Military Unique Deployment Guide Thinklogical VDS

Thinklogical, LLC
100 Washington Street
Milford, Connecticut 06460 U.S.A.
Telephone: 1-203-647-8700
Fax: 1-203-783-9949
www.thinklogical.com

Value Your Content
thinklogical®
Trust Our Proven Ingenuity

Value Your Content

thinklogical®

Trust Our Proven Ingenuity

Copyright Notice

Thinklogical® LLC
100 Washington Street
Milford, Connecticut 06460 U.S.A.
Telephone: 1-203-647-8700

Title: Military Unique Deployment Guide
Subject: Thinklogical VDS Deployment Guide
Revision: F, December 2014

MX48 Router

thinklogical®

Table of Contents

Summary of Changes

Version	Date	Change Description
A	3/21/14	Initial Revision
B	10/1/14	Updated SUT diagram
C	10/2/14	Added information regarding logging and passwords
D	10/10/14	Revised conditions of fielding and logging information
E	12/9/14	Revised administrator access and setup instructions, audit logging information
F	12/15/14	Added document title, POC, and revision block, revised Conditions of Fielding

SYSTEM POC.

Mr. Lawrence Wachter
100 Washington Street, Milford, CT 06460,
Office: 203-647-8720
Larryw@thinklogical.com

PREFACE

Conventions Used in this Manual

Throughout this manual you will notice certain conventions that bring your attention to important information. These are **Notes** and **Warnings**. Examples are shown below.

⚠ **Note: Important Notes appear in blue text preceded by a yellow exclamation point symbol, like this.**

A note is meant to call the reader's attention to helpful information at a point in the text that is relevant to the subject being discussed.

🛑 **Warning! All Warnings appear in red text, followed by blue text, and preceded by a red stop sign, like this.**

A warning is meant to call the reader's attention to critical information at a point in the text that is relevant to the subject being discussed.

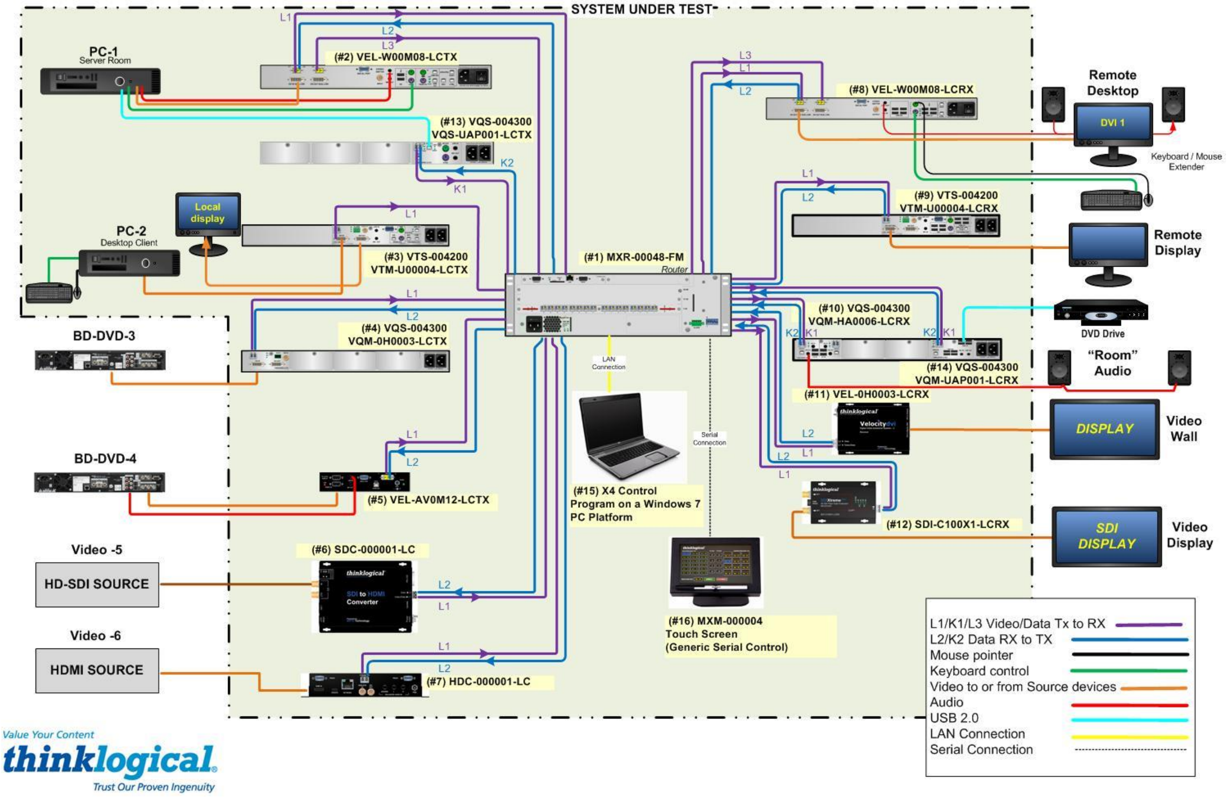
BEFORE STARTING ANY PROCEDURE, IT IS RECOMMENDED THAT YOU READ THE INSTRUCTIONS THOROUGHLY!

1 Introduction

This document describes the configuration and setup requirements for a Thinklogical, Velocity Closed Video Matrix Switching Solution, Revision 4. This system includes video distribution as well as other computer interfaces such as keyboard and mouse. Video and KVM extension is provided by a fiber optic Transmitter Module connected to a fiber optic Receiver Module. The computer video and interfaces are digitally transmitted at 6.25Gbps using Video and KVM Transmitter Modules. These computer video and interfaces are re-generated at the Receiver Module. The 6.25 Gbps of bandwidth over fiber optic provides signal integrity, allowing for uncompressed video, with no frame dropping. The Matrix Router allows connection of any Transmitter Module to any Receiver Module.

2 System Features

2.1 Example System



2.2 Video and KVM Transmitter and Receiver Modules

Thinklogical Video and KVM extenders fully support digital video (SDI, HDMI, DVI single link and dual-link), analog video, PS2, USB-HID, 2.0, serial, keyboard, mouse, CD quality audio, and 10/100 network extension. These extenders also feature- stereo emitter for active 3D applications, simple plug and play, dry contact annunciator provides an alarm warning in the event of a power failure or a unit overheating, front panel status monitoring and control, they are also fully compatible with Velocity line.

2.3 Matrix Router (MX48)

Thinklogical MX and VX routers are true non-blocking matrix switches and leverage bi-directional signal capability, and range in size from 48 x 48 up to 640 x 640. Thinklogical routers are expandable to provide 5 duplex ports up to 640 duplex ports, for directional video routing and switching. Our non-blocking routers allow multiple input signals to be available at one output. Every input and output is capable of up to 6.25 Gbps of bandwidth. It has Multi-Mode and Single-Mode fiber capabilities using industry standard SFP+ optics. Thinklogical routers allows for all critical system components including power supplies, cooling fans and pluggable optics (SFP+) to be hot-swappable. The hot-swappable I/O boards allow the router to be reconfigured without interrupting signal processing by powering down the router. In addition, the dual redundant power supplies ensure continuous, uninterrupted power.

Power Supplies

One power supply is standard with the MX48 Chassis. However, an optional dual redundant power supply is available to ensure continuous, uninterrupted power. The supplies are current sharing which means the supplies equally share the load. If a power supply were to fail, the single power supply can withstand the entire current load of the MX48 system. Although the router functions properly with one Power Module, it is recommended that both Modules preferably be connected to two independent power sources (for redundancy). Additionally, the hot-swappable feature allows for easy replacement of a module (in case of failure) without interrupting the routers system functionality.

Fan Tray

The MX48 uses 3 DC fans all located conveniently in one modular fan tray. The tray is designed to move air horizontally through the enclosure. This hot-swappable fan tray allows for easy replacement of the module (in case of failure) without interrupting the system functionality. Any 2 DC fans will adequately cool either system.

The Fan Tray is also equipped with an Annunciator Port for the use of alarms. The system alarms can be configured to trigger an external control system.

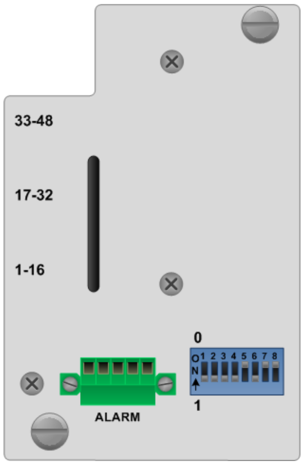
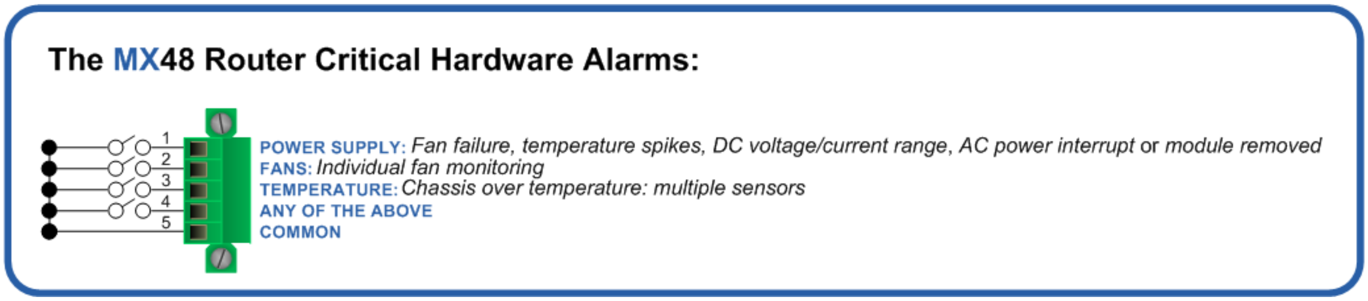


Figure 6: MX48 Fan Tray with Alarm Annunciator

The Critical Hardware Alarms are as follows:



The MX48 Router Critical Hardware Alarms:

POWER SUPPLY: *Fan failure, temperature spikes, DC voltage/current range, AC power interrupt* or *module removed*
FANS: *Individual fan monitoring*
TEMPERATURE: *Chassis over temperature: multiple sensors*
ANY OF THE ABOVE
COMMON

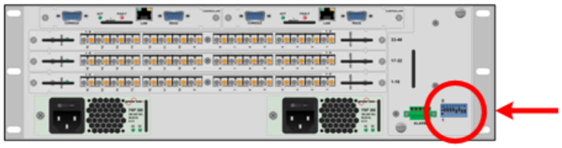
Figure 7: Alarm Descriptions and Drawing for the MX48

Controller Card

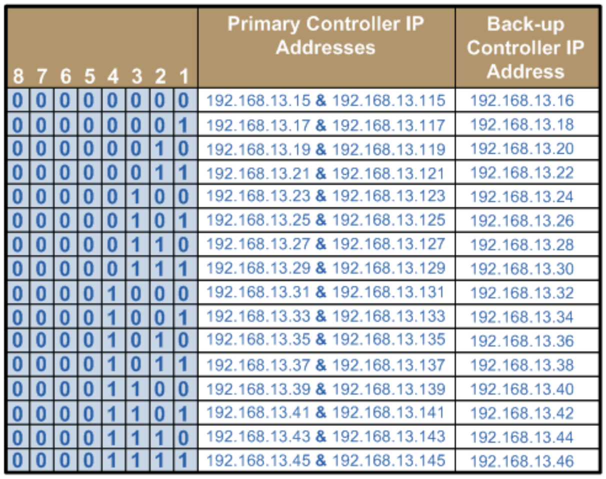
The hot-swappable Controller Card connects the Router to an External CPU. The serial port can also be used for 3rd party controller integration (such as Crestron, AMX or home-spun interfaces). Also, the X4 Configurator Software (Appendix D) can be used to control the Router via the LAN port.

If the MX48 Router is to be controlled via ethernet, it will require a static IP address. This value can be set via the DIP switch to the values listed below. Factory default setting will be **192.168.13.15**.

MX48 Router DIP Switch Location & Settings



MX48 Router Rear Panel



8	7	6	5	4	3	2	1	Primary Controller IP Addresses	Back-up Controller IP Address
0	0	0	0	0	0	0	0	192.168.13.15 & 192.168.13.115	192.168.13.16
0	0	0	0	0	0	0	1	192.168.13.17 & 192.168.13.117	192.168.13.18
0	0	0	0	0	0	1	0	192.168.13.19 & 192.168.13.119	192.168.13.20
0	0	0	0	0	0	1	1	192.168.13.21 & 192.168.13.121	192.168.13.22
0	0	0	0	0	1	0	0	192.168.13.23 & 192.168.13.123	192.168.13.24
0	0	0	0	0	1	0	1	192.168.13.25 & 192.168.13.125	192.168.13.26
0	0	0	0	0	1	1	0	192.168.13.27 & 192.168.13.127	192.168.13.28
0	0	0	0	0	1	1	1	192.168.13.29 & 192.168.13.129	192.168.13.30
0	0	0	0	1	0	0	0	192.168.13.31 & 192.168.13.131	192.168.13.32
0	0	0	0	1	0	0	1	192.168.13.33 & 192.168.13.133	192.168.13.34
0	0	0	0	1	0	1	0	192.168.13.35 & 192.168.13.135	192.168.13.36
0	0	0	0	1	0	1	1	192.168.13.37 & 192.168.13.137	192.168.13.38
0	0	0	0	1	1	0	0	192.168.13.39 & 192.168.13.139	192.168.13.40
0	0	0	0	1	1	0	1	192.168.13.41 & 192.168.13.141	192.168.13.42
0	0	0	0	1	1	1	0	192.168.13.43 & 192.168.13.143	192.168.13.44
0	0	0	0	1	1	1	1	192.168.13.45 & 192.168.13.145	192.168.13.46

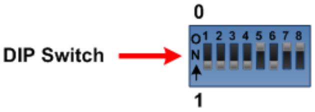


Figure 8: MX48 Router DIP Switch Locations and Setting

The simplest network connection is an isolated network with only the MX48, the control server, and any control clients using static IP addresses. The MX48 can be set to any of the above settings. The control server must be at **192.168.13.9**, and the control clients could then be set to any other addresses in the **192.168.13.X** family.

If static IP addresses for the control server and its clients are not possible, then the control server will require two (2) network interfaces with one interface set to the static address **192.168.13.9** and dedicated to the MX48 Router(s) while the other network interface can be configured as required by the facility's network administrator.

A **Back-Up Controller Card is optional** to ensure uninterrupted functionality if the Primary Controller Card should fail or need to be replaced. The Primary Controller Card should always be in the left controller slot. This card must have a LAN connection that allows it to communicate with both the Primary Controller and a server having an IP address of **192.168.13.9**. Without this interface the back-up controller will never take control of the router.

3 Connecting to the Matrix Router

All physical connections to the product use industry-standard connectors. Non-supplied cables that may be needed are commercially available. All connections are found on the rear of the unit.

3.1 Fiber Optic Cable

Requirements

Thinklogical recommends SX+ Laser Enhanced (50µm) fiber for your Matrix Router and Velocity Extension System. Multi-mode fiber has the ability to extend up to a maximum of 1000m, where Single-mode fiber has the ability to extend distances beyond 1000m.

Handling Fiber Optic Cable

Unlike copper cabling, fiber optic cable requires special handling. A small speck of dust or a scratch to the ferrule tip (the end of the connector) can attenuate the optical signal so that it becomes unusable.

STOP **Warning! The ends of the connectors (the ferrule) should never come in contact with any foreign object, including fingertips.**

STOP **Warning! Minimum bend radius must be 1.5". Be careful not to pinch the fiber when using ties.**

Installing Fiber into Input/Output Cards

Step 1: Grasp the LC connector of the fiber optic cable by the sides and remove the dust cap.

Step 2: Open the LC retractable and carefully insert the fiber connector into the SFP+ port until it locks into place.

Removing Fiber from Input/Output Cards

Step 1: The LC connector has a locking feature that can be released by depressing the latch-release tab located on the side of the connector. With the tab depressed, slowly remove the cable by pulling the connector straight out of the SFP+ port.

Step 2: Immediately install a dust cap on the ferrule to protect the fiber tip.

3.2 Connecting to a Control Computer

⚠ **Note: The Control Computer is supplied separately from the Matrix Router.**

The MX48 is controlled via a dedicated external Control module. This allows for customization as well as ease of control and administration with access provided via a network connection (browser).

Basic controls and status of the Matrix Router are executed using ASCII commands over either the serial (RS232) port or the LAN (10/100base-T) port. The serial port can be used for 3rd party controller integration (such as Crestron, AMX or home-spun interfaces). The X4 Configurator Software (Appendix D) can be used to control the Router via the LAN port.

3.3 Connecting to Thinklogical® Velocity Extenders

The MX and VX Matrix Routers are designed to work with any Thinklogical® product designed with the MRTS technology (e.g. Velocity Extenders). The Matrix Routers and Velocity Extenders are a new, unique class of cost-effective matrix switching and KVM extension designed for a variety of high-performance computing environments. Comprised of a fiber-in, fiber-out matrix switch and a fiber-optic KVM extender (with a transmitter and receiver), this complete system provides transparent and secure routing, switching and extension of video and high-speed data peripherals to remote destinations with ease.

Connecting to the Receiver

The Velocity Receiver serves as the Destination (desktops, theaters, conference rooms, editing suites, control consoles, video walls, etc). Depending on your configuration, your KMASS devices (audio, keyboard, mouse, etc) are first connected to the Receiver using standard cables. Power can then be supplied to the unit. The Receiver then connects to the Matrix Router Receiver (Downstream) ports using fiber (Multi-mode fiber for distances up to 1000m; Single-mode fiber for distances beyond 1000m).

Connecting to the Transmitter

The Transmitter serves as the Source (computer and video entities). Depending on your configuration, your local KMASS devices (keyboard, mouse, etc) are first connected. The video sources (e.g. computers) are then connected followed by any local video devices. Power can then be supplied to the unit. The Transmitter connects to the Matrix Router Transmitter (Upstream) ports using fiber (Multi-mode fiber for distances up to 1000m; Single-mode fiber for distances beyond 1000m).

4 Configuration and Maintenance for Secure Applications

When used in a secure application, the Matrix Router and External Computer (Management workstation) used to manage the Router must be located in a physically secure environment to which only trusted administrators have authorized access. Similarly, the server used to manage the Matrix Router must be physically protected and have suitable identification/authentication mechanisms to ensure that only trusted administrators have access.

4.1 Condition of Fielding

When the system is deployed into an operational environment, the following security measures (at a minimum) must be implemented to ensure an acceptable level of risk for the sites' Designated Approving Authority:

a. The Thinklogical VDS solution must be deployed on a physically and logically separated isolated network with no external connections.
b. The system must be configured with Telnet disabled.
c. The system must be configured with File Transfer Protocol disabled.
d. The Management workstation must be co-located with Thinklogical's VDS solution. Therefore, it can only be managed locally. There will be no remote access to the solution.
e. Touch screen Controller must only use a serial connection to the Router. Wi-Fi must be verified as disabled or nonexistent.
f. PC1 and PC2 must be government provided CAC enabled and fully STIG workstation.
g. The Thinklogical VDS solution cannot cross the converged Local Area Network (LAN).
h. The site must use manual document logging for auditing purposes. These Audit logs will be maintained by the site and will incorporate initial setup, administrative functions, updates, root access, and any other access to the system. Instructions for creating the Audit log will be specified in Thinklogical's Deployment Guide.
i. The site must use role-based security for user access and management of the vendor's device.
j. The site must disable all local user accounts on the device after initial setup/configuration with the exception of one emergency administrative account.
k. `The site must ensure that the emergency administrative account's userid and password are locked up in separate safes, both of which are not accessible by any one individual, and procedures are implemented to log all access and usage.
l. The site must ensure that the emergency administrative account meets all DoD userid and password complexity requirements.
m. The site must ensure all unused ports are closed.
n. The site must use a STIG-compliant CAC-enabled workstation for management of the solution.
o. The configuration must be in compliance with the Thinklogical Velocity Video Matrix Switching Solution Revision 4 military-unique features deployment guide.
p. The site must register the system in the Systems Networks Approval Process Database <https://snap.dod.mil/index.cfm> as directed by the DSAWG and Program Management Office. There will be a standardized list of emergency accounts and passwords.

4.2 Administrator Access and Setup

There are only two methods by which the administrator can access the Matrix Router Controller Configuration. Using the serial console directly connected to the Matrix Router or using SSH access by connection to the LAN port. The following steps describe secure setup of the Matrix Router.

4.2.1 Using the serial console directly connected to the Matrix Router: It should be noted that, while no administrator password is required to use the serial console (by default), physical access to the router is required. Therefore, the router should be stored in a physically secure location to avoid unauthorized access. The serial console must be configured to require an administrator password (as shown 4.2.1.1) that will assume the same security that is listed below, under "Password Security."

4.2.1.1 The administrator must force logins on the console port by entering the command using the console port:

```
sed –i '/^ttyS0::/s!ttyS0!##ttyS0!;/^#ttyS0/s/#ttyS0/ttyS0/' /etc/inittab
```

4.2.1.2 The administrator must add an appropriate banner by adding the text file: /etc/dodbanner.txt

Example of dodbanner.txt:

##

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

###

4.2.1.3 The administrator must run the following commands to implement the banner:

```
cat /etc/dodbanner.txt >>/etc/issue
cat /etc/dodbanner.txt >>/etc/issue.net
sed -i '/^#Banner none/aBanner /etc/dodbanner.txt' /etc/sshd_config
```

4.2.2 Using SSH access- The router allows SSH connections to the router for management purposes. SSH sessions are authenticated using an encrypted password file.

Password Security: For security purposes, the router defaults to using the Message-Digest Algorithm (MD5) and shadow passwords**. It is highly recommended that you do not alter these settings.** If you select the older Data Encryption Standard (DES) format, passwords will be limited to eight alphanumeric characters (disallowing punctuation and other special characters) with a modest 56-bit level of encryption. **The single most important thing you can do to protect the router is create a strong password.**

4.2.3 Creating Strong Passwords: The password can contain up to 127 characters and cannot contain a space.

4.2.3.1 The administrator must require passwords that contain at least one uppercase alphabetic character.

4.2.3.2 The administrator must require passwords that contain at least one lowercase alphabetic character.

4.2.3.3 The administrator must require passwords that contain at least one numeric character.

4.2.3.4 The administrator must require passwords that contain at least one special character.

4.2.3.5 The administrator must require passwords to contain no more than three consecutive repeating characters.

4.2.3.6 The administrator must require at least four characters be changed between the old and new passwords during a password change.

4.2.3.7 The administrator must not use dictionary words for passwords.

4.2.3.8 The administrator must prohibit the reuse of passwords within five iterations.

4.2.4 Logging of User Logins - The router must be configured to log all root logins and user logins using SSH.

4.2.4.1 The administrator must run the following command to force the log of all logins to the file: /var/log/auth

```
grep -sq '^auth' etc/syslog.conf || echo 'auth.* /var/log/auth' >>etc/syslog.conf
```

4.2.5 Router SSH Configuration Files - The following changes must be made to the Router configuration files:

4.2.5.1 Add the following line into the "/etc/sshd_config"
Ciphers aes128-ctr,aes192-ctr,aes256-ctr

4.2.5.2 Add the following line into the "/etc/sshd_config"
MACs hmac-sha1

4.2.5.3 Add the following line into the "/etc/ssh_config"
Ciphers aes128-ctr,aes192-ctr,aes256-ctr

4.2.5.4 Add the following line into the "/etc/ssh_config"
Tunnel=no

4.2.6 Router SysLog Files - The following defines default SysLog configuration and files used for auditing purposes. Configuration of SysLog logging is located in "/etc/syslog.conf".

4.2.6.1 System messages are logged to "/var/log/messages"

4.2.6.2 Application Program Interface (API) messages are logged to "/var/log/api"

4.2.6.3 System errors are logged to "/var/log/error"

4.2.6.4 System Critical errors are logged to "/var/critical"

4.2.6.5 System auth.* messages are logged to "/var/log/auth"

4.3 Manual Document Log and Audit Log

System Login access is not required for operation or regular maintenance of the Thinklogical VDS. This interface is only required for administrative use when setting initial conditions for deployment. The Thinklogical Matrix Router must be located in a physically secured area, and must be deployed on a physically and logically separated isolated network with no external connections. Firmware upgrades are done by simply replacing a removable memory card (SD card) inside the Matrix Router as described in Section 5.2.1.

4.3.1 Manual Document Log - As a condition of fielding, administrators must enforce a manual function of maintaining a log of personnel which details access to the physically secured area. Minimum information to be logged includes name, date, time, and action performed.

Name	Date	Time	Action

4.3.2 Manual Audit Log - As a condition of fielding, administrators must enforce a manual function of auditing the manual Document log and auditing the Router SysLog auth.*

file (/var/log/auth). Minimum information to be entered into the Audit log includes name, date, time, and action performed (including root access from auth.* file).

Router Access and auth.* file entry	Date	Time	Action Performed and auth.* file entries

5 Restricted Switching and Partitioning

Thinklogical's Matrix Router uses two methods for secure routing. One is known as **Restricted Switching** and the other is known as **Partitioning**. These methods can be deployed singularly or jointly, depending on security requirements.

5.1 Restricted Switching

Restricted Switching provides multiple levels of security classification domains on the same Matrix Router. Each destination must ensure that no unauthorized content is displayed or accessed, therefore, each input and output needs to be prioritized. Priorities can range from 1 to the total number of ports in the Matrix Router. An output can connect to an input with a priority greater than, or equal to, its priority. Thus, a priority level of 1 on an output can connect to any input (priority 1, 2, 3…).

The user must provide a table defining the priorities for each input and output of the switch matrix. This table is in the form of a comma separated value (csv) file. This file contains the values in three columns: **Port Type** (i=input, o=output), **Port Number** and **Port Priority**. For example:

```
“Type”    “Port”      “Priority”
"i",       1,          1
"i",       2,          2
"i",       3,          3
"i",       4,          1
"i",       5,          3
"o",       1,          1
"o",       2,          3
"o",       3,          2
"o"        4,          4
"o",       5,          1
```

Output 1 can connect to ports 1-5.
Output 2 can connect to ports 3 and 5.
Output 3 can connect to ports 2, 3, and 5.
Output 4 cannot connect to any ports.
Output 5 can connect to ports 1-5.

Note that Port Direction (i or o) is in quotes and that the table must use only the following ASCII printable characters:

Double quotes (or speech marks),	character code = 34	(")

Lower case i	character code = 105	(i)
Lower case o	character code = 111	(o)
Comma	character code = 44	(,)
Carriage Return	character code = 13	(CR)
Line Feed	character code = 10	(LF)

The Matrix Router will interpret the Restricted Switching Table (csv file) during the boot-up. Any errors that occur during the Restricted Switching Table interpretation process will be logged in the messages file at the following location: **var/log/messages**

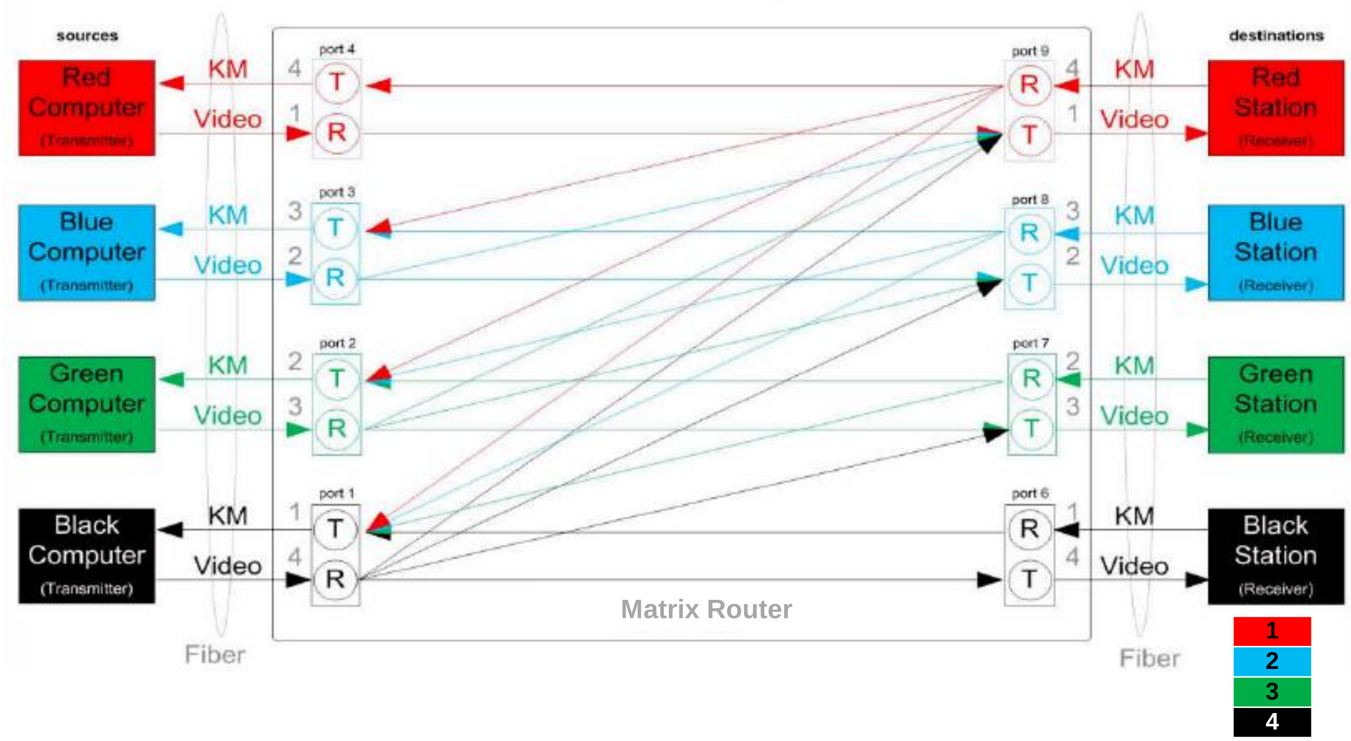
It is recommended that the **Messages File** be reviewed and any errors and the Restricted Switching Table be corrected before implementing multiple levels of security classification domains on the same Matrix Router. It is also recommended that **Restricted Switching** be fully tested before implementing multiple levels of security classification domains on the same Matrix Router.
The Restricted Switching Table files for the Matrix Router are stored on the Controller Card at the following location:

var/local/router/restrict/upstream.csv

Restricted switching is disabled when Restricted Switching Table files are removed. By default, when there are no Restricted Switching Table files, all input and output ports will have a priority of 1. All Matrix Routers are shipped without Restricted Switching Table files stored on the Controller card and therefore do not restrict any connection.

Restricted Switching Example with Matrix Router

Restricted Switching Priority Scheme for four levels of security managed by one Matrix Router:



This scenario shows four levels of security managed by one VX router.
For video:

- destination workstations in the red network can see what is transmitted by source computers in the black, green, blue, and red networks
- destination workstations in the blue network can see what is transmitted by source computers in the black, green, and blue networks
- destination workstations in the green network can see what is transmitted by source computers in the black and green networks

• destination workstations in the black network can see what is transmitted by source computers in the black network only

For keyboard and mouse:
• destination workstations in the red network can control source computers in the black, green, blue, and red networks
• destination workstations in the blue network can control source computers in the black, green, and blue networks
• destination workstations in the green network can control source computers in the black and green networks
• destination workstations in the black network can control source computers in the black network only

Restricted switching is configured via firmware loaded to the Matrix router. The configuration file for this scenario would look like (where the first value is "i" for input or "o" for output, the second value is the port number, and the third value is the priority level).

```
"i",1,4
"i",2,3
"i",3,2
"i",4,1
"i",6,1
"i",7,2
"i",8,3
"i",9,4
"o",1,1
"o",2,2
"o",3,3
"o",4,4
"o",6,4
"o",7,3
"o",8,2
"o",9,1
```

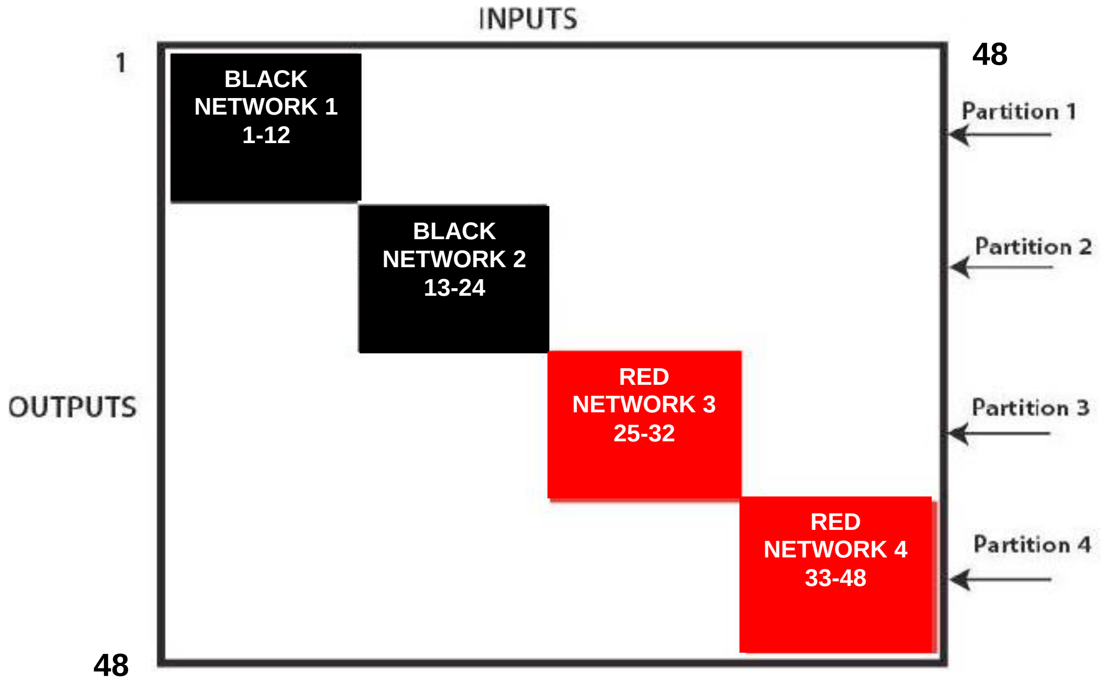
Important Notes:
• The MX48 Router can support 48 priority levels.

Note: When using a Back-up Controller configuration, both controllers must have the same Restricted Switching Table file(s).

5.2 Partitioning

Partitions allow Matrix Router sources and destinations to be segregated. Therefore, destination work stations will only receive signals that are transmitted from source computers in the same partition. In addition, it is impossible for a source computer to be inadvertently routed outside of its designated partition as the signals will not be transmitted.

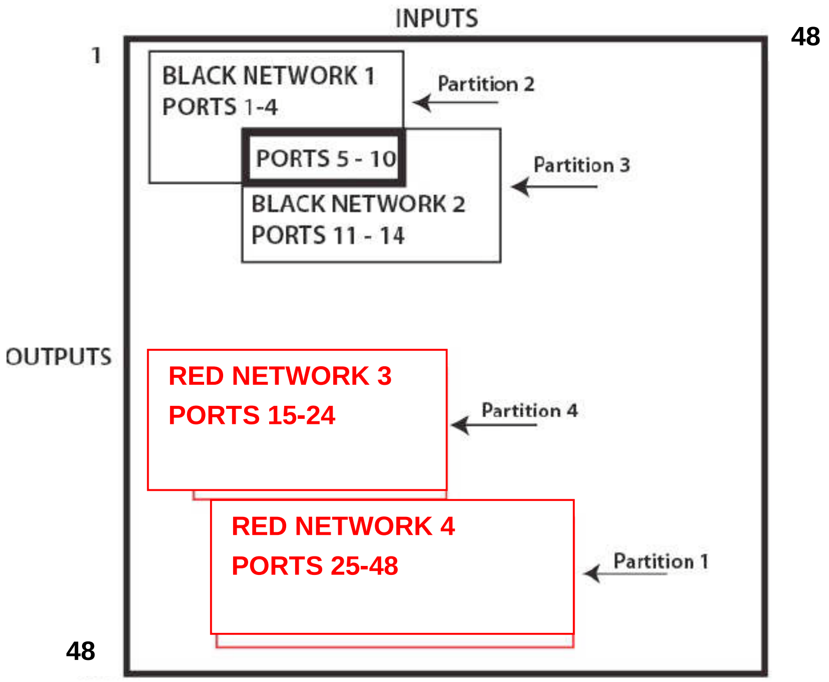
Example: MX48 Router with four distinct partitions:



Four partitions set up for secure routing and extension applications. Signals are only capable of transmitting and receiving within a single partition and not across partitions

The maximum number of partitions is the number of ports that make up the Matrix Router. An MX48 can be configured with up to 48 partitions. There are also overlapping partition configurations.

The following example shows a MX48 Router with an overlapping partition:



A MX48 with four partitions: Ports 5-10 are accessible to both partitions 2 and 3.

The user must provide a table defining the partitions. This table is in the form of a comma separated value (CSV) file located in **/var/local/router/partition** on the Matrix Router. This file contains the port number and the partitions to which it belongs. The configuration file for the above scenario looks like this:

“Port,”	“Partition”	“Port,”	“Partition”
1,	2	13,	3
2,	2	14,	3
3,	2	15,	4
4,	2	16,	4
5,	2,3	17,	4
6,	2,3	18,	4
7,	2,3	19,	4
8,	2,3	20,	4
9,	2,2	21,	4
10,	2,3	22,	4
11,	3	23,	4
12,	3	24,	4

All ports not listed will default to partition 1. Ports can be manually added to partition 1.

5.3 Secure Application Examples

The Diagrams on page 14 show the MX48 Router in a secure application. **The highly secure components are described as the Red Network and the other, lower security components are described as the Black Network.** The Red Network, containing the computers (sources), is shown in a physically secure environment along with the MX Router, the computer server used to manage the Router, and the Network Hub. The Network Hub is a dedicated network used only to connect the MX Router to the computer server. This dedicated network does not connect to any other components and does not extend beyond the physically secure environment. The dedicated network connection may be replaced by a direct serial connection (RS-232) between the MX Router and the computer server.

⚠ **Note: The MX Router and the computer server used to manage the Router must be protected according to the highest security classification of any component in the entire network application.**

⚠ **Note: The optical connections and DESTINATION receiver designated as Red Network must be physically secure.**

The MX Router can be configured to prevent accidental connection from the Red Network to the Black Network using the Restricted Switching feature. For example, a MX48 Router could be configured with the following csv file:

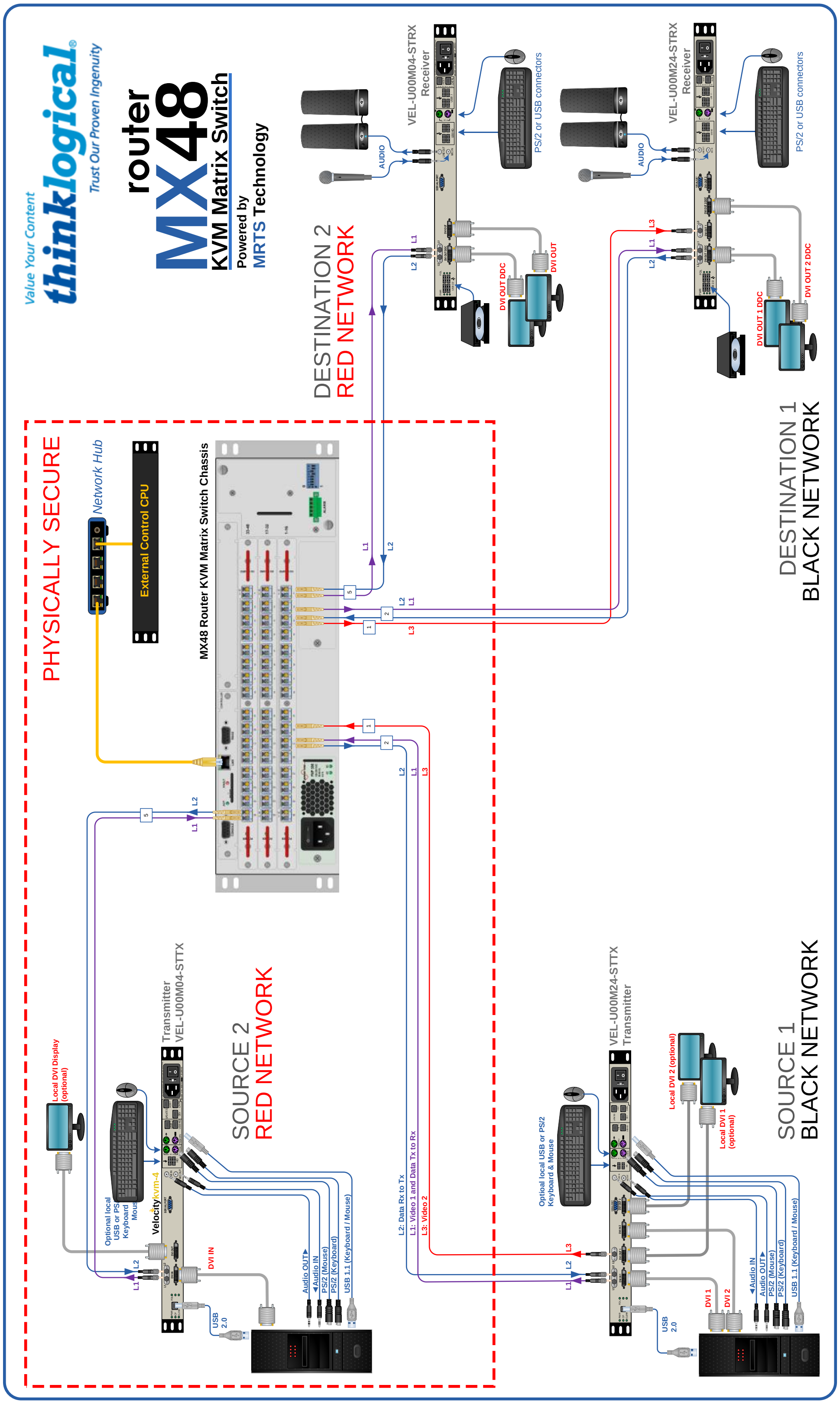
```
I,1,2
I,2,2
O,2,2
I,42,2
O,41,2
O,42,2
I,5,1
O,5,1
I,45,1
O,45,1
```

The following connection rules will apply:

SOURCE 2 can be connected only to DESTINATION 2.
SOURCE 1 can be connected to both DESTINATION 1 and DESTINATION 2.

The configuration of the MX Router should be reviewed regularly to ensure that it continues to meet organizational security policies concerning:

- Changes in the MX Router configuration
- Changes in the organizational security policy
- Changes in the threats presented from non -trusted network interfaces
- Changes in the administration and operation staff or the physical environment of the MX Router



MX48 Secure Application

6 Set-Up and Installation

⚠ **Note: Insure that all thumb screws are finger tight so that all the modules are properly held in the chassis.**

1. Carefully remove the MX48 Router from its shipping container. Inspect the router to make certain that no damage occurred during shipment.

2. All of the I/O cards are installed at the factory to meet the configuration. Insure that the I/O cards are properly seated in the unit. All of the I/O cards have thumb screw retainers.

3. After checking the I/O cards, go to the bottom of the unit. There is a power supply located in the bottom part of the chassis. Verify that the power supply is secure in the chassis.

4. Located to the right of the power module is a fan tray. The fan tray has thumb screws holding it into the chassis. Verify that the fan tray is secure. Cooling is accomplished by the fan trays and fans in the power supply units. Air is forced into the chassis from the fan tray. This cools the vertically mounted I/O cards, the integrated circuits on the Backplane, as well as removing any heat generated by the power module.

⚠ **Note: If mounting the chassis in a rack, insure that none of the fans have restricted air flow.**

5. The temperature in the chassis is monitored in several locations. The power supply has an internal temperature sensor that is monitored constantly for any conditions that may indicate a problem. Other temperature sensors are mounted in the fan trays, on the Controller card(s), on the I/O cards, and on the Backplane.

6. As a further safeguard, all fan speeds are monitored and any fan speed that does not meet specification will cause the unit to set alarm condition.

STOP **Warning! Do not remove the Front Door when the unit is powered. The Backplane Integrated Circuits will overheat when operating without the Front Door attached.**

⚠ **Note: All of these conditions send out notifications prior to shut down. For a detailed list of the alarm descriptions, see Figure 7: *Alarm Descriptions and Drawing* on page 7.**

7. When the MX Router has been inspected and found to be in good condition, the installation process can begin.

How to Install or Replace Input/Output Cards

Note: A shutdown is not required prior to installing/replacing Input/Output Cards.

Step 1
Turn the two thumbscrews counterclockwise until they disengage from the chassis. Pull the card out using both handles.

Warning! Do not pull on the thumbscrews when removing the module – damage may occur!

OR
If a blank panel is present, remove the blank panel from the desired location using the thumbscrews.

Step 2
Place the new module upright so that the POWER LED is on the top. Grasp the module by the handles or by the outer edge of the aluminum housing. The card should slide freely until it reaches the backplane connector. At this point, use just enough force to firmly engage the card with the mating connector.

Warning! If the module does not slide into the connector, do not force it! Damage may occur. Remove the card and start over.

Step 3
Once the module is completely seated, hand-tighten the thumbscrews.

Warning! Do not tighten the thumbscrews with a screwdriver.

How to Install or Replace a Controller Card

Note: The left Controller slot is always Primary.

Note: Replacing the Active Controller Card will interrupt service.

When replacing a Controller Card in a system with redundant controllers you may remove the Controller that is not active (Active LED is Off) without interrupting service. Before removing a Primary Controller that is active you should cause a Fail-over to the Back-up Controller. This can be done by removing the LAN connection from the active Controller and waiting approximately 20-50 seconds for the Back-up Controller to take control, as indicated by the Active LED. After the Primary Controller is removed and replaced (following Steps below), the Primary Controller will re-take control of the system and become the Active Controller.
Step 1

Turn the thumbscrews counterclockwise until they disengage from the chassis. Pull the Controller Card out using both black handles.

Step 2
Place the new module upright so that the ACTIVE LED is on the top. Grasp the module by the handles or by the outer edge of the aluminum housing. The card should slide freely until it reaches the backplane connector. At this point, use just enough force to firmly engage the card with the mating connector. Place the new module upright so that the ACTIVE LED is on the top. Grasp the module by the handles or by the outer edge of the aluminum housing. The card should slide freely until it reaches the backplane connector. At this point, use just enough force to firmly engage the card with the mating connector.

Warning! If the module does not slide into the connector, do not force it! Damage may occur. Remove the card and start over.

Step 3
Once the module is completely seated, hand-tighten the thumbscrews.

Warning! Do not tighten the thumbscrews with a screwdriver.

How to Install New Firmware

Firmware for the Matrix Router is stored on an SD card that is located in the Controller card. Access to the SD card is gotten by removing the Controller card as described in the steps above. Firmware upgrades are done by simply replacing this SD card. Please note that the Matrix Router should be deployed in a secured room/closet with access limited to only authorized, administrative staff.

How to Replace a Fan Tray

The MX48 uses three DC fans to move air horizontally through the enclosure. Be sure not to block the air vents on the front and rear of the unit, and leave at least 2" of space on both sides.

Note: Be sure to leave adequate ventilation space on both sides of the units (2" minimum), especially if units (e.g. Extenders) are being stacked above or below the MX48 Router.

Note: No shutdown is required prior to replacing the Fan Tray.

Step 1
Turn the four thumbscrews counterclockwise until they disengage from the chassis.

Step 2
Pull the Fan Tray module out using both black handles.

Step 3
Place the new module so that the aluminum housing is on the bottom. Hold the new Fan Tray by the black handles and slide the aluminum housing into the black card guides.

Warning! Do not operate the unit without a Fan Tray installed for greater than 10 minutes.

Step 4
Hand-tighten the thumbscrews.

Warning! Do not tighten the thumbscrews with a screwdriver.

How to Replace a Power Supply

Warning! Disconnect the power cord before proceeding!

Note: If ONE power supply is installed: shutdown IS required.
If TWO power supplies are installed, shutdown IS NOT required.

The Power Modules are universal input 120-240VAC 50-60Hz. Use the proper power cord for your region (supplied with the unit). Although the router functions properly with one Power Module, it is recommended that both Modules preferably be connected to two independent power sources (for redundancy).

Step 1
Grasp the black handle with one hand.

Step 2
Slide the green tab to the left with the other hand.

Step 3
Pull the Power Module out of the chassis.

Step 4
Insert the new Power Module into the chassis and slide it in until it reaches the backplane connector. The module should slide freely until it reaches the backplane connector. At this point, use just enough force to firmly engage the card with the mating connector.

Warning! If the module does not slide into the connector, do not force it! Damage may occur. Remove the module and start over.

7 Regulatory & Safety Compliance

⚠ **Note: The following Safety and Compliance Declarations are pending approval.**

7.1 Safety Requirements

Symbols found on the product

Markings and labels on the product follow industry-standard conventions. Regulatory markings found on the products comply with domestic and many international requirements.

Regulatory Compliance

Thinklogical®'s MX48 is designed and made in the U.S.A. MX48 has been tested by a certified testing laboratory and found to be compliant with the following standards (both domestic USA and many international locations):

North America

Safety

ANSI/UL60950-1: 1st Edition (2003)

CAN/CSA C22.2 No. 60950-1-03

LASER Safety

CDRH 21CFR 1040.10

Class 1 LASER Product

Electromagnetic Interference

FCC CFR47, Part 15, Class A

Industry Canada ICES-003 Issue 2, Revision 1

Australia & New Zealand

This is a Class A product. In a domestic environment this product may cause radio interference, in which case the user may be required to take adequate measures.

European Union

Declaration of Conformity

Manufacturer's Name & Address:

Thinklogical®
100 Washington Street
Milford, Connecticut 06460 USA
Telephone 1-203-647-8700

These products comply with the requirements of the Low Voltage Directive 72/23/EEC and the EMC Directive 89/336/EEC.

7.2 Standards with Which Our Products Comply

Safety

CENELEC EN 60950-1, 1st Edition (2001)

LASER Safety

IEC60825:2001 Parts 1 and 2

Class 1 LASER Product

Electromagnetic Emissions

EN55022: 1994 (IEC/CSPIR22: 1993)

EN61000-3-2/A14: 2000

EN61000-3-3: 1994

Electromagnetic Immunity

EN55024: 1998 Information Technology Equipment-Immunity Characteristics

EN61000-4-2: 1995 Electro-Static Discharge Test

EN61000-4-3: 1996 Radiated Immunity Field Test

EN61000-4-4: 1995 Electrical Fast Transient Test

EN61000-4-5: 1995 Power Supply Surge Test

EN61000-4-6: 1996 Conducted Immunity Test

EN61000-4-8: 1993 Magnetic Field Test

EN61000-4-11: 1994 Voltage Dips & Interrupts Test

7.3 Supplementary Information

The following statements may be appropriate for certain geographical regions and might not apply to your location.

This Class A digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numérique de la classe A respecte toutes les exigencies du Règlement sur le matérial brouilleur du Canada.

STOP **Warning! This is a Class A product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take corrective measures.**

⚠ **Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications in which case the user may be required to take adequate corrective measures at their own expense.**

⚠ **Note: This Class A digital apparatus complies with Canadian ICES-003 and has been verified as being compliant within the Class A limits of the FCC Radio Frequency Device Rules (FCC Title 47, Part 15, Subpart B CLASS A), measured to CISPR 22: 1993 limits and methods of measurement of Radio Disturbance Characteristics of Information Technology Equipment.**

⚠ **Note: The user may notice degraded audio performance in the presence of electromagnetic fields.**

⚠ **Note: If using a keyboard that is noise susceptible, a ferrite ring on the keyboard cable may be needed to comply with Immunity Requirements**

Product Serial Number

Thinklogical® products have a unique serial number, imprinted on an adhesive label that is fixed to the bottom of the chassis. The serial number includes a date-code. The format for the date-code is 2 digits for the month, 2 digits for the day and 2 digits for the year, plus two or three digits for a unique unit number. This serial number is also found on the original shipping carton.

Connection to the Product

Connections and installation hardware for our products use industry-standard devices and methods. All wiring connections to the customer equipment are designed to minimize proprietary or customized connectors and cabling. Power connections are made with regionally appropriate power cords and approved methods.

8 How to Contact Us

8.1 Customer Support

Thank you for choosing a Thinklogical® product for your application. We appreciate your business and are dedicated to helping you successfully use our product. Thinklogical® is here to help you.

Thinklogical® is an engineering company and you will receive the information you require directly from our most knowledgeable engineers. We believe that the first line of support is the design engineer that developed the product. Therefore, your questions will be handled promptly by our in-house engineers who are most familiar with your products.

To contact Thinklogical®, use the following telephone numbers and internet-based methods.

Website

Check out our website for current product offerings, support information and general information about all of the products we offer.

Our internet website offers product information on all current systems, including technical specification sheets and installation guides (for viewing online or for download), product diagrams showing physical connections and other information you might need.

Internet: **www.thinklogical.com**

⚠ **Note: Most online documents are stored as Adobe Acrobat "PDF" files. If you do not have the Adobe Acrobat reader needed to view PDF files, visit www.adobe.com for a download.**

Email

Thinklogical® is staffed **Monday through Friday from 8:30am to 5:00pm**, Eastern Time Zone. We will try to respond to your email inquiries promptly, use the following email addresses for your different needs:

info@thinklogical.com – Information on Thinklogical® and our products.

sales@thinklogical.com – Sales Department - orders, questions or issues.

support@thinklogical.com – Product support, technical issues or questions, product repairs and request for Return Authorization.

Telephone

Telephone Sales: Contact our expert sales staff via telephone in Milford, CT at **1-203-647-8700** or if in the continental US, you may use our **toll-free number 1-800-291-3211**. We are here Monday through Friday from 8:30am to 5:00pm, Eastern Time Zone. Ask for your representative's direct dial phone number when you call.

Telephone Product Support: Contact Product Support via telephone in Milford, CT at **1-203-647-8700**. The support lines are manned Monday through Friday, 8:30am to 5:00pm, Eastern Time Zone.

International Sales: Please contact our US sales staff in Milford, CT at **1-203-647-8700**. We are here Monday through Friday, 8:30am to 5:00pm, Eastern Time Zone (same as New York City). If leaving a voice message please provide a "best time to call back" so we may reach you at your convenience.

Our switchboard attendant will direct your call during regular business hours. We have an automated attendant answering our main telephone switchboard after regular business hours and holidays. You can leave voice messages for individuals at any time. Our Sales Representatives have direct numbers to speed up your next call to us.

Fax

Our company facsimile number is **1-203-783-9949**. Please indicate the nature of the fax on your cover sheet and provide return contact information.

8.2 Product Support

Thinklogical's® support personnel are available **Monday through Friday from 8:30am to 5:00pm**, Eastern Time Zone. If your application requires assistance at some time outside of our normal business hours, please contact us beforehand and we will do our best to make arrangements to help you with your Thinklogical® products.

Warranty

Thinklogical® warrants this product against defects in materials and workmanship for a period of one year from the date of delivery. Thinklogical® and its suppliers disclaim any and all other warranties.

⚠ **Note: Thinklogical® Inc. products carry a one year warranty, with longer term available at time of purchase on most products. Please refer to your product invoice for your products Warranty Terms & Conditions.**

Defect remedy shall be the repair or replacement of the product, provided that the defective product is returned to the authorized dealer within a year from the date of delivery.

If you wish to return your device, contact the Thinklogical® authorized dealer where you purchased the device, or if you purchased directly, call Thinklogical® at **1-800-291-3211** (USA).

Return Authorization

In the event you must return a product to Thinklogical® directly, please contact **Customer Support** at **1-800-291-3211** or **1-203-647-8700**. Customer Support will ask you to describe the problem and will issue you a **R**eturn **M**erchandise **A**uthorization number (RMA#). Pack the device in its original box, if possible, and return it with the RMA# printed on the outside of the box.

⚠ **Note: DO NOT return a product to Thinklogical® without a *Return Material Authorization*.**

Return address for products with Return Material Authorization:

Thinklogical®, LLC
Attn: RMA#
100 Washington Street
Milford, CT 06460 USA

PH: 1-800-291-3211 (USA only)

Our Address

If you have any issue with a product, have product questions or need technical assistance with your Thinklogical® system, please call us at **1-800-291-3211 (USA only)** or **1-203-647-8700** and let us help. If you'd like to write us, our mailing address is:

Thinklogical® LLC.
100 Washington Street
Milford, CT 06460 USA

APPENDIX A: MX48 TOUCHSCREEN

The touchscreen allows you to easily make connections with minimal set up time for your MX48 router. The touchscreen is connected via the ***RS232 serial connection*** on the back of the MX48 router. The serial port on the MX48 can be configured to work with the touch screen or our ASCII interface. The router ships with the ASCII interface enabled.

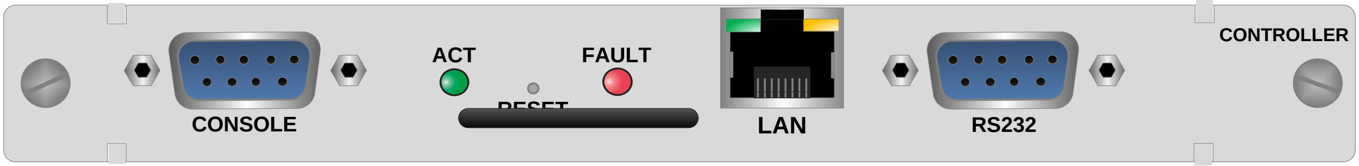


Figure C1: Controller Card

To enable your touchscreen, connect a computer's network port to the RJ45 LAN port on the MX48 using a crossover cable or through a network hub. The MX48 is shipped with a default IP Address of 192.168.13.15 (which can be changed using the dip switches on the rear panel - see Section 2.3 MX48 Modules, Controller Card).

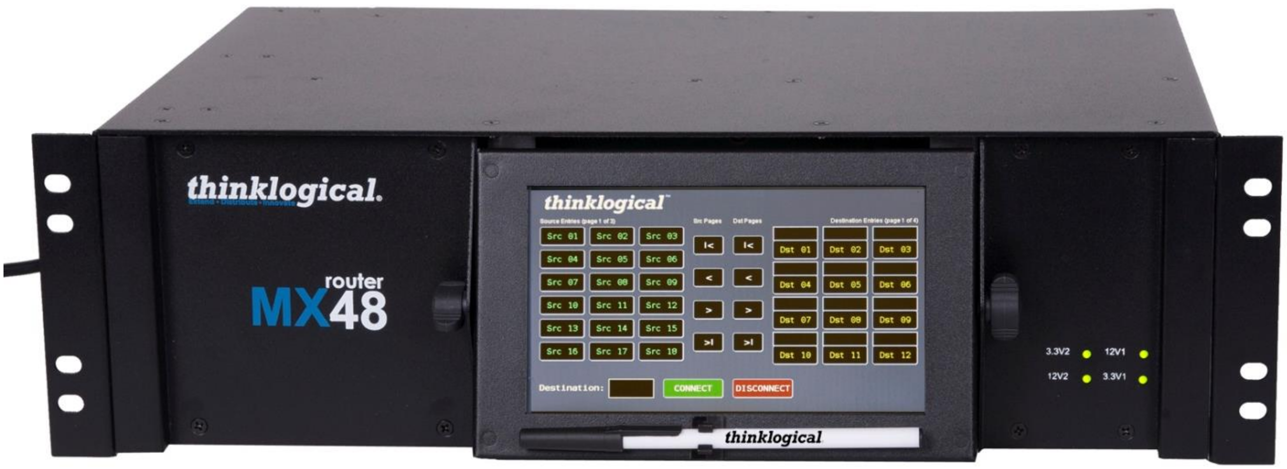
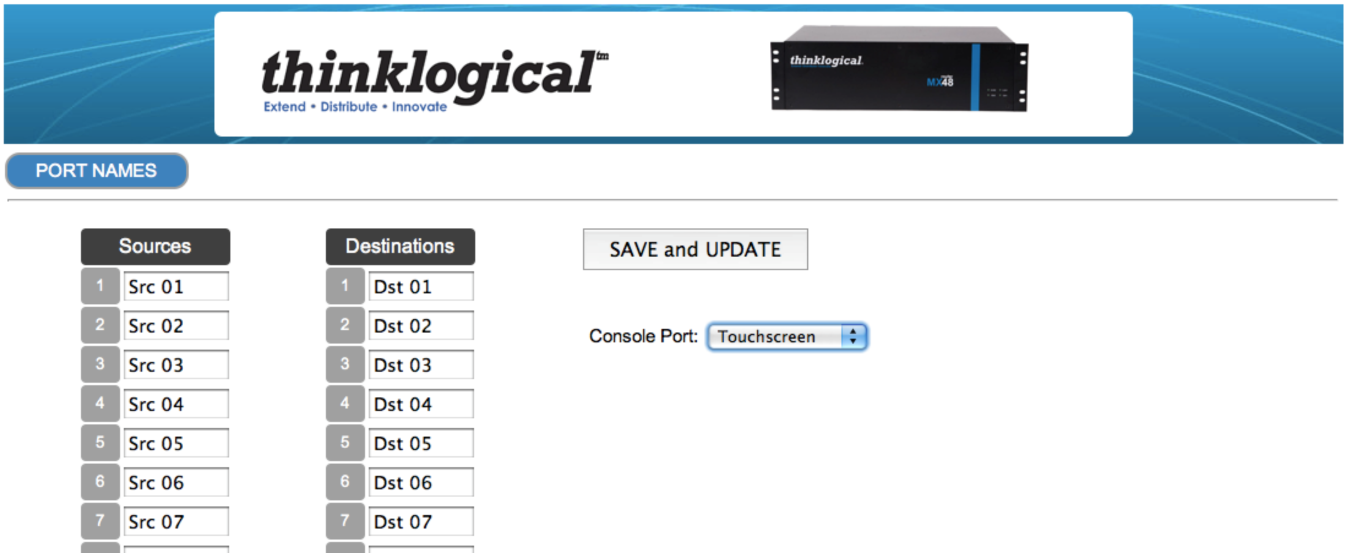


Figure C2: MX48 Router with Front-Mounted Touchscreen (MXR-000048-FM)

Set your computer to use the static address 192.168.13.9 and netmask 255.255.255.0 . From here, open a browser and type in the address of the MX48 router (http://192.168.13.15). Check the 'Touchscreen enable' box to allow control of the touchscreen via the serial port.

The names of Sources and Destinations can also easily be changed from this page using the browser. Set a web browser to the IP address of the MX48. Make any changes to the names and be sure to press the "SAVE and UPDATE" button before disconnecting.



PORT NAMES

Sources		Destinations	
1	Src 01	1	Dst 01
2	Src 02	2	Dst 02
3	Src 03	3	Dst 03
4	Src 04	4	Dst 04
5	Src 05	5	Dst 05
6	Src 06	6	Dst 06
7	Src 07	7	Dst 07

SAVE and UPDATE

Console Port: Touchscreen

Figure C3: Naming Sources and Destinations

The touch screen allows the user to easily make and break connections. To make a connection, select both a destination and a source (they turn blue when selected) and press “CONNECT”. To break a connection, select a destination (it turns blue when selected) and press “DISCONNECT”.

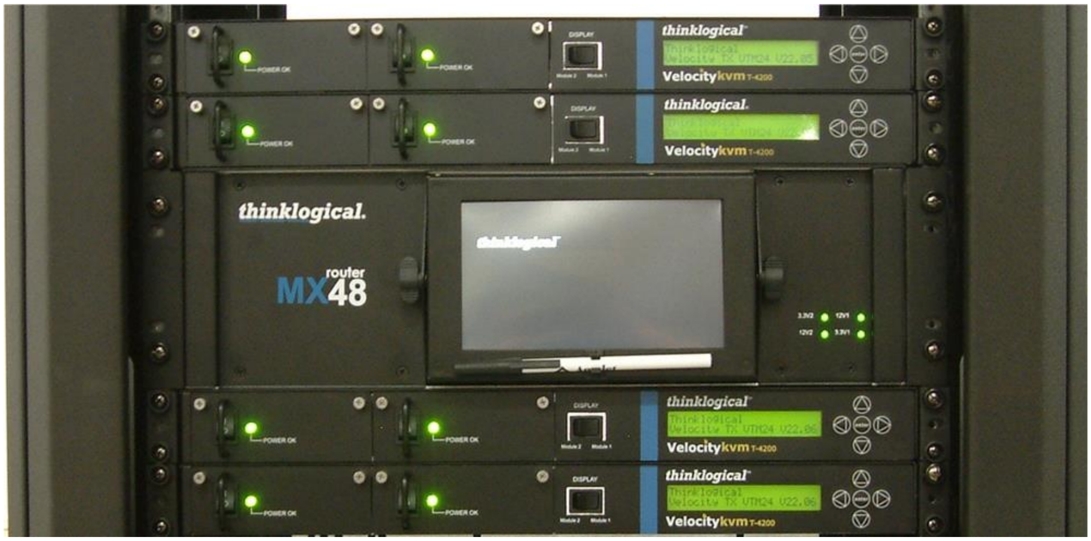


Figure C4: Rack-Mounted Touchscreen displayed in a rack
with Thinklogical® VelocityKVM T-4200 units

APPENDIX B: X4 CONFIGURATOR SOFTWARE

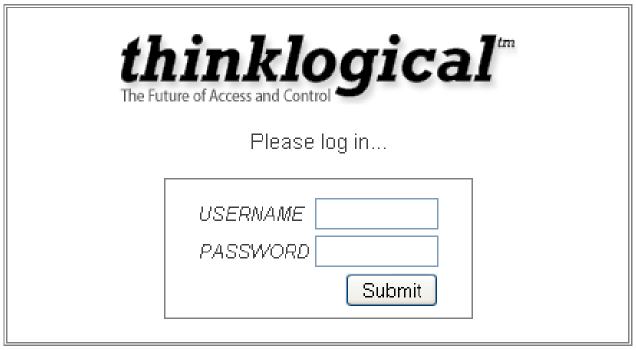
The X4 Configurator Software allows for easy and intuitive setup and control of the switching between source computer or video entities and user display destinations such as desktops, theaters, conference rooms, editing suites, control consoles, video walls, biomedical imaging arenas, satellite mapping, etc. In addition, single video sources may be multi-cast (one to more than one) or broadcast (one to all) to desired destinations. Additionally, macro presets may be created for saving and recalling commonly used input and output ties.

To control the MX48 with the X4 Configurator software, an external Control Rack Computer is required. The Control Rack Computer requires its network to be configured. In addition, each MX48 requires a static IP address used to identify it. Router information is stored by IP Address so it should not change. A web browser is used to manage the MX48(s).

One or more MX48 Routers can be controlled via a web-based software package running on a Control Rack Computer running Microsoft Windows or Linux.

Once the network(s) are configured and the control software is running, the control pages can be accessed from any connected client PC by starting a browser and setting the URL to http://192.168.13.9 (if running on a static network) or the name/address of the control server as set by the network administrator.

The user will be greeted with the following login screen:



Please log in...

USERNAME

PASSWORD

The installation software includes two default accounts as show below. Please log in using the admin username for first time set up.

Username:	**admin**	**Password:**	**admin**
Username:	**user**	**Password:**	**user**

CONNECTIONS

When logged in, you will land on the Connections page. This page displays destinations on the left side of the screen and sources on the right. The interface comes preconfigured with examples of ten (10) sources and ten (10) destinations. The first five are single head sources and the second five are dual head sources. These are simply examples and will need to be changed for your location configuration.

To make a Connection

a. Click a source to select it
b. Click one or more destinations to make a connection

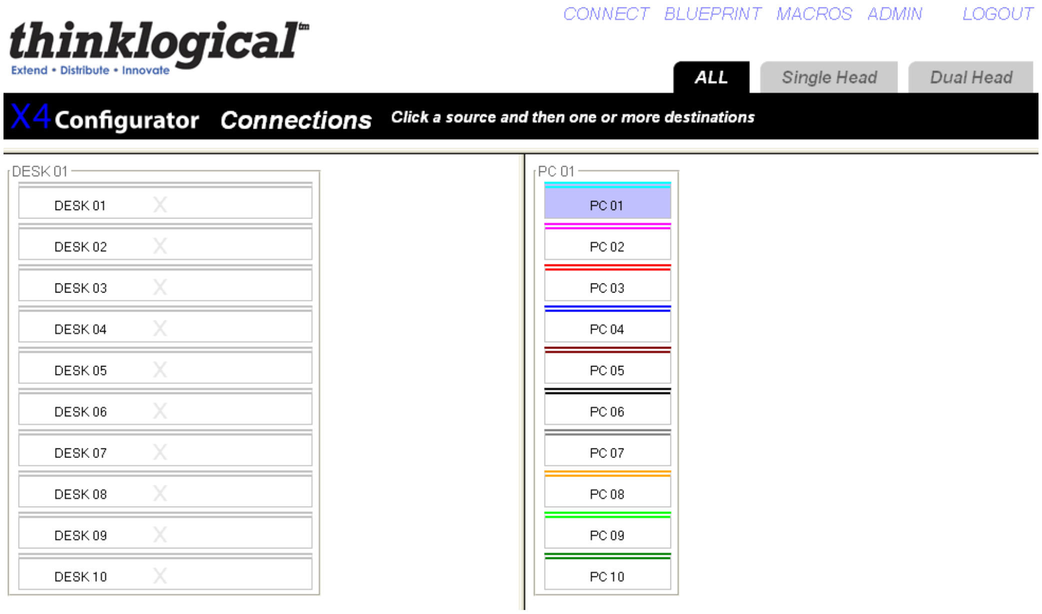


Figure D1: PC 01 has been selected as a source

A connection is made when the name of the source appears in half of the destination box, and the 'X' becomes the same color as the stripe(s) above the source. Many additional destinations can be clicked and connected to the same source. Only the first destination connected will have control of the keyboard and mouse, but all connected destinations will be able to see the same video.

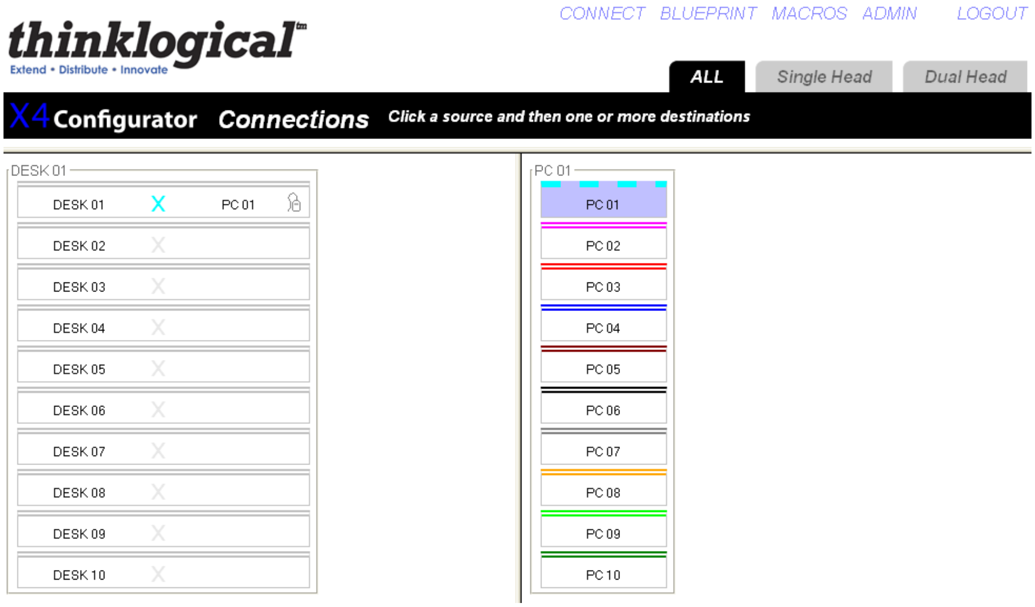
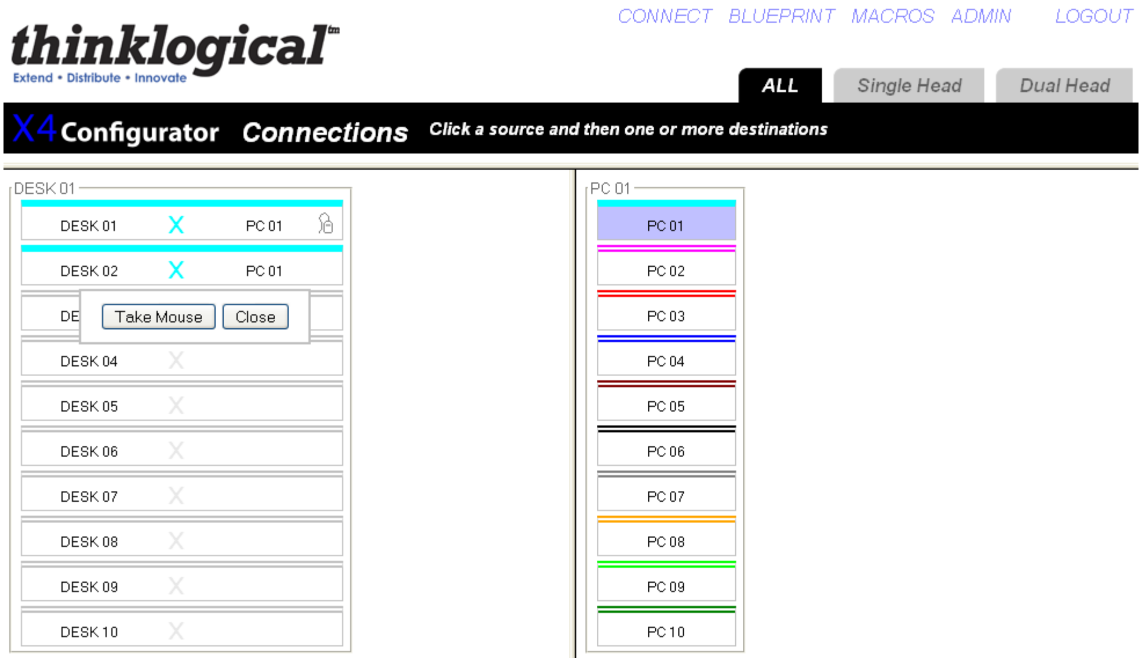


Figure D2: Source PC01 has been connected to Destination DESK 01

To “take” control of the keyboard and mouse on a different connection right click mouse and select “Take Mouse”.



Click a source and then one or more destinations

Figure D3: Take control of keyboard and mouse

To disconnect a source from a destination you simply click the 'X' on the destination to break the connection.

ADMINISTRATION

When logged in as administrator you can edit

a. Stations
b. Groups
c. Router
d. Macros
e. Tests
f. Snapshots

To edit Stations, Groups, Macros and Router click on the ADMIN page at the top of the web interface.

⚠ **NOTE- There is a "Backup" button located on each page that will save a backup file to your desktop for all the current settings. This will allow you to revert to previous settings by reverting to saved files.**

You can alternately edit all of these files via .csv files located in X4>setup>folder. Changes made via .csv can be saved and will automatically update on the web interface. See additional notes in the section Configuration File Structure.

You can also review log files and perform tests on the Administration page.

STATIONS

Stations are descriptions of signal sources or display devices that should be treated as a single entity. A computer is an example of a source station, and the monitor(s), keyboard, and mouse at a user's desk is one example of a destination station.

For example: A computer can have multiple video outputs that will most often be connected to multiple monitor's at the user's desk, so in this case we could say that the "source station" (computer) has two or more "ports". Similarly, a "destination station" might have multiple "heads" (monitors) and each monitor will be connected through its extender to output ports on the switch.

Some stations may need to be protected from accidental (or malicious) connections and disconnections by unauthorized users. To facilitate this, each station has one or more fields used to specify which "groups" (collections of users) can see and control that station.

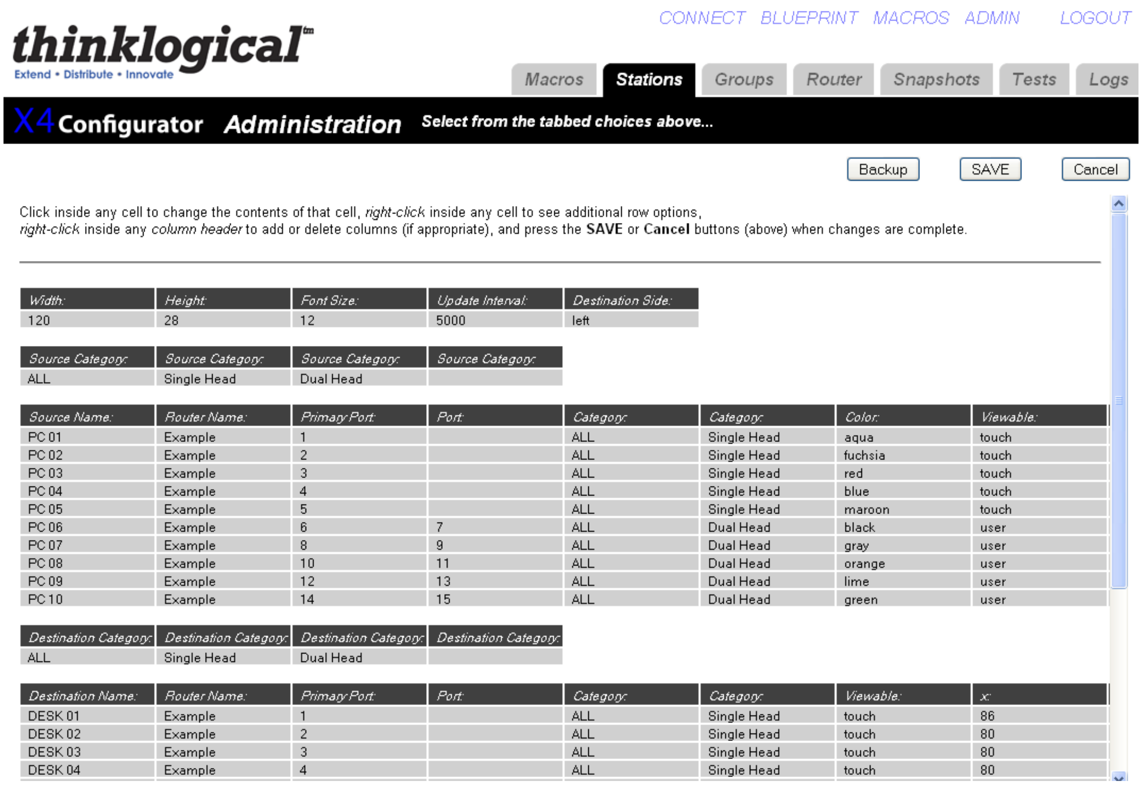
So from this it is clear that station needs: a name, one or more ports within a switch chassis, and some way to determine who has access to the station ("Viewable" or "Viewed By").

In addition, sources can have different colored stripes across the top to help make connections easier to see. When a destination is connected to a source, the "X" that separates the destination from its active source is given the same color as that assigned to the source. If a connected destination or source has the cursor over it, the stripes at the top of the source and all the destinations connected to it will become thicker and turn the color of that source to make connections easier to discern at a glance.

To edit settings for the stations, click on the Stations tab. From here you can edit all line items and columns.

a. Source name
b. Router name
c. Primary port (single head)
d. Port (two or more heads)
e. Category
f. Color (Source)
g. Viewable

You can also edit width, height and font size for window view and periodic update time.


CONNECT BLUEPRINT MACROS ADMIN LOGOUT
Macros
Stations
Groups
Router
Snapshots
Tests
Logs
X4 Configurator Administration
Select from the tabbed choices above...
Backup
SAVE
Cancel

Click inside any cell to change the contents of that cell, *right-click* inside any cell to see additional row options, *right-click* inside any *column header* to add or delete columns (if appropriate), and press the **SAVE** or **Cancel** buttons (above) when changes are complete.

Width:	*Height:*	*Font Size:*	*Update Interval:*	*Destination Side:*
120	28	12	5000	left

Source Category:	*Source Category:*	*Source Category:*	*Source Category:*
ALL	Single Head	Dual Head	

Source Name:	*Router Name:*	*Primary Port:*	*Port:*	*Category:*	*Category:*	*Color:*	*Viewable:*
PC 01	Example	1		ALL	Single Head	aqua	touch
PC 02	Example	2		ALL	Single Head	fuchsia	touch
PC 03	Example	3		ALL	Single Head	red	touch
PC 04	Example	4		ALL	Single Head	blue	touch
PC 05	Example	5		ALL	Single Head	maroon	touch
PC 06	Example	6	7	ALL	Dual Head	black	user
PC 07	Example	8	9	ALL	Dual Head	gray	user
PC 08	Example	10	11	ALL	Dual Head	orange	user
PC 09	Example	12	13	ALL	Dual Head	lime	user
PC 10	Example	14	15	ALL	Dual Head	green	user

Destination Category:	*Destination Category:*	*Destination Category:*	*Destination Category:*
ALL	Single Head	Dual Head	

Destination Name:	*Router Name:*	*Primary Port:*	*Port:*	*Category:*	*Category:*	*Viewable:*	*x:*
DESK 01	Example	1		ALL	Single Head	touch	86
DESK 02	Example	2		ALL	Single Head	touch	80
DESK 03	Example	3		ALL	Single Head	touch	80
DESK 04	Example	4		ALL	Single Head	touch	80

Figure D4: View of Stations on the Administration Page

The MX48 Router uses .csv formatted spreadsheet files as configuration files. Since the files can be created and modified with a spreadsheet, the interface is designed to mirror the experience of editing on a spreadsheet. You can edit each line item by clicking within the cell to change and type the change. In fields where there are a restricted number of choices, a pop-up menu will appear with available choices for the cell. You can close the pop-up by clicking on the title bar at the top of the table.

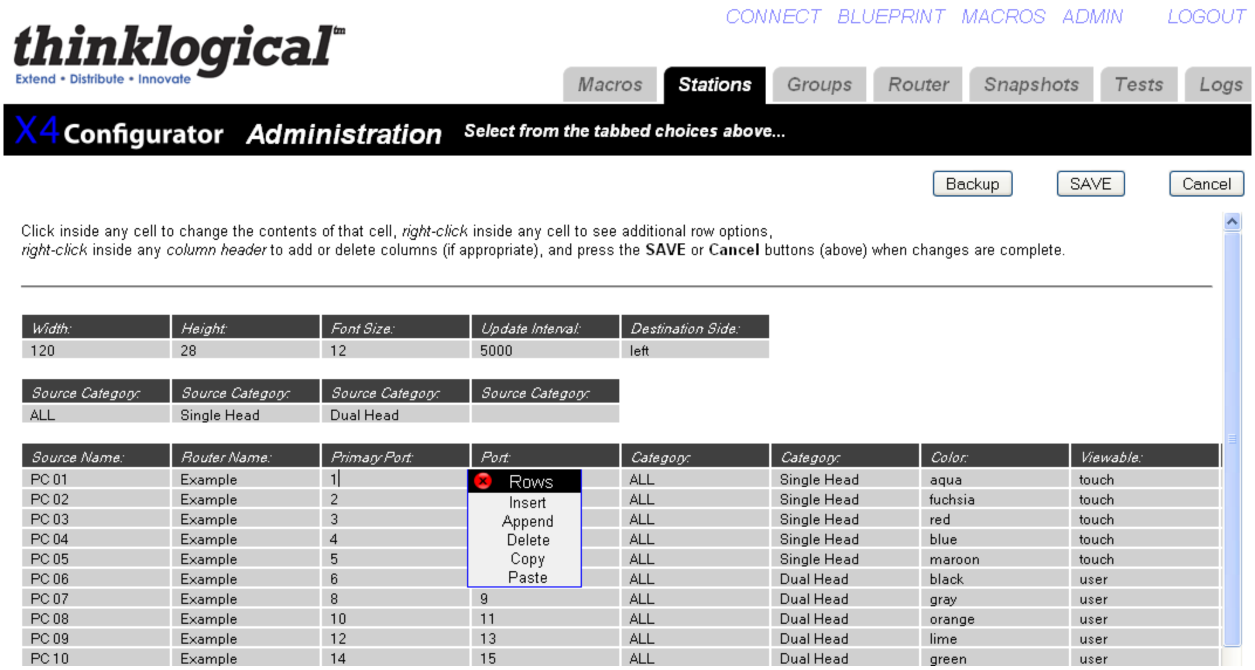
While "Width", "Height", "Font Size", and "Update Interval" apply to all the elements in the page (or, in the case of "Update Interval", the behavior of the page itself), most often the rows will describe just one of many items. In the images shown here, those rows are descriptions of source stations as indicated by the "Source Name" heading for the first column.

In these cases, changes to the line will affect only the one "object" described by the line.

You can edit each line item by selecting which cell to change and type the change. In some fields there will be a pop-up box which will show you a table with available selections for the cell. You can close the pop-up by clicking on the title bar at the top of the table.

To edit a row right click on the line to select your function.

a. Insert-adds a blank line above selected line item
b. Append-adds a blank line below selected line item
c. Delete
d. Copy
e. Paste
f. Close


CONNECT BLUEPRINT MACROS ADMIN LOGOUT
thinklogical™
Extend • Distribute • Innovate
Macros
Stations
Groups
Router
Snapshots
Tests
Logs
X4 Configurator Administration
Select from the tabbed choices above...
Backup
SAVE
Cancel
Rows
Insert
Append
Delete
Copy
Paste

Click inside any cell to change the contents of that cell, *right-click* inside any cell to see additional row options,
right-click inside any *column header* to add or delete columns (if appropriate), and press the **SAVE** or **Cancel** buttons (above) when changes are complete.

Width:	*Height:*	*Font Size:*	*Update Interval:*	*Destination Side:*
120	28	12	5000	left

Source Category:	*Source Category:*	*Source Category:*	*Source Category:*
ALL	Single Head	Dual Head	

Source Name:	*Router Name:*	*Primary Port:*	*Port:*	*Category:*	*Category:*	*Color:*	*Viewable:*
PC 01	Example	1		ALL	Single Head	aqua	touch
PC 02	Example	2		ALL	Single Head	fuchsia	touch
PC 03	Example	3		ALL	Single Head	red	touch
PC 04	Example	4		ALL	Single Head	blue	touch
PC 05	Example	5		ALL	Single Head	maroon	touch
PC 06	Example	6		ALL	Dual Head	black	user
PC 07	Example	8	9	ALL	Dual Head	gray	user
PC 08	Example	10	11	ALL	Dual Head	orange	user
PC 09	Example	12	13	ALL	Dual Head	lime	user
PC 10	Example	14	15	ALL	Dual Head	green	user

Figure D5: How to edit a row on the Stations Page

The viewable column in stations denotes which groups are able to view the connections. The administrator can view all sources and destinations. You can set up various groups (as seen in the next section) and restrict which pages are viewable by group.

To add additional columns on the web interface right click on the column to select your function:

a. Append to add an additional column
b. Delete column if you wish to remove
c. Close to close the pop-up window

Make sure to **SAVE** changes before exiting this menu.

GROUPS

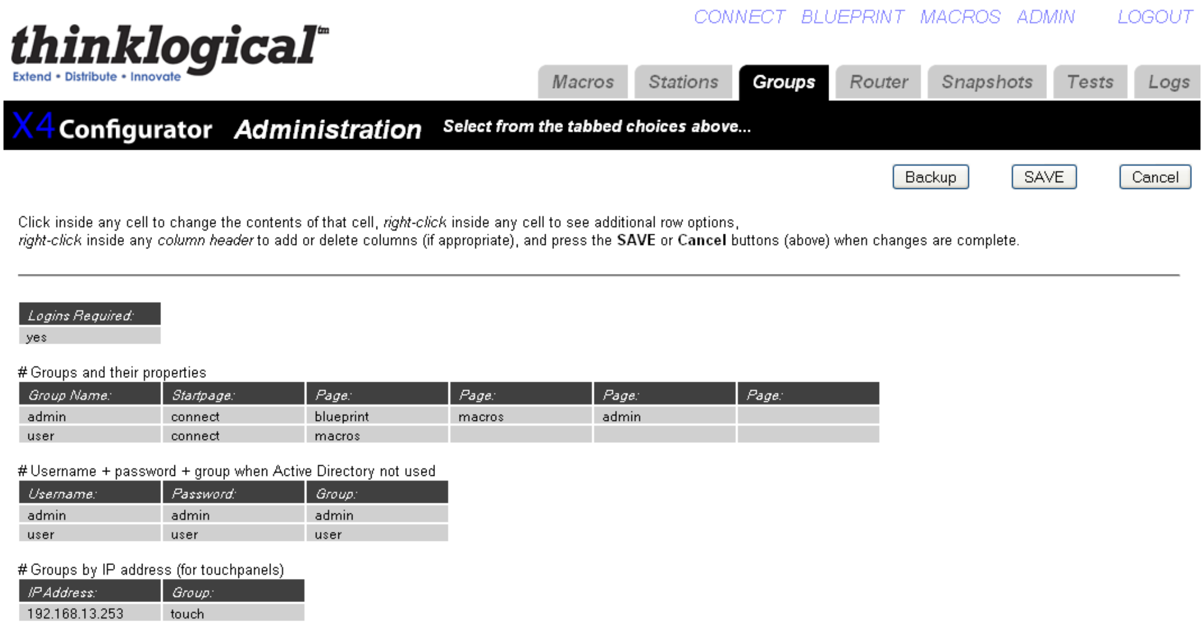
"Groups" are used to restrict access to stations and macros. The admin account can access any page, macro, or stations. Other collections of users - "groups" - can be defined to have their access rights strictly limited to specific assets.

You can change settings for Groups via the tab at the top of the Admin page. These settings can also be changed with a spreadsheet program or text editor modifying the .csv file directly.

The Groups admin page includes

1. Logins Required (Yes or No)
2. Groups and their properties
   a. Create/edit group name
   b. Select/edit Start Page for each group
   c. Select/edit pages that are viewable for the group (Macros, Studio, Blueprint, etc)

3. User names and Passwords
    a. Create/edit user names and passwords
    b. Select which group to which each user will be assigned when they successfully log in
4. Specific IP addresses which will automatically be assigned to a group without requiring login (touchscreens).



Click inside any cell to change the contents of that cell, *right-click* inside any cell to see additional row options, *right-click* inside any *column header* to add or delete columns (if appropriate), and press the **SAVE** or **Cancel** buttons (above) when changes are complete.

Logins Required:
yes

Groups and their properties

Group Name:	*Startpage:*	*Page:*	*Page:*	*Page:*	*Page:*
admin	connect	blueprint	macros	admin	
user	connect	macros			

Username + password + group when Active Directory not used

Username:	*Password:*	*Group:*
admin	admin	admin
user	user	user

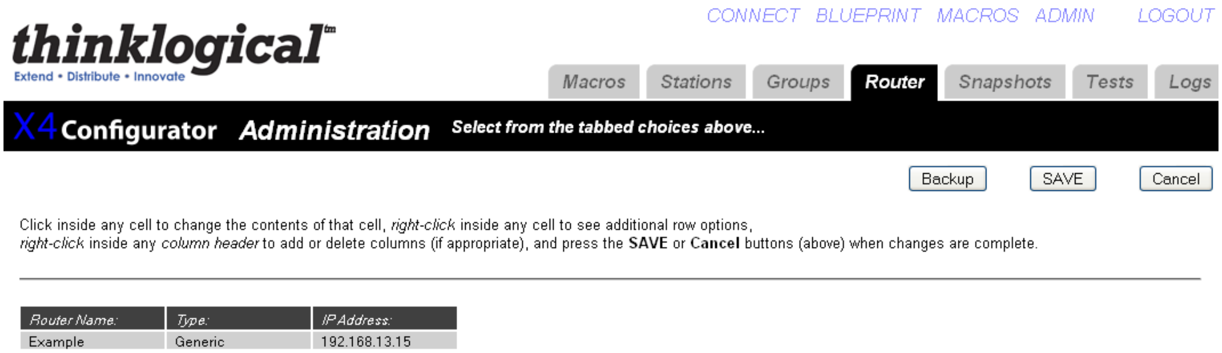
Groups by IP address (for touchpanels)

IP Address:	*Group:*
192.168.13.253	touch

Figure D6: View of Groups from Administration Page

ROUTER
The router tab will allow you to add or edit the router name, type and address.
The file named "router.csv" is set at the factory and will almost never need to be modified.

If additional physical routers are added later, and you wish to control them using the same X4 Configurator Software, then each new router will require a new line in the table that sets the name, type, and address for that router.



Click inside any cell to change the contents of that cell, *right-click* inside any cell to see additional row options, *right-click* inside any *column header* to add or delete columns (if appropriate), and press the **SAVE** or **Cancel** buttons (above) when changes are complete.

Router Name:	*Type:*	*IP Address:*
Example	Generic	192.168.13.15

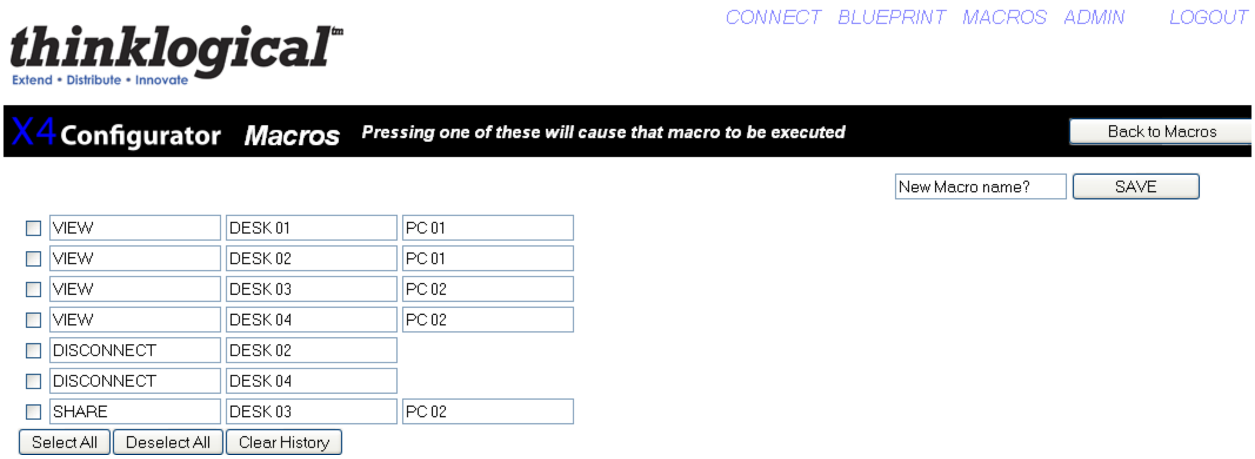
Figure D7: View of Router from Administration Page

MACROS

A macro is a sequence of operations the user can create, save, and recall to repeat steps that will be used frequently.

There are three ways to create, edit and delete any macros.

1. On the Macro Page there is a button at the far right titled "Macro from History". When pressed, it displays the steps that have been previously executed from that browser. Select the steps you would like to be part of the Macro, name the Macro and click SAVE.
2. On the ADMIN Page when the Macro tab has been selected you are able to create and save a new macro without executing the steps. You can also edit existing macros, rename macros, and delete macros.
3. Using a text editor or spreadsheet program (Excel, OpenOffice), one can create, save, edit, and delete macros directly.



□	VIEW	DESK 01	PC 01
□	VIEW	DESK 02	PC 01
□	VIEW	DESK 03	PC 02
□	VIEW	DESK 04	PC 02
□	DISCONNECT	DESK 02	
□	DISCONNECT	DESK 04	
□	SHARE	DESK 03	PC 02

Figure D8: Create a Macro from History

TOUCHSCREENS

A touchscreen allows user-friendly access to the Thinklogical X4 Configurator software for simple actions to be made with the touch of the screen. The unit connects independently ***to a network*** and with a one time configuration, the set-up is easily performed.

There are two ways to configure a touchscreen. One is to use a USB keyboard connected directly to the touchscreen and make any necessary changes directly on that panel. The other is to connect one or more touchscreens to a network and log into them remotely. Both methods are described below.
In both cases, you will first need to decide the IP address of the web server before configuring the touchscreen(s).

Direct Configuration:

1. Attach the USB keyboard to a USB port on the Touchscreen
2. Press Ctrl - Alt - F1 on the Touchscreen to go into text mode
3. When the login appears, type in the following-

   username: root
   password: emac_inc

Remote Configuration: Each touchscreen is shipped with DHCP enabled by default.

1. Attach one or more touchscreens to a network with a DHCP server
2. Use "ssh" to access each touchscreen in turn
3. When the login appears, type in the following-

   username: root
   password: emac_inc

To set up the network:

1. Type cd/home/user/
2. Using vi, edit “interfaces”
3. In the section for eth1,

   a. Modify dhcp line to say “static”
   b. Insert a line "address 192.168.13.161" (with whatever IP address you've chosen for this Touchscreen)
   c. Add "netmask 255.255.255.0"
   d. Save and exit

The completed interface file should look something like this after modification:

```
# /home/user/interfaces -- configuration file for ifup(8), ifdown(8)

# The loopback interface
auto lo
iface lo inet loopback

allow-hotplug eth0
iface eth0 inet static
address 192.168.13.171
netmask 255.255.255.0
gateway 192.168.13.1
```

To set the browser to find the server:

1. Type cd/home/user/
2. Using vi, edit “homepage” (a single line file that, by default, reads: "http://192.168.13.9/touch")

   a. Change the IP address to match that of the web server machine
   b. Save and exit

The files have now been configured, but the Touchscreen will not use them yet:

3. Type “sync”
4. Type “reboot”

The touchscreen will blank its screen and reboot with the new values. If you are using the Remote Configuration method on multiple touchscreens, watch to see which panel blanks and reboots so you can tell which one you've just configured and label it with the proper IP address.

The touchscreen starts up in Detail mode by default. The buttons shown at the bottom of the screen are command buttons which perform a task. Connect will connect your destination to a source by pressing, where Take Mouse will ‘take the mouse’ from all other connections and give it to the source/destination combination the user has selected. You can also run Macros by clicking on the Macros button and then run the selected Macro.

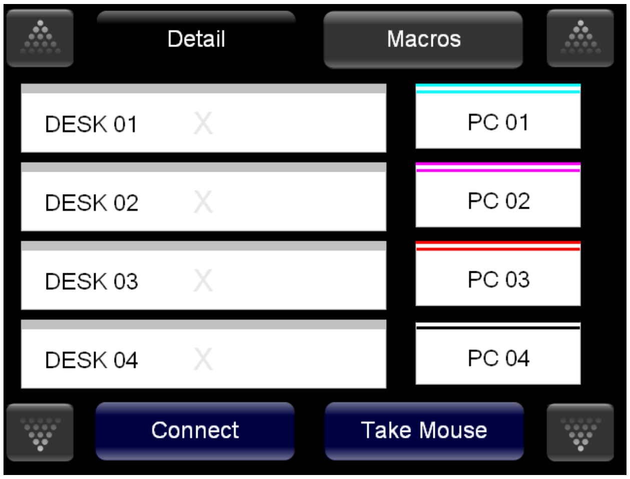


Figure D9: View of Touch Screen

TESTS

The Test tab allows you to test the port connections of a VX Router.

How to Perform a Test

a. From the Router drop down list, select the router you want to test.
b. Choose from the 'Select a Test' drop down menu:
   1. 1 to 1, 2 to 2, etc
   2. Broadcast chosen source to all
   3. Cycle through sources
   4. Cycle through destinations

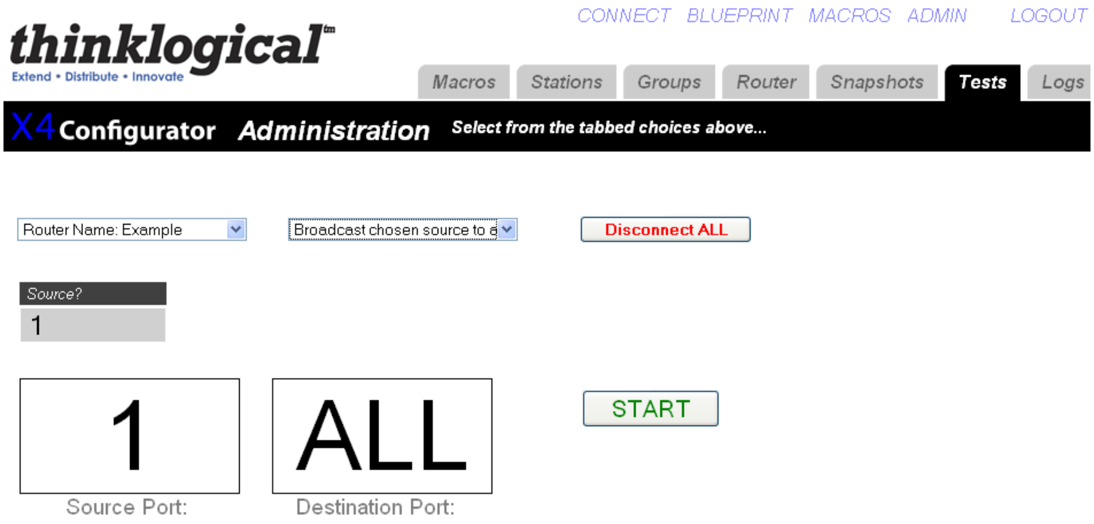

CONNECT BLUEPRINT MACROS ADMIN LOGOUT
thinklogical
Extend • Distribute • Innovate
Macros
Stations
Groups
Router
Snapshots
Tests
Logs
X4 Configurator Administration
Select from the tabbed choices above...
Router Name: Example
Broadcast chosen source to a
Disconnect ALL
Source?
1
1
ALL
START
Source Port:
Destination Port:

Figure D10: Test Function

SNAPSHOTS

Snapshots are recorded and executed from the "Snapshot" tab of the ADMIN page. Snapshots are a way of recording and saving the connections of every single port on one or more routers, including whether or not they are connected at all. When a snapshot is played back or "executed" every port will be reset to the connections that were present when the snapshot was recorded.

⚠ **NOTE- This process can be disruptive. It should only be used to set all connections to a known state. Since every port is reset and reconnected, even ports that are already connected the same way the snapshot recorded will temporarily lose their connections before being reconnected.**

To create a new snapshot, select “"Create New Snapshot" from the pull-down list. “Press to record” will appear and should be pressed when the system is connected and ready to be recorded. A name box will also appear with a default name for the new snapshot. Clicking the "Press to Record" button will cause the system to interrogate every port and save the settings to a new .csv file in the setups/snapshots/ directory with the same name as the snapshot.
To change the name of a snapshot or delete it, select it from the pull-down list. Its name will appear in the text input box next to "Change name here", as well as a "Delete This Snapshot" button. To change the name, change the text in the input box. To delete it, click the "Delete" button and then accept the action on the confirmation pop-up.
Existing Snapshots will appear as buttons and selecting one of these buttons will execute the snapshot after an “Are you sure?” confirmation pop up.

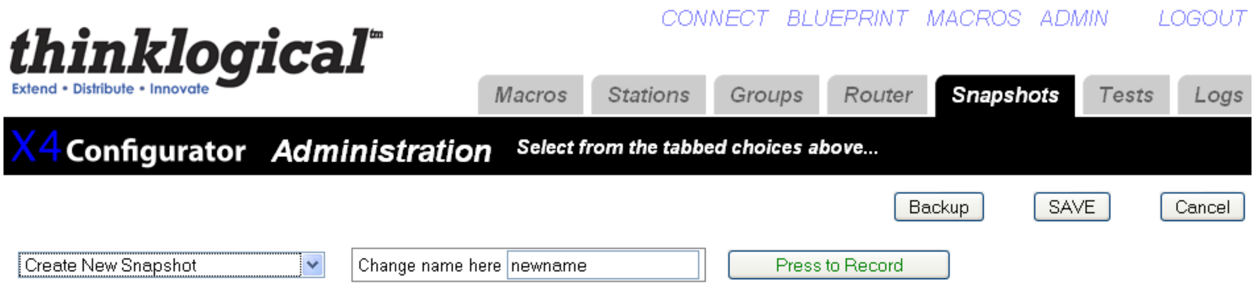


Figure D11: Snapshots

STUDIO
The Studio view is an alternate view for the Connections tab. Connecting ports in the Studio view is a different process and has additional options. To add this page see Groups section.

To make a connection, select both a destination and a source (in any order). They will turn blue when selected.

"TAKE" will cause any existing destinations for the selected source to be disconnected, and then the chosen destination will be given the only connection for the chosen source, as well as having control of the mouse and keyboard.

"(VIEW)" will not disturb any existing connections from the source, but the new destination will not receive control of the keyboard/mouse. This is useful if a user wishes to monitor a source without disturbing any existing users of that source.

The (VIEW) button is rendered with parenthesis to remind users that VIEW only gives them the ability to see the source and not control it. Destination boxes with sources that are connected using VIEW will show the source name in parenthesis meaning that the source can be seen but not controlled. Only one destination will show the source name without parenthesis, and that is the one with the keyboard mouse channel.

⚠ **NOTE: If no other destination is using the source at the time the (VIEW) button is pressed, then the new destination will also get control of the keyboard/mouse.)**

"SHARE" is a hybrid of the first two commands. No existing video connections for the given source are broken, but the new destination will also receive control of the keyboard/mouse. This is useful when two or more user destinations are viewing the same source and they wish to take turns controlling the keyboard and mouse. The video will be present at both destinations, but whoever presses SHARE last will have control of the keyboard/mouse.

And as described previously in the (VIEW) section, if SHARE is used to connect a source to a destination, the source name will appear *without* parenthesis in that destination and *with* parenthesis in any other previous destinations also showing that source.

There are also Lock and Unlock buttons to keep control of chosen sources and destinations. When a user has a source or destination (or both) locked, they can be assured that no other user will be able to take video, keyboard or mouse from that source.

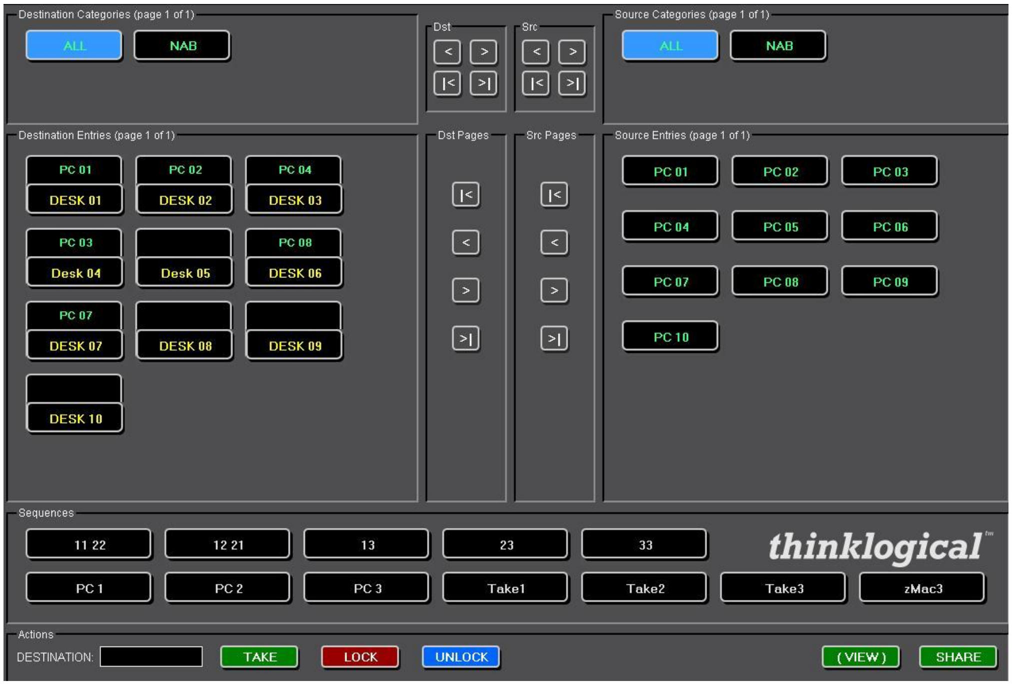
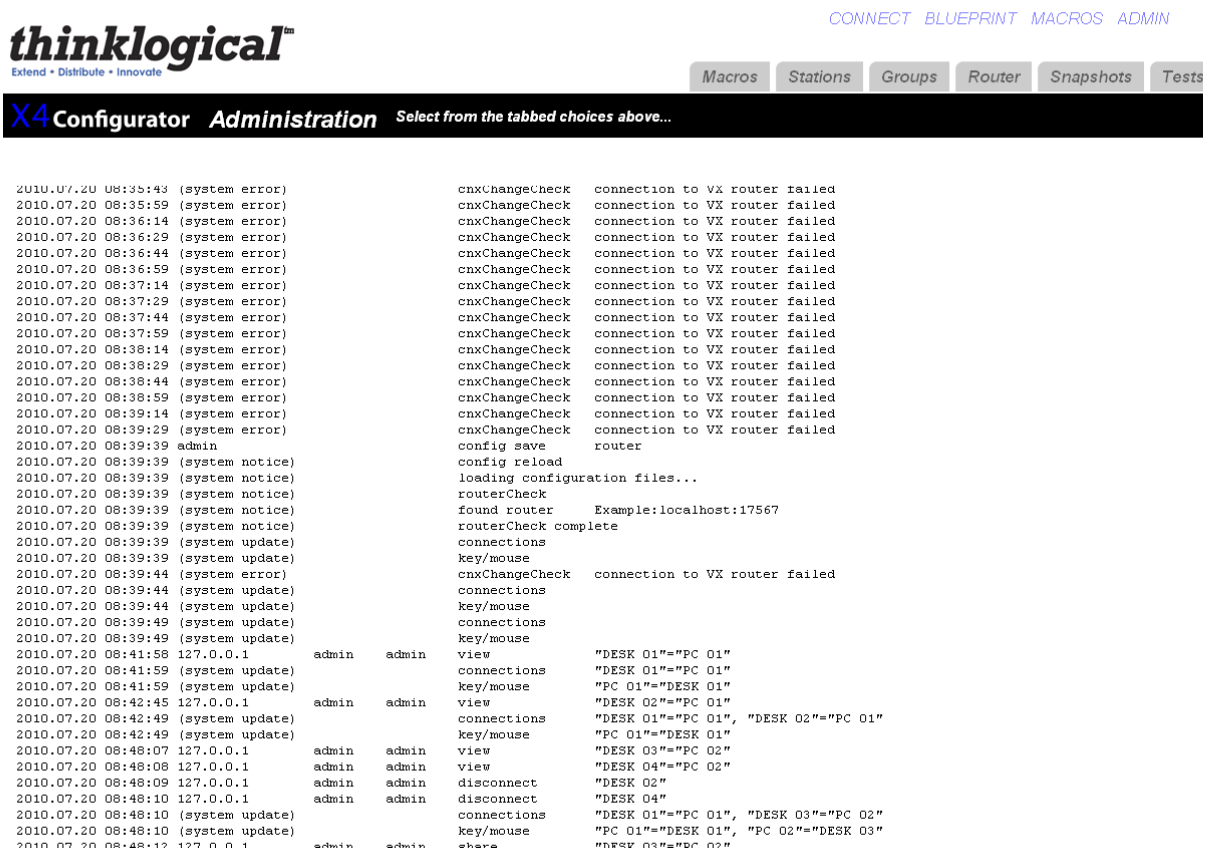


Figure D12: Studio View

LOGS

To view a log of the activity of the switch you can click on the Logs tab under ADMIN. This will allow you view logins, operations, connections, errors and system updates.


CONNECT BLUEPRINT MACROS ADMIN
thinklogical™
Extend • Distribute • Innovate
Macros
Stations
Groups
Router
Snapshots
Tests
X4 Configurator
Administration
Select from the tabbed choices above...

```
2010.07.20 08:35:43 (system error)                  cnxChangeCheck   connection to VX router failed
2010.07.20 08:35:59 (system error)                  cnxChangeCheck   connection to VX router failed
2010.07.20 08:36:14 (system error)                  cnxChangeCheck   connection to VX router failed
2010.07.20 08:36:29 (system error)                  cnxChangeCheck   connection to VX router failed
2010.07.20 08:36:44 (system error)                  cnxChangeCheck   connection to VX router failed
2010.07.20 08:36:59 (system error)                  cnxChangeCheck   connection to VX router failed
2010.07.20 08:37:14 (system error)                  cnxChangeCheck   connection to VX router failed
2010.07.20 08:37:29 (system error)                  cnxChangeCheck   connection to VX router failed
2010.07.20 08:37:44 (system error)                  cnxChangeCheck   connection to VX router failed
2010.07.20 08:37:59 (system error)                  cnxChangeCheck   connection to VX router failed
2010.07.20 08:38:14 (system error)                  cnxChangeCheck   connection to VX router failed
2010.07.20 08:38:29 (system error)                  cnxChangeCheck   connection to VX router failed
2010.07.20 08:38:44 (system error)                  cnxChangeCheck   connection to VX router failed
2010.07.20 08:38:59 (system error)                  cnxChangeCheck   connection to VX router failed
2010.07.20 08:39:14 (system error)                  cnxChangeCheck   connection to VX router failed
2010.07.20 08:39:29 (system error)                  cnxChangeCheck   connection to VX router failed
2010.07.20 08:39:39 admin                           config save      router
2010.07.20 08:39:39 (system notice)                 config reload
2010.07.20 08:39:39 (system notice)                 loading configuration files...
2010.07.20 08:39:39 (system notice)                 routerCheck
2010.07.20 08:39:39 (system notice)                 found router     Example:localhost:17567
2010.07.20 08:39:39 (system notice)                 routerCheck complete
2010.07.20 08:39:39 (system update)                 connections
2010.07.20 08:39:39 (system update)                 key/mouse
2010.07.20 08:39:44 (system error)                  cnxChangeCheck   connection to VX router failed
2010.07.20 08:39:44 (system update)                 connections
2010.07.20 08:39:44 (system update)                 key/mouse
2010.07.20 08:39:49 (system update)                 connections
2010.07.20 08:39:49 (system update)                 key/mouse
2010.07.20 08:41:58 127.0.0.1       admin    admin  view             "DESK 01"="PC 01"
2010.07.20 08:41:59 (system update)                 connections      "DESK 01"="PC 01"
2010.07.20 08:41:59 (system update)                 key/mouse        "PC 01"="DESK 01"
2010.07.20 08:42:45 127.0.0.1       admin    admin  view             "DESK 02"="PC 01"
2010.07.20 08:42:49 (system update)                 connections      "DESK 01"="PC 01", "DESK 02"="PC 01"
2010.07.20 08:42:49 (system update)                 key/mouse        "PC 01"="DESK 01"
2010.07.20 08:48:07 127.0.0.1       admin    admin  view             "DESK 03"="PC 02"
2010.07.20 08:48:08 127.0.0.1       admin    admin  view             "DESK 04"="PC 02"
2010.07.20 08:48:09 127.0.0.1       admin    admin  disconnect       "DESK 02"
2010.07.20 08:48:10 127.0.0.1       admin    admin  disconnect       "DESK 04"
2010.07.20 08:48:10 (system update)                 connections      "DESK 01"="PC 01", "DESK 03"="PC 02"
2010.07.20 08:48:10 (system update)                 key/mouse        "PC 01"="DESK 01", "PC 02"="DESK 03"
2010.07.20 08:48:12 127.0.0.1       admin    admin  share            "DESK 03"="PC 02"
```

Figure D13: View of Log File

CONFIGURATION FILE STRUCTURE

The configuration files (stations, groups, router, macros) all share a similar structure. The files are encoded in the .csv (comma separated values) format to allow easy access from spreadsheet programs, text editors, and the web-server program itself.

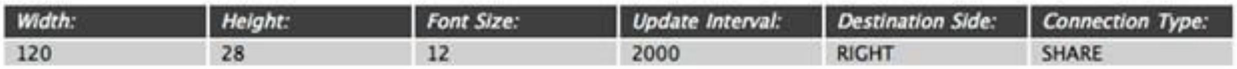
There are four kinds of rows: ***blank, comments, headers, and values***. If a row is blank, it is ignored. This allows the creation of white space between blocks of data.

If the first character in the first field of a row is ‘#’, then the contents of the entire row will be ignored . This gives the administrator the ability to enter and save comments.

If the first field in a row ends with ‘:’ (colon), then the program interprets the entire row as a series of “headers”. A header describes the meaning and usage of all the fields below the header in that column, until a new series of headers replaces the current ones and supplies new meanings for the values below it.

There are three ways of interpreting the values found in the fields below a header:

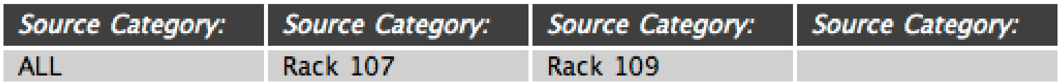
The first is “global”. This value is assigned to the name defined in the header above it and it will apply throughout the application. Examples of a global value would be: “Font Size”, “Connection Type”, and “Update Interval”.



Width:	Height:	Font Size:	Update Interval:	Destination Side:	Connection Type:
120	28	12	2000	RIGHT	SHARE

Figure D14: Global Values

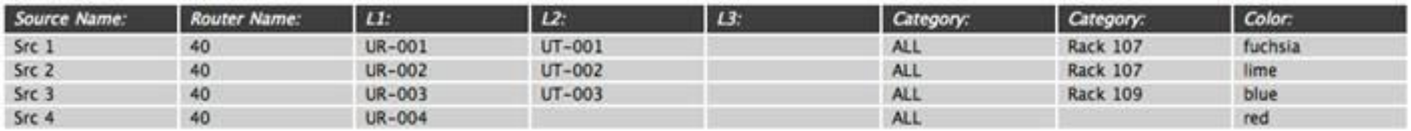
The second type of value is part of a list. If there are multiple headers with the same name, then the values found below those headers will be added to a list with that name. Examples of lists include “Source Category”, “Destination Category”, and “Viewable”.



Source Category:	Source Category:	Source Category:	Source Category:
ALL	Rack 107	Rack 109	

Figure D15: List Values

The final type of value is defined when the entire row is meant to be thought of as an “object”. A good example of an object would be a “station” which has its own name, some number of input and/or output ports that should all be switched at the same time, and additional other fields.

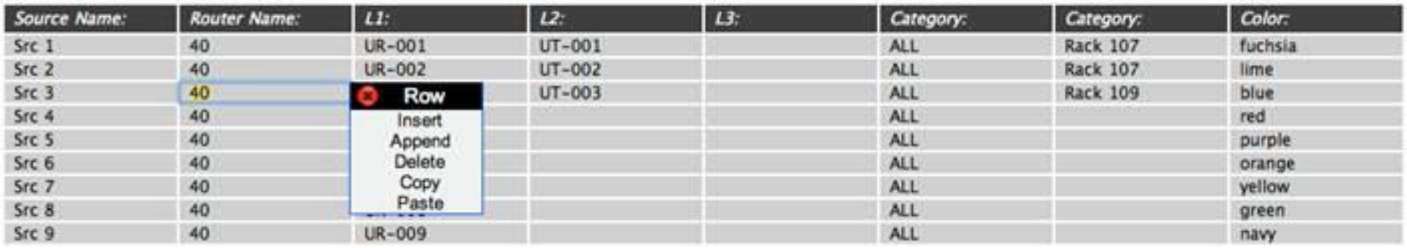


Source Name:	Router Name:	L1:	L2:	L3:	Category:	Category:	Color:
Src 1	40	UR-001	UT-001		ALL	Rack 107	fuchsia
Src 2	40	UR-002	UT-002		ALL	Rack 107	lime
Src 3	40	UR-003	UT-003		ALL	Rack 109	blue
Src 4	40	UR-004			ALL		red

Figure D16: Object Values

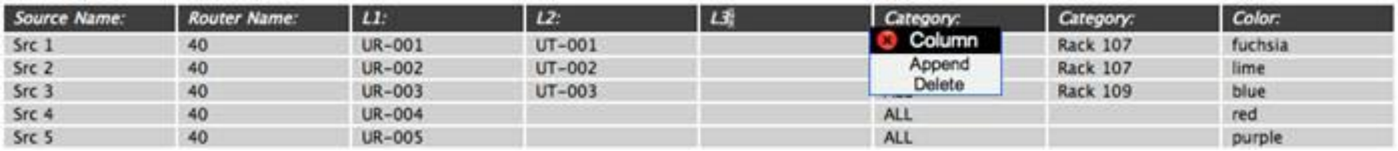
In the example above, the station with the source name “Src 1” has fields for the router name “40”, the ports used in that router (“UR-001” and “UT-001”), the categories that will show it (“ALL” and “Rack 107”), and the color that this source and the destinations will display when they are connected (“fuchsia”).

X4 Configurator imitates a simplified model of a spreadsheet within the user’s browser. Rows can be added or removed by left-clicking on any of the light gray “value” rows and choosing the proper choice from the drop down menu. New columns can be added by right-clicking on any of the dark “header” fields and selecting “Append” or “Delete” from the drop down menu.



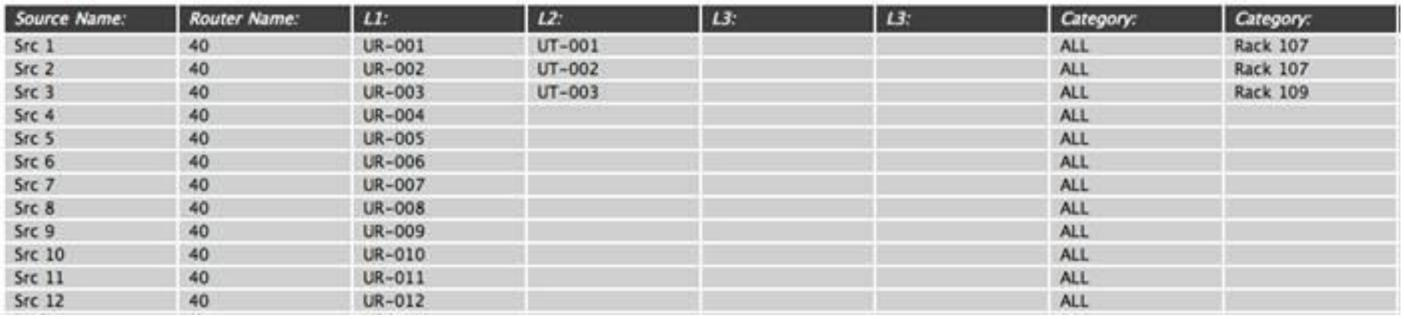
Source Name:	Router Name:	L1:	L2:	L3:	Category:	Category:	Color:
Src 1	40	UR-001	UT-001		ALL	Rack 107	fuchsia
Src 2	40	UR-002	UT-002		ALL	Rack 107	lime
Src 3	40		UT-003		ALL	Rack 109	blue
Src 4	40				ALL		red
Src 5	40				ALL		purple
Src 6	40				ALL		orange
Src 7	40				ALL		yellow
Src 8	40				ALL		green
Src 9	40	UR-009			ALL		navy

Figure D17: Right clicking a row



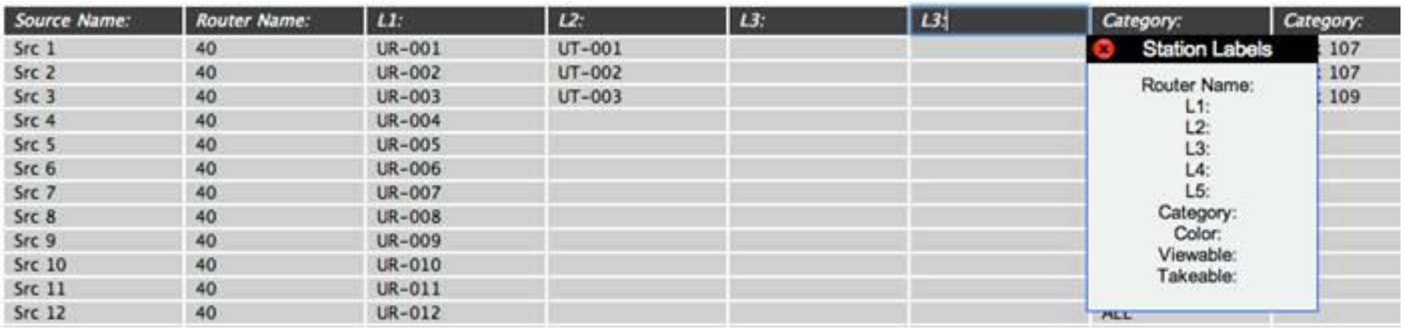
Source Name:	Router Name:	L1:	L2:	L3:	Category:	Category:	Color:
Src 1	40	UR-001	UT-001			Rack 107	fuchsia
Src 2	40	UR-002	UT-002			Rack 107	lime
Src 3	40	UR-003	UT-003			Rack 109	blue
Src 4	40	UR-004			ALL		red
Src 5	40	UR-005			ALL		purple

Figure D18: Right clicking a column



Source Name:	Router Name:	L1:	L2:	L3:	L3:	Category:	Category:
Src 1	40	UR-001	UT-001			ALL	Rack 107
Src 2	40	UR-002	UT-002			ALL	Rack 107
Src 3	40	UR-003	UT-003			ALL	Rack 109
Src 4	40	UR-004				ALL	
Src 5	40	UR-005				ALL	
Src 6	40	UR-006				ALL	
Src 7	40	UR-007				ALL	
Src 8	40	UR-008				ALL	
Src 9	40	UR-009				ALL	
Src 10	40	UR-010				ALL	
Src 11	40	UR-011				ALL	
Src 12	40	UR-012				ALL	

Figure D19: After selecting “Append” from the “Column” drop down



Source Name:	Router Name:	L1:	L2:	L3:	L3:	Category:	Category:
Src 1	40	UR-001	UT-001				107
Src 2	40	UR-002	UT-002				107
Src 3	40	UR-003	UT-003				109
Src 4	40	UR-004					
Src 5	40	UR-005					
Src 6	40	UR-006					
Src 7	40	UR-007					
Src 8	40	UR-008					
Src 9	40	UR-009					
Src 10	40	UR-010					
Src 11	40	UR-011					
Src 12	40	UR-012				ALL	

Figure D20: Left click a column header to see header name choices

While each file uses a similar method to define and populate various objects, the kinds of objects created by each file depends on the file name and the software module that reads it.

1. "groups.csv" will be read and interpreted by the module "groups.pyc" to create user groups, individual user accounts, and IP addresses that will always be assigned to specific groups.
2. "stations.csv" will be read and interpreted by "stations.pyc" to set general values for station button sizes and fonts, and also to create the source and destination objects and their constituent ports.
3. "macros" is a directory. Within it are individual files - one for each macro. Since macros can be limited to specific groups, there are "Group:" columns at the top that set who can see and execute each group.