.
Previous Period		Changes current page to show previous data collection period in the historical session. **Important!** This may not always be the period immediately previous. The periods used in the historical session can be randomly defined during the creation of the session.
Current Period		Changes to current period.
Next Period		Changes current page to show next data collection period in the historical session. **Important!** This may not always be the period immediately following. The periods used in the historical session can be randomly defined during the creation of the session.
Auto-update		By selecting this icon, the user enters auto-replay mode. The previous and next icons will no longer be displayed.

Historical Playback Information page

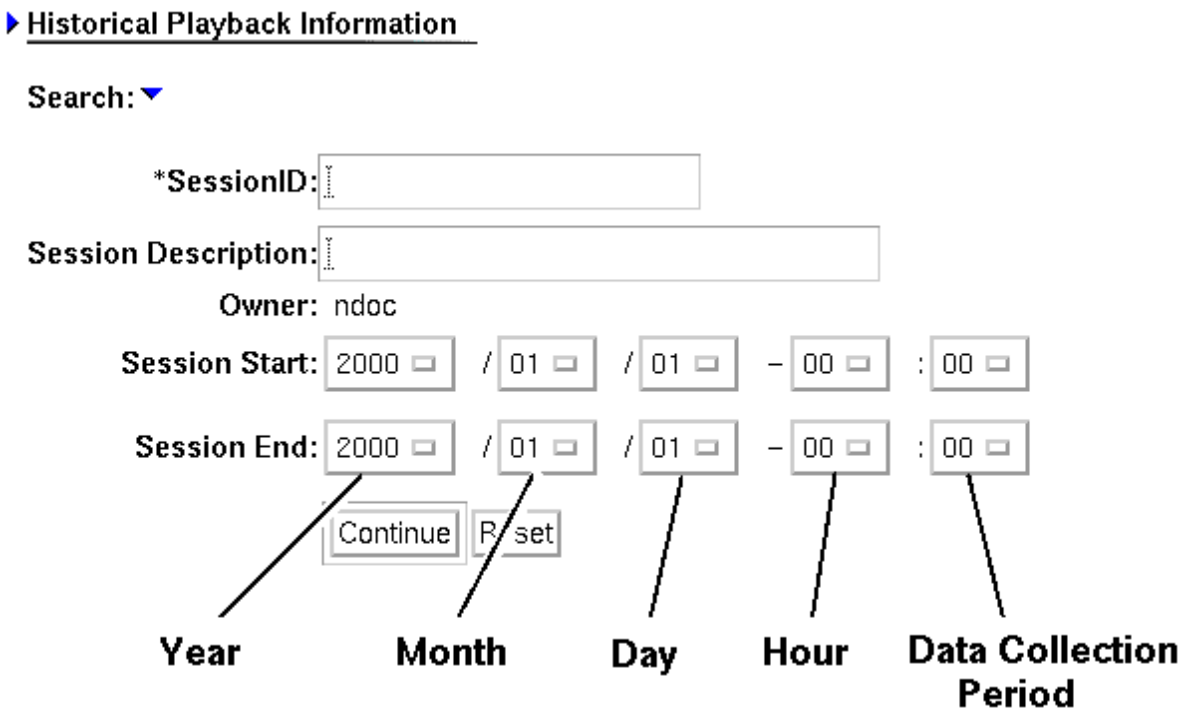
Purpose

Selecting the “New” toolbar button from the search result container page will access the new Historical Playback Information page (Figure 7). Constraints for setting up historical data sessions are:

- Only two historical sessions can be active on a host.
- An historical data session cannot span more than 48 hours.
- All pages shown on the GUI (Graphic User Interface) display data for the same data collection period.
- Only data in the current or historical databases can be used in Historical Data sessions.

Reference: “Reference data” (p. 2) in the *System Overview*

Figure 10 New Historical Playback Information page



Network Views (map) administration

Overview

Purpose

There are several user definable preferences that can be customized to provide the optimal use of the system and define individual preferences. These include:

- Network Views
- Styles
- Alert Groups
- Shape Facets

Contents

This section contains the following topics:

Network View Administration	9-26
Network View Style Administration	9-30
Network View Alert Group Administration	9-33
Network View Shape Facet Administration	9-36

Network View Administration

Overview

Users who have editing permission have access to network view administration through the GUI so they can select thumbnail images, labels, background images, and more.

Accessing the page

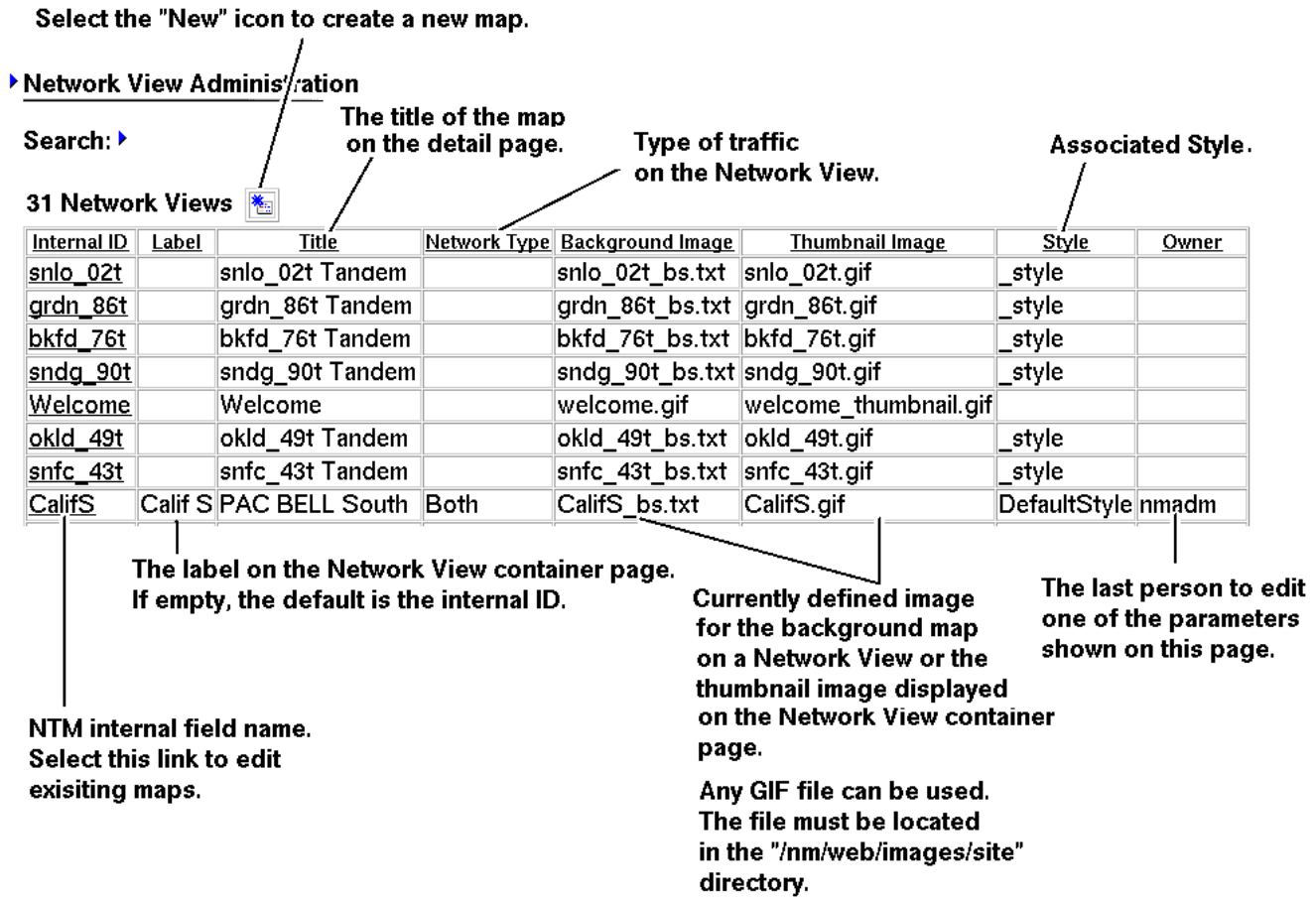
The Network View administration page (Figure 11) is accessed by selecting “Network Views” from the Administration launch page (Figure 1) or through “Network View Administration” on the navigation links while on a network view.

Using the page

Selecting the Network View Administration navigation link displays the Network View Administration page (Figure 11). The user can:

- Select the underlined Internal ID to edit an existing map
- Create a new map using the “New” toolbar icon

Figure 11 Network View Administration page

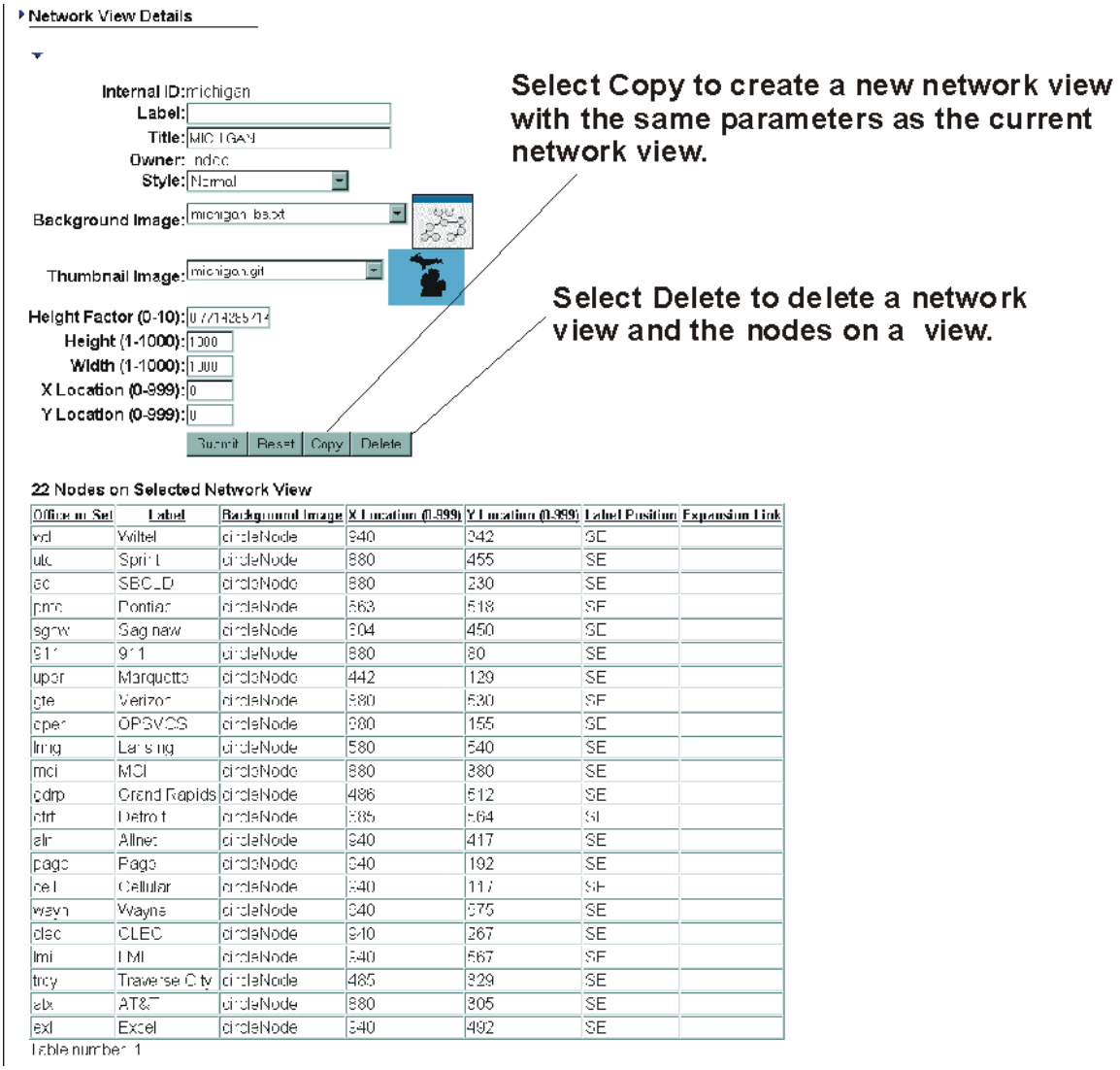


Existing maps

The Network View Details page (Figure 12) appears after selecting the underlined link on the Network Views Editing page (Figure 11).

This display allows the user to change properties for existing displays for things such as label, office type, image size and location. The Network View Details page will display all the nodes currently residing on a network view. It is also possible to delete maps using the “Delete” button on this page.

Figure 12 Network View Details



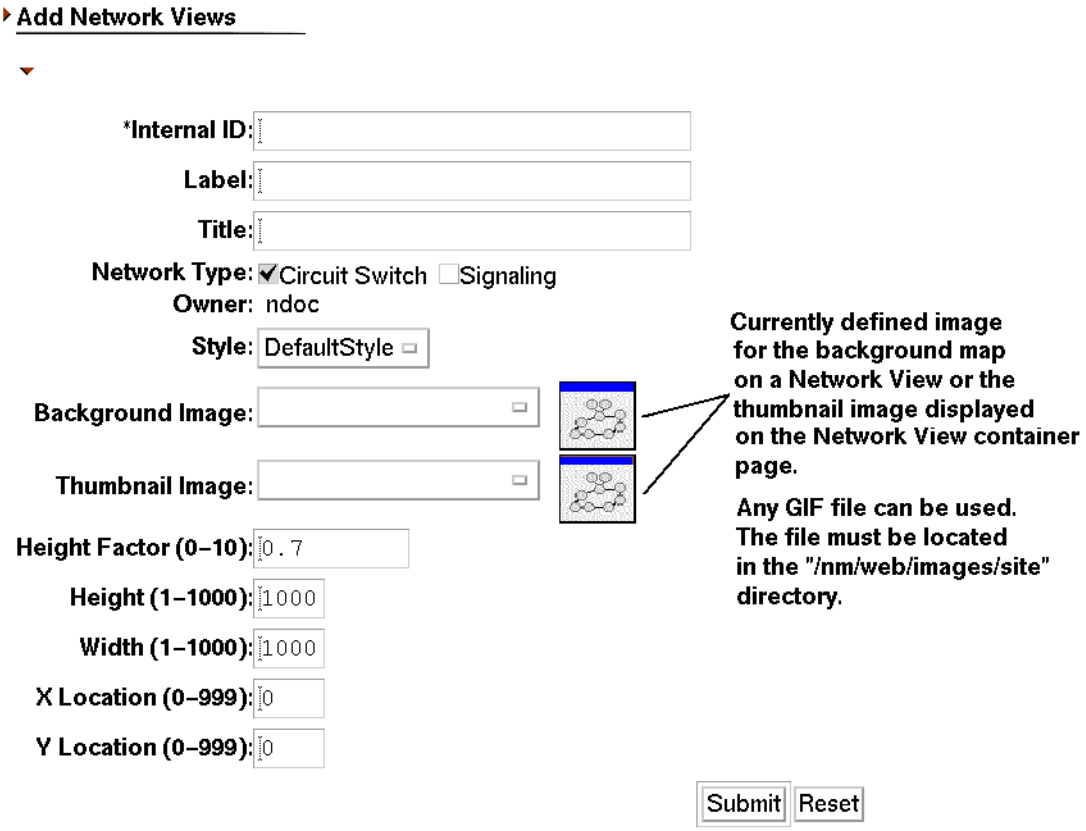
Notes:

1. Background images for maps converted from existing DCS maps show only the default icon. However, the map displays properly in the Network View mode.
2. Any GIF image can be used for the background or thumbnail image. The GIF file must be in the “/nm/web/images/site” directory.

New maps

The Add Network Views display (Figure 13) appears after the “New” icon has been selected from the Network View Administration page (Figure 11). The display appears with no default images or labels defined. It does provide defaults for image size and location.

Figure 13 Add Network Views page



Network View Style Administration

Purpose

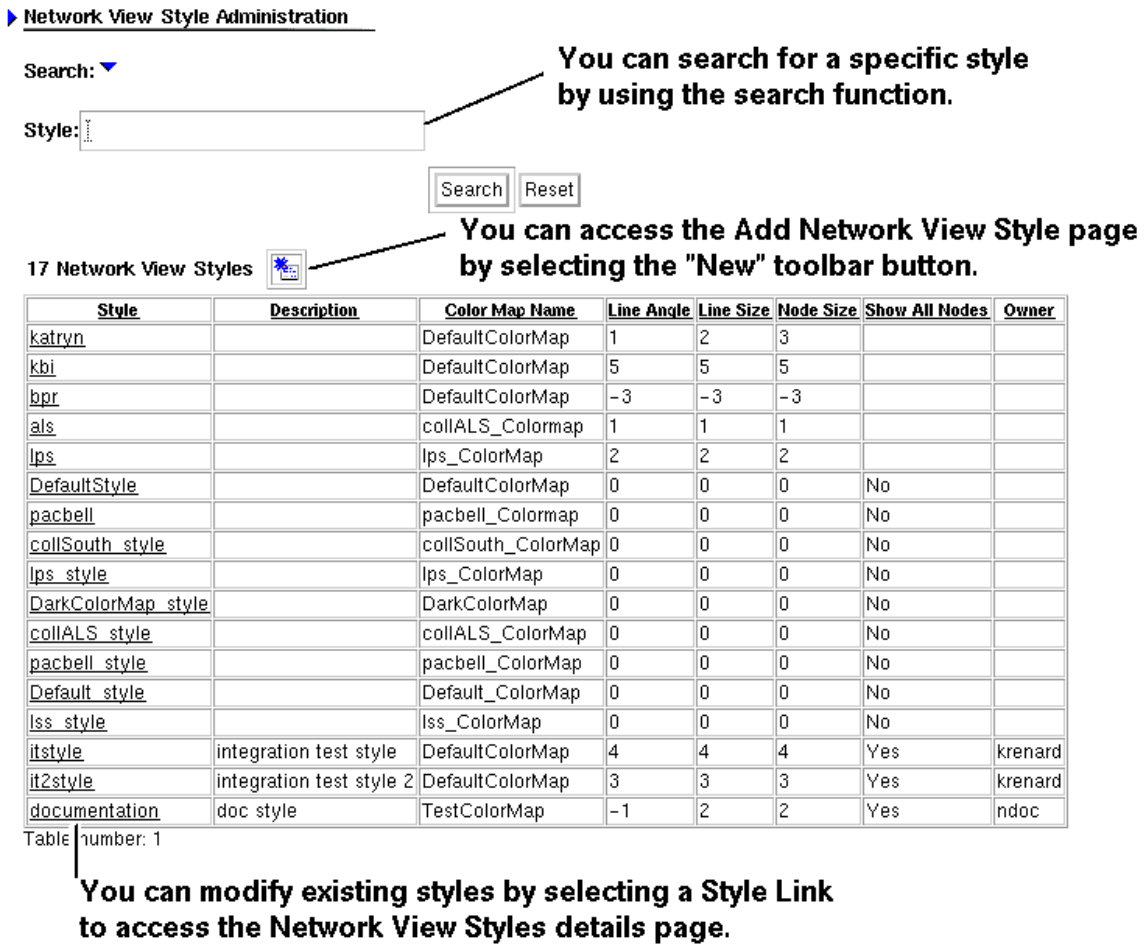
Users can select various attributes to be applied to network views. The Style Administration page allows the user to search and modify a specific style or to create a new one.

Accessing the page

The Network View Style Administration page (Figure 14) is accessed by selecting “Styles” from the Administration launch page (Figure 1) or through “Style Administration” on the navigation links while on a network view.

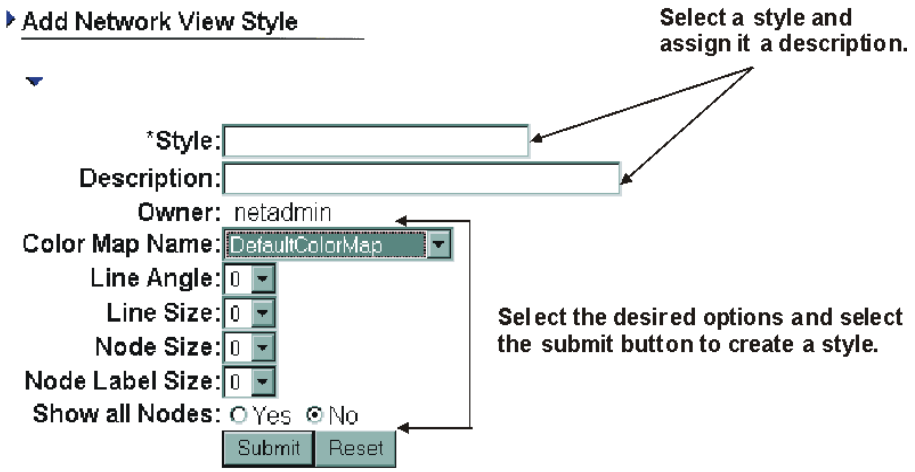
Reference: “Network View Administration” (p. 26)

Figure 14 Network View Style Administration page



Style	Description	Color Map Name	Line Angle	Line Size	Node Size	Show All Nodes	Owner
katryn		DefaultColorMap	1	2	3		
kbi		DefaultColorMap	5	5	5		
bpr		DefaultColorMap	-3	-3	-3		
als		collALS_Colormap	1	1	1		
lps		lps_ColorMap	2	2	2		
DefaultStyle		DefaultColorMap	0	0	0	No	
pacbell		pacbell_Colormap	0	0	0	No	
collSouth_style		collSouth_ColorMap	0	0	0	No	
lps_style		lps_ColorMap	0	0	0	No	
DarkColorMap_style		DarkColorMap	0	0	0	No	
collALS_style		collALS_ColorMap	0	0	0	No	
pacbell_style		pacbell_ColorMap	0	0	0	No	
Default_style		Default_ColorMap	0	0	0	No	
lss_style		lss_ColorMap	0	0	0	No	
itstyle	integration test style	DefaultColorMap	4	4	4	Yes	krenard
it2style	integration test style 2	DefaultColorMap	3	3	3	Yes	krenard
documentation	doc style	TestColorMap	-1	2	2	Yes	ndoc

Figure 15 Add Network View Style page



Network View Alert Group Administration

Purpose

The Alert Group Administration function allows users to associate alert groups with alert types to customize their Alerts table.

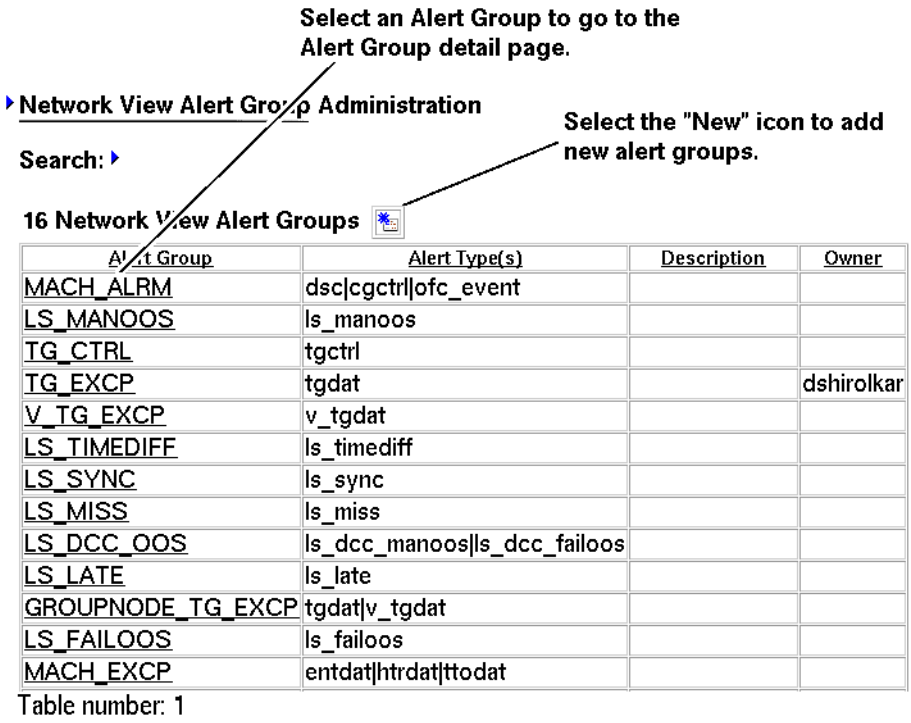
Accessing the page

The Alert Group Administration page (Figure 16) is accessed by selecting “Alert Groups” from the Administration launch page (Figure 1) or through “Alert Group Administration” on the navigation links while on a network view.

Container page

The Network View Alert Group Administration container page (Figure 16) contains a data table in which the results of a search are shown. The Alert Group Reference displays allow the user to add, delete, or modify the alert groups that are used to map alerting information to the facets of the Network View node shapes. Access to the Alert Group Administration container page, however, is limited to users with the Network View Administration permission.

Figure 16 Network View Alert Group Administration container page



Alert Group	Alert Type(s)	Description	Owner
MACH_ALRM	dsc|cgctrl|ofc_event		
LS_MANOOS	ls_manoos		
TG_CTRL	tgctrl		
TG_EXCP	tgdat		dshirolkar
V_TG_EXCP	v_tgdat		
LS_TIMEDIFF	ls_timediff		
LS_SYNC	ls_sync		
LS_MISS	ls_miss		
LS_DCC_OOS	ls_dcc_manoos|ls_dcc_failoos		
LS_LATE	ls_late		
GROUPNODE_TG_EXCP	tgdat|v_tgdat		
LS_FAILOOS	ls_failoos		
MACH_EXCP	entdat|htrdat|ttodat		

Table number: 1

Important! To view changes, the Network View Server should be restarted. See "Restarting the network view server" (p. 52).

Network View Alert Group Details page

The Network View Alert Group Details page displays the alert types for a particular alert group. It has two modes. If it is launched from the New Toolbar icon of the Network View Alert Group Administration container page, the detail page is in new mode (Figure 17). If it is launched from the search icon, the detail page is in modify mode (Figure 18).

Figure 17 Add Network View Alert Group

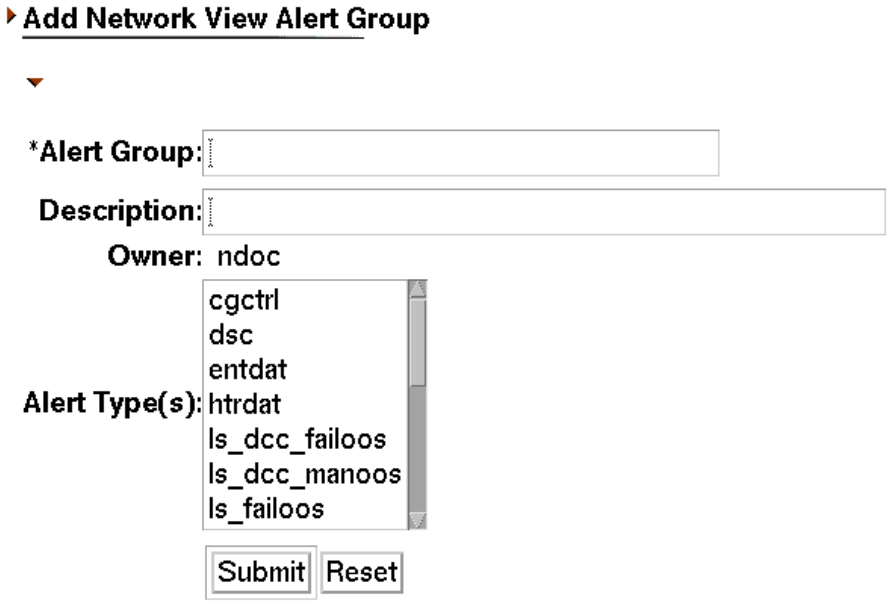
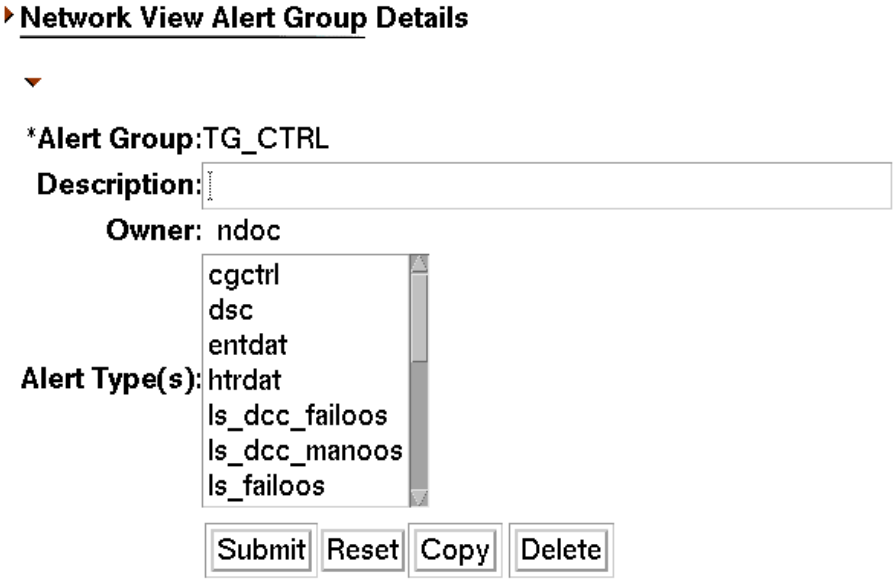


Figure 18 Network View Alert Group Details Page



Network View Shape Facet Administration

Purpose

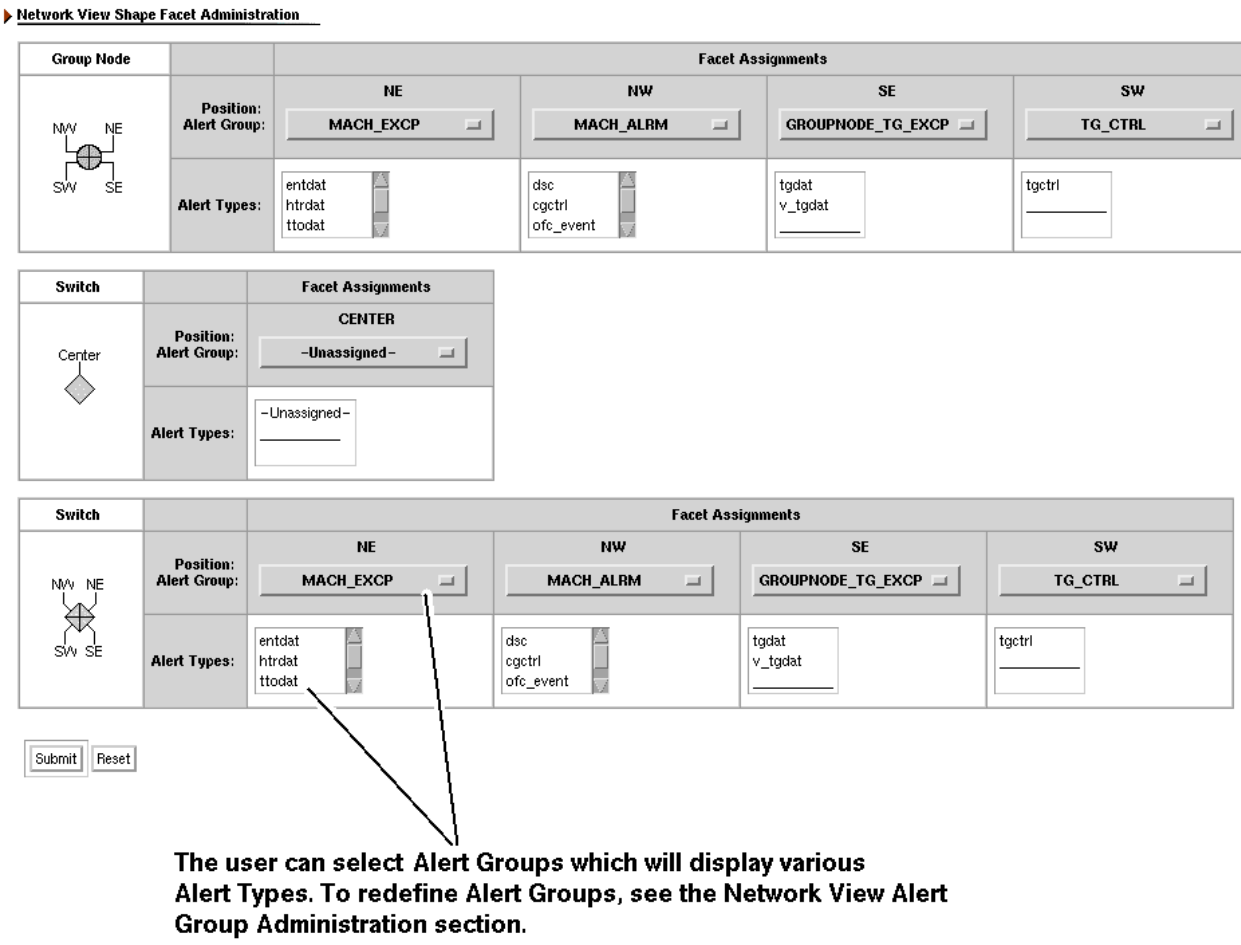
The Shape Facet Administration page (Figure 19) allows users to assign alert groups to the facets of the various Network Views.

Accessing the page

The Shape Facet Administration page (Figure 19) is accessed by selecting “Shape Facets” from the Administration launch page (Figure 1) or through “Shape Facet Administration” on the navigation links while on a network view.

Reference: “Network View Alert Group Administration” (p. 33)

Figure 19 Network View Shape Facet Administration



Important! To view changes, the Network View Server should be restarted. See "Restarting the network view server" (p. 52).

Parameter Sets administration

Overview

Purpose

The Parameter Sets page (Figure 20) lists the parameter sets that are available for the appropriate control category. Each parameter set links to a Parameter Set detail page (Figure 21) that can be used to view and edit the details of the set.

Contents

This section contains the following topics:

Parameter Sets container page	9-40
Parameter Sets detail pages	9-41

Parameter Sets container page

Purpose

The Parameter Sets page can be accessed by selecting “Parameter Sets” from the Administration launch page (Figure 1). The Parameter Sets container page can also be accessed via navigation links from all Code Control, Protective TG Control and Other Control pages (the Expansive TG Control pages do not use Parameter Sets).

Figure 20 Parameter Sets page — Code controls

Parameter Sets

Code Control Protective Trunk Group Control Other Controls

10 Code Control Parameter Sets

Name	Control Type	Default	Description	Owner
Gap None	cg		Gap none for all network element types.	System
Gap 10 Calls per 5-Minutes	cg		Gap rate of 10 calls per 5-minutes for all network element types.	System
Gap 20 Calls per 5-Minutes	cg		Gap rate of 20 calls per 5-minutes for all network element types.	System
Gap 150 Calls per 5-Minutes	cg		Gap rate of 150 calls per 5-minutes for all network element types.	System
Gap 300 Calls per 5-Minutes	cg		Gap rate of 300 calls per 5-minutes for all network element types.	System
Gap 30 Calls per 5-Minutes	cg		Gap rate of 30 calls per 5-minutes for all network element types.	System
Gap All	cg		Gap all calls for all network element types.	System
Gap 600 Calls per 5-Minutes	cg		Gap rate of 600 calls per 5-minutes for all network element types	System
Gap 60 Calls per 5-Minutes	cg		Gap rate of 60 calls per 5-minutes for all network element types.	System
Gap 5 Calls per 5-Minutes	cg	✓	Gap rate of 5 calls per 5-minutes for all network types.	netadmin

Table number: 1

Parameter Sets detail pages

Purpose

The Parameter Sets detail page is accessed via the “New” toolbar button or links in the Name column of the Parameter Sets container page. This page displays the parameter selections for a particular parameter set.

Page modes

The Parameter Set detail page has three modes:

- View Only Mode — Without administration permission
  - Allows you to view a parameter set as output only
- Modify Mode — selected from the link in the Name column
  - Allows you to modify or delete an existing parameter set
  - Control parameters are represented using menus and picklists
- New Mode — Accessed through the “New” toolbar button
  - Allows you to specify a new parameter set.
  - Change the control type attribute which changes the contents of the control parameter table
  - Control parameters are represented using menus and picklists

Important! If you do not have permission to create or modify parameter sets, they are displayed as “view only”.

Figure

Figure 21 shows an example of a Parameter Sets detail page.

Figure 21 Parameter Sets detail page: Call gap control, New mode

Link Status Shape Facet Administration

Purpose

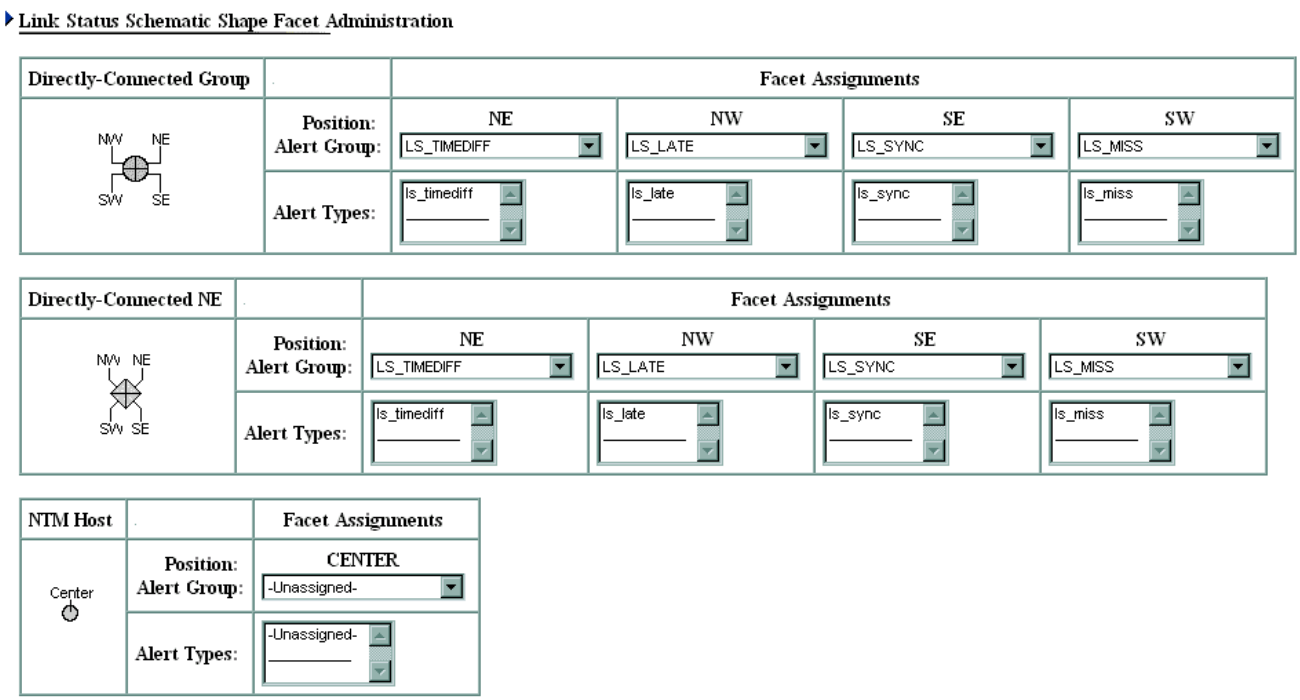
The Link Status Shape Facet Administration page (Figure 22) allows users to assign alert groups to the facets of the Link Status Schematic node shapes.

Accessing the page

The Link Status Shape Facet Administration page (Figure 22) is accessed by selecting "Link Status Shape Facets" from the Administration launch page (Figure 1) or through "Shape Facet Administration" on the navigation links while on a the Link Status Schematic.

Reference: "Link Status Schematic" (p. 7)

Figure 22 Link Status Shape Facet Administration



Important! To view changes, the Network View Server should be restarted. See "Restarting the network view server" (p. 52).

Client Downloads

Purpose

The Client Downloads links allow access to files necessary for browsers to display information in alerts tables, discretes, maps and System Status Display pages. Under this section the link to download latest Java plugin is available.

Important! Users must have permission to download and install these files.

Feature Listing

Purpose

By selecting the Show Features link a search window will be returned. From this search window you can select either; enabled, disabled or all features available on your system.

For more information regarding feature descriptions, see the Purchasable Features description in the *System Overview* guide.

General tasks on the Administration pages

Overview

Purpose

This section provides the procedures for general tasks on the Administration pages.

Contents

This section contains the following topics:

Changing user defaults	9-48
Changing user permissions	9-50
Changing passwords	9-51
Restarting the network view server	9-52
Starting and stopping the web server	9-53
Starting and stopping the LDAP server	9-54
Adding users	9-55
Deleting users	9-57
Changing a table layout	9-58
Creating a table layout	9-59
Creating a network view style	9-60
Creating a historical session	9-61
Making a historical session active	9-63
Changing a parameter set	9-65
Creating a parameter set	9-66

Changing user defaults

Instructions

Follow these steps to change user defaults:

Important! Any user may change their default settings.

1 Click the Web User Administration link in the Navigation Frame on the NTM Launch page.

Result: The Web User Administration window appears.

2 Make changes by selecting the desired options.

3 Select the Submit button.

Result: Changes are submitted to the server.

END OF STEPS

□

Changing skins

Instructions

Follow these steps to change your browser default skin:

Important! Any user may change their skin settings.

1 Click the Web User Administration link in the Navigation Frame on the NTM Launch page.

Result: The Web User Administration window appears.

2 Make changes by selecting the desired skin option.

3 Select the Submit button.

Result: Changes are submitted to the server.

Important! A new skin will not be reflected until another GUI page is selected.

END OF STEPS

□

Changing user permissions

Instructions

Follow these steps to change user permissions:

Important! System Administrators may change permissions.

1 Click the Administration link in the Navigation Frame on the NTM Launch page.

Result: The Administration Launch page appears.

2 Select the Web User icon.

Result: The Web User Administration window appears.

3 Review or change a user's permissions by clicking on the Web User ID shown in the list.

4 Web user permissions are changed by making selecting the checkbox labeled "Permissions". To allow permission for Network View, Table Layout, or Parameter Sets select the desired pick boxes.

5 Select the Submit button.

Result: Changes are submitted to the server.

END OF STEPS

□

Changing passwords

Instructions

Follow these steps to change passwords:

Important! Administrators may change password parameters by setting defaults in the *"/nm/web/sup_soft/http/conf/pwa.conf"* file.

Reference: "Password administration" (p. 7)

1 Click the Administration link in the Navigation Frame on the NTM Launch page.

Result: The Administration Launch page (Figure 1) appears.

2 Select the Change Password option.

Result: The Change Password window appears.

3 Enter the desired password in the Password field.

4 Re-enter the password in Verify Password field.

5 Select the Submit button.

Result: The User is immediately prompted to enter the new password before any action can be taken through the GUI.

6 Enter the new password entered in Step 3.

END OF STEPS

□

Restarting the network view server

Purpose

This procedure must be done to display changes made by editing or adding network views.

Reference: “Network View Administration” (p. 26)

Instructions

Follow these steps to restart the network view server:

1 While viewing a map, select “Network View Server” from the navigation links.

Result: The Network View Server Administration window (Figure 23) appears.

2 Select the “Restart Server” button to stop and restart the Network View Server.

END OF STEPS

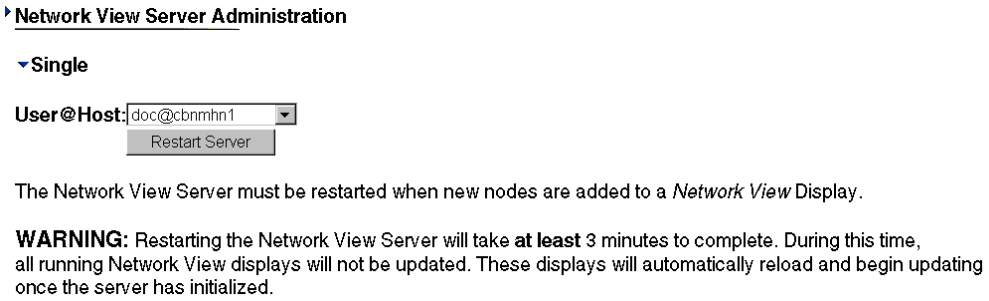
Figure

Figure 23 provides an example of a Network View Server Administration page.

WARNING

Please note the warning on this page pertaining to this task. It may result in a temporary loss of network monitoring on the Network Views.

Figure 23 Network View Server Administration



Starting and stopping the web server

Instructions

Follow these steps to start or stop the web server:

Important! All NTM Web GUI access will be denied while the web server is stopped.

1 Log in as `nmadm`

2 Restart the server:

- To restart the Server, enter `/sbin/service ntm_webserver restart`

END OF STEPS

□

Starting and stopping the LDAP server

Instructions

Follow these steps to start or stop the LDAP server:

Important! All NTM Web GUI access will be denied while the web server is stopped.

Important! The `service` command in 8920 NTM software uses parameter *`ntm_ldap`*. In order to start/stop ldap service execute the following command: `service ntm_ldap start/stop` instead of `service ldap start/stop`.

1 Log in to the NTM host as `nmadm`

2 Enter: `cd /nm/web/sup_soft/ldap/bin`

3 Stop or start the server:

- To stop the Server, enter `./stop`
- To start the Server, enter `./start`

Result: The “slapd” process should always start unless one is already running in which case an “address already in use” message will be displayed.

The “slurpd” process will only be started on hosts configured as a supplier for LDAP replication.

Hint: In order to start or stop LDAP server you will be asked to provide nmadm password.

END OF STEPS

□

Adding users

Instructions

Follow these steps to add users:

Important! Users should be added following the procedures found in Chapter 2, "Adding and Removing Users on the Host" in the *System Administration Guide*.

1 Click the Administration link in the Navigation Frame on the NTM Launch page.

Result: The Administration Launch page (Figure 1) appears.

2 Select the Web User icon.

Result: The Web User Administration window (Figure 3) appears.

3 Click on the "New" toolbar button.

Hint: To review or change a user's permissions, click on the Web User ID shown in the list.

Result: The Web User Information form appears.

4 Enter the new user's information

5 Select the Submit button.

Result: Changes are submitted to the server.

Important! Important! In order to use all capabilities of the `GUI`, when creating a new `GUI` user the `GUI` user's assocaited `Host UID(s)` should belong to one of the following default groups *snm, nm, ntmgui*. If the provided Host UID belongs to a group different than one of these then the group name must be added to the following sudoers entry:

```
nsadmin,root ALL=(%nsgroup, %nm, %snm, %ntmgui) NOPASSWD:ALL
```

Example:

```
nsadmin,root ALL=(%nsgroup, %nm, %snm, %ntmgui,%newgroup) NOPASSWD:ALL
```

where: %newgroup represents the additional user group to be supported by the GUI

END OF STEPS

Deleting users

Instructions

Follow these steps to delete users:

Important! Users should be deleted following the procedures found in Chapter 2, "Adding and Removing Users on the Host" in the *System Administration Guide*.

1 Click the Administration link in the Navigation Frame on the NTM Launch page.

Result: The Administration Launch page (Figure 1) appears.

2 Select the Web User icon.

Result: The Web User Administration window (Figure 3) appears.

3 Click on the Web User ID shown in the list.

Result: The Web User Information window (Figure 2) appears.

4 Select the Delete button.

Result: A conformation window appears.

5 Select OK.

Result: Changes are submitted to the server.

END OF STEPS

□

Changing a table layout

Instructions

Follow these steps to change a table layout:

Important! Users must have Table Layout Administration permission to change table layouts.

1 Click the Administration link in the Navigation Frame on the NTM Launch page.

Result: The Administration Launch page (Figure 1) appears.

2 Select the Table Layout icon.

Result: The Table Layout search window appears (Figure 5).

3 Select the table layout type desired and select search.

Result: All default table layouts will appear (Figure 6).

4 Select the table layout to be changed by selecting the table name from the Layout Name column.

Result: A Table Layout window will appear displaying the fields as currently defined.

5 Make the changes as needed.

6 Select the Submit button.

Result: Changes are submitted to the server.

END OF STEPS

□

Creating a table layout

Instructions

Follow these steps to create a table layout:

Important! Users must have Table Layout Administration permission to create a table layout.

1 Click the Administration link in the Navigation Frame on the NTM Launch page.

Result: The Administration Launch page (Figure 1) appears.

2 Select the Table Layout icon.

Result: The Table Layout search window appears (Figure 5).

3 Select the table layout type desired and select search.

Result: All default table layouts will appear (Figure 6).

4 Select the “New” toolbar button.

Result: A Table Layout window (Figure 7) will appear displaying the fields available to be used.

5 Make the changes as needed.

6 Select the Submit button.

Result: Changes are submitted to the server.

END OF STEPS

□

Creating a network view style

Instructions

Follow these steps to create a network view style:

Important! Users must have Network View Administration permission to create a style.

1 Click the Administration link in the Navigation Frame on the NTM Launch page or the Style Administration link from the navigation links while on a network view.

Result: The Administration Launch page (Figure 1) appears.

2 If accessed through the Administration link then select the Network View icon.

Result: The Network View Style Administration window appears (Figure 14).

3 Click on the “New” toolbar button.

Hint: To modify or change an existing style, click on the Style name shown in the list.

Result: The Add Network View Style form (Figure 15) appears.

4 Add the information into the form.

5 Select the Submit button.

Result: Changes are submitted to the server.

END OF STEPS

□

Creating a historical session

Instructions

Follow these steps to create a historical session:

Important! Users must have Historical Playback Administration permission to create a session.

1 Click the Administration link in the Navigation Frame on the NTM Launch page.

Result: The Administration Launch page (Figure 1) appears.

2 Select the Historical Session icon.

Result: The Historical Session Administration Search window appears.

3 Perform a search.

Result: All sessions requested are displayed.

4 Click on the “New” toolbar button.

Hint: To modify or change an existing style, click on the Historical Session ID shown in the list.

Result: The Historical Playback Information form (Figure 10) appears.

5 Add the information into the form.

Result: A data collection period list appears

6 Select any or all the periods to be placed in the historical session.

7 Select the Submit button.

Result: Changes are submitted to the server.

END OF STEPS

Making a historical session active

Instructions

Follow these steps to make a historical session action:

Notes:

1. Users must have Historical Playback Administration permission to create a session.
2. Only two sessions can be active at any time.

1 Click the Administration link in the Navigation Frame on the NTM Launch page.

Result: The Administration Launch page (Figure 1) appears.

2 Select the Historical Session icon.

Result: The Historical Session Administration Search window appears.

3 Perform a search for all session.

Result: All sessions available are displayed.

4 If two sessions are currently active, one must be inactivated before another session can be made active. To do this, select the active session you wish to deactivate by clicking on the session ID.

Result: The Historical Playback Information form (Figure 10) appears with the selected session defined.

5 Change the status button to Inactive.

6 Select the Submit button.

Result: Changes are submitted to the server.

7 Select the session you wish to make active.

Result: The Historical Playback Information form (Figure 10) appears with the selected session defined.

8 Change the status button to Active.

9 Select the Submit button.

Result: Changes are submitted to the server.

END OF STEPS

□

Changing a parameter set

Instructions

Follow these steps to change a parameter set:

Important! Users must have Control Parameter Set Administration permission to change parameter sets.

1 Click the Administration link in the Navigation Frame on the NTM Launch page.

Result: The Administration Launch page (Figure 1) appears.

2 Select the Parameter Sets icon.

Result: The Parameter Sets container window appears (Figure 20).

3 Select the parameter set desired by clicking on the Set name in the Name column.

Result: The Parameter Sets Detail page appears (Figure 21).

4 Make the changes as needed.

5 Select the Submit button.

Result: Changes are submitted to the server.

END OF STEPS

□

Creating a parameter set

Instructions

Follow these steps to create a parameter set:

Important! Users must have Control Parameter Set Administration permission to create Parameter Sets.

1 Click the Administration link in the Navigation Frame on the NTM Launch page.

Result: The Administration Launch page (Figure 1) appears.

2 Select the Parameter Sets icon.

Result: The Parameter Sets container window appears (Figure 20).

3 Click on the “New” toolbar button.

Result: The Parameter Sets Detail form appears.

4 Add the information into the form.

5 Select the Submit button.

Result: Changes are submitted to the server.

END OF STEPS

□

10 Searching using Modifiers and Regular Expressions

Overview

Purpose

Modifiers and regular expressions can be used to create very specific searches in NTM. They can be used to find specific switches or trunk groups, or sets of network elements or trunk groups even if you only know part of the name.

Contents

This appendix contains the following topics:

Modifiers and Regular expressions	10-2
Modifiers	10-3
Examples of Modifiers	10-4
Additional Examples of Regular Expressions	10-6
Regular expression reference for NTM	10-7

Modifiers and Regular expressions

Overview

Modifiers and Regular expressions may be used with the fields on many NTM search pages used to specify:

- network elements
- sets
- trunk group suffixes
- link Ids
- User Comment fields

Refine button

To use modifiers and regular expressions in these fields, enter the modifier or regular expression in the field and click on the REFINE button associated with the field or the SEARCH button at the bottom of the page.

If you enter a modifier or regular expression in the field and click the REFINE button, you will get a list of network elements or set names that match your criteria. Enter "/." and click the REFINE button to list all available network elements. You may then select a network element or set from this list and retrieve data on that network element or set.

Important! If you enter a regular expression in a search field and tab without completely identifying a network element the system will not complete the name.

Important! If you leave a blank search field and click the REFINE button the system will not provide any information or reply with an empty list of network elements.

Search button

If you click the SEARCH button, you get a container page showing data for the network elements whose names or set assignments match your modifier or regular expression. In the case of the User Comment field, you will get a container page showing the mark assignments and comments for the trunk group(s) that match your search.

Important! Using modifiers or regular expressions should not be confused with the "Completion" operation that occurs with network element and sets fields. "Completion" results from tabbing out of a field and allowing the system to finish the network element or set name. Completion will return the closest match for the substring as defined in the RSPTE File.

Modifiers

Purpose

Modifiers are a broad category of search syntaxes that allows a user to restrict the data displayed by specifically narrowing the criteria through the use of modifiers in the input fields. A common subset of modifiers referred to in this appendix are called regular expressions.

Required

For modifiers to work correctly user must always preceded the modifier with “/”.

Poorly formed modifiers

The following are an either poorly formed modifiers or entirely incorrect examples of using a modifier.

A poorly formed modifier would be using part of an office name without a leading “/”. Without the '/' leading indicator, the partial office name would be looked up using the auto-completion and the system would determine the closest office name in the rspte file. Suffix and most other text like input fields are taken at face value.

Incorrectly formed search criteria

An incorrectly formed search would be entering some part of a search string followed by an asterisk in a Network Element search field. An example of this would be:

```
portlan*
```

This does not mean anything to NTM system, and would be taken as the literal string 'portlan*' with the SQL fragment looking like “ENT_ID = 'portlan*'”.

> **Important!** Using regular expressions should not be confused with the “Completion” operation that occurs with network element and sets fields. “Completion” results from tabbing out of a field and allowing the system to finish the network element or set name. Completion will return the closest match for the substring as defined in the RSPTE File.

□

Examples of Modifiers

Like operation against a search string

This operation supports the ANSI sql LIKE operator, i.e. the use of '%' and the like.

```
/lk/searchstring%
```

If used in the CLLI field the SQL fragment would look like “ENT_ID LIKE '*searchstring*%'”, i.e. “Find all things that start with the *searchstring* and end in anything else”.

Not Like operation against a search string

```
/nlk/searchstring%
```

If used in the CLLI field this modifier would cause the following SQL fragment “ENT_ID NOT LIKE '*searchstring*%'”, i.e. “Find all things that DO NOT start with the *searchstring* and end with anything else”.

Enhanced regular expression match against a search string

```
/re/searchstring
```

If used in the CLLI field this modifier is very specific and would request that the extended regular expression be used in the SQL fragment “sys.ext_reg_cmp(ENT_ID,'*searchstring*') == 0", i.e. “Find all inputs that have the pattern '*searchstring*' in them”.

Another example would be:

```
/re/searchstring[0-9]
```

Find all of the inputs that have the pattern *searchstring* followed by the numbers 0 to 9 anyplace in them.

Inverse enhanced regular expression match against a search string

```
/nre/searchstring
```

If used in the CLLI field the inverse of an enhanced regular expression matched against a *searchstring* would occur. The SQL fragment would look like “sys.ext_reg_cmp(ENT_ID,'*searchstring*') != 0", i.e. “Find all inputs that do not have the pattern '*searchstring*' in them”.

Strict equals

An example of strict equals would be:

```
/eq/searchstring
```

For completeness, strict equals was added, but this one does not usually have to supply this

Not equals operation against a search string

An example of not equals operation against a *searchstring* would be:

```
/ne/searchstring
```

If this were used in the CLLI field this request for strict not equals the SQL fragment would look like “ENT_ID != '*searchstring*'”, i.e. “Find everything that is strictly not equal to “*searchstring*””.

Traditional Modifier

The original modifier was modified to look and see if it is possible to do a LIKE operation otherwise it will perform a regular expression operation.

For example, a simple pattern request would be:

```
/searchstring
```

If this were used in the CLLI field this would get turned into something like “ENT_ID LIKE '%*searchstring*%'” in the SQL fragment. You can use the LIKE operation to make something that is very similar to a “contains” operation.

For example, a more complex pattern request would be:

```
/searchstring|sneeze
```

This would get turned into the following on the where clause of the SQL “sys.ext_reg_cmp(ENT_ID,'*searchstring*|sneeze') == 0"

Another complex example would be:

```
/searchstring[0-9]
```

i.e. “Find all of the inputs that have the pattern *searchstring* followed by the numbers 0 to 9 anyplace in them”.

□

Additional Examples of Regular Expressions

Matching specific characters

The following regular expression matches all network element names that contain clmboh.

```
/clmboh
clmboh123, abclmboh, xyzclmboh123
```

Matching specific characters at the start of a string

The following regular expression matches all network element names that start with clmboh.

```
/^clmboh
clmboh123, clmbohabc, clmboh123xyz
```

Matching specific characters at the end of a string

The following regular expression matches all network element names that end with 51t.

```
/51t$
clmboh1251t, clvdoh3451t, chcgil5651t
```

Matching characters using OR

The following regular expression matches all network element names that start with lsan or grdn.

```
/^lsan|^grdn
lsanca0470t, lsanca07ds0, grdnca0250t, grdnca01ds0
```

Matching a range of characters

The following regular expression matches all network element names that start with lsan, contain one or more digits, and end in t. (Using this expression without the asterisk would return strings containing only one digit.)

```
/lsan[0-9]*t
lsanca0470t, lsanca070t, lsanca0250t
```

References

"Mastering Regular Expressions: Powerful Techniques for Perl and Other Tools", Jeffrey E. F. Friedl, O'Reilly Associates, 1st Edition January 1997, ISBN 1-56592-257-3

Regular expression reference for NTM

Table

Table 1 provides a list of regular expressions, their descriptions, and examples of their uses.

Table 1 Regular expression reference

Regular Expression	Description	Example
/ (slash)	Used to begin a regular expression. **Important!** The "/" must begin the regular expression to prevent the system from interpreting it as a literal string.	
^	Used to match strings starting with specified characters.	/^clmboh matches strings starting with clmboh
$	Used to match strings ending with specified characters.	/51t$ matches strings ending with 51t
Any alphanumeric character	Matches itself.	a matches a 9 matches 9
. (period)	Matches any character.	
| (vertical bar)	Inclusive OR.	/^lsan|^grdn matches strings starting with lsan or grdn.
[ ] (square brackets)	Used to indicate a range of characters.	[0-9] matches one of any digit from 0 to 9. [0-9]* matches zero or more of any digit from 0 to 9. (Note that this is not the same thing as the Linux asterisk.) /lsanca[0-9]t matches lsanca2t, lsanca8t, etc. /lsanca[0-9]*t matches lsanca0470t, lsanca0250t, etc.

Important! Your search will not be successful if the string you are searching for does not actually exist in your RSPTE File or Sets File.

11 Training Objectives and Exercises

Overview

Purpose

This Appendix contains objectives and exercises that accompany Alcatel-Lucent Learning course number OS3192.

Objectives

This course prepares network managers for duties as NTM network managers. Students learn to use the graphical user interface to view network data and apply controls. This course is designed to enable students to:

- Retrieve and view data using the NTM GUI
- Perform network management operations through the GUI

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, “Getting Started with the Browser-based GUI”

Objectives

This lesson is designed to teach you how to:

- Use each of the five basic types of pages.

- Recognize five of the GUI Form Elements.
- Interpret the Exception Level Indicators.
- Use the toolbar area.
- Interpret Error Messages.
- Explain Manual vs. Automatic Update mode.

Exercises

1 Circle each of the following that is ***not*** found on a container page?

- number of trunk groups displayed on the screen
- destination type
- total number of trunk groups that were retrieved by your search
- data collection
- set file name (if populated on the search page)

2 Match the GUI form elements in Column A with the function in Column B.

	Column A		Column B
___	Text Fields	**A**	Allows use of regular expressions to find network elements or set names.
___	Radio Buttons	**B**	Other form elements are a composite of the basic elements described above.
___	Refine Button	**C**	Used to submit requests to the web server.
___	Execute Button	**D**	Consists of a box into which values such as CLLI codes or network element names may be entered.
___	Composite Elements	**E**	Multiple buttons choices appear to the right of the label.

3 `True or False.` When the OEXL object appears in a tabular format, sorting is performed according to the highest OEXL in exception fields.

4 Match the Icon Names in Column A with the function in Column B.

	Column A		Column B
___	New	**A**	Launches the Network View Alerts window restricted to all alerts for this Network View.
___	Previous Period	**B**	Clicking this icon opens another browser window showing only the display without any of the browser buttons.
___	Projection Mode	**C**	Allows for addition of information.
___	Show Alerts	**D**	Changes current pages to show previous data collection period.

5 What indicates the occurrence of an execution error?

_____

_____

_____

6 Fill in the blanks. The search criteria may be changed only in _____ update mode. In _____ mode, the search criteria are displayed as output only.

Chapter 2, “Network Elements”

Objectives

This lesson is designed to teach you how to:

- Use the three Network Element pages.
- Describe Audits.

Exercises

1 Name the three data categories in the Network Element Data Types?

_____

_____

_____

2 On the Network Elements search page, what does User@<Host> mean?

_____

_____

3 What is an OEXL indicator?

_____

_____

4 What are the two main functions of an audit?

_____

_____

5 What are the two types of audits?

_____

_____

Chapter 3, “Network Connections”

Objectives

This lesson is designed to teach you how to:

- Retrieve data from Trunk Groups
- Retrieve signaling link measurements and linkset events

Exercises

1 In the search criteria on the Trunk Groups search page, give me an example of a data restriction you could use.

_____

2 What does a Triangle Node represent?

_____

3 What does a Circle Node represent?

_____

4 On your Notes page, draw a final trunk group and indicate the NearEndNE, the FarEndNE-Suffix, and the trunk group of interest?

5 Fill in the blank. Linkset data is collected every _____ minutes.

6 Do you need to fill in the User@Host drop down menu to retrieve signaling link measurements in the Advanced Search Mode?

_____

□

Chapter 4, “Network Views”

Objectives

This lesson is designed to teach you how to:

- Use the Network Views search/container page.
- Use the Network View Detail page to locate Maps and Nodes.

- Change Network Views.
- Access the Alerts Table pages.

Exercises

1 Match the search criteria in Column A with the function in Column B.

	Column A		Column B
___	TG-Set	**A**	This displays current ID and host information.
___	Style Override	**B**	This field allows the user to choose display Suspect Data.
___	User@Host	**C**	You can select the type of data displayed by restricting it to a specific alert type.
___	Finals Only	**D**	Selecting this option restricts the view to only trunk groups that belong to the selected set.
___	Alert Types	**E**	Select a "Style" to apply defined attributes to associate with a network view.
___	TG Threshold Level	**F**	This restricts the trunk groups displayed to Final Trunk Groups.
___	Suspect Data Filter	**G**	Minimum exception threshold level. Values are 1–10.

2 What two types of nodes are on the map?

_____

_____

3 Fill in the blank. You can link a node on the map display to another Network View using the Link Expansion field found by selecting the right mouse _____ button while over a node.

4 How can you add, move, modify, or delete text on the map display?

_____

5 Does the Alerts Table container page support manual and automatic updates?

_____

6 Can you access the Alerts Table through the navigation link while viewing the Network Views container page, individual network views or the Alerts Table icon?

_____

□

Chapter 5, “Controls”

Objectives

This lesson is designed to teach you how to:

- View, add and modify the three sub-type controls.
- Validate a Control Request.
- Set parameters.
- Use Control Request pages to apply Expansive and Protective Trunk Group Controls and Code Controls.

Exercises

1 What are the three major Controls sub-types?

_____

2 Can you manipulate both active and potential controls?

_____

3 Fill in the blank. Once controls have been retrieved, you may select one or more of them on which to perform the _____ action.

4 The Code Control Request page is displayed after the validation, with four differences. Name one of the differences.

_____

5 The parameter area provides two modes of operation. What are they?

_____

6 What is a parameter set?

_____

7 What is a potential control?

_____

□

Chapter 6, “Destinations”

Objectives

This lesson is designed to teach you how to:

- Use Destination Code pages to administer manual hard to reach assignments and automatic hard to reach parameters.

Exercises

1 In the Destination Codes search page you may restrict the display on a measurement, a value, and an operator. Give an example of how to set this field.

_____

2 Name the three things that Destination Assignments allows you to administer.

_____

_____

_____

3 `True or False.` For the Manual HTR Assignments search option, you may search for destination assignments by network element or code.

_____

4 Does Inhibited (I) retrieve data for a list of codes placed on the HTR list by a network element?

_____

5 Can you set the automatic HTR threshold definition? If so, how?

_____

6 The Automatic HTR Parameter Set Assignments page has a two-part search. For the initial search the user must select one of the following options that result in a second part of the search parameter being displayed. Give me ***one*** of the two options.

_____

□

Chapter 7, "Other Functions"

Objectives

This lesson is designed to teach you how to:

- Use Error Log pages to obtain different error messages.
- Navigate the Control Log to view current and historic information.
- Send and Receive Broadcast Messages.
- Use the Exception Status and Mark Assignment pages to administer Network Element and Trunk Group Exceptions.
- Use Audible Alarms to choose different alarms.
- Compare Alerts using the Discrete Alert to Alerts Using the Trunk Group Data Alerts.

Exercises

1 If you enter "minor" in the Error Log search page, what happens?

_____

_____

_____

2 On the Error Log Container page what does the cyan indicator mean?

_____

_____

3 `True or False.` A broadcast message page must be active in order for broadcast messages to appear.

4 On the Exception Status and Mark Assignment page, what happens after a mark or status is added or changed?

_____

_____

5 What happens when an alert is filtered?

_____

_____

□

Chapter 8, “Link Status”

Objectives

This lesson is designed to teach you how to:

- Use Link Status Table pages to obtain Link Status information.

Exercises

1 Does the Link Status container page support manual and automatic updates?

_____

□

Chapter 9, “GUI Administration”

Objectives

This lesson is designed to teach you how to:

- Access Web Info and Table Layouts with or without Web Administration permission and Passwords.

- Operate Historical Data Playback for the Browser-based GUI.
- Administer Network View attributes Network View Display (Map) Administration.
- Create, modify, and delete parameter sets.
- Administer Network View attributes for the Link Status Schematic.
- Access Browser Support files through the Client Download link.

Exercises

1 Name two ways a user can log onto the GUI as an administrator and perform administrative functions.

_____

_____

2 How many historical sessions can be active on a host?

_____

3 After selecting the Network View Administration navigation link and displaying the Network Views Editing page you can do the following:

_____

_____

_____

4 What are the three modes in the Parameter Set detail page?

_____

_____

_____

□

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).

T

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

A

Accessing the Network View Administration Function, 9-26, 9-30

Accessing the Shape Facet Administration Function, 9-36, 9-43

Adding a Node, 4-11

Adding and Modifying Automatic HTR Parameter Set Assignments, 6-24

Adding and Modifying Controls, 5-3

Adding and Modifying Manual Hard To Reach Assignments, 6-22

Adding Users, 9-55

Administer LSS Time Difference, 8-13

Administration
- Password, 9-7
- Shape Facet, 9-36, 9-43
- Web User, 9-3

Administration Launch Page, 9-4

Alarm/Discrete Indicator, 1-21

Alert Group Administration, 9-33

Alert Group Administration Container Page, 9-33

Alert Group Detail Page, 9-34

Alerts Table, 4-19

Alerts Table Container Page, 4-22

Alerts Table Search Page, 4-19

Analysis, Map, 4-6

Area, Map Page Search, 4-2

Area, Parameter, 5-6

Arrow Indicator, 1-23

Assignments
- Destination, 6-9
- Manual HTR, 6-10

Audits
- Search Criteria, 2-21

Audits Container Page, 2-23

Audits Details Page, 2-24

Automatic Hard To Reach Parameter Set Assignments Container Page, 6-17

Automatic HTR Parameter Set Assignments, 6-15

Automatic HTR Parameter Set Assignments – NANP All NPA, 6-16

Automatic HTR Parameter Set Assignments – NANP Home or Designated NPA, 6-16

Automatic HTR Parameter Set Assignments Search Criteria, 6-15

Automatic HTR Parameter Set Definitions (4ESS), 6-13

Automatic HTR Parameter Set Definitions Request Page, 6-13

Automatic HTR Parameter Set Definitions Search Criteria, 6-13

B

Broadcast Message
- Receiving a, 7-11
- Sending a, 7-11

Broadcast Messages, 7-11

C

Changing a Parameter Set, 9-65

Changing a Table Layout, 9-58

Changing Display Settings, 4-10

Changing Passwords, 9-51

Changing User Permissions, 9-50

Code Control Request Page, 5-13

Code Controls, 5-7

Code Controls Container Page, 5-11

Code Controls Search Page, 5-8

Codes
- Destination, 6-3

Container Page
- Alert Group Administration, 9-33
- Automatic Hard To Reach Parameter Set Assignments, 6-17
- Error Log, 7-5
- Historical Session, 9-20

Link Status, 8-5

Links/Linksets, 3-21, 3-27

Manual HTR Assignments, 6-11

Network Elements, 2-8

Parameter Sets, 9-40

Table Layout, 9-15

Container Page, Audits, 2-23

Container Page, Code Controls, 5-11

Container Page, Expansive TG Control, 5-35

Container Page, Network Elements, 2-8

Container Page, Protective TG Controls, 5-22

Container Page, Trunk Groups, 3-7

Container Pages, 1-12

Control Log Display, 7-8

Control Log Search Page, 7-8

Control Pages, General Tasks on the, 5-57

Controls, 3-14

Controls Sub-Type Selection, 5-2

Controls, Code, 5-7

Controls, Expansive TG, 5-27

Controls, Protective TG, 5-19

Controls, Viewing, 5-2

Creating a Historical Session, 9-61

Creating a Network View Style, 9-60

Creating a New Historical Session, 9-23

Creating a New Table Layout, 9-16

Creating a Parameter Set, 9-66

Creating a Table Layout, 9-59

Creating New Nodes, Text or Timestamp, 4-9

D

Data Presentation, 2-11, 2-12

Data Table View
Network Elements Container Page, 2-8, 8-27

Data Table View for Discrete Data
Network Elements Container Page, 2-9

Data Types
Network Element, 2-4

Data Types, Network Element, 2-4

Deleting a Control, 5-4

Deleting a Node, 4-12

Deleting Users, 9-57

Destination Assignments, 6-9

Destination Codes, 6-3

Destination Codes Container Page, 6-6

Destination Codes Details Page, 6-7

Destination Codes Search Criteria, 6-4

Destination Codes Search Page, 6-4

Destination Pages
General Tasks on the, 6-19

Detail Page
Alert Group, 9-34

Network Views, 4-5

Parameter Set, 9-41

Details Page
Expansive TG Control, 5-36

Details Page, Audits, 2-24

Details Page, Network Element, 2-11

Details Page, Trunk Group, 3-8

Details Pages, 1-14

Discrete Indicator, 1-21

Display Options
Network Views, 4-8

Display Options, Network (Map), 4-8

Display, Control Log, 7-8

Displaying the Screen in Projection Mode, 4-9

E

Editing Map Nodes, 4-31, 4-37, 4-39, 4-40

Element Types, Output, 1-21

Error
Execution, 1-26

Presentation, 1-26

System, 1-26

Error Log, 7-3

Error Log Container Page, 7-5

Error Presentation, 1-26

Exceeding the Defined Thresholds, 9-8

Exception List View
Network Element Container Page, 2-9

Excluding Users from Password Thresholds, 9-9

Executing a Control Request, 5-4

Execution Errors, 1-26

Existing Maps, 9-27

Expansive TG Control Container Page, 5-35

Expansive TG Control Details Page, 5-36

Expansive TG Control Request Page, 5-37

Expansive TG Controls, 5-27

Expansive TG Controls Search Page, 5-30

F

Facets of Nodes, 4-6

Facets Shapes and Alert Information, 8-11
File
Error Log, 7-3
HTR, 11-1

G General Tasks on the Control Pages, 5-57
General Tasks on the Destination Pages, 6-19
General Tasks on the Map Pages, 4-31
General Tasks on the Network Views Pages, 4-31
Graphic User Interface (GUI) and Browsers, 1-3
GUI Form Elements, 1-20

H Hiding/Showing an Area, 1-23
Historical Session
Creating a New, 9-23
Historical Session Administration, 9-19
Historical Session Container Page, 9-20
Historical Session Playback Toolbar Icons, 9-22
Historical Session Search Page, 9-20
Host User ID Selection, 1-28
HTR File, 11-1

I Indicator
New Data, 1-29
Instance Page, Network (Map), 4-5

L Launch page, 1-9
LDAP Server
Starting/Stopping, 9-54
Legend, Network View, 4-17
Link Status, 8-3, 8-7
Link Status Container Page, 8-5
Link Status Search Page, 8-4
Linked Nodes, 4-7
Links and Linksets, Signaling, 3-19, 3-23
Links/Linksets Container Page, 3-21
Log
Error, 7-3

M Making a Historical Session Active, 9-63
Manual HTR Assignments, 6-10
Manual HTR Assignments Container Page, 6-11
Manual HTR Assignments Search Criteria, 6-10
Manual HTR Assignments Search Page, 6-10
Manual vs. Automatic Update, 1-29
Map Analysis, 4-6
Map Nodes, Editing, 4-31, 4-37, 4-39, 4-40
Map Page Search Area, 4-2
Map Pages, General Tasks on the, 4-31
Messages
Broadcast, 7-11
Modifying a Node, 4-12
Modifying Automatic Hard To Reach Parameter Sets, 6-23
Modifying Passwords, 9-9
Mouse Menu Options, 4-16
Moving a Node, 4-16

N Network (Map) Display Options, 4-8
Network (Map) Instance Page, 4-5
Network Element Container Page Exceptional List View, 2-9
Network Element Data Types, 2-4
Network Element Details Page, 1-16, 2-11
Network Elements
Search Criteria, 2-5, 2-17, 3-16, 3-31, 5-18
Network Elements Container Page, 2-8
Data Table View for Discrete Data, 2-9
Network Elements Search Page, 2-5, 4-19
Network Map Style Administration, 9-36, 9-43
Network View Administration, 9-26
Network View Legend, 4-17
Network View Server, Restarting the, 9-52
Network Views Container Page Search Area, 4-2
Network Views Detail Page, 4-5
Network Views Display Options, 4-8
Network Views Pages
General Tasks on the, 4-31
Network Views Style Administration, 9-25
New Data Indicator, 1-29
New Maps, 9-28
New Period Indicator, 4-7
Node
Adding, 4-11
Deleting, 4-12
Modifying, 4-12

Moving, 4-12
Node, Deleting a, 4-12
Node, Modifying a, 4-12
Node, Moving a, 4-16
Nodes on a Network View, 4-11
Nodes, Editing Map, 4-31, 4-37, 4-39, 4-40
Nodes, Types of, 4-7

O
Options, Network (Map) Display, 4-8
Output Element Types, 1-21
Overall Exception Level Indicator, 1-21

P
Page Search Area, Map, 4-2
Pages in the GUI, 1-7
Parameter Area, 5-6
Parameter Set Detail Page, 9-41
Parameter Sets, 5-6
Parameter Sets Administration, 9-39, 9-44
Parameter Sets Container Page, 9-40
Password
Administration, 9-7
Changing, 9-51
Composition, 9-8
Exceeding the Defined Thresholds, 9-8
Excluding Users, 9-9
Expiration, 9-8
Modifying, 9-9
Resetting, 9-10
Password Administration, 9-7
Password Composition, 9-8
Password Expiration, 9-8
Presentation, Data, 2-11, 2-12
Procedure
Starting the System, 8-13
Protective TG Control Request Page, 5-24
Protective TG Controls, 5-19
Protective TG Controls Container Page, 5-22
Protective TG Controls Search Page, 5-20

R
Receiving a Broadcast Message, 7-11
Recommended Browser User Preferences, 1-3
Reference Data, 3-10
Regular Expression, 10-1
Request Page
Automatic HTR Parameter Set Definitions, 6-13
Request Page, Code Control, 5-13
Request Page, Expansive TG Control, 5-37
Request Page, Protective TG Control, 5-24
Resetting Passwords, 9-10
Restarting the Network View Server, 9-52
Retrieving Destination Assignment Data, 6-21
Retrieving Destination Data, 6-20

S
Saving Changes, 4-9
Search Area, 1-29
Network Views Container Page, 4-2
Search Area in Advanced Search Mode, 1-11
Search Area, Map Page, 4-2
Search Criteria for Audits, 2-21
Search Criteria for Network Elements, 2-5, 2-17, 3-16, 3-31, 5-18, 5-47
Search Criteria on the Trunk Groups Search Page, 3-4, 3-25, 4-4, 4-20
Search Page
Audits, 2-21
Automatic Hard To Reach Parameter Set Assignments, 6-15
Automatic HTR Parameter Set Definitions, 6-13
Error Log, 7-4
Link Status, 8-4
Links/Linksets, 3-20, 3-24
Network Elements, 2-5
Table Layout, 9-14
Search Page, Code Controls, 5-8
Search Page, Control Log, 7-8
Search Page, Expansive TG Controls, 5-30
Search Page, Network Elements, 2-5, 4-19
Search Page, Protective TG Controls, 5-20
Search Page, Trunk Groups, 3-4
Search Pages, 1-10
Sending a Broadcast Message, 7-11
Sets, Parameter, 5-6
Setting Time Delay, 9-20
Shape Facet Administration, 9-36, 9-43
Signaling Link Details Page, 3-21, 3-27, 3-34
Signaling Links and Linksets, 3-19
Starting/Stopping the LDAP Server, 9-54

Starting/Stopping the Web Server, 9-53
Status
Link, 8-3, 8-7
System
start, 8-13
System Errors, 1-26

T
Table Layout
Changing, 9-58
Creating, 9-59
Creating a New, 9-16
Table Layout — Administration, 9-13
Table Layout Container Page, 9-15
Table Layout Search Page, 9-14
Tasks
Using the Graphic User Interface, 1-35
Tasks for Web User Administration, 9-47
Tasks on the Control Pages, General, 5-57
Tasks on the Map Pages, General, 4-31
Tasks on the Trunk Groups Page, 3-14
Text on a Network View, 4-14
TG Control Container Page, Expansive, 5-35
TG Control Details Page, 5-36
TG Control Request Page, Expansive, 5-37
TG Control Request Page, Protective, 5-24
TG Controls Container Page, Protective, 5-22
TG Controls Search Page, Expansive, 5-30
TG Controls Search Page, Protective, 5-20
TG Controls, Expansive, 5-27
TG Controls, Protective, 5-19
Timestamp on a Network View, 4-15
Tool Bar Area, 1-24
Toolbar Area, 1-29
Toolbar Icon
Historical Session Playback, 9-22
Toolbar icon functions, 1-24
Trend Data, 3-13
Trunk Group Container Page, 1-13
Trunk Group Details Page, 1-15, 3-8
Trunk Groups Container Page, 3-7
Trunk Groups Page, Tasks on the, 3-14
Trunk Groups Search Page, 3-4
Trunkgroup Controls, 3-14
Trunkgroup Reference Data, 3-10
Types of Nodes, 4-7

U
Update
Automatic, 1-29
Manual, 1-29
User ID
Host, 1-28
Users
Adding, 9-55
Using Network View Administration, 9-26
Using the GUI on Various Platforms and Browsers, 1-3

V
Validating a Control Request, 5-3
View Legend, Network, 4-17
Viewing Controls, 5-2

W
Web Server
Starting/Stopping, 9-53
Web User — Administration, 9-3
Web User Administration
Tasks for, 9-47
Web User Administration Page, 9-6
Web User Information Page, 9-5