RTS

Innovating the Future of Global Communications

Trunk Supervisor Technical Manual

up to and including version 1.9.0

PROPRIETARY NOTICE

COPYRIGHT NOTICE

WARRANTY AND SERVICE INFORMATION

For warranty and service information, refer to the appropriate web site below:

RTS Intercoms ..... www.rtsintercoms.com/warranty
RTS Digital
RTSTW
AudioCom
RadioCom
Intercom Headsets.....www.telex.com

CUSTOMER SUPPORT

Technical questions should be directed to:

Customer Service Department
Bosch Security Systems, Inc.
www.telex.com

TECHNICAL QUESTIONS EMEA

Bosch Security Systems Technical Support EMEA
http://www.rtsintercoms.com/contact_main.php

DISCLAIMER

The manufacturer of the equipment described herein makes no expressed or implied warranty with respect to anything contained in this manual and shall not be held liable for any implied warranties of fitness for a particular application or for any indirect, special, or consequential damages. The information contained herein is subject to change without prior notice and shall not be construed as an expressed or implied commitment on the part of the manufacturer.

Table of Contents

CHAPTER 1

Introduction

IMPORTANT:
- Verify the appropriate physical connections between the hardware has been made, as described in the Trunk Master Installation Manual.
- Verify Trunk Edit was properly used to configure the trunk connections for the trunk master.

NOTE: It is important that AZedit be used to configure each ADAM matrix in the trunking system, in addition to configuring the trunk master using Trunk Edit.

Trunk Supervisor is a Microsoft Windows compatible application allowing users of a trunking system to continuously monitor and test the trunking system in real time. This software connects to the Trunk Master via an Ethernet or RS-232 serial connection. With the addition of a RT-2M or AutoTIMs interface, this software also provides the necessary configuration for testing of trunk lines. These interfaces require an additional RS-232 serial connection.

IMPORTANT: An audio analyzer is required if you are doing automated trunk testing. It is an option that allows Trunk Supervisor to test trunk lines.

Trunking

Trunking is a way of connecting multiple ADAM frames together. With intelligent trunking, fewer lines are allocated through a process called *dynamic allocation*. Dynamic allocation allows the system designer to build fewer lines of communication which can carry conversations from one system to the other, as it is unlikely all users on each system communicate back and forth constantly. For example, a matrix composed of 100 users may be able to use 16 lines to connect to another system of 100 users. This design allows for 16 individual conversation at any given point in time, through the use of dynamic allocation. As the first person initiates communication between systems, they are assigned to Trunk 1. The second person to initiate a communication is assigned to Trunk 2. The third person is assigned to Trunk 3, and so on. If the first person finishes talking, the system then releases Trunk 1 which allows it to be used by the next person to initiate communication. This process is considered intelligent trunking by automatically initiating a dynamic change in the system to allow for efficient utilization of fewer lines.

CHAPTER 2

Installation

Application Requirements

Minimum Software Requirements

- Windows XP[1]
- Microsoft Data Access Objects v3.6
- Microsoft Jet Engine v4.0 or higher

Minimum Hardware Requirements

- Pentium 233-MHz processor or faster (300MHz is recommended)
- At least 64MB of RAM (128MB is recommended)
- At least 1.5GB of available space on the hard disk
- CD-ROM or DVD-ROM drive
- Keyboard and mouse
- Video adapter and monitor with Super VGA (800 x 600) or higher resolution
- Sound card

1. *Trunk Supervisor is a 32-bit Windows application designed to run under Windows XP/Vista/7. It may run under Windows 8, but has not yet been tested in this configuration.*

Installation

To **install Trunk Supervisor**, do the following:

1. From the Trunk Supervisor folder, double-click the **SETUP.EXE**.
   The Installation Wizard begins.
2. Follow the installation wizard, taking **all the defaults**.

   NOTE: The default installation directory is: C:\TELEX|TKSUPV\V190. This can be changed, if desired.

During the installation, the following are created:

- installation directory (default or user-defined)
- BIN directory - created under the installation directory. The BIN directory houses the TKSUPV.EXE application and the release notes.
- TKSUPV.EXE shortcut on the Program submenu of the Start menu of the taskbar. The shortcut is labelled Trunk Supervisor V1.9.0

  NOTE: The location of this shortcut, and its name, cannot be modified during the installation process. You can move, rename, or delete this shortcut afterwards. If you move or rename it, it will not be removed as part of the uninstall process.

CHAPTER 3

Configuration

Configuration Window

The **Configuration** window, shown in Figure 1, houses the majority of configuration options for the Trunk Supervisor. The tabs in the configuration window are dynamic, meaning if an Audio Analyzer is selected on the Configuration page, three (3) additional tabs appear in the Configuration window (Test Parameters, Test Schedule, and Test Options tabs).

NAVIGATION: To open the Configuration window, select **View|Configuration...** from the menu bar.
OR
Press **Ctrl+V**, then **Alt+Enter** on the computer keyboard.

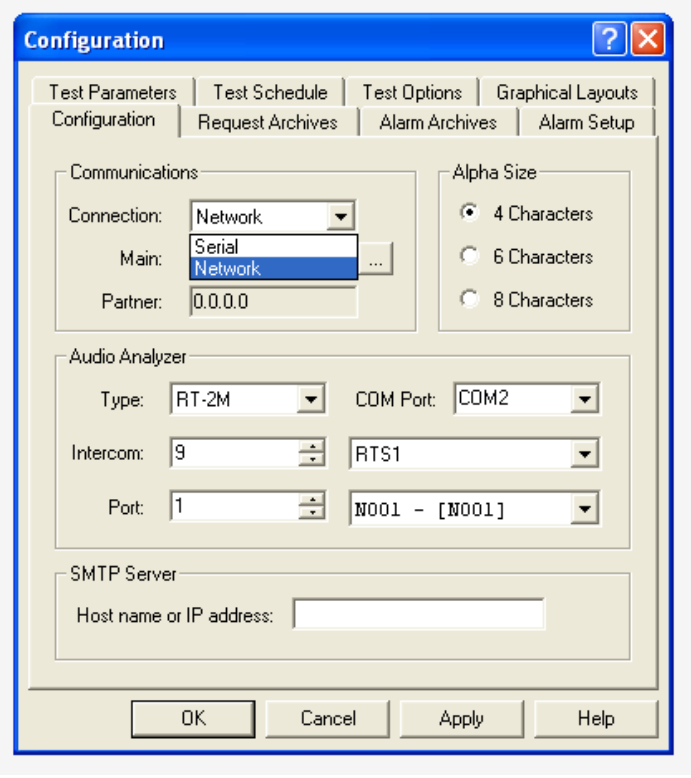


FIGURE 1. Configuration Window

Configuration Tab

After the Trunk Supervisor software is finished installing, the Configuration page, shown in Figure 1, is normally the first window used to establish network connections to the primary and optional secondary Trunkmaster, the audio analyzer, SMTP Server, as well as the number of alphas displayed.

Trunk Master systems can be set up as either standalone or redundant. If the system is constructed as a standalone, then an IP Partner is not shown and can be ignored. If the system is constructed with a redundant trunk master, then an IP Address appears in the IP Partner field.

Port Forwarding

It is possible to have a trunk master on a private network accessible via the Internet. If port-forwarding is properly programmed into the routers, a connection can be established between two (2) private networks through the routing systems. For example, Trunk Supervisor on one private network can connect over the internet to a second private network where a trunk master resides. The routers on the trunk master's private network must be programmed to port-forward UDP ports 27410 and 27415 to the trunk master's private IP Address. If an intercom is to be connected that resides on a private network other than that of the trunk master, then UDP port 27415 must also port-forward to the intercom private IP Address on the router where the intercom resides.

Communications

Network Connection

To **establish network connections**, do the following:

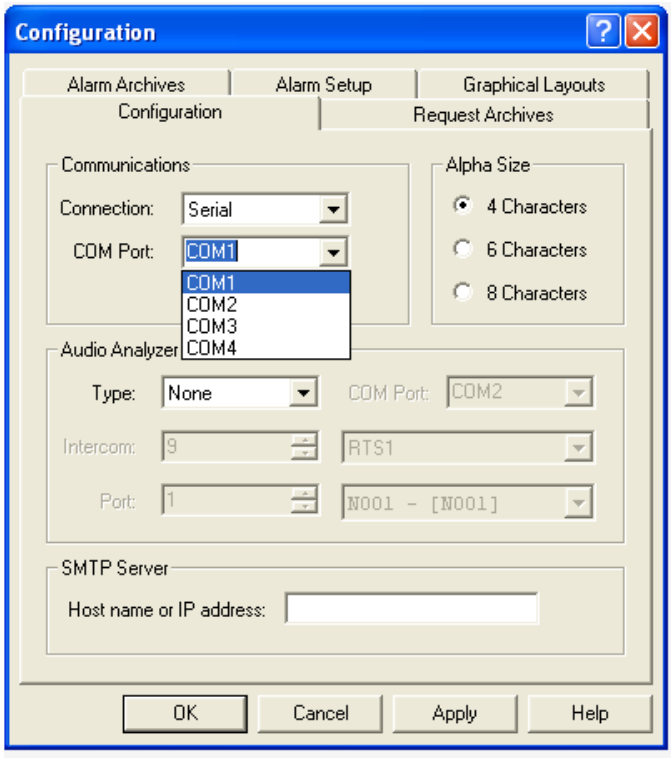
1. From the View menu, select **Configuration...**.
   The Configuration window appears.
2. From the Connection drop down menu, select **Network**.
3. In the Main field, enter the **IP Address of the primary Trunk Master**.
   OR
   Click the **browse button** to open the Available Trunk Masters window and select a **trunk master** from a list of available devices.
   If the trunking system has a redundant trunk master, the Partner IP Address field populates; if there is no redundant trunk master, then the Partner IP Address field is ignored.

IMPORTANT:	This tool only finds trunk masters residing on the same unfiltered subnet and can take a few minutes to do so on large subnets, such as a Class A or B. If the network search utility locates a Trunk Master, single click on the unit you want. Do not click the OK button until you have verified the chosen trunk master is the intended machine.

Serial Connection

To **establish serial connections**, do the following:

1. From the View menu, select **Configuration...**.
   The Configuration window appears.
2. From the Connection drop down menu, select **Serial**.
   The COM Port drop down menu appears.



3. From the COM port drop down menu, select the **COM port** to be used for communication with the Trunk Master.
   OR
   In the COM port drop down menu field, enter the **COM port name** to be used for communication with the Trunk Master.

Alpha Size Group Box

The size of the alphas displayed throughout the Trunk Supervisor application are configured on the Configuration tab as well.

To **set the alpha size**, do the following:

In the Alpha Size group box, select the **4 Characters radio button**.
OR
In the Alpha Size group box, select the **6 Characters radio button**.
OR
In the Alpha Size group box, select the **8 Characters radio button**.

Audio Analyzer Group Box

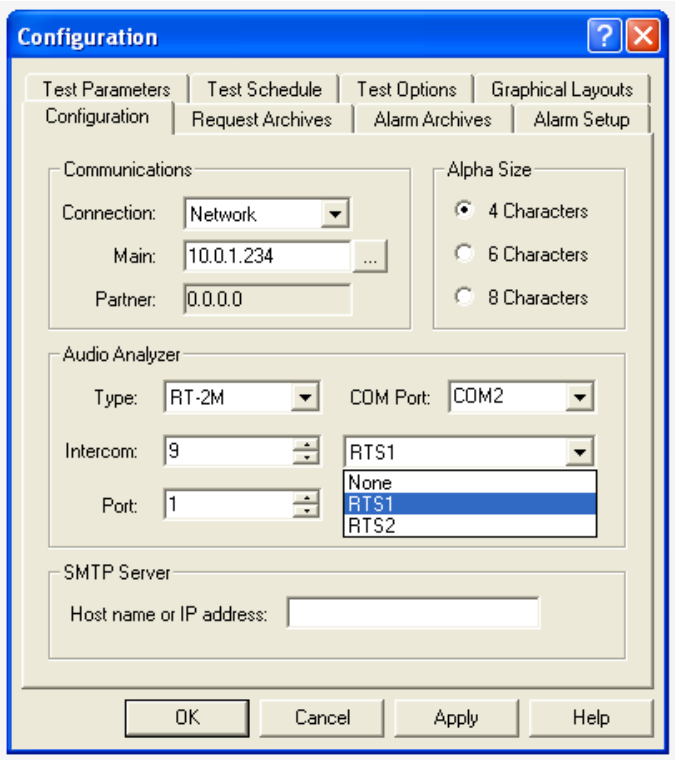
(Optional) An **Audio Analyzer** is a device that tests and measures audio performance over audio lines in electronic devices. There are currently two (2) audio analyzers compatible with RTS systems; Auto-TIMS and the RT-2M device. Check the hardware to verify which model is connected and select the appropriate model.

IMPORTANT: Currently, the only method of communication with an audio analyzer is via RS-232 serial connection directly to the computer running Trunk Supervisor. Hardware data flow control (CTS & RTS) is used on the audio analyzer serial cable, it is important to verify you are using a serial cable that has continuity on all pins.

The audio analyzer requires an audio connection to a port of one (1) of the matrix systems that is part of the trunk network so that it rout audio down the various trunking paths and back to the audio analyzer in order to test the lines.

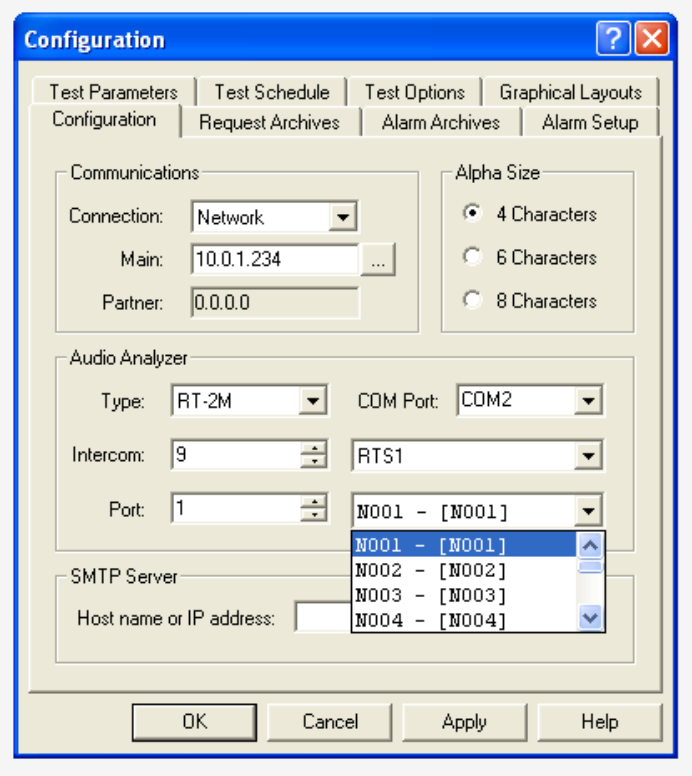
To **configure an audio analyzer on your system**, do the following:

1. From the Type drop down box, select the **type of audio analyzer** being used.
2. From the COM Port drop down menu, select the **COM port** to be used for audio analysis.



3. Using the arrow buttons in the Intercom spin box, select the **Intercom number** of the specified matrix.
   OR
   From the Intercom drop down menu (next to the spin box), select **a connected matrices by name**.

NOTE: The Intercom number is directly related to the TrunkEdit Intercom Setup listing of matrices.



4. Using the arrow buttons in the Port spin box, select the **an intercom port**.
   OR
   From the Intercom drop down menu (next to the spin box), select **a connected intercom port**.
5. Click **Apply**.
   The modifications are applied to the application.

SMTP Server (Optional)

The **SMTP Server Group Box** is used to configure SMTP for the Trunk Supervisor application. For more information, see “Advanced Trunk Supervisor Settings” on page 57.

Host Name or IP Address Field

The **Host Name or IP Address** field is used to enter the IP Address or Host name (if a DNS server is available) of an approved email server on the network.

Graphical Layouts Tab

The **Graphical Layouts Tab**, shown in Figure 2, is used to configure the Graphical Usage View.

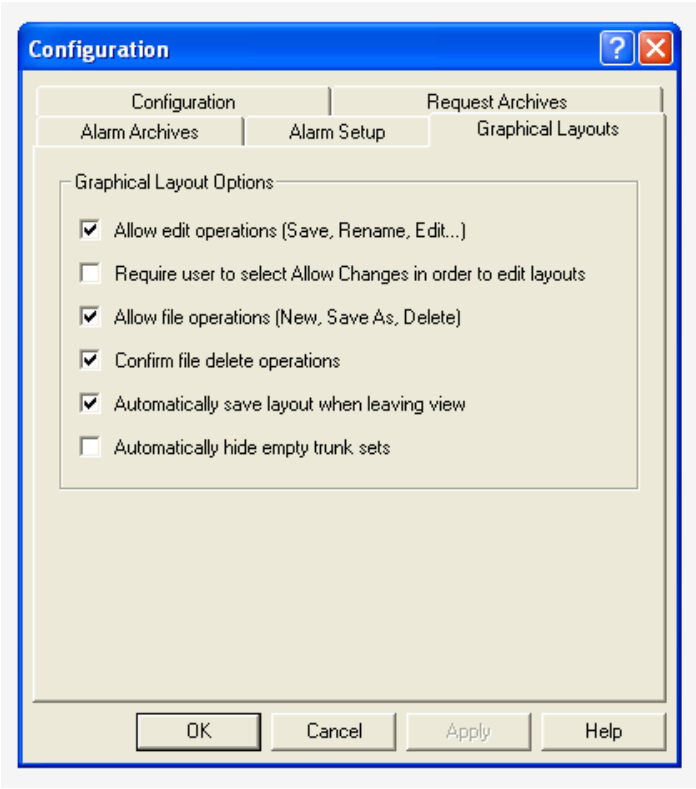


FIGURE 2. Graphical Layouts Tab

Graphical Layout Options Group Box

Allow Edit Operations (Save, Rename, Edit...) Check Box

The **Allow Edit Operations (Save, Rename, Edit...)** check box allows the user to save various layout views in the Graphical Usage view. Users can save or rename views from the File menu. They can also delete views using the File menu, as well.

Require User to Select Allow Changes in Order to Edit Layouts Check Box

The **Require User to Select Allow Changes in Order to Edit Layouts** check box prevents users from making unintentional changes by requiring them to select Allow Changes before being able to edit the graphical views.

Allow File Operations (New, Save As, Delete) Check Box

The **Allow File Operations (New, Save As, Delete)** check box allows the user to select New or Save As in the File menu, creating icons with either a user-generated name or a default name, such as view1, view2, etc. Views can also be deleted by selecting the view to be deleted, then from the File menu, select Delete.

Confirm File Delete Operations Check Box

The **Confirm File Delete Operations** check box enables a confirmation message to appear any time a view is deleted.

IMPORTANT:	This operation cannot be undone

Automatically Save Layout When Leaving View Check Box

The **Automatically Save Layout When Leaving View** check box ensures the current layout does not snap back to a default configuration when the user selects another view.

Automatically Hide Empty Trunk Sets Check Box

The **Automatically Hide Empty Trunk Sets** check box hides trunks in the graphical view that are not fully configured. Clear this check box if you want to see all trunks, fully or partially configured.

Alarm Setup Tab

The **Alarm Setup** tab, shown in Figure 3, determines what conditions generate an alarm and how those alarms are handled. This is also the area where email addresses and pager addresses are entered for notification purposes.

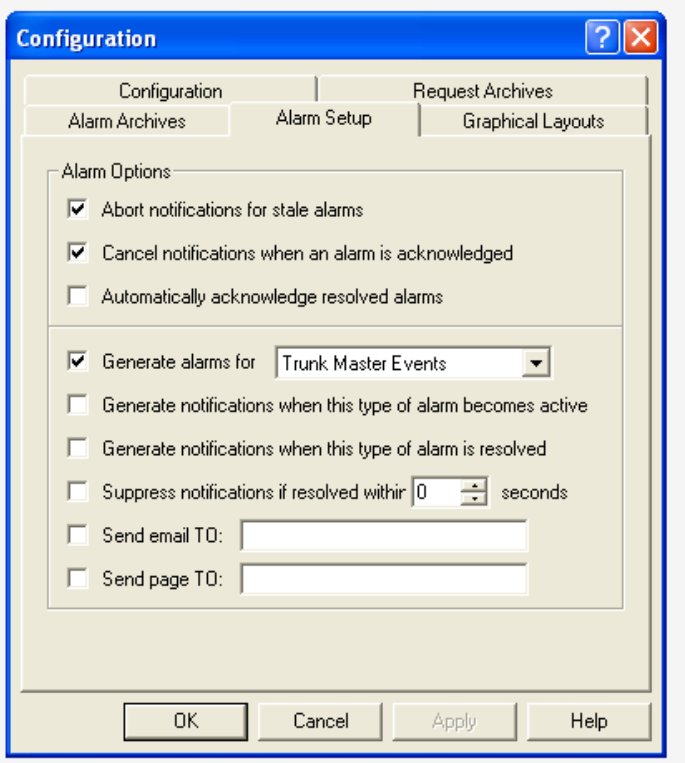


FIGURE 3. Alarm Setup Tab

Abort Notifications for Stale Alarms Check Box

The **About Notifications for Stale Alarms** check box allows alarm notifications that have been displayed for several minutes to automatically disappear.

Cancel Notifications when an Alarm is Acknowledged Check Box

The **Cancel Notification when an Alarm is Acknowledged** check box prevents notifications from being sent if the alarm is acknowledged.

Automatically Acknowledge Resolved Alarms Check Box

The **Automatically Acknowledge Resolved Alarms** check box allows resolved alarms to be recognized automatically.

Generate Alarms For... Check Box and Drop Down Menu

The **Generate Alarms For...** check box and drop down menu is used to choose specific alarm behavior. The check box must be selected to use this option.

Available options for this field are: *Trunk Master Events*, *Intercom Events*, or *Trunk Request Busy Events*.

Generate Notifications When This Type of Alarm is Resolved Check Box

The **Generate Notifications When This Type of Alarm is Resolved** check box activates notifications when an alarm is triggered for the chosen type of alarm in the Generate alarms for...drop down menu.

Suppress Notifications if Resolved Within.... Seconds Check Box

The **Suppress Notifications if Resolved Within... Seconds** check box allows the user to set the amount of time, in seconds, to wait before sending notifications. This is helpful in the case and operator is typically observing the system but wants to be notified of any issues if they are away from the computer.

Sent Email TO Field

The **Sent Email TO** field is used to enter an email address(es) to which notifications are sent when events occur. This feature is only enabled when if the SMTP server information is entered in the Configuration tab.

Send Page TO Field

The **Send Page TO** field is used to enter an pager address(es) to which notifications are sent when events occur. This feature is only enabled when if the SMTP server information is entered in the Configuration tab. This option properly formats the message for pagers.

Alarm Archives Tab

The **Alarm Archives** tab, shown in Figure 4, is used to set up how the alarm archives perform. It is split into two (2) parts:

- Archive Schedule
- Archive Maintenance

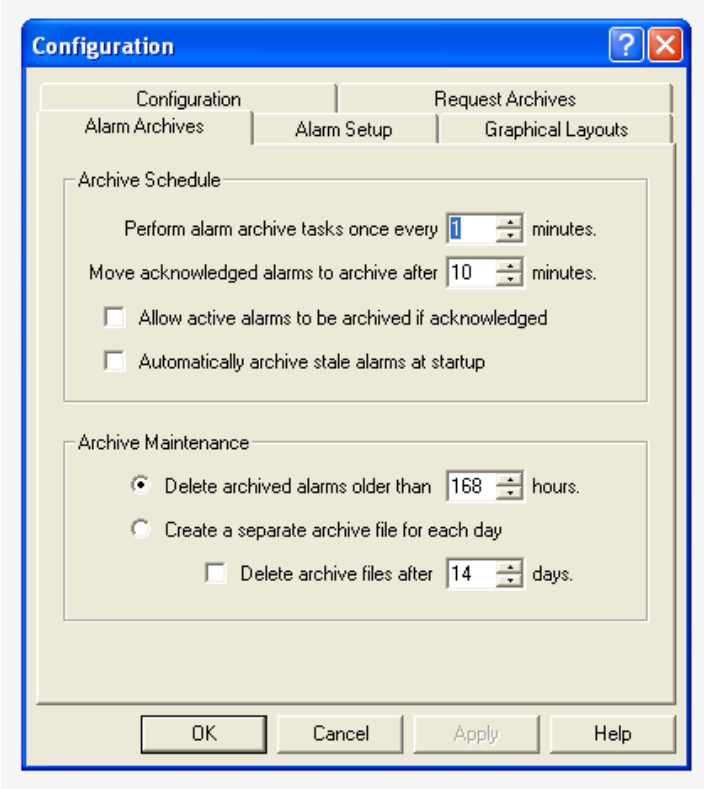


FIGURE 4. Alarm Archives Tab

Archive Schedule Group Box

The **Archive Schedule** parameters set on this tab determine how and when the information is archived.

Perform Alarm Archive Tasks Once Every... Minutes Spin Box

The **Perform Alarm Archive Tasks Once Every... Minutes** spin box is used to set the time interval, in minutes, between archiving.

Move Acknowledged Alarms To Archive After... Minutes Spin Box

The **Move Acknowledged Alarms To Archive After...Minutes** spin box is used to set the time, in minutes, the system waits before archiving the alarms.

Allow Active Alarms To Be Archived if Acknowledged Check Box

The **Allow Active Alarms To Be Archived if Acknowledged** check box enables the system to mark an active alarm for archival once it is acknowledged.

Automatically Archive Stale Alarms At Startup Check Box

The **Automatically Archive Stale Alarms At Startup** check box enables the system to archive alarms that have been active for a long period of time.

Archive Maintenance Group Box

The **Archive Maintenance** parameters determine how archive records are stored and when they are deleted.

Delete Archived Alarms Older Than... Hours Radio Button and Spin Box

The **Delete Archived Alarms Older Than... Hours** radio button and spin box allows the user to set the time, in hours, the system waits before purging archived alarms.

Create a Separate Archive File for Each Day Radio Button

The **Create a Separate Archive File for Each Day** radio button enables the system to create daily archive files for later review.

Delete Archive Files After... Days Check Box and Spin Box

The **Delete Archive Files After... Days** check box and spin box gives the user the option of deleting daily archive files after a number of days when they may no longer be relevant.

Request Archives Tab

The **Request Archives** tab, shown in Figure 5, is used set up how the request archives performs. Trunk Supervisor tracks the keys a keypanel user presses to speak to other users over a trunk, which is referred to as a request. These requests are then archived in a file known as a request archive file. This tab is split into two (2) sections:

- Archive Schedule
- Archive Maintenance

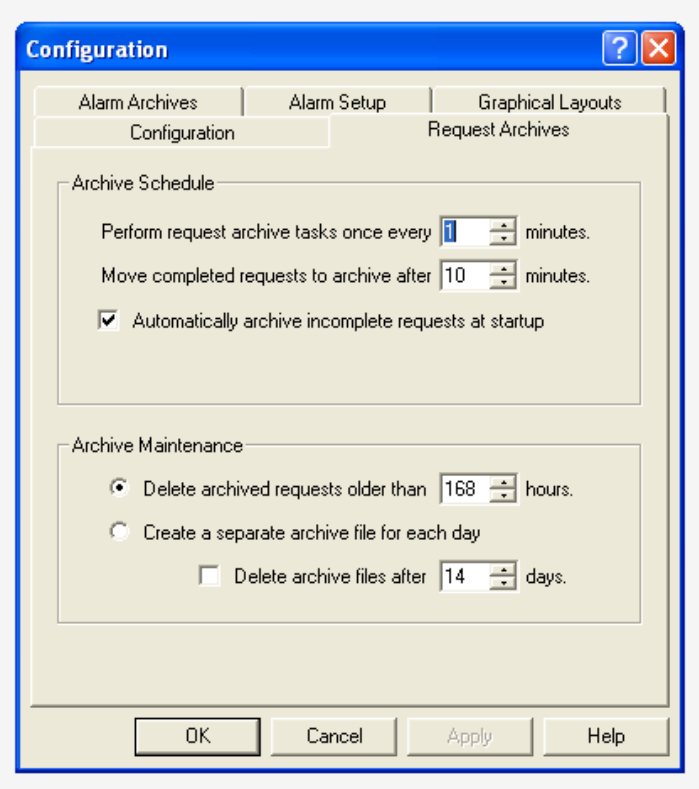


FIGURE 5. Request Archives Tab

Archive Schedule Group Box

The Archive Schedule group box is used to determine how and when request information os archived.

Perform Request Archive Tasks Once Every... Minutes Spin Box

The **Perform Request Archive Tasks Once Every...Minutes** spin box allows the user to set the interval, in minutes, between archiving the trunking requests.

Move Completed Requests to Archive After... Minutes Spin Box

The **Move Completed Requests to Archive After...Minutes** spin box is used to set the time, in minutes, the system waits before archiving the requests.

Automatically Archive Incomplete Requests At Startup Check Box

The **Automatically Archive Incomplete Requests At Startup** check box enables the system to archive requests made but not completed when the application opens.

Archive Maintenance Group Box

The **Archive Maintenance** group box is used to determine how archive records are stored and when they are deleted.

Delete Archived Requests Older Than...Hours Radio Button and Spin Box

The **Delete Archived Requests Older Than...Hours** radio button and spin box allows the user to set the time the system waits before purging archived requests.

Create a Separate Archive File For Each Day Radio Button

The **Create a Separate Archive File For Each Day** radio button enables the system to save daily archive files for later review.

Delete Archive Files After... Days Check Box and Spin Box

The **Delete Archive Files After... Days** check box and spin box gives the user the option of deleting daily archive files after a number of days when they may no longer be relevant.

Audio Analyzer Test Options

The **Test Parameters** and **Test Schedule** Tabs, shown in Figure 6, only appear in the Configuration window when an Audio Analyzer is installed in the system (see “Audio Analyzer Group Box” on page 12). The Audio Analyzer passes audio over the trunks and compares the audio received to determine the amount of audio loss compared to the amount of audio transmitted.

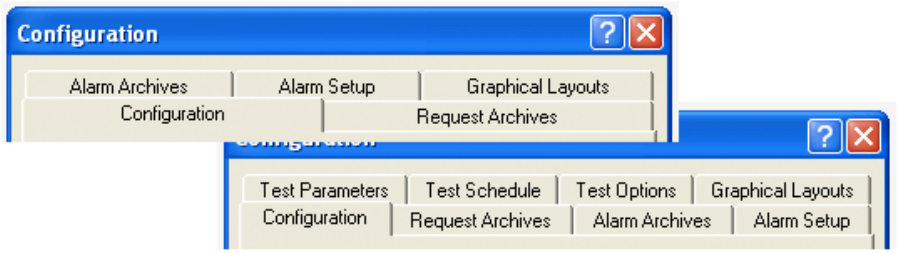


FIGURE 6. Audio Analyzer Test Options

Test Parameters Tab

The **Test Parameters** tab, shown in Figure 7, is used to set up the RT-2M or AutoTIMs unit for testing trunk lines. The amount of loss allowed, test tone frequency, test tone levels, test sensitivity, and termination parameters are all set from this tab.

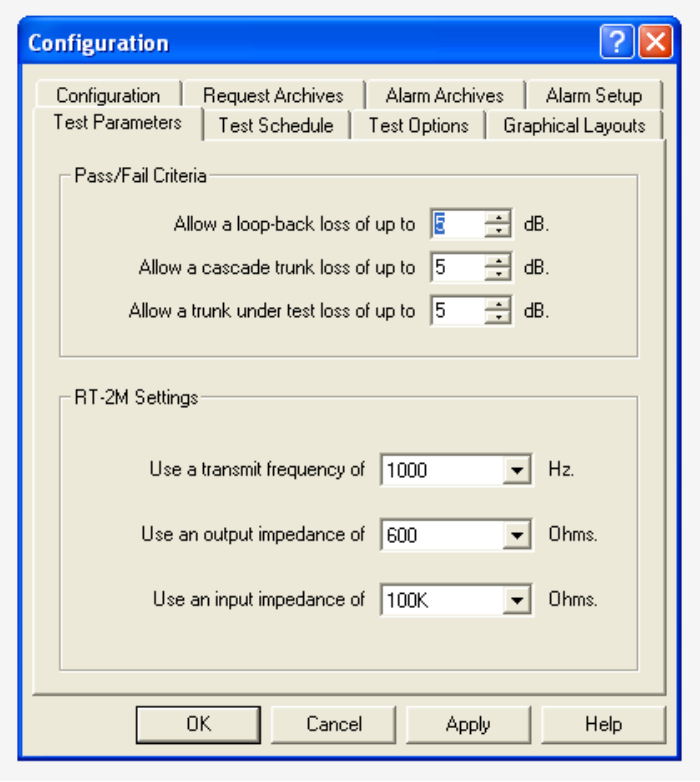


FIGURE 7. Test Parameters Tab

Pass/Fail Criteria Group Box

Allow a Loop-back Loss of Up To... dB Spin Box

The **Allow a Loop-back Loss of Up To...dB** spin box allows the user to manage the amount of acceptable audio loss before a trunk is considered to fail by the trunking system.

The default value for this field is *5dB*.

Allow a Cascade Trunk Loss of Up To... dB Spin Box

The **Allow a Cascade Trunk Loss of Up To...dB** spin box allows the user to set a different amount of audio loss when the trunk makes multiple hops across more than one (1) trunked matrix system.

The default value for this field is *5dB*.

Allow a Trunk Under Test Loss of Up To... dB Spin Box

The **Allow a Trunk Under Test Loss of Up To...dB** spin box allows the user to set the amount of acceptable audio loss of a trunk under test.

The default value for this field is *5dB*.

RT-2M Settings Group Box

The **RT-2M Settings** group box only appears when Trunk Supervisor detects an RT-2M unit.

Use a Transmit Frequency of... Hz Drop Down Menu

The **Use a Transmit Frequency of... Hz** drop down menu is used to determine the audio frequency used by the audio analyzer to test the trunks.

The default value for this field is *1000Hz*.

Use an Output Impedance of... Ohms Drop Down Menu

The **Use Output Impedance of... Ohms** drop down menu is used to change the output impedance of the audio analyzer.

The default value for this field is *600 Ohms*.

Use an Input Impedance of... Ohms Drop Down Menu

The **Use an Input Impedance of... Ohms** drop down menu is used to change the input impedance of the audio analyzer.

The default value for this field is *100k Ohms*.

AutoTIMs Settings Group Box

The **AutoTIMS Settings** group box only appears when Trunk Supervisor detects an AutoTIMS unit.

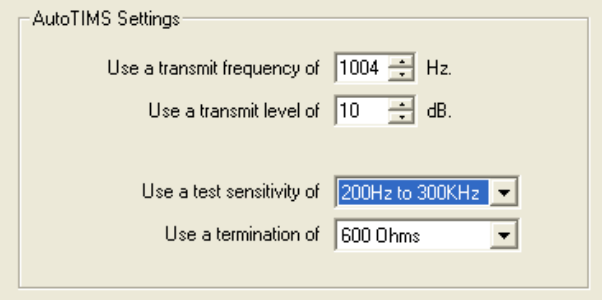


FIGURE 8. AutoTIMS Settings

Use a Transmit Frequency Of... Hz Drop Down Menu

The **Use a Transmit Frequency Of... Hz** drop down menu is used to determine the audio frequency used by the audio analyzer to test the trunks.

The default value for this field is *1004Hz*.

Use a Transmit Level Of... dB Drop Down Menu

The **Use a Transmit Level Of...dB** drop down menu is used to determine the audio output level used by the audio analyzer to test the trunks.

The default value for this field is *10dB*.

Use a Test Sensitivity of... Drop Down Menu

The **Use a Test Sensitivity of...** drop down menu is used to choose the level of sensitivity of the audio analyzer. The recommended sensitivity is 40Hz to 20Hz because this is the human vocal range.

The available options for this field are: 200Hz to 300kHz and 40Hz to 20kHz.

Use a Termination of... Drop Down Menu

The **Use a Termination of...** drop down menu is used to choose the different termination values for the audio analyzer.

The default value for this field is *600 Ohms*.

Test Schedule Tab

The **Test Schedule** tab, shown in Figure 9, is used to determine when trunk testing by the RT-2M or AutoTIMS unit occurs. Testing can be disable by selecting the Never option. It takes approximately 10 to 15 seconds to test a trunk line.

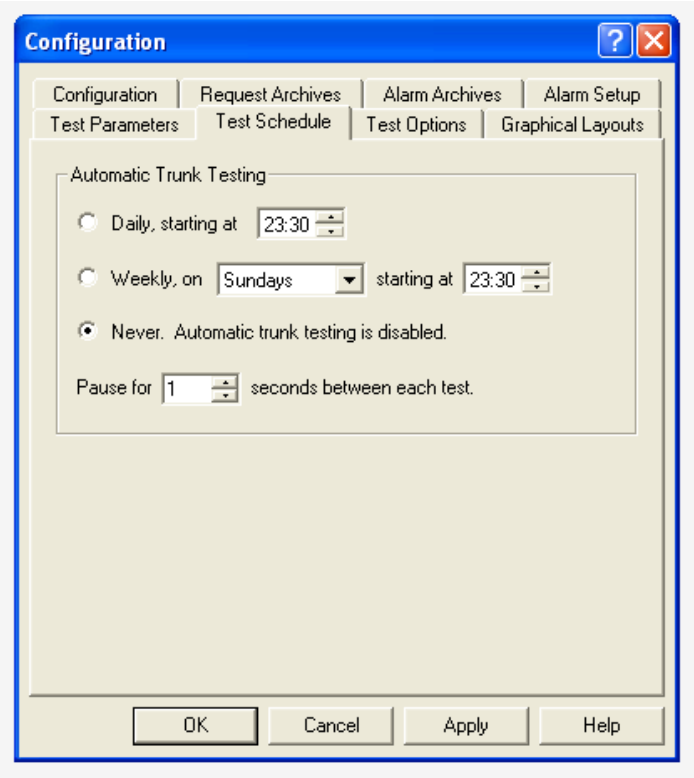


FIGURE 9. Test Schedule Tab

Automatic Trunk Testing Group Box

Daily, Starting At... Radio Button and Spin Box

The **Daily, Starting At...** radio button and spin box allows the user to schedule a daily test starting at a given hour of the day. The Trunk Supervisor's computer clock is used to determine the trigger time.

This clock displays military time.

Weekly, On... Starting At... Radio Button, Drop Down Menu, and Spin Box

The **Weekly, On...Starting At...** radio button, drop down menu, and spin box allows the user to schedule a weekly test starting at a given hour of the day. The Trunk Supervisor's computer clock is used to determine the trigger time.

This clock displays military time.

Never. Automatic Trunk Testing is Disabled Radio Button

The **Never. Automatic Trunk Testing is Disabled** radio button allows the user to disable automatic testing.

Pause For... Seconds Between Each Test Spin Box

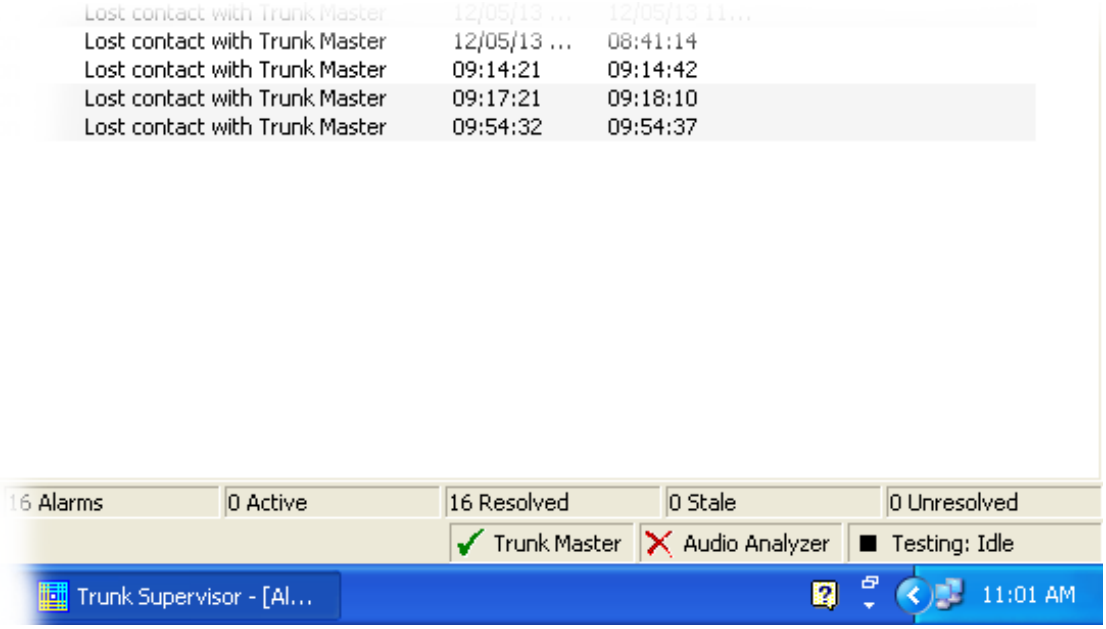
The **Pause For... Seconds Between Each Test** spin box allows the user to set the time, in seconds, between each automatic trunk test.

Status Bar

The **Status Bar** is used to display a quick status on the primary connection dependencies of Trunk Supervisor. The status bar display is controlled from the View menu on the menu bar.

To **display the status bar**, do the following:

> From the View menu, select **Status Bar**.
The Status Bar displays at the bottom right of the main Trunk Supervisor window.



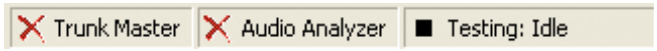
Understanding the Status Bar

The **Status Bar** shows the status of three components of the Trunk Supervisor connection, the Trunk Master, the audio analyzer, and the trunk testing status.

NOTE: If the optional audio analyzer is also configured and the settings applied, the red X should change to a green check and the name changes from Audio Analyzer to the appropriate name of the analyzer (RT-2M or AutoTIMS).

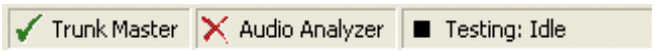
Indicators

- A red X indicates the connection cannot be established or has been broken.



- A green check mark shows the connection has been successfully established and is active.

Before connections have been configured have been configured in the configuration window, the status bar should display as follows:



Once the Trunk Master settings have been entered and applied the status on the Trunk Master box should change from a red X to a green check box, displayed as follows:

CHAPTER 5

Trunk Master Navigation Bar

The Trunk Master navigation bar is split into five (5) areas:

- Intercoms
- All Alphas
- All Requests
- All Trunks
- Trunk Conflicts

Intercoms View

The **Intercoms** view allows you to view specific information regarding each intercom. Click on the main Intercom icon to view the following information:

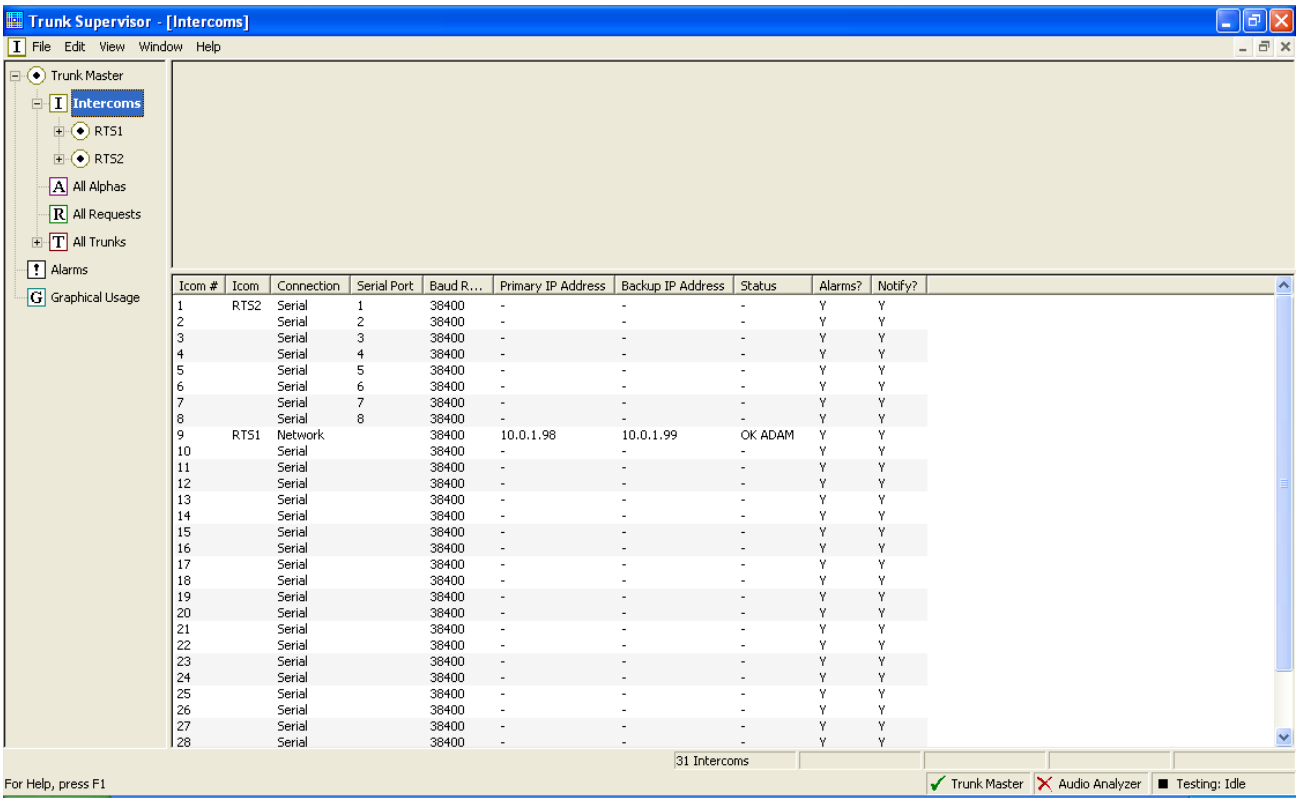


FIGURE 10. Intercoms View

Column	Description
Icom #	The Icom # column displays the number assigned to the intercom to identify it in the system.
Icom	The Icom column displays the name assigned to the intercom to identify it in the system.
Serial Port	The Serial Port column displays the serial port on the trunk master to which the intercom is connected.
Baud Rate	The Baud Rate column displays the baud rate used by the intercom.
Status	The Status column displays the status of the intercom and the intercom type.
Alarms?	The Alarms? column displays if alarms are enabled on the intercom.
Notify?	The Notify? column displays if notifications are enabled on the intercom.

All Alphas View

The **All Alphas** view displays every alpha function for all trunked intercoms (default). This information can be pared down using the Intercom and All Function filters at the top of the view.

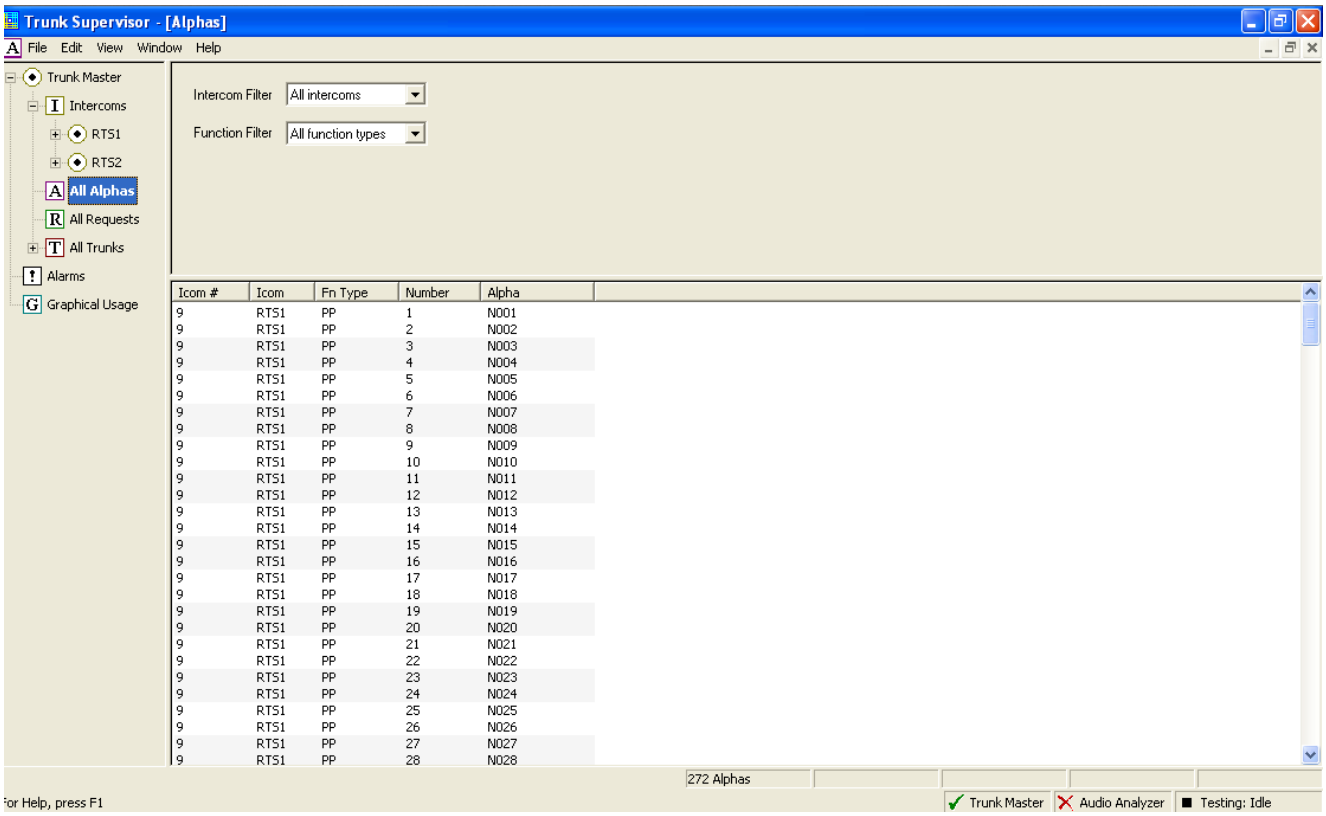


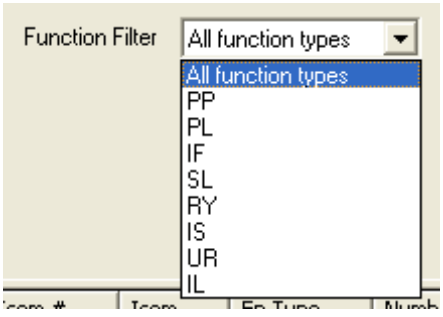
FIGURE 11. All Alphas View

To **change from All Intercoms to a specific intercom**, do the following:

> From the For... drop down menu, select the **specific intercom** you want to display.

To **change from All functions to a specific intercom**, do the following:

> From the Function Filter drop down menu, select the **function** you want to display.



The Alpha information is separated into columns and the entries can be sorted by clicking the column heading.

Column	Description
Icom #	The **Icom #** column displays the number assigned to the intercom to identify it in the system.
Icom	The **Icom** column displays the name assigned to the intercom to identify it in the system.
FN Type	The **FN Type** column displays the type of function: • PP – Point-to-Point • PL – Party Line • IF – Intercom Fold Back (IFB • SL – Special List • RY – Relay • IS – Isolate (ISO)
Number	The **Number** column displays the number assigned to the function.
Alpha	The **Alpha** column displays the alpha assigned to the function.

All Requests View

The **All Request** view, shown in Figure X, is used to view all requests in the trunking system, or a subset of requests in the system depending on the filter choices. A request is an individual conversation such as Point-to-Point, IB, PL, etc... For example, A person talking to three (3) people would generate three (3) requests.

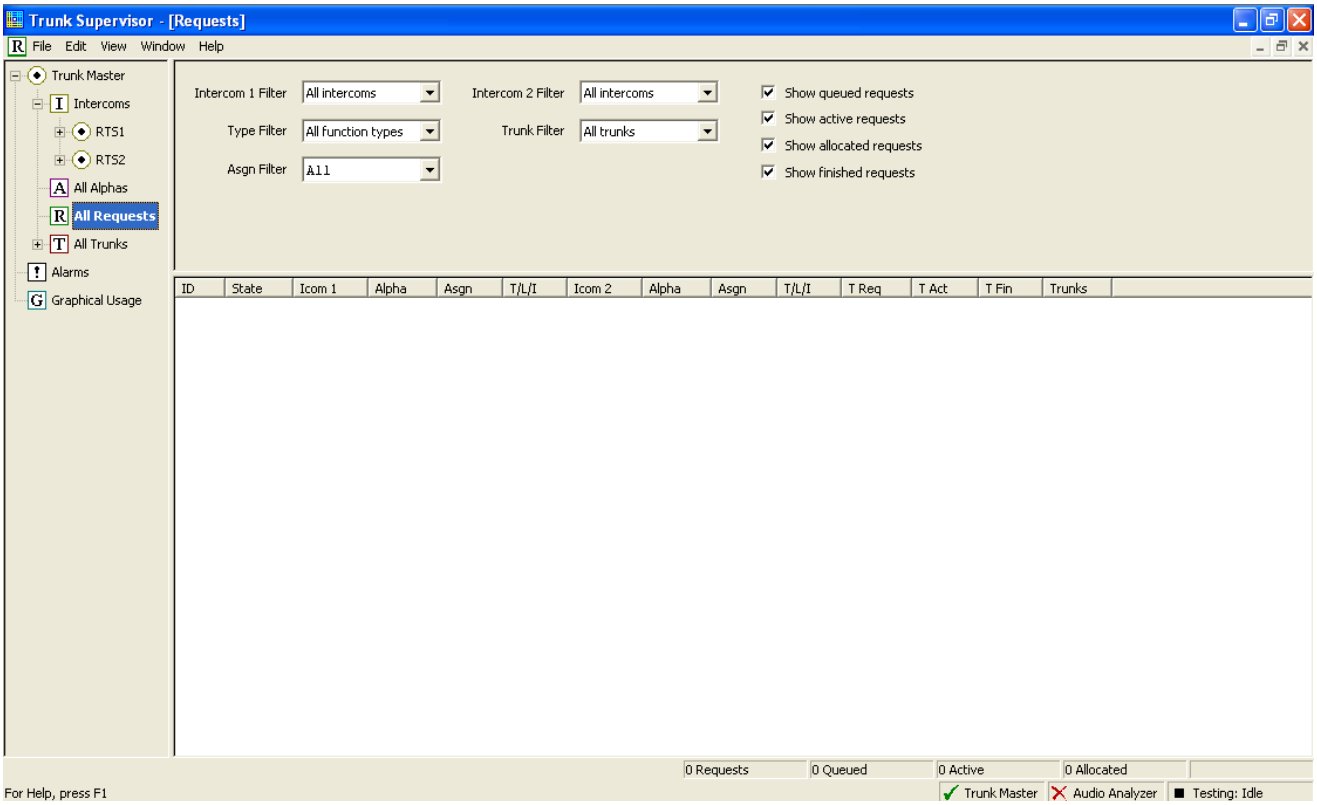


FIGURE 12. All Requests View

The information is displayed in a table format and be sorted via the filters mentioned above, as well as, the column headings.

Column	Description
ID	The **ID** column displays the number assigned to the request.
State	The **State** column displays the state of the request. There are six (6) states: • Allocated – the trunk is allocated, but not be used (key is off). • Queued – there is a request, but there has not been an allocation because either the destination is busy or it is a wait-to-talk channel. • Active – the trunk is allocated and in use. • Finished – the request has been completed and the allocation has cleared. • Incomplete – the current status is old from a reset.
Icom 1	The **Icom 1** column displays the name of the intercom at one end of the trunk.
Alpha	The **Alpha** column displays the alpha assigned to the intercom port.
Asgn	The **Asgn** column displays the genera assignment to the intercom function (for example, N001).

Column	Description
T/L/I	The **T/L/I** column displays the current status of the key. • Talk • Listen • Inactive
Icom 2	The **Icom 2** column displays the name of the intercom at the other end of the trunk.
Alpha	The **Alpha** column displays the alpha assigned to the port at the other end of the trunk.
Asgn	The **Asgn** column displays the genera assignment to the intercom function (for example, N002).
T/L/I	The **T/L/I** column displays the current status of the key. • Talk • Listen • Inactive
T Req	The **T Req** column displays the time the request was made.
T Act	The **T Act** column displays the time the request was activated.
T Fin	The **T Fin** column displays the time the request was finished.
Trunks	The **Trunks** column displays the trunk allocated for the request.

All Trunks View

The **All Trunks** view, shown in Figure X, is used to view the definitions and statuses of all trunks in the system. By using the options and filters at the top of the window, the user can filter the data to see only trunks between two (2 specified intercoms and/or specific trunk information.

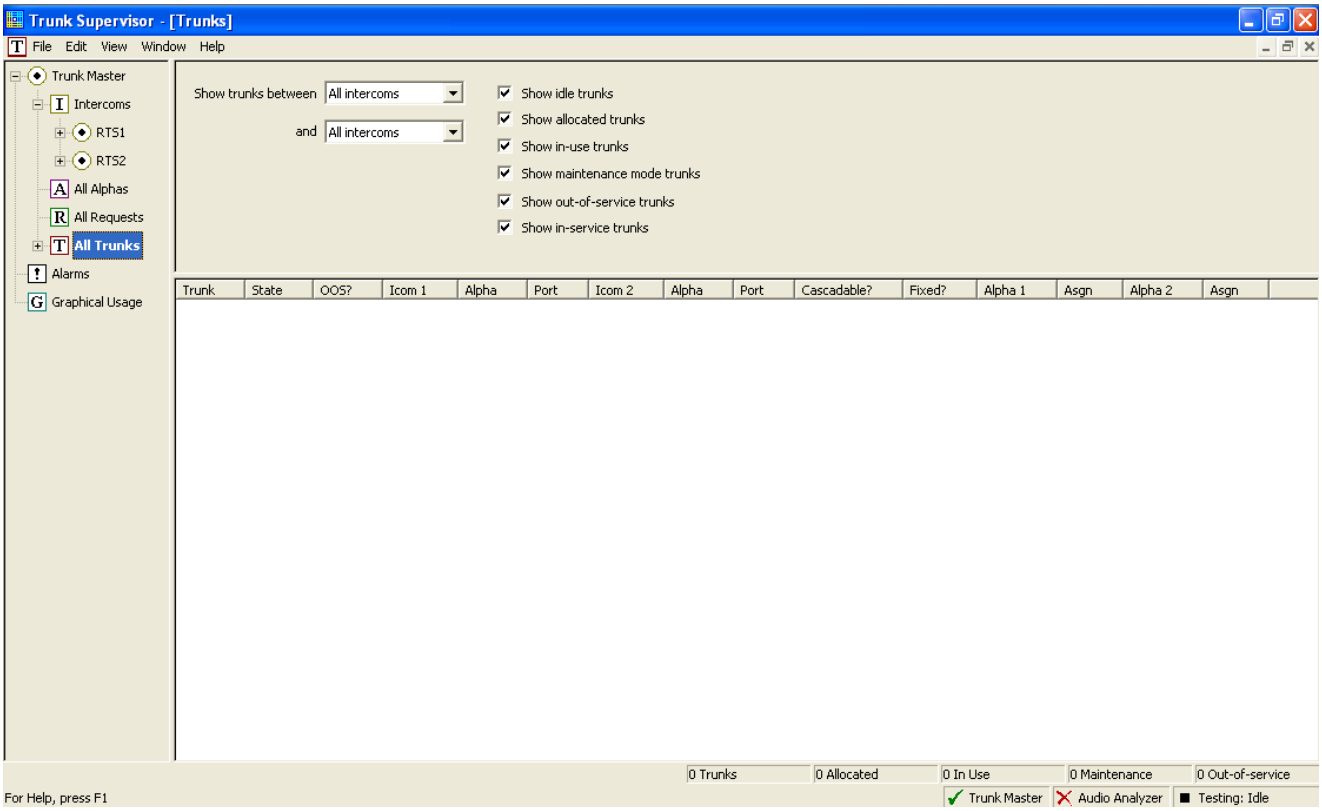


FIGURE 13. All Trunks View

As with all the views, the information is arranged in a table format and the data can be sorted by clicking on the column headings.

Column	Description
Trunk	The **Trunk** column displays the number assigned to the trunk.
State	The **State** column displays the state of the trunk. There are six (6) states: • Pass – passed test by AutoTIMS or RT-2M. • Fail – failed test by AutoTIMS or RT-2M. • Error – an undefined error on the AutoTIMS or RT-2M. • Pending – queued for testing by AutoTIMS or RT-2M. • Testing – currently being tested by AutoTIMS or RT-2M. • Skipped – forced to skip (i.e., maintenance mode or in-use).
Icom 1	The **Icom 1** column displays the name of the first intercom in the link.
Alpha	The **Alpha** column displays the alpha assigned to port on the first intercom.
Port	The **Port** column displays the generic reference to the port on the first intercom.
Icom 2	The **Icom 2** column displays the name of the second intercom in the link.

Column	Description
Alpha	The **Alpha** column displays the alpha assigned to port on the second intercom.
Port	The **Port** column displays the generic reference to the port on the second intercom.
Test Status	The **Test Status** column displays the pass or fail status of the last test.
Test Time	The **Test Time** column displays the date and time of the last test.
Test Information	The **Test Information** column displays measurements and parameters used in the last test including if the test was cascaded through another intercom system.
Cascadable?	The **Cascadable?** column displays if the trunk can be cascaded.
Fixed?	The **Fixed?** column displays if the trunk is fixed between points.
Alpha 1	The **Alpha 1** column displays the name of the alpha currently using the port at the first end of the trunk.
Asgn	The **Asgn** column displays the generic name of the assignment currently using the trunk at the first intercom end.
Alpha 2	The **Alpha 2** column displays the name of the alpha currently using the port at the second end of the trunk.
Asgn	The **Asgn** column displays the generic name of the assignment currently using the trunk at the second intercom end.
Auto Test?	The **Auto Test?** column displays if automatic testing by AutoTIMS or RT-2M is allowed on this trunk.
Alarms?	The **Alarms?** column displays if alarms are enabled for failure on this trunk.
Notify?	The **Notify?** column displays if a notification is sent on failure of this trunk.

Trunk Conflicts View

The **Trunk Conflicts** view is used to display a list of trunks whose definitions conflict with one (1) or more other trunk definitions because they share the same intercom and port number on at least one (1) end.

The information is displayed in a table format and can be sorted by clicking on the column headings.

Column	Description
Trunk #	The Trunk # column displays the number of the trunk definition.
Icom 1	The **Icom 1** column displays the name of the intercom system at the first end of the trunk.
Alpha	The **Alpha** column displays the name of the intercom port at the first end of the trunk.
Port	The **Port** column displays the name of the intercom port at the first end of the trunk.
Icom 2	The **Icom 2** column displays the name of the intercom system at the other end of the trunk.
Alpha	The **Alpha** column displays the name of the intercom port at the other end of the trunk.
Port	The **Port** column displays the name of the intercom port at the other end of the trunk.
Conflicts with Trunk #	The **Conflicts with Trunk #** column displays the number of the conflicting trunk definition.
Icom 1	The **Icom 1** column displays the name of the intercom system at the first end of the trunk.
Alpha	The **Alpha** column displays the name of the intercom port at the first end of the trunk.

Column	Description
Port	The **Port** column displays the name of the intercom port at the first end of the trunk.
Icom 2	The **Icom 2** column displays the name of the intercom system at the end of the trunk.
Alpha	The **Alpha** column displays the name of the intercom port at the other end of the trunk.
Port	The **Port** column displays the name of the intercom port at the other end of the trunk.

CHAPTER 6

Alarms

Alarms View

The **Alarms** view shows alarms in the system. The default is to show all alarms, but the view may be reduced by using the check box/menu selection filters at the top of the window.

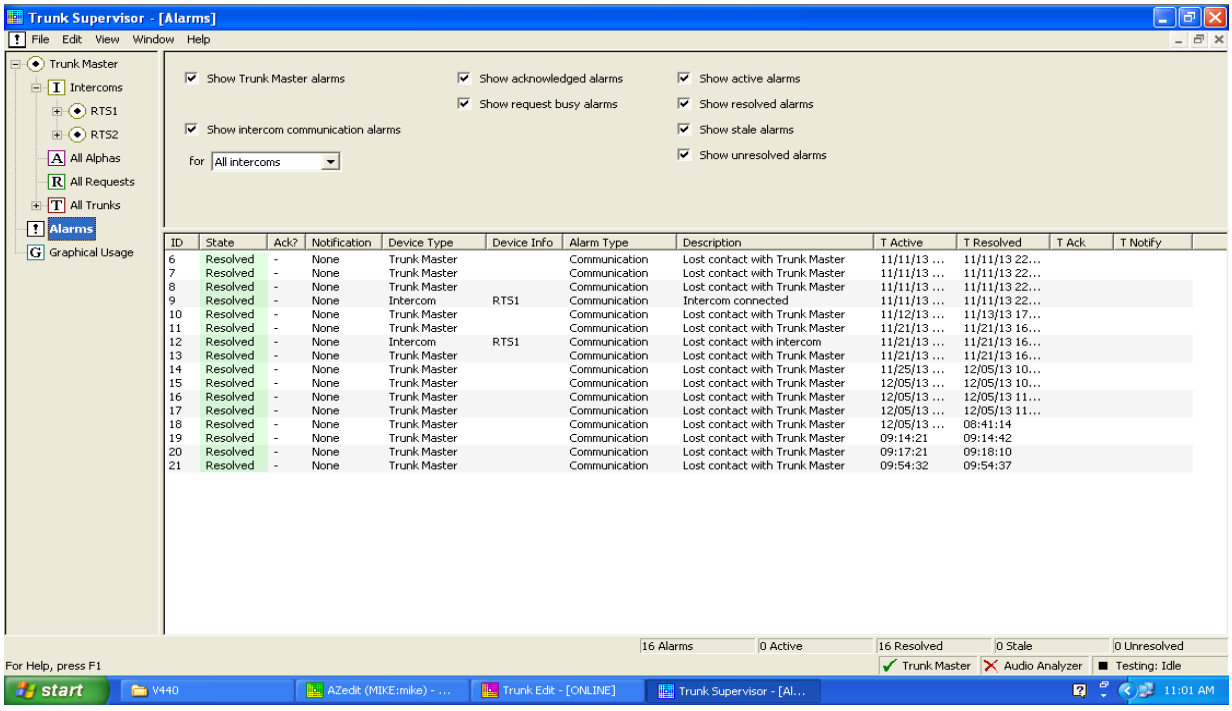


FIGURE 14. Alarms View

Show Trunk Master Alarms Check Box

The **Show Trunk Master Alarms** check box enables Trunk Supervisor to monitor and display Trunk Master Alarms.

Show Intercom Communication Alarms Check Box

The **Show Intercom Communication Alarms** check box enables Trunk Supervisor to display alarms generated when a connection to an intercom is established or broken.

For... Drop Down Menu

The **For...** drop down menu is used to select either all intercoms in the trunk system or a specific intercom for which alarms are displayed.

Show RT-2M Alarms or AutoTIMS Alarms Check Box (only when Audio Analyzer is configured)

The **Show RT-2M Alarms** or **AutoTIMS Alarms** check box is used to enable alarms for either the RT-2M or AutoTIMS to be displayed in the Alarm view.

Show Acknowledged Alarms Check Box

The **Show Acknowledged Alarms** check box is used to display alarms that have been seen by the user. Once a user have viewed the alarm, the Ack? column shows a Y. Clear this check box to suppress these alarms from displaying.

Show Request Busy Alarms Check Box

The **Show Request Busy Alarms** check box is used to display those alarms generated when a user requests a trunk line that is busy. Clear this check box to suppress these alarms from displaying.

Show Active Alarms Check Box

The **Show Active Alarms** check box is used to display active alarms currently in process. For example, if a configured intercom is not responding, then such an alarm is considered active until it is removed from the intercom list or reconnected. Clear this check box to suppress these alarms from displaying.

Show Resolved Alarms Check Box

The **Show Resolved Alarms** check box is used to display alarms that were active but are now resolved. For example, an intercom that lost connection and was restored. Clear this check box to suppress these alarms from displaying.

Show Stale Alarms Check Box

The **Show Stale Alarms** check box is used to display alarms that have not been resolved but are shutdown. Clear t his check box to suppress these alarms from displaying.

Show Unresolved Alarms Check Box

The **Show Unresolved Alarms** check box is used to display all unresolved alarms. Unresolved alarms are those that have not been closed. Clear this check box to suppress these alarms from displaying.

Info Bar 1 (page statistics at bottom of the view)

Alarms display field – displays the total number of alarms listed.

Active display field – displays the total number of active alarms.

Resolved display field – displays the total number of resolved alarms.

Stale display field – displays the total number of stale alarms.

Unresolved display field – displays the total number of unresolved alarms

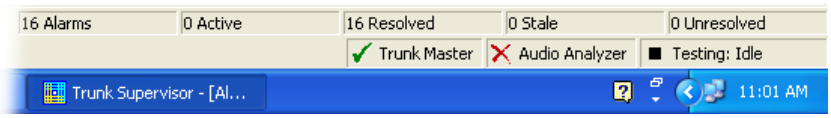


FIGURE 15. Info Bar 1

Alarms Information View

The **Alarms Information** view displays alarm information for each alarm and is arranged in a table format and can be sorted by clicking on the table headings.

Column	Description
ID	The **ID** column displays the number assigned to the alarm
State	The **State** column displays the current state of the alarm. Available options are: • *Active* – lost contact • *Stale* – Unresolved, but shutdown • *Resolved* – Regained contact
Ack?	The **Ack?** column displays the either a Y for Yes or an N for No. **>**Right click on the **column entry** to access a popup menu to select Y or N.
Notification	The **Notification** column display the status of the notification of the alarm. Available options are: • *None* – no notification for the alarm • *Pending* – notification is pending • *Canceled* – notification is canceled • *Sent* – notification has been sent • *Suppressed* – alarm occurred, but cleared before notification was sent • *Aborted* – notification was aborted • *Error* – There was an error in sending notification
Device Type	The **Device Type** column displays the type of device. Available options are: • *Intercom* • *Trunk* • *AutoTIMS or RT-2M*
Device Info	The **Device Info** column displays the intercom name or trunk ID.
Alarm Type	The **Alarm Type** column displays the type of alarm. Usually a test failure or loss of communications.
Description	The **Description** column displays information on alarms, such as “lost contact with intercom” or “loss unmeasurable”.
T Active	The **T Active** column displays the date and time an alarm became active.
T Resolved	The **T Resolved** column displays the date and time an alarm was resolved.
T Ack	The **T Ack** column displays the date and time the alarm was acknowledged.
T Notify	The **T Notify** column displays the date and time the notification was sent.

CHAPTER 7

Graphical Usage View

The **Graphical Usage** view allows the user to create custom views of the system. Intercoms are represented by circles in the view.

- A single circle indicates an intercom communicating with the Trunk Master at 38.4K baud.
- A circle with a dot indicates an intercom communicating at 9600 baud.

NOTE: Generally, intercoms communicating at 38.4k baud are local units, while those communicating at 9600 baud are remotely located with respect to the Trunk Master.

The color of the circle represents whether an intercom is communicating or not.If the circle is blue, the intercom is talking. If the circle is purple, the intercom is silent.

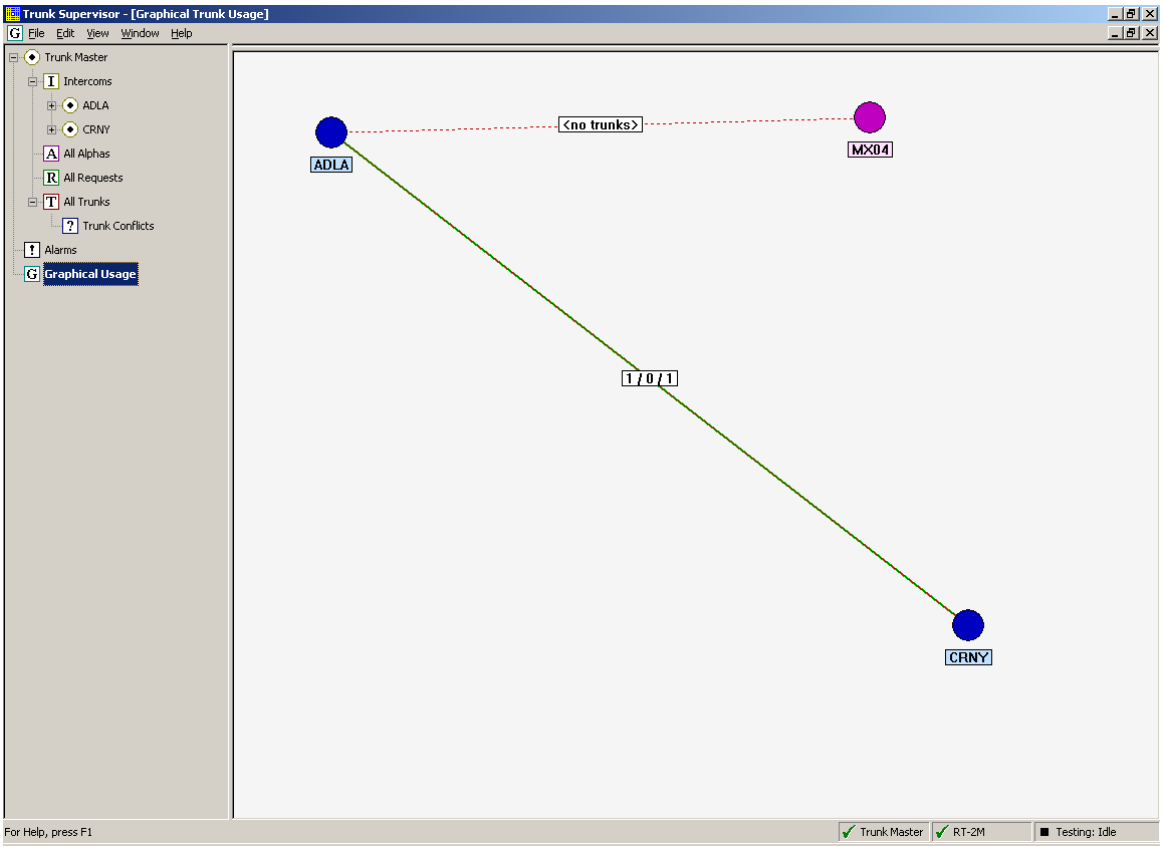


FIGURE 16. Graphical Usage Window

The line thickness showing the connections between the intercoms indicates the number of trunk between them. One (1) pixel of width indication one (1) trunk, two (2) pixels indicate two (2) trunks, and so on. A dashed line indicates there are no trunks between the two (2) intercoms. The color of the lines indicate the status of the trunk:

Line Color	Status Indicated
Red	Trunk in use
Yellow	Trunk is allocated
Green	Trunk is idle

Contextual Menu

When you right click the mouse in certain areas of the application window a pop-up menu presenting additional menus specific to the window appears.

Menu Item	Description
Select an intercom to show...	This allows you to choose an intercom to show
Hide intercom caption	This option hides the intercom caption below the circle representing the Intercom.
Show all hidden intercoms	This option shows all available intercom in the view.
Show trunk captions	This option shows labels for each intercom such as the name of the intercom.
Hide trunk captions	This option hides the intercom caption so only the graphical representation of the intercom is used.

CHAPTER 8

Diagnostic Logs

The **Diagnostic Logging** window, shown in Figure 17, is used to enable logging, adjusting the number of days to keep log files, setting the maximum size of log files, and setting the levels of various items to log.

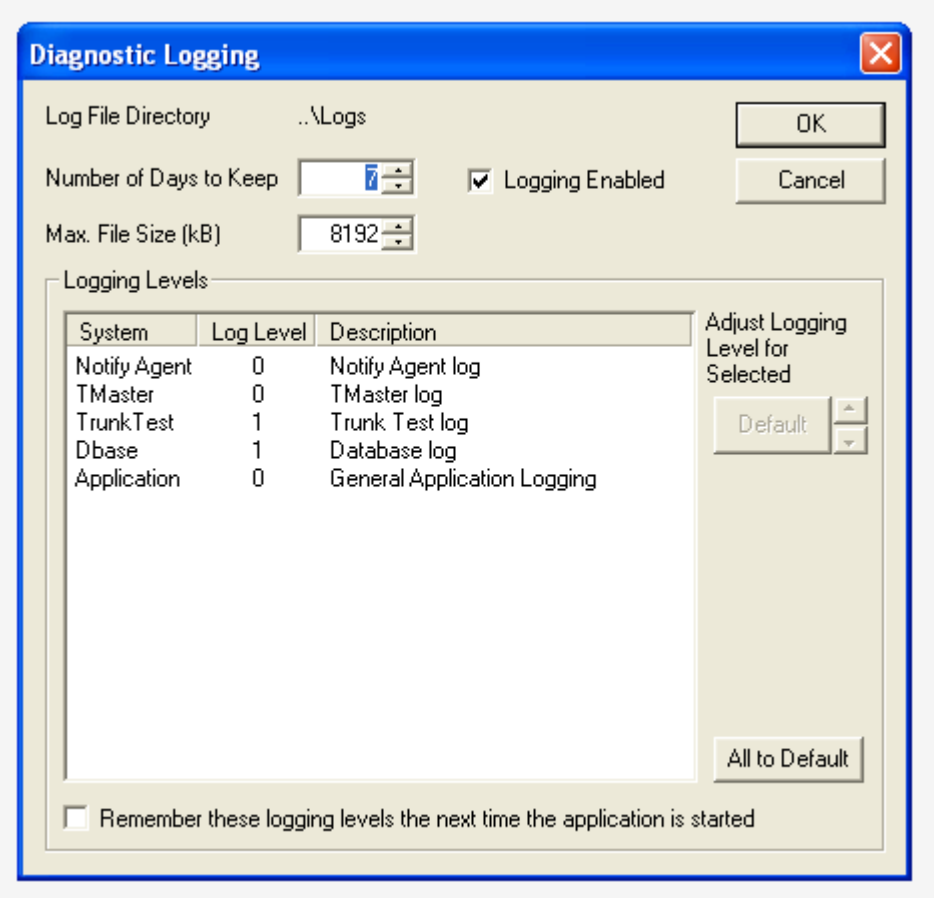


FIGURE 17. Diagnostic Logging Window

Log File Directory Display

The **Log File Directory** display shows the directory to which the daily log files are saved. One log file per day is generated in this folder. The location of the logs folder can be found in the Trunk Supervisor parent folder.

IMPORTANT: The location of the log files cannot be changed.

Number of Days to Keep Combo Box

The **Number of Days to Keep** combo box is used to configure the number of days to keep the log files before the system removes them.

Logging Enabled Check Box

The **Logging Enabled** check box is used to enable logging. If this box is not selected, the log files are not saved.

Max. Files Size (kB) Combo Box

The **Max File Size (kB)** combo box is used to set the upper limit to the file size of a log. This helps when logging levels are set too high or an error occurs and excessive log output is produced, it won't use up the space on the hard drive, which could cripple the computer Trunk Supervisor is active on. This option can be set to a generous level, but not exceptionally high.

TIP: This parameter if used in conjunction with the Number of Days to Keep parameter provides an excellent method of managing the space log files use on the hard drive.

Logging Levels Group Box

The **Logging Levels** group box is used to configure the levels of the types of events being logged.

System Column

The **System** column displays the different types of items tracked by the log file:

Notify Agent – Notification events. Default is 0 (catastrophic)

TMaster – Trunk Master events. Default is 0 (catastrophic)

TrunkTest – Trunk Testing events. Default is 1 (errors)

Dbase – Database events. Default is 1 (errors)

Application – General Application events. Default is 0 (catastrophic)

Log Level Column

The **Log Level** column is used to set the level to which a log is written to the log file.

IMPORTANT:	Unless instructed by an RTS engineer, it is not recommended to set logging levels higher than 3. It is rare to use anything but the defaults.

The available log levels are available:

0 Catastrophic –	A condition has happened that most likely causes the application to completely shut down.
1 Error –	A condition preventing certain parts of the application from operating, but may not result in complete shut down of the application.
2 Warning –	A condition which the application considers irregular, but is not critical.
3 Info –	These log entries are purely informational. they give the user insight into what the application is working on at any given time.
4 Protocol –	These log entries are more detailed than Info level entries and are primarily used for debugging purposes.
5 Debug –	These log entries are only used by programmers for debugging the application. Only use this level of debugging is instructed by an RTS engineer.
6 - 10 Unused –	Do not set logging levels greater than 5.

To **change the logging level**, do the following:

1. From the System column, select the **system event** you want to modify the logging level.
2. Using the Adjust Arrows next to the default button, adjust the **logging level up or down**, as desired.

Description Column

The **Description** column is used to display the description of the System event.

Default Button and Adjust Arrows

The **Default** button and Adjust arrows are used to set the selected system event to its default value or to increase/decrease the logging levels. To change the system event log level, use the adjust arrows to either increase or decrease the default value.

All to Default Button

The **All to Default** button is used to set all system events to the default log level values.

Remember these logging levels the next time the application is started Check Box

The **Remember these logging levels the next time the application is started** check box is used to save the modifications to the logging levels after shut down. This means the application remembers the settings you have made the next time the application is opened.

APPENDIX A

Menu Quick Reference Guide

System Menu Bar

File Menu

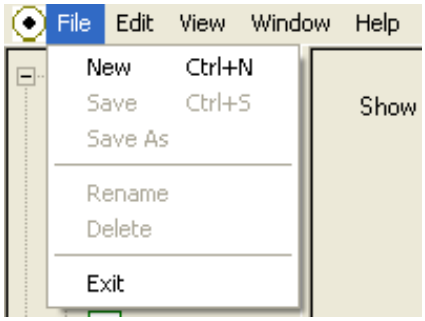


FIGURE 18. File Menu

New	Creates a new view in the graphic usage section
Save	Saves the graphical usage view. (only active when Graphical Usage section is selected in the side bar)
Save As	Creates a duplicate of the graphical usage view currently selected. (only active when Graphical Usage section is selected in the side bar)
Rename	Allows the user to rename the selected view. (only active when Graphical Usage section is selected in the side bar)
Delete	Deletes the currently selected graphical usage view (only active when Graphical Usage section is selected in the side bar)
Exit	Quits the application.

Edit Menu

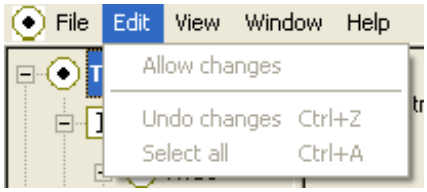


FIGURE 19. Edit Menu

Allow Changes	When selected, allows changes to be made to the graphical views. When not selected, prevents inadvertent changes from being made to the graphical views. (only active when Graphical Usage section is selected in the side bar)
Undo Changes	Allows the user to undo a change made to a view. Changes made prior to a save cannot be undone.
Select All	Selects all objects in the view window.

View Menu

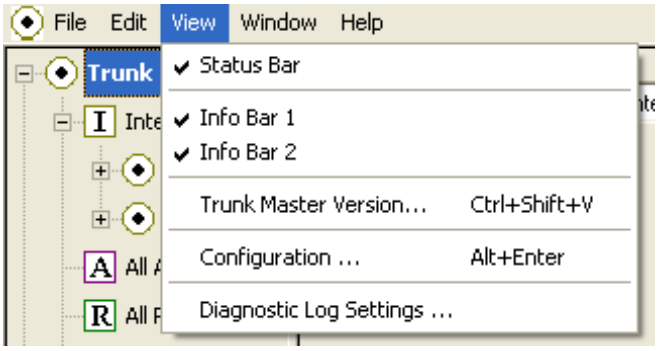


FIGURE 20. View Menu

Status Bar	Removes or allows the bar at the bottom of the active window to display the current status of the Trunk Master, Audio Analyzer, or the Trunk Testing Status.
Info Bar 1	Depending on the sidebar selection, the menu bar appearing at the bottom the window display the status of objects within the window, such as number of trunks, number of trunks allocated, number of requests, etc.
Info Bar 2	Provides a second row of quick information for the selected section.
Trunk Master Version...	This menu displays the current Trunk Master software version. This can only be selected when a Trunk Master is connected.
Configuration...	This menu item opens the application Configuration window.
Diagnostic Log Settings...	This menu item opens the Diagnostic Log Settings window.

Window Menu

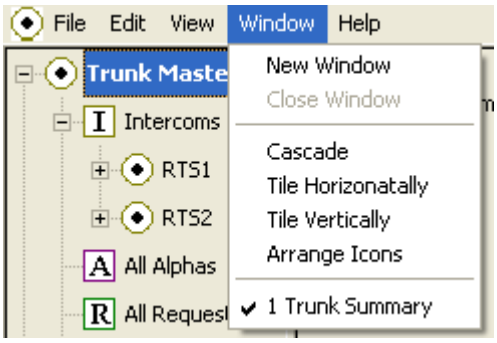


FIGURE 21. Window Menu

New Window	This menu item creates a duplicate window of Trunk Supervisor. This means you can create separate windows for each intercom summary. The result of this is only obvious if the window currently being worked in is not maximized.
Close Window	This menu item closes the currently opened window.
Cascade	This menu item causes all open windows to descend from the top left side of the window to the bottom right side of the window.
Tile Horizontally	This menu item divides the open window space between all the window, putting the first window listed at the top left adding windows horizontally until the next row is created.
Tile Vertically	This menu item divides the open window space between all the window, putting the first window listed at the top left adding windows vertically until the next column is created.
Arrange Icons	This menu item arranges icons within the application.
Window Instance Selection	This portion of the menu lists all the current window instances created by the user. If the you wanted to make a particular window previously viewed active, select it from this list.

Side Bar Navigation

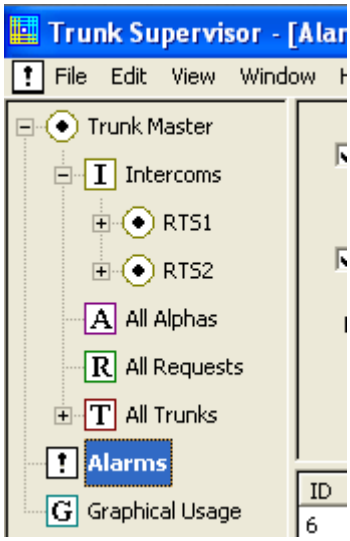


FIGURE 22. Side Bar Navigation

Trunk Master

The **Trunk Master** menu tree allows the user to see the overall activity in the trunking system. This allows the user to filter information to tailor it to their needs.

Intercoms

The **Intercom** menu item allows the user to view the Trunk Edit view of the Trunk Master connections to verify all connections are properly set up without having to switch to Trunk Edit.

Intercom Summary

The **Intercom Summary** displays information specific to a connected intercom. This list grows and shrinks as to what is being defined or modified in Trunk Edit, as an expected or connected intercom system.

All Alphas

The **All Alphas** item displays all available alpha of all the connected intercom in the trunking network, not only those set aside for trunking.

All Requests

The **All Requests** item displays all requests made by keypanel users for trunks. When troubleshooting a trunk request, this is a good starting point.

All Trunks

The **All Trunks** item lists all defined trunks in the trunking system.

Alarms

The **Alarms** item allows the user to filter any alarms sent by the system. This is useful when building a trunking system to identify when certain connections were established or failed.

Graphical Usage

The **Graphical Usage** item is a representation of the overall trunking system allowing users to get a visual idea of the activity and connectivity of the entire trunking system at a glace. This is especially useful when trying to evaluate the network design for excessive trunk cascading when ca indicate the trunking network is becoming over-worked.

Help Menu

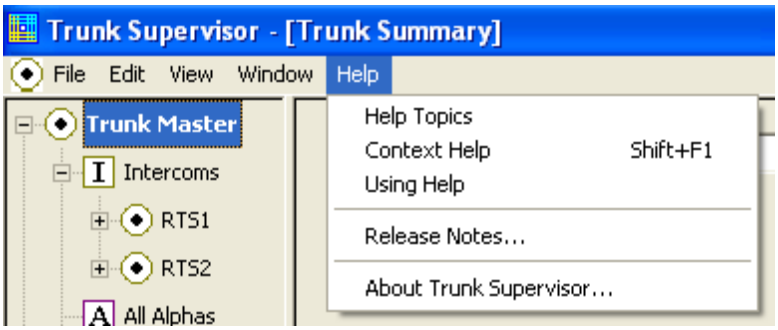


FIGURE 23. Help Menu

Help Topics	This menu item opens a help search box used to find particular information from the help file.
Context Help	This menu item activates the context sensitive help. This means the cursor into a question mark allowing the user to click on the area of interest and open the relative help file.
Using Help	This menu item opens the Help start page. From this page, you can search the help files for information about the application.
Release Notes...	This menu item opens the current release notes for Trunk Supervisor. These notes are used to relay information directly to the user about modifications made in each version.
About Trunk Supervisor	The menu item opens an informational window providing basic information about Trunk Supervisor such as the major and minor version of the product.

APPENDIX B

Troubleshooting

IMPORTANT: When troubleshooting cabling issues, it is important the cable and termination are properly verified BEFORE plugging in the equipment. Varying levels of voltage are used for various standards. For example, RS-232 uses 3 to 15 volts (can be as high as 25 volts in some applications; whereas, RS-485 lines are typically 5volts (up to as much as 12 volts). Connecting a 25-volt RS-232 line into a 5-volt RS-485 device could potentially destroy the internal circuitry of the RS-485 hardware driver.

Do not depend on protection circuits and always verify all connections before use.

General Connection Troubleshooting

While differing electrical standards are used in the communications field, many troubleshooting techniques are common to most situations. We suggest using these techniques to troubleshoot situations where a new connection cannot be established or an existing connection has been interrupted.

- Continuity – It is a common mistake to assume continuity of either the cable or individual wires. There are several ways of testing continuity with purpose-built split-end testers or by applying low voltage across common at the other end using the continuity mode of a multimeter.
- Reversals – It is best to check continuity for each pin/wire to rule out pin reversals. However, not all cables are meant to be pin-to-pin (also known as straight-thru). In the case of RS-232 a null-modem cable purposefully reverse the transmit and receive pins on one end so that two hosts (terminal equipment) can be directly connected together. Similarly, a network crossover cable allows two host devices to be directly connected together as if they were going through a network hub or switch.
- Interference – The greater distance a copper cable runs, the greater its capacitive and inductive ability. While techniques like shielding and balanced signaling provide protections against interference, they cannot eliminate interference altogether.
- Resistance – Electrical cables with sufficient length can interfere with signaling when the reactance of the cable is sufficient to resist the change in flow of electricity essential to communication. Employing professional grade cable purpose-built for the intended use is the best way to safeguard against electrical resistance issues.

Network Troubleshooting

If a connection cannot be established to the trunk master from the Trunk Supervisor, do the following:

1. Use a software utility that can pin the trunk master's IP Address from the computer or same physical Ethernet connection running the Trunk Supervisor. If the Trunk Master does not respond to the network ping, then verify the physical network connections to the Trunk Master are correct.
2. If the physical Ethernet connections are verified, then contact your Network Administrator to verify ports have not been blocked or a firewall has not been enabled along the network route.
3. A crossover cable can also be used to connect a computer directly to the Trunk Master to verify the unit is responding to the network. There may be multiple Ethernet connections on the back of the Trunk Master, all of which may cause the link LED to activate, but only one is used by the Trunk Master software. Typically, the Ethernet the Trunk Master uses is the Ethernet on the card in one of the expansion slots.

Serial Troubleshooting

There are three (3) primary types of serial connections used in the RTS matrix systems – RS-232, RS-485, and USB. It can be difficult to troubleshoot when it does not work since it may not immediately be obvious if it is a hardware failure or software misconfiguration. When the target piece of equipment is suspected to be bad, it is generally advisable to establish the serial adapter in use is working properly. This is done by testing the serial adapter hardware with equipment known to be working properly, which could be another serial adapter. RS-232 can be wired in a loopback configuration where the receive and transmit pins are tied together so anything transmitted form the adapter is returned to the adapter. A terminal emulator can then be used to verify proper operation of the hardware.

Single-Ended Serial Signaling Considerations (RS-232, RS-423, PS/2, I2C, SCSI, etc)

Single-ended signaling standards use a single wire to transmit logic along with a drain to complete the circuit. In the case of RS-232, there is a wire for receive logic and a wire for transmit logic along with other wires for signal control that all rain through a common drain (multiple ground pins are present but are rarely isolated from each other). If problems occur, try the following:

1. Check overall continuity.
2. Make sure the cable being used is appropriate for the given purpose (null modem or not).
3. Make sure the cable length does not exceed the recommended length for the baud rate being used. Many factors influence these numbers including the purity of the metal used and even the temperature of the environment the cable is in.

Use a CAT-5 network cable (max 55pF per meter) standard, the following distances are typical for RS-232:

Data Rate (bps)	Distance (Meters)	Distance (Feet)
2400	60	196.9
4800	30	98.4
9600	15	49.2
19200	7.6	24.9
38400	3.7	12.1
56000	2.6	8.5

Balanced Serial Signaling Considerations (RS-485, RS-422, Serial ATA, PCI Express, 10 Gigabit Ethernet)

Balanced serial connections depend on sending the signal on two (2) wires. The signal on the first wire is unaltered, on the second wire, the signal's polarity is inverted. When the signal is recombined, any interference shows up as a difference between the two (2) signals and is rejected.

If problems occur, try the following:

1. Check overall continuity.
2. Make sure not to reverse the pins on either end of the connection. RS-485 and RS-422 are very intolerant to pin reversals.
3. Check overall cable length. RS-485 can typically go as far as 4000 feet at 400–800Mbps over CAT-5 cables.
4. Lack of termination can greatly reduce the distance a differential signal can travel due to reflections and reception of outside electromagnetic interference. Terminate the differential signal wires by cross-connection the two (2) wires with a resistor equal to the characteristic impedance of the cable (for example, 24awg cable typically has an impedance of 120 Ohms).

Connection to the RT-2M Audio Analyzer

The serial cable between the Trunk Supervisor computer and the RT-2M must have a null-modem cable with all pins connected. The serial connection between the two (2) systems uses hardware flow control so the CTS and RTS pins are used.

All Trunks in Maintenance Mode

If an audio analyzer is selected in the View|Configuration|Configuration Tab, the Test Options tab appears with a section titled *After testing a trunk...*, allowing the *Leave failed trunks in maintenance mode* option to be selected. If this option is selected, then trunks that fail are placed into maintenance mode and not be automatically tested again so it can be returned to service.

Unless there is a specific reason to activate this option, it is best to leave it inactive.

APPENDIX C

Advanced Trunk Supervisor Settings

The most common configuration options for Trunk Supervisor are available via the Configuration window (see X). However, there are a number of other customization options only available through editing the registry directly.

To **open the registry**, do the following:

1. From the Start menu, select **Run...**.
2. At the Run command, type **regedit**.
   The registry editor window appears.
3. In the left navigation, select **HKEY_CURRENT_USER\Software\Telex\tksupv**.
   A list of advanced customization options appear. (defaults shown in brackets).

Preferences\AutoUpdateSortOrder (0)

This option controls whether the sort order on list views is automatically updated with the list data is changed. When enabled, this can make the display visually distracting if the list data is changed frequently.

Allowable values for this setting are:
0 – The list is not automatically re-sorted when a data update occurs.
1 – The list is automatically re-sorted when a data update occurs.

Preferences\AlternateLineShading (2)

This option controls the shading of alternate lines in the list views.

Allowable values for this setting are:
0 – No line shading
1 – Shade every other line
2 – Shade every other pair of lines
4 – Shade every other set of 4 lines

NOTE: The alternate line shading color offset is now a customizable registry setting.

Preferences\AutoSynchronizeTreeView (1)

This option controls whether the navigation tree tries to remain synchronized to what is being displayed in the list view. For instance, if the user changes a filter settings, or navigates by using a context menu of the list view, the navigation tree updates itself and expands to show the current navigation node.

Allowable values for this setting are:
0 – Disable auto synchronization of the navigation
1 – Enable auto synchronization of the navigation

Preferences\CompactDBThreshold (0x00a00000)

This option sets the threshold (default 10MB) for determining if the database should be compacted at start up.

Preferences\CompactDBTimeout (20)

This option sets the timeout before automatically compacting the database at start up if no user input is received.

Preferences\CompactDB (1)

This option sets whether the auto-response is to compact (1) or not compact (0).

Preferences\JetEngineVersion (4)

This option lets you force which Jet Engine is used to create the main database (and compatible archive databases).

Allowable values for this setting are:
3 – Use Jet V3.x
4 – Use Jet V4.x

Preferences\ShowNamelessIntercoms (0)

This option controls whether undefined intercoms appear in the navigation tree an in combo boxes showing lists of intercoms.

Allowable values for this setting are:
0 – Don’t show undefined intercoms
1 – Show undefined intercoms

Settings\AlarmSetup\EmailFromAddress (TKSUPV)
Settings\AlarmSetup\EmailFromDisplayName (Trunk Supervisor)
Settings\AlarmSetup\EmailReplyTo (<null>)

These options are strings that appear in the headers of email (and even pager messages, if desired). They control the appearance of who the notification emails are from, and which email address receives replies, if necessary.

By default, email messages appear to come from Trunk Supervisor (with an email address of TKSUPV), and the Reply To field is empty.

Settings\AlarmSetup\IncludeFromAddressInPagerMessages (0)
Settings\AlarmSetup\IncludeReplyToInPagerMessage (0)

These options control whether the From and Reply To address fields are included in pager messages.
In general, it is a good idea to omit this information from pager messages as there is typically not enough room on the pager display to include these fields and still display the actual alarm messages.

NOTE: These settings have been renamed in V1.6.0 and higher. They used to be called IncludeEmailFromInPagerMessages and IncludeEmailReplayToInPagerMessages. The default values for the new settings are imported from the old settings.

Allowable values for these settings are:
0 – Omit the field from pager messages
1 – Include the field in pager messages

Settings\AlarmSetup\EmailSMTPLoginType (0)
Settings\AlarmSetup\EmailUsername (<null>)
Settings\AlarmSetup\EmailPassword (<null>)

These options are for advanced SMTP use and may be necessary if your SMTP server requires authentication in order to send email. If this is the case, you need to supply a Username and Password, as well as changing the EmailSMTPLoginType to one of the following values.

Allowable values for these settings are:
0 – Authentication not required, Username and Password are not necessary
1 – CRAM MD5 Authentication Required
2 – Authentication Login required
3 – Plain Login required
Please see your email administrator if it is necessary to provide a login.
These values are used for both email and pager messages.

Settings\AlarmSetup\EmailSMTPPort (25)

This option sets the SMTP port to use. Most SMTP servers use Port 25 by default, so you should not likely need to change this setting. This value is used for both email and pager messages.

Settings\AlarmSetup\EmailXMailer (Trunk Supervisor)
Settings\AlarmSetup\PagerXMailer (Trunk Supervisor)

These options set email and pager fields indicating the mailing program name. They are optional fields and need not be changed.

Settings\Preferences\Colors\...

There are a larger number of color setting parameters under this key. All of the colors are stored as RGB values in hex where the value 0x00BBGGRR indicates the color components for Red (RR), Green (GG), and Blue (BB), and each two digit hex number can have a value of 0x00 to 0xff (0-255).

Black is 0x00000000
White is 0x00ffffff
Pure Red is 0x000000ff
Pure Green is 0x0000ff00
Pure Blue is 0x00ff0000

Most of the entries consist of some combination of RGB components.

Each of the parameters names should be self-explanatory, and you can edit these color entries directly, if necessary.

Settings\Configuration\AutoTIMSTimeout (10)

This value is the AutoTIMS communication timeout value in seconds. Versions priority to v1.04.01 had hard coded value of five (5) seconds. The default value is no 10 seconds, and can be adjusted here.

Settings\Configuration\RT-2M\TunaroundTime (1000)

This value is the RT-2M response timeout in milliseconds. The default value of 1000 milliseconds (1 second) was found to suffice in testing, but can be adjust here, if necessary. The minimum response timeout that can be specified is 100 milliseconds.

Settings\Configuration\SyncTrunkMasterClock (1)

This value specifies whether Trunk Supervisor should synchronize the TM-2000 clock to the Trunk Supervisor clock. The default value of one (1) enables such synchronization, same as for version 9.0.x and earlier. Specify a value of zero (0) to diable such synchronization.

Settings\TestParameters\RT-2M\OutputFloat (1)

This value specifies whether the RT-2M output are connected to ground. The default non-zero (1) value leaves the outputs floating so as to avoid ground loops when the RT-2M is connected to a (balanced pair) intercom port. Specify a value of zero (0) to have the RT-2M connect the outputs to ground.

Settings\TestParameters\RT-2M\OutputLevel (1000)

This value specifies the level in mVp (milliVolts-peak) of the signal transmitted to test a trunk. The default of 1000 (1.0Vp) should suffice, but can be adjusted here, if necessary. Any value from 100 (0.1Vp or -20dBVp) to 3000 (3.0Vp or approx. 9.5dBVp)

Settings\TestParameters\RT-2M\InputDeemphasis (0)

This option specifies whether to apply de-emphasis to the RT-2M inputs. The default (zero) value disables de-emphasis; specify a non-zero value (for example, 1) to have de-emphasis applied.

Settings\TestParameters\RT-2M\InputMICSensitivity (500)

This value specifies the MIC sensitivity to be configured for the RT-2M inputs in tenths of a mV/Pa. This parameters is likely irrelevant for the loss testing performed by the Trunk Supervisor, but can be adjusted here, if necessary. Any value from 500 (corresponding to a sensitivity of 50.0mV/Pa) to 50000 (i.e., 5000.0 mV/Pa) can be specified.

Settings\TestParameters\RT-2M\MultitoneLength (250)

This value specifies the duration in milliseconds of the pre-trigger signal transmitted prior to the signal used to test the trunk. The default of 500 milliseconds is intended to give the trunk under test time to react to the presence of the test signal without unduly increasing the time it takes to perform a test. Any duration from 0 milliseconds to 5000 milliseconds (5 seconds) can be specified.

Settings\TestParameters|RT-2MMultitoneLength (250)

This value specifies the duration in milliseconds by which to extend the signal used to test the trunk. The default of 250 milliseconds is intended to give the trunk under test time to stabilize to the test signal without unduly increasing the time it takes to perform a test. Any duration from 0 to 1000 milliseconds (1 second) can be specified.

Settings\TestParameters|RT-2M\TrunkSetupDelay (500)

This value specifies the worst case delay in milliseconds to set up a trunk. The start of the test is delayed by this amount to give the intercoms involved additional time to establish a (loopback) connection to the trunk under test. The default of 500 milliseconds should suffice, but can be adjusted here, if necessary. Any value from 0 to 1000 (1 second) can be specified.

Settings\TestParameters\RT-2M\TrunkLatency1 (2000)
Settings\TestParameters\RT-2M\TrunkLatency2 (3500)
Settings\TestParameters\RT-2M\TrunkLatency3 (5000)

The nature of the multi-tone testing performed by the RT-2M requires that Trunk Supervisor take the latency of the trunk into account when setting up the test. These values specify the series of (possible) trunk latencies, in milliseconds, that the Trunk Supervisor should consider when testing a trunk, in order from shortest possible latency to longest.

The Trunk Supervisor performs an initial test assuming the trunk latency is no longer than the shortest trunk latency configured (i.e. TrunkLatency1). If the actual latency of the trunk is shorter than this, the test succeeds and the RT-2M is able to measure the loss of the trunk. Otherwise, the test fails, in which case the Trunk Supervisor repeats the test, but assuming the trunk latency is no longer than the next longer latency configured (TrunkLatency2). If this test fails as well, then the Trunk Supervisor repeats the test one final time using the longest latency configured (TrunkLatency3).

The default of 2000, 3500, and 5000 milliseconds (2.0, 3.5, and 5.0 seconds) form a series of latencies intended to minimize the total time it take st to test most trunks, while ensuring a measurement is obtained for high latency trunks such as satellite uplinks. The initial (shortest latency of 2.0 seconds should exceed the actual latency of most trunk in practice, meaning only one test needs to be performed for most trunks. No (usable) trunk is likely to have a latency that exceeds the final (longest) latency of 5.0 seconds. These defaults can be adjusted here, if necessary, subject to the following restrictions:

- Any latency from 50 milliseconds to 30,000 milliseconds (0.05 second to 30.0 seconds) may be specified. Latencies shorter than 50 milliseconds (approx.) are ignored; latencies longer than 30,000 milliseconds (approx.) are truncated to 30,000 milliseconds.
- The latencies must be specified in (non-decreasing) order from shortest to longest. A configure latency shorter than the previous latencies (if any) is ignored.

For example, if the following values were configured:

- TrunkLatency1 – 0
- TrunkLatency2 – 5000 (5.0 seconds)
- TrunkLatency3 – 2500 (2.5 seconds)

Then, the Trunk Supervisor would ignore the latencies specified by TrunkLatency1 and TrunkLatency3.

Settings\TestParameters\RT-2M\NoiseFloor (50)

This value specifies the maximum loss (attenuation) in dB permitted when the Trunk Supervisor attempts to determine whether or not the RT-2M received the signal used to test the trunk. The Trunk Supervisor compares this value to the input headroom measured by the RT-2M after a test completes. If the headroom exceeds this value, the Trunk Supervisor interprets this as meaning the RT-2M did not receive the signal because the actual trunk latency is long than assumed when the test was set up. The default of 50dB should suffice but can be adjusted here, if necessary.

APPENDIX D

IP Networking 101

This section covers basic network configuration set up and testing. Also covered are basic concepts and operations, including the difference between **LAN** (Local Area Network) and **WAN** (Wide Area Network) networks and how IP Addressing is used.

In a networked environments, such as a company, typically there are many computers connected together using a router or a switch. In larger companies, there may be several different routers distributed in buildings and plant locations. A router allows any LAN-side computer to communicate with other computers and devices outside the LAN. Routers send data packets from one place to another place on a network. Routers use network addresses to route packets to the correct destination. For example, in a TCP/IP network, the IP Address of the network interface is used to direct router destination.

Because routers help computers inside the LAN communicate with computers outside of the LAN, the security of a company's network may be compromised by gaps, made by open ports in the router. Security measures may have been instituted to compensate for these vulnerabilities. Consult your network administrator to learn about the security measures taken to protect you network. **VPN** (Virtual Private Network) is a security measure taken to protect the intelligence of the LAN. A computer outside the network must have an address or key known by the VPN to allow access to the LAN. Many companies use a VPN to connect two (2) different LANs, allowing the transfer of data between the two (2) networks.

LAN vs WAN

Local Area Network

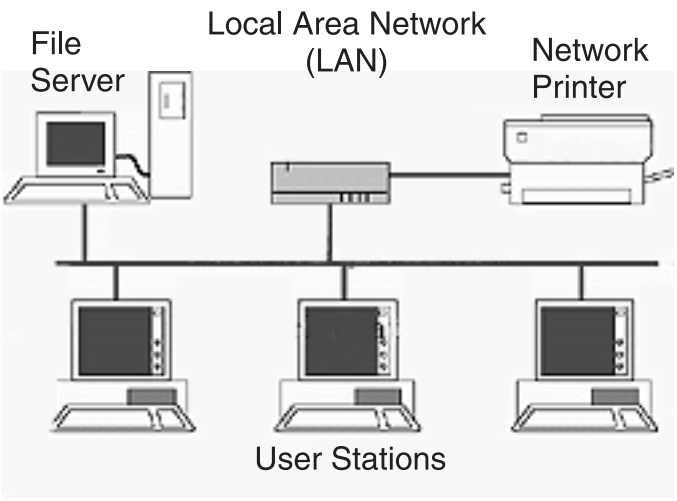


FIGURE 24. Local Area Network

Simply put, a LAN is a computer network connecting a relatively small area (for example, a single building or group of buildings). Most LANs connect workstations and computers to each other. Each computer (also known as a node), has its own processing unit and executes its own programs; however it can also access data and devices anywhere on the LAN. This means many users can access and share the same information and devices. A good example of a LAN devices is a network printer. Most companies cannot afford the budgetary or hardware expense of providing printers for each of its users; therefore, one printer (or device) is placed on the LAN where every user can access the same printer.

The LAN uses IP Address to route data to different destinations on the network. An IP Address is a 32-bit numeric address consisting of four (4) numbers separated by periods (for example, 1.160.10.240).

NOTE: For more information on IP Addresses, see your local network administrator.

Wide Area Network

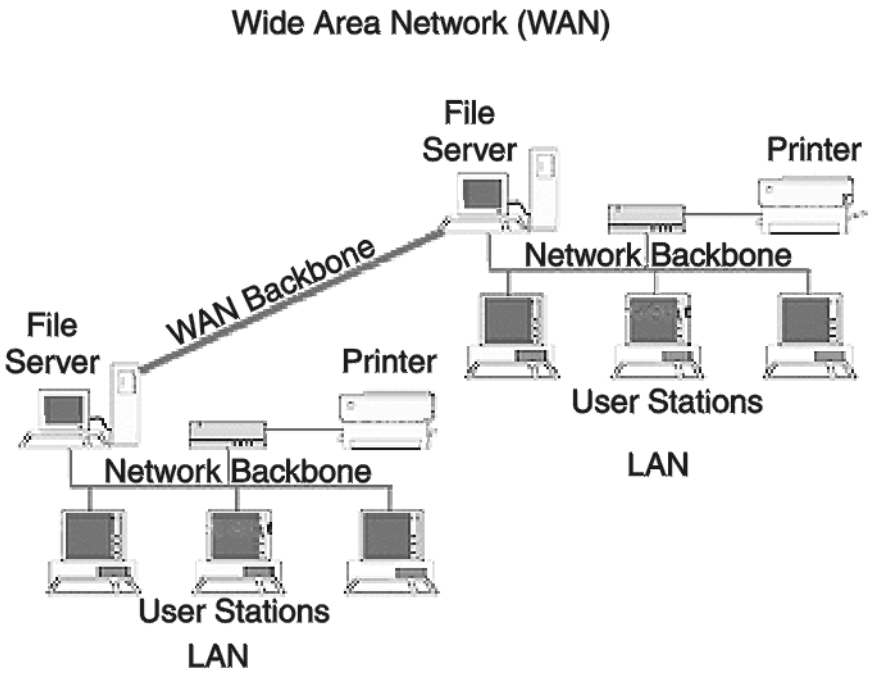


FIGURE 25. Wide Area Network

A WAN connects two (2) or more LANs and can span a relatively large geographical area. For example, Bosch headquarters in Burnsville, MN is connected to several branch offices in Nebraska and Arkansas over a WAN. The largest WAN in existence is the Internet.

Access the WAN

Fig X shows LAN IP Addresses using a common IP Address, 10.2.100.X (192.168.X.X is another common address). Most devices are shipped with these addresses as default. It is recommended to use these addresses for LANs.

Network Address Translation

Using the initial IP Address, then converting it to a valid WAN IP Address is how **NAT** (Network Address Translation) works, in theory. Once the IP Address is changed, the network interface device (such as a router, gateway, switch, etc) is responsible for keeping track of which computers on talking on various ports. For example, if two (2) local devices (PC1 and PC2) both wanted to communicate over port 1031, the network interface device would have to modify one of the ports request to the next available port, 1032.

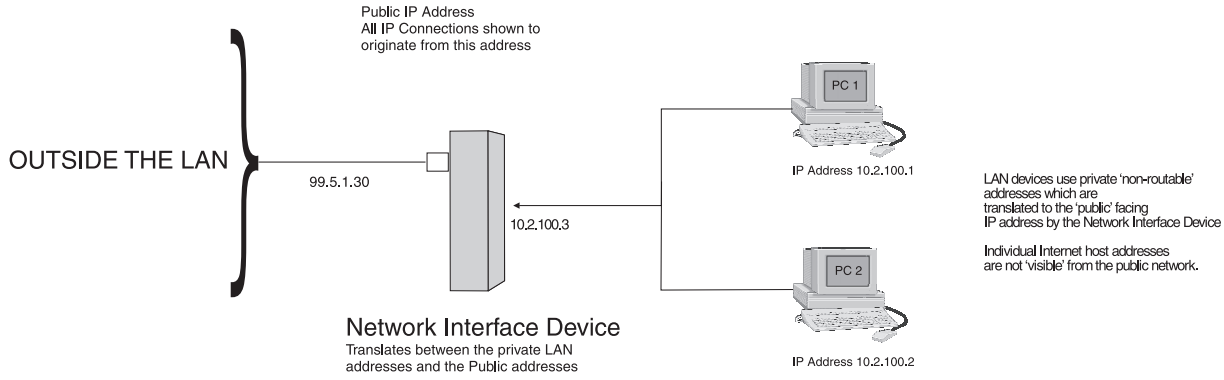


FIGURE 26. Network Address Translation

Ports

In general, a network port is an endpoint to a logical connection. the port number identifies what type of port it is. For example, port 80 is used for HTTP traffic. When you type an address into the address bar of a web browser, your computer tries to find an IP Address for the URL you are requesting (http://www.boschcommunications.com). To obtain this address, the computer contacts a DNS server (Domain Name Server). once the IP Address is found, it tries to connect to the http port of the3 network device (port 80. See Table X for a list of well-known port numbers.

TABLE 1. Well-known TCP Port Numbers

Port Number	Description
1	TCP Port Service Multiplexer (TCPMUX)
5	Remote Job Entry (RJE)
7	ECHO
18	Message Send Protocol (MSP
20	FTP-Data
21	FTP - Control
23	Telnet
25	Simple Mail Transfer Protocol (SNMP)
29	MSG ICP
37	Time
42	Host Name Server (Nameserv)
43	Whols
49	Login Host Protocol (Login)
53	Domain Name Server (DNS)
69	Trivial File Transfer Protocol (TFTP)
70	Gopher Service
79	Finger
80	HTTP
103	X.400 Standard

TABLE 1. Well-known TCP Port Numbers

Port Number	Description
108	SNA Gateway Access Server
109	POP2
110	POP3
115	Simple File Transfer Protocol (SFTP)
118	SQL Services
119	Newsgroup (NNTP
137	NetBIOS Name Service
139	NetBIOS Datagram Service
143	Interim Mail Access Protocol (IMAP)
150	NetBIOS Session Service
156	SQL Server
161	SNMP
179	Border Gateway Protocol (BGP)
190	Gateway Access Control Protocol (GACP)
194	Internet Relay Chat (IRC)
197	Directory Location Services (DLS)
389	Lightweight Directory Access Protocol (LDAP)
396	Novell Netware Over IP
443	Hyper Text Transfer Protocol (HTTP)
444	Simple Network Paging Protocol (SNPP)
445	Microsoft-DS
458	Apple Quick Time
546	DHCP Client
547	DHCP Server
563	SNEWS

Each network device can be set up to respond or not respond to the various ports. The function of responding or *hosting a service* is called *serving*.

TABLE 2. Packet Translation

	Source		Destination		Source		Destination	
	IP Address	Port No.	IP Address	Port No.	IP Address	Port No.	IP Address	Port No.
To Internet	10.2.100.2	1031	192.156.136.22	80	99.5.1.30	1031	192.156.136.22	80
From Internet	192.165.136.22	80	99.5.1.30	1031	192.156.136.22	80	10.2.100.2	1031

If a second workstation on the LAN wants to communicate to the same server, and happens to use the same source port number, then the LAN translates the source port number as well as the source IP Address. In Table 2, a second LAN computer wants to access a web page. The NAT device now uses port 1032 for this connection where it used port 1031 in Table 3.

TABLE 3. Packet Translation II

	Source		Destination		Source		Destination	
	IP Address	**Port No.**	**IP Address**	**Port No.**	**IP Address**	**Port No.**	**IP Address**	**Port No.**
To Internet	10.2.100.1	1031	192.156.136.22	80	99.5.1.30	1032	192.156.136.22	80
From Internet	192.165.136.22	80	99.5.1.30	1032	192.156.136.22	80	10.2.100.1	1031

Amazingly, all the address translation occurs automatically in order to make web browsing and other functions easier. This is also a way for large web hosting services to speed up the network by having different devices perform different functions.

IP Addresses

Find Your Computer's IP Address

To **find your IP Address using ipconfig**, do the following:

1. From the Start menu, select **Run...**.
2. At the Run command, type **CMD**.
   A Command Prompt window appears.
3. At the prompt, type **ipconfig**.
4. Press **Enter**.
   The IP configurations appear for your machine, such as the DNS suffix, IP Address, Subnet Mask, and Default Gateway.
5. At the prompt, type **Exit** to close the window.

NOTE: If you want more detailed parameters for your machine, type ipconfig/All. This screen shows the computers network configuration settings.

Ping a Computer

Pinging a computer on the network makes sure it is able to be seen and receive messages on the network.

NOTE: You can also ping your RVON card to verify it is responding over he network by substituting the card's IP Address in place of the computer IP Address.

To **ping a computer (or RVON) on the network**, do the following:

1. From the Start menu, select **Run...**.
2. At the Run command, type **CMD**.
   A Command Prompt window appears.
3. At the prompt, type the **IP Address of the computer or RVON card** you want to ping (for example, 10.2.100.130).
4. Press **Enter**.
   A Successfully Ping message appears.
   OR
   If the computer you are pinging is not responding to the pin, a time-out message appears.

Possible Pitfall with Routers, Gateways, and Switches

Anytime computers communicate through routers, gateways, and switches, they may be allowed or denied the connection. Network interface devices can be configured to block specific outgoing requests, as well as incoming requests, based on the IP Address and/or port. This is one of the security mechanisms of a router. This also happens when broadcast messages are sent and received.

To view the path an IP Address takes to retrieve information, do the following:

1. From the Start menu, select **Run...**.
2. At the Run command, type **CMD**.
   A Command Prompt window appears.
3. At the prompt, type **tracert <IP ADDRESS>** (for example, tracert 10.2.250.6) you want to trace.
4. Press **Enter**.
   The details of the tracer route are displayed.

   NOTE: If the IP Address/port in or out is denied to the incoming or outgoing message, a *Request Timed Out* message appears.
5. When you are finished, type **Exit** to close the Command Prompt window.

RVON Configuration

RVON Cards use ports for communication of audio and control packets. Because routers can be configured to block certain incoming and outgoing request, you need to open the following ports in your network to all WAN connections to and from a network interface device. See Table X for the port needing to be opened for RVON cards to operate properly.

TABLE 4.

Port	Description
2076	UDP Call Control Signalling
2077	UDP Audio Packets
2080	TCP Telex Keypanel Protocol
2081	UDP Pass Through Serial
2082	TCP Firmware Download
2100	Remote Administration
2102	Authentication Server

APPENDIX E

Trunking 101

A User's Guide to Trunking

Very large systems, split operation and trunking

Trunking is similar to the long distance telephone system. In the case of RTS ADAM matrix intercom systems, this analogy is close to reality.

What is meant by a Large System? How big is BIG? With older technology (pre-TDM), systems were limited to a certain size because of physical size and cost, not because of any particular technological or logistic limitations.

Today, intercom matrices, in general, and RTS intercom matrices, in particular, have a higher absolute limit, and a larger typical size. For example, in the early 1980s, a well-appointed, high-end sports truck of the type which would serve an NFL game, would likely have had 12 PL channels, six (6) IFB channels and six (6) ISO channels. Today, most network size trucks carry 64 channels or more in the ADAM matrix, and in some cases, over 100 channels. Intercoms have grown to carry program audio for monitoring, support 10, 15, or 20+ cameras, a host of graphic operators, and statistics personnel. What is typical today was unimaginable less than 20 years ago.

Matrix sizes

TABLE 5. Comparison of Relative System Sizes

Matrix	Ports
RTS Zeus Matrix Intercom System	24 ports fixed
RTS ADAM-CS Matrix Intercom System	8 – 64 ports in groups of 8
RTS ADAM Matrix Intercom Single Frame	8 – 136 ports in groups of 8
RTS ADAM Matrix Intercom Multiple Frames	136 – 1000 ports in groups of 8

These are the numbers of ports available in a single RTS Intercom Matrix. Other manufacturers offer systems in sizes from eight (8) to approximately 500 ports. As you can see, size is not a limitation in most cases. At the time of this writing, the largest known single matrix intercom system in service is a RTS ADAM of 672 ports at NBC in New York.

Advantages of multiple small matrices

Many factors guide the design in favor of smaller individual systems. If the system is needed for four (4) separate studios in a facility, which never or very rarely work together, it may make more sense to use four (4) separate system. Some of the very good reasons for doing this might include the following:

- Cost: Four (4) 128-port system cost less than one (1) 512-port system.
- Reliability: A fire in rack room does not destroy the single entire system.
- Manageability: Four (4) different control studios have four different crews only affecting the setup of their operation.
- Shorter cable runs: The matrix for a given group of panels can be physically closer to those panels.
- Easier to expand a single matrix if the needs for one area grow.

Advantages of a single large matrix

- Operations require ability for any of the 512 users to communicate with any of the other users.
- Desire for single point of administration, control, troubleshooting, and monitoring.
- Design of the facility is highly decentralized operationally, and day to day, different portions of the facility must work together.
- Certain users must work with all the facilities, and giving them four (4) separate keypanels (one (1) per system) is just not an option.

Hybrid Designs

Certain requirements drive you to separate matrices, but one (1) or two (2) key factors seem to demand a single matrix. A couple of different options or hybrid designs can be used in these cases. The first and simplest is to define a few common points of contact between the intercom matrices. For example, a television complex has two (2) studios and two (2) control rooms. Normally control A works with studio A, and control B works with studio B. Occasionally, the wall between the two (2) studio opens and there is a need for control A to work with the cameras in the combined studio A and B. Furthermore, the normal method of operating has the cameras in each studio receiving two (2) channels of intercom; a Technical PL, created in

the intercom configuration, and a Production PL, also created in the intercom configuration of the respective matrices for studio A and studio B.

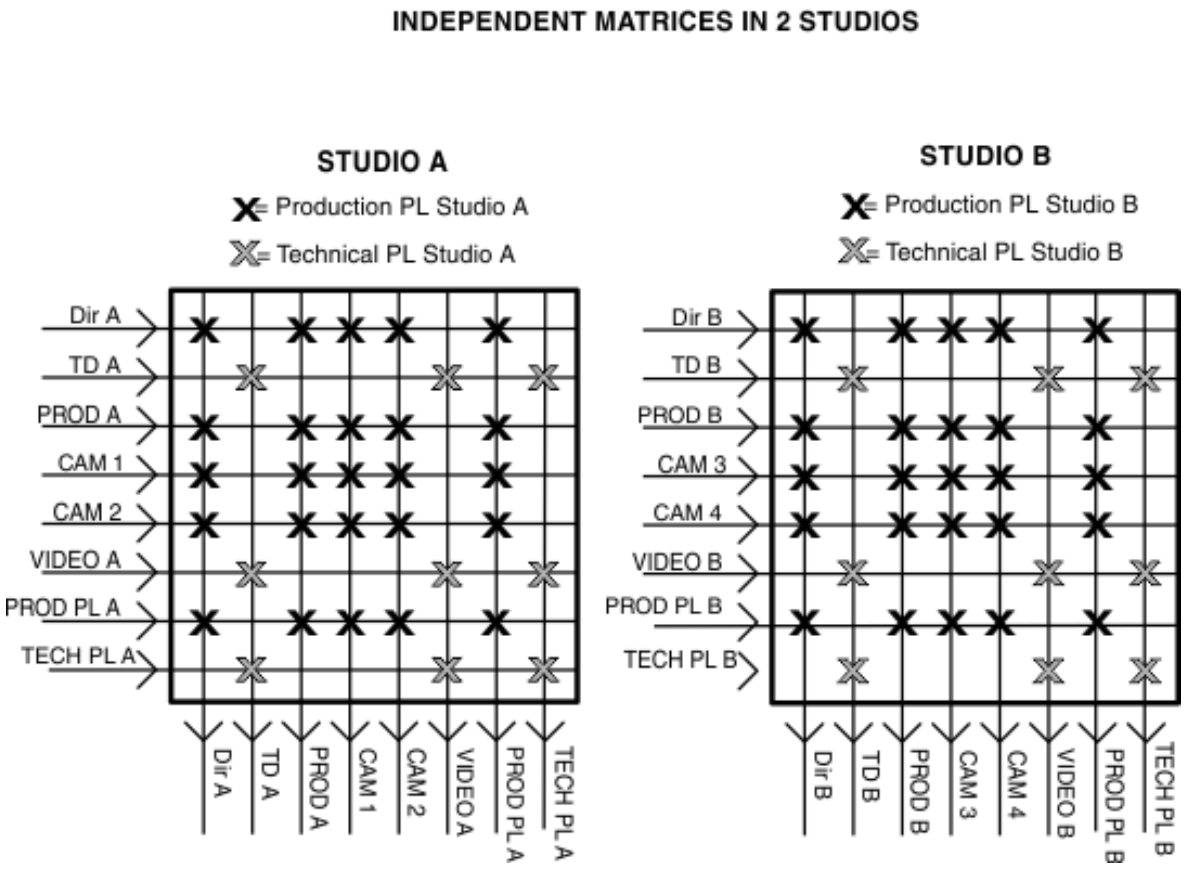


FIGURE 27. Separate Studios, Separate Intercom

Unintelligent Trunking

Unintelligent trunking means that no system intelligence is employed to establish the trunks. For example, a quick way of allowing the combined operation is to configure (using AZedit) the production and technical PLs of each matrix to include two (2) available sets of ports on a jackfield. Connect the output of production PL from stud A to the input of production PL for studio B, and the output of production PL from studio B to the input production PL for studio A and the same for the technical PLs.

Now, any conversations on production PL for A control is also available to the studio B cameras for both talking and listening and the same is true for the technical PL.

Intelligent Trunking

In intelligent trunking, the trunk master figures out which matrix has which ports and keys track of it for you. The Trunk Master is a computer designed to route trunk lines between intercom systems. For example, if you assign “ADIR” from the stud A matrix to a panel on the matrix for control room B, the system knows it has to configure and establish a trunk to allow the conversation to take place. It does this automatically, establishing the trunk, monitoring trunk usage, and releasing the trunk when the conversation is completed.

Limitations

Why not use trunking and avoid huge matrices? The reason trunks are not used for every system is because there are a limited number of trunk lines and once they are all in use, calls must wait and/or get busy signals. So, when systems are trunked together, consideration should be made to the number of trunk lines needed in relation to the number of users in the system.

Intelligent trunking, through the use of the trunk master, continuously monitors and reports on the status of trunk utilization, including the maximum number of trunks used at one given time. With good historical data, you can determine the number of trunks your system needs to allot for seamless operation.

NOTE: No matter how much research and planning you put into determining the number of trunks you need, there always exists the unforeseen possibility you may run out of trunks lines.

Another limitation with trunking is for each line you trunk you are giving up a port that could have otherwise been used for two (2) keypanels (one at each matrix). Having too many trunk lines you can inadvertently limit the number of keypanels allowed on the matrix. In turn, you may spend more money to buy additional ports for each matrix.

Limitations aside, trunk can be a good solution for many applications. Trunk works best when limited numbers of trunks are required to support occasional usage. Trunking works well when many matrices need to be interconnected. Intelligent trunking can simultaneously handle automated routing between more than 20 matrices. A side benefit of a multi-system trunked environment is the Trunk Master can determine and establish trunk paths via multiple hops if needed due to trunk usage. If the trunks from matrix A to B are all in use, the possibility exists for the trunk master to route a signal from A to C and from C to B, bypassing the bottleneck.

Another advantage of trunking is there is no requirement for the individual matrices involved to be in close proximity. Systems, which are hundreds or thousands of miles away, have been successfully trunked using a variety of media for transporting the 9600 bps data and audio between sites. Intelligent trunking has been implemented using LAN, WAN, copper, satellite feeds, microwave links, fiber, and combinations of these to transport the audio and data between matrices and the trunk master.

A final methodology for distributing large matrices is a function of the manner in which multiple ADAM frames are interconnected. When two (2) ADAM frames, each 128 ports, are connected together, they become functionally a single 256-port intercom system. The interconnect between the two frames is via a Bus Expander, which transports all 128 ports between the two (2) frames without rendering any of them unusable for keypanels.

The physical interconnect between the frames with bus expanders can either be via a pair of coaxial cables, which can be used for distances up to 1000 feet, or via a pair of fiber optic cables, which can run for over 100 meters. The signal sent over the fiber or coax is a multiplexed data stream, running at approximately 220megabits/second. Since this data rat is lower than the 270 megabit CCIR-601 serial digital video standard, many of the asynchronous devices that can transport serial digital video can be used for this signal to achieve even greater distances.

By using the Bus Expander with multiple ADAM frames, a single electrical matrix can be located floors or buildings apart within a complex, and yet function as a single large matrix.

APPENDIX F

Terminology

General Terminology

Trunkmaster – The Trunkmaster is the primary piece of hardware required for trunking. It is comprised of a customized Linux operating system designed to run on a standard, but highly specific hardware. It is responsible for coordinating the communication of multiple ADAM frames and or system.

Trunk Edit – Trunk Edit is the software interface application used to configure the Trunkmaster. This application runs on a Microsoft Windows compatible computer. After the proper connections have made, this application configures the Trunkmaster's firmware. This tells the Trunkmaster which connections to expect data from and which matrix it is being sent from.

Trunk Supervisor – Trunk Supervisor is a Microsoft Windows compatible application allowing the user of an RTS trunking system to monitor and test the trunking system in real time. It is a software application that configures the firmware on the chassis.

Front-End/Back End – Generally speaking, industrial-grade electronic equipment has very high standards of operation. While it may be annoying if a smart phone or general use computer becomes corrupt or ceases to operate, it would be catastrophic if industrial equipment failed in the same manner. A requirement of industrial electronics is failover or redundant protection. This means that when a component of the system fails, it automatically switches to a backup resource, giving a technician time to be notified and repair the primary component.

RTS matrix and trunking systems are designed to satisfy these industrial grade requirements. RTS system cores are built on the terminal-server methodology, meaning the core operating system is a fully autonomous, highly specialized processing unit that is configured using a remote terminal.

The software is meant be accessible and easy-to-use, whereas the firmware is typically proprietary and focused on reliability rather than user interface. This design methodology is most used in industrial application and is the most proven design methodology. Trunk Supervisor, TrunkEdit, AZedit, and IPEdit are all examples of software applications that configure the hardware and firmware of ADAM and Trunkmaster systems. Because the user is the client and the ADAM or Trunkmaster is the server, when making changes the software reports it is uploading the changes. This can be confusing for peer-to-peer environment users, where it is typically assumed their computer is always the server.

Contextual Menus – Contextual menus are also known as shortcut menus or pop-up menus. Right-clicking the mouse in certain areas of the application window activates a pop-up menu with additional menu options that apply to the specific area of the window. As with the system menus at across the top of the window, this is a service most operating systems provide to the application so the specific appearance of this menu is dictated by the host operating system. The implementation of these menus are optional and may not always be implemented in every area.

Network Terminology

Bridge – A bridge is a device connecting two (2) LAN, or two (2) segments of the same LAN using the same protocol, together. Sometimes called transparent bridges, they work at the OSI model Layer 2. Simply put, they are not concerned with protocols. Their main job is to pass data to a destination address predetermined in a data packet

With a bridge, all of your computers can be on the same network subnet. This means the computers can communicate with each other and have their own Internet connection.

NOTE: If you assign your own IP Addresses, take care to use the same first three (3) octets of the IP Address for each computer (for example, 192.168.0.X).

Domain Name Server (DNS) – A DNS server is an Internet service that translates domain names (for example, in the URL http://www.bosch.com, the domain name is bosch.com) into IP Addresses. The Internet is based on IP Address which are numeric. Since domain names are alphabetic, a DNS server must be used to translate the domain name into an IP Address.

Gateway –

A gateway is a node on a network that serves as an entrance to another network. The gateway routes traffic from one computer to an outside network serving web pages. For example, the gateway for a home computer is the ISP (Internet Service Provider) that connects the user to the Internet.

In a corporate environment, the gateway often acts as a proxy server and a firewall. Gateways are similar to routers and switches because they forward data to the destination and provide the data path to a destination.

Hub –

A hub is a common connection point for devices in a network. A hub has multiple ports. When a data packets arrives at a hub, it is copied and distributed to all of its ports so all nodes on the LAN can see the packets.

- passive hub - this hub serves as a conduit for the data, enabling it to go from one (1) device to another.
- switching hub - this hub reads the destination address of each packet and then forwards the data packet to the appropriate port.
- intelligent switch - this hub includes additional features enabling administrators to monitor traffic through the hub.

IP Address –

An IP Address is an identifier or numerical name for a computer or device on a network. Data between computers are routed over the network using these addresses to identify the computer the message is being sent to and the computer the message is being sent from.

The format of an IP Address is a 32-bit numeric address written as four (4) numbers separated by periods. For example, an IP Address looks like 10.100.1.1.

NOTE: When working within an isolated network (meaning there is no Internet access), IP Addresses can be assigned at random, as long as they are unique to each device. When the isolated network is connected to the Internet, registered IP Addresses must be obtained. This is to prevent duplication of addresses.

The four (4) numbers in an IP Address are used in different ways to identify a particular network and host on that network.

There are three (3) classes of Internet Addresses:

- Class A - supports 16 million hosts on each of 127 networks (i.e., 192.xxx.xxx.xxx)
- Class B - supports 65,000 hosts on each of 16,000 networks (i.e., 192.168.xxx.xxx)
- Class C - supports 254 hosts on each of 2 million networks (i.e., 192.168.1.xxx)

LAN – A LAN (Local Area Network) is a computer network connecting a relatively small area (a single building or group of buildings). Most LANS connect work stations and devices to each other. Each computer (also known as a node), has its own processing unit and executes its own processing unit and executes it own programs. It can also access data and devices anywhere on the LAN. This means many users can access and share the same information and devices. A good example of a shared LAN device is a network printer.

A LAN uses IP Addresses to route data to different destinations on the network. And IP Address is a 32-nit numeric address written as four (4) numbers separated by periods (1.160.10.240).

Port – A port, when referring to TCP and UDP networks, is an endpoint in a logical connection. The port number identifies the type of port it is. For example, port 80 is used for HTTP traffic.

Router – A router is a device that forwards data packets over networks. Most commonly, a router is connected to at least two (2) networks (normally LANs or WANs). Routers are located at gateways, the place where two (2) networks are connected. Routers do little data filtering, they mainly deliver the data.

Subnet – A subnet is a portion of a network that shares a common address component. On a TCP/IP network, a subnet is described as all computers or devices whole IP Address have the same prefix.

Subnetting a network is useful because it provides security for the network as well as increases performance of the network. IP network are divided using subnet masks.

Switch – A switch is a device that filters and forwards data packets between networks. Switches operate at the data layer, and sometimes at the network layer.

WAN A WAN (Wide Area Network) connects two or more LANs and can span a relatively large geographical area. The largest WAN is the Internet.

Notes

Bosch Security Systems, Inc.
12000 Portland Avenue South
Burnsville, MN 55337 U.S.A.
www.boschcommunications.com