PESA
Internet Remote Control
(PIRC)
Protocol

PESA Switching Systems, Inc.
330-A Wynn Drive Northwest
Huntsville, AL 35805-1961
http://www.pesa.com
(256) 726-9200

Document No. 81-9062-0448-0 Revision B

Service and Ordering Assistance

PESA Switching Systems, Inc.
330-A Wynn Drive Northwest
Huntsville, AL 35805-1961 USA
www.pesa.com

Main Office
(256) 726-9200 (Voice)
(256) 726-9271 (Fax)

Service Department
(256) 726-9222 (Voice) **(24 hours/day, 7 days/week)**
(256) 726-9268 (Fax)
service@pesa.com

National Sales Office

PESA Switching Systems, Inc.
35 Pinelawn Rd., Suite 99-E
Melville, NY 11747 USA
(800) 328-1008 (Voice)
(631) 845-5020 (Voice)
(631) 845-5023 (Fax)

All information, illustrations and specifications contained in this publication are based on the latest product information available at the time of publication approval. The right is reserved to make changes at any time without notice.

Comments concerning this document are welcome, and should be directed to: techpubs@pesa.com

Printed in the United States of America.

Table of Contents

Tables

Chapter 1 – Introduction

This document describes the PESA Internet Remote Control (PIRC) protocol. Where appropriate, this protocol uses commands common to other Internet protocols, or to the PESA CPU Link protocol.

This protocol is the property of PESA Switching Systems, Inc. PESA reserves the right to change this protocol at any time without notification to users.

NOTE

We expect to make changes to the protocol when we release V2.0. These changes may be such that V1.x commands may no longer be functional. Among the changes, responses sent back from the PIRC server might be changed to enforce better consistency.

Chapter 2 – Protocol Description

The PIRC protocol describes a set of commands that allow for control of a PESA routing system from remote sites. This protocol describes route configuration and action commands that are acted on by the controller. This protocol is usually transmitted via TCP/IP socket connections and is based on common Internet protocols.

Internet Protocols

Most common Internet protocols are defined in an RFC (Request for Comment) document, which itemizes the send and receive commands and response codes.

Requests are normally 3 or 4 character commands that describe the operation.

Many Internet protocols are strictly request-response based. A response code can be uniquely associated with a specific request. In the case of the PIRC protocol, however, the server can send unsolicited responses to the client.

Command Summary

To reduce communications bandwidth, most commands refer to sources, destinations, levels, and groups by number. It is the responsibility of the connected device to translate the number code to meaningful names, based on the configuration files. Most commands can be abbreviated using the first three characters.

There are two command modes, client and administrative. The client commands are executed after the connecting device logs on as a client. These commands handle most of the real-time routing functions. As many user sessions can be open simultaneously, as there are authorized user licenses.

The administrative commands require the connecting device to log on in administration mode before it sends any command. Only one administration session can be open at any time.

Table 1. User Mode Commands

Command	Description
BLOCK	Aggregates commands
CFG	Get the configuration data for destinations, sources, and levels in a composite command
DEV	Requests device type/name/version (Ocelot, 3300, 3500)
LOCK	Locks a destination
MODE	Controls where unsolicited responses are allowed. Values: SYNC (synchronous request-response pairs – default), MON (monitor)
PING	Keeps the TCP connection open. The controller must receive a ping from a client every 30 seconds to avoid a timeout.
QUIT	Logoff/disconnect
RAW	Send CPU link protocol command (without checksum) Forces mode to SYNC
STAD	Status of a specific destination STAD 3
STAT	Full status
SWA	Switch all
SWL	Switch (level specifications)
USER	Logs user into the system Mode initialized to SYNC

Table 2. Administrative Mode Commands

Command	Description
ADMN	Logs user into Administration mode
BYE	Finishes the Administration mode
CLOSE	Terminates the server service application.
GET	Retrieves files from the WCE controller
KEY	Writes new license key to the registry
PUT	Copies files to the WCE controller
REBOOT	Reboots the server controller
RESTART	Restarts the server service application without reset
USR	Retrieves the maximum number of users licensed

Command Syntax

PIRC Protocol commands and responses are terminated with <LF>. Arguments are separated from the command keyword, and from one another, by spaces.

- <COMMAND> <ARG1> <ARG2><LF>

The TCP/IP transport protocol verifies data integrity so no checksum information is included in this protocol. Since TCP/IP connections are port-based and are unique, no user id information is required on a per-command basis.

PIRC Commands are case insensitive. CPU Link commands passed through the RAW command must follow the appropriate PESA CPU Link rules for case, spaces, and delimiters.

Response Codes

The PIRC Server defines the response codes shown in Table 3.

Table 3. Response Codes

Code	Value
SUCCESS	250
LOGIN_REDIRECT	253
BLOCK_COMPLETE	255
BUSY	400
DESTINATION_LOCKED	410
TRANSMISSION_ERROR	411
UNKNOWN_DEVICE	501
INVALID_LOGIN	503
INVALID_COMMAND	504
INVALID_PERMISSION	505
INVALID_DESTINATION	506
INVALID_SOURCE	507
INVALID_LEVEL	508
PARSE_ERROR	510
BLOCK_PARSE_ERROR	511
FUNCTION_NOTALLOWED	520
UNDEFINED	599
Full status	STAT
Single Destination Status	STAD
Configuration	CFG
MAX_LICENSES	512

User Mode Commands

BLOCK

The BLOCK command is used to aggregate multiple PIRC commands into a single request. The BLOCK command simply concatenates other PIRC commands together, delimited by “ :: “ (space, colon, colon, space).

Table 4. BLOCK

Command	BLOCK <CMD1> :: <CMD2> :: <CMD3>
Response	255 – All commands listed in the block have been completed.
	511 – Unable to parse the block command.
Example	Send: BLOCK SWL 1 1 3 :: STAT :: SWA 4 2 :: STAD 4 :: TEST Receive: 250 (from SWL) STAT DST 001 0 000 000 001 DST 002 0 000 000 000 250 (from SWA) STAD DST 004 0 002 002 002 504 (from TEST, an invalid command) 255 (Block complete)

The BLOCK command can be used to automatically append a MODE 1 command to switch directives and other commands, since every command except MODE 1 deactivates the monitor mode for unsolicited responses. For more information, see “MODE” on page 9.

CFG

The CFG command provides a destination, source, and level configuration report for the switch. The response returned by this command may be lengthy.

Table 5. CFG

Command	CFG
Response	CFG <NUMDST> <NUMSRC> <NUMLEV> DST <DST> <FLAG> <EXP-1> <EXP-2> DST <DST> <FLAG> <EXP-1> <EXP-2> SRC <SRC> <FLAG> <EXP-1> <EXP-2> SRC <DST> <FLAG> <EXP-1> <EXP-2> LEV <LEV> <FLAG> <EXP-1> <EXP-2> LEV <LEV> <FLAG> <EXP-1> <EXP-2> Command successfully exchanged with client. There are 2 EXP fields that denote future information that may be included with the data. <NUMDST>, <NUMSRC>, and <NUMLEV> denote the routing controllers physical characteristics, NOT the number of returned destinations, sources, and levels in the CFG command.
Example	For a three level system with four sources and four destinations, with permission granted ONLY for destinations 1 and 3: Send: CFG Receive: CFG 4 4 3 DST 001 1 EXPANSION EXPANSION DST 003 1 EXPANSION EXPANSION SRC 001 1 EXPANSION EXPANSION SRC 004 1 EXPANSION EXPANSION LEV 001 1 EXPANSION EXPANSION LEV 002 1 EXPANSION EXPANSION LEV 003 1 EXPANSION EXPANSION Destination 1 is valid and destination 3 is valid. Destinations 2 and 4 are NOT reported, since there is no permission for those destinations. Source 1 is valid and source 4 is valid. Sources 2 and 3 are NOT reported, since there is no permission for those sources. Levels 1, 2, and 3 are valid, which means that all levels are reported back.

The security.txt permission list file determines the list of destinations, sources, and levels.

- The list of destinations should not be considered a complete list, since user privilege may prohibit use of a particular destination.
- The list of sources should not be considered a complete list, since user privilege may prohibit use of a particular source.
- The list of levels should not be considered a complete list, since user privilege may prohibit use of a particular level.

The CFG command pulls permission data from the security.txt file.

If a destination, source, or level is returned with a flag value of 0, then no permission has been granted for that item. The actual version of the protocol returns only those items for which permission has been granted (flag value of 1); future revisions to the protocol may return all items with only the flag control being used to indicate whether permission has been granted.

DEV

The DEV command returns the device type/name under control of the PIRC server.

Table 6. DEV

Command	DEV
Response	250 <Device> – Device type request accepted; device name is returned.
	501 – Unable to determine device type.
Example	Send: DEV<CRLF> Receive: 250 3500,V3.3:0

LOCK

The LOCK command issues a lock command for switches that support the notion of a lock. For switches that do not support locks, the lock is implemented at the PIRC server layer.

Table 7. LOCK

Command	LOCK <DST> <On/Off flag> The flag is 0 for OFF and non-zero for ON.
Response	250 – Command successfully exchanged with device.
	505 – Permission Error.
	510 – Unable to parse command.
Example	Send: LOCK 1 1 Receive: 250

MODE

The MODE command is directive to the PIRC server from the client that unsolicited commands (e.g. STAT, STAD, STAR) are acceptable. Normally, this command is issued with the MON option (1) if the client will be idle for a period of time. While in the MON mode, the controller can send STAT commands to the client through the TCP/IP connection. The MON mode makes it possible to see what actions other users have made to the switch since STAT responses will be sent to the applet as a result of switch commands made by other users. In addition, STAT responses will be sent to the applet whenever physical device settings have been changed.

The SYNC mode (0) is the normal mode, which maintains a command/response direct relationship.

Any command other than "MODE 1" automatically resets the controller to MODE SYNC. There is no provision for automatically returning to the MON mode; the applet must command it.

At this time, only STAT responses are made in the MON mode.

Option is 0 for SYNC, 1 for MONITOR.

Table 8. MODE

Command	MODE <OPTION>
Response	250 – Command successfully exchanged with device.
	400 – Busy, try again later.
	500 – Unable to change mode.
Example	Send: MODE 1 Receive: 250 STAD DST 001 1 002 002 002 STAR DST 002 0 002 002 002 DST 003 0 002 002 002 Unsolicited STAT response received some time after the MON mode went into effect. The STAT response indicated a setting change for destination 1. Later, another unsolicited STAT response was delivered for destination 2 as well as destination 3.

PING

The PING command is required to keep track of the clients. The server application must watch for client activity in intervals at least 30 seconds to prevent zombie threads in the server if a connection crashes or goes down.

PIRC servers watch for this ping and if this is not received in an interval longer than 30 seconds, the thread that handles the socket is terminated.

Table 9. PING

Command	PING
Response	250 – Acknowledged.
Example	Send: PING Receive: 250

QUIT

The QUIT command should be called by the application when terminating a session. (Optional)

Table 10. QUIT

Command	QUIT
Response	250 – Success. Quit accepted. Closing PORT.
	400 – Unable to quit – busy.
	505 – Permission denied.
Example	Send: QUIT Receive: 250

RAW

The RAW command is a means of exchanging low-level routing controller specific commands the routing controller transparently through the PIRC server. No processing is done to the command string with the exception of appending a properly calculated checksum to the command prior to transmitting it to the routing controller.

Checksums are not included in the specific command string. The PIRC server adds the checksum prior to termination. No logical-virtual mapping is performed. The return string does include the checksum sent from the switch.

The RAW command may be used to extend the protocol to the extended features of the routing control system.

Table 11. RAW

Command	RAW <Routing Control Specific Command string>
Response	250 <Response> – Command successfully exchanged with device.
	505 – Permission error.
	510 – Unable to parse command.
Example	Send: RAW Y001 Receive: 250 00100000005000:6
Security	The user must be correctly logged in to use this command. The command is not activated until the security module is activated, which means that the users must log-in and authenticate.

STAD

This command interrupts the caching routine to do an immediate STATUS query on the specified destination. Unlike the STAT command which queries the cache/memory map of the controller, this command can be used to specifically poll the unit for settings.

The STAD command is a subset of the STAT command, requesting the status of a particular destination only.

Table 12. STAD

Command	STAD <DST>
Response	STAT DST <DST> <LS> <SRC AT LEV1> <SRC AT LEV2> <SRC AT LEV3> ... Command successfully exchanged with device
Example	Send: STAD 3 Receive: STAD DST 3 0 1 1 1 Destination 3 (the requested destination) is not locked and has all levels from source 1.

STAT

The STAT command provides a full system status for the switch.

Table 13. STAT

Command	STAT
Response	STAT DST <DST> <LS> <SRC AT LEV1> <SRC AT LEV2> <SRC AT LEV3> ... Command successfully exchanged with device.
Example	For a three level system with four sources and four destinations: Send: STAT Receive: STAT DST 001 0 002 002 002 DST 002 0 004 004 004 DST 003 1 001 001 000 DST 004 0 002 001 002 Destination 1 is not locked and has all levels from source 2. Destination 2 is not locked and has all levels from source 4. Destination 3 is locked and has level 1 from source 1, level 2 from source 1, and level 3 unassigned (0). Destination 4 is not locked and has level 1 from source 2, level 2 from source 1, and level 3 from source 2.
Security	The user must be correctly logged in to use this command. The command is not activated until the security module is activated, which means that the users must log-in and authenticate.

The device.txt configuration file determines the list of destinations. The list of destinations should not be considered a complete list, since user privilege may prohibit use of a particular source or destination.

The STAT command pulls status from the controller cache.

The STAT command will not send back any destinations that the user does not have permission to see. The STAT command will put the value “000” for the source if there is no permission for the source or the level.

SWA

The SWA command switches all levels of the specified source to the specified destination.

Table 14. SWA

Command	SWA <DST> <SRC>
Response	250 – Command successfully exchanged with device.
	505 – Permission error.
	510 – Unable to parse command.
Example	Send: SWA 3 4 Receive: 250
Security	The SWA command can raise a security violation even when both the destination number and the source number (the required arguments to the command) are granted privilege. For this command to be accepted through the security of the protocol, ALL levels must be granted to the user.

SWL

The SWL command switches a single level on a specific destination. This command is the most basic router controlling commands of the protocol. The SWL command is typically used when a breakaway is performed by the controlling application/applet.

Table 15. SWL

Command	SWL <DST> <SRC> <LEV>
Response	250 – Switch command accepted.
	505 – Permission error.
	510 – Unable to parse command.
Example	To switch level 4 of destination 2 to source 1. Send: SWL 2 1 4 Receive: 250
Security	The source, destination, and level must be granted permission for this command to pass the security check.

USER

The USER command is required TWICE to access the server. First, the USER must connect to the PIRC port (usually port 4000) and issue a single USER command with a valid username and password. If successful, the user is redirected to another port, such as 4001 or 4004. The client must re-login (authenticate) in order to activate the security module, which permits the remainder of the PIRC protocol.

Table 16. USER

Command	USER username password
Response	250 – Successful login.
	253 PORT <num> – Successful login; reconnect at PORT <num>.
	503 – Invalid login.
	510 – Parsing error. Username or password not supplied.
Example	Port 3000 Send: USER pesa eroute Receive: 253 PORT 4001 Close Port 3000 Port 4001 Send: USER pesa eroute Receive: 250 <Perform commands>

Administration Mode Commands

ADMN

The ADMN command is required twice to access the controller. First, the user must connect to the PIRC port (usually port 4000) and issue a single ADMN command with a valid username and password. If successful, the user is redirected to another PORT, such as 4001 or 4004. The client must re-login (authenticate) in order to activate the security module, which permits the remainder of the PIRC protocol.

After a user successfully logs in to ADMN mode and executes any necessary administrative commands, a BYE command is required to close the administration session. Also, a RESTART command must be sent to the server application to set the new configuration.

Table 17. ADMN

Command	ADMN username password
Response	250 – Successful login.
	253 PORT <num> – Successful login; reconnect at PORT <num>.
	503 – Invalid login.
	510 – Parsing error. Username or password not supplied.
Example	Port 4000 Send: ADMN Administrator password Receive: 253 PORT 4001 Close Port 3000 Port 4001 Send: ADMN Administrator password Receive: 250 <Perform commands>

BYE

BYE finishes the Administration mode and closes the associated session. In order to free the administration session socket for future sessions, the client must sent the command after the administration session has terminated. Failure to do so, will block the administration socket until the ping timeout closes that session.

Table 18. BYE

Command	BYE
Response	OK – Administration Logout has been started.
Example	Send: BYE Receive: OK

CLOSE

The CLOSE command terminates the server application. It provides the possibility for updates or remote maintenance of the PIRC server machine from any machine connected to the same TCP/IP network.

Table 19. CLOSE

Command	CLOSE
Response	OK – Application shutdown has begun.
Example	Send: CLOSE Receive: OK

GET

The GET command allows the user to retrieve configuration files from the persistent storage of the PIRC server. The return value will be a string buffer containing the contents of the remote file. The string buffer will contain a series of "%20%" which must be replaced with CRLF before writing to a file.

Table 20. GET

Command	GET <filename> Valid filenames include: Password.txt Device.txt Lev.txt Security.txt Src.txt Dst.txt Grp.txt
Response	File not found – The File is corrupt or deleted.
	File too large – The File is bigger than 64 Kb.
	<File as described above> – Successful Retrieve
Example	Send: GET password.txt<LF> Receive: pesa pesa%20%guest password%20%…

KEY

The key command creates or updates the license key in the registry. This key is a 12 character encrypted alphanumeric string that contains the maximum number of users allowed to login to the PIRC server at any one time. After the KEY command, a RESTART command is necessary to update the new value.

Table 21. KEY

Command	KEY <12-length string>
Response	OK – The new key is saved in the registry
	ERR – The registry writing failed.
Example	Send: KEY oegfpifofgep Receive: OK

PUT

The PUT command allows the user to copy a configuration file from their PC to the PIRC server's persistent storage. Each line that is read from the file must be appended with a "%20%". The PIRC server replaces the %20% with a CRLF when saving the string buffer to the persistent storage.

Table 22. PUT

Command	PUT <filename> <string buffer>
Response	End of file Error – EOF was found.
	Access denied Error – There are not permissions to open the file.
	Sharing violation Error – The File is open for another process.
	OK – Successful transfer.
Example	Send: PUT password.txt "pesa pesa%20%guest password%20% …" <CRLF> Receive: OK

REBOOT

The REBOOT command allows the user to remotely restart the PIRC server by performing an operative system warm-boot.

Table 23. REBOOT

Command	REBOOT
Response	Rebooting NOW – Controller shutdown process has begun.
Example	Send: REBOOT Receive: Rebooting NOW All connections to the server are closed.

RESTART

The RESTART command allows the user to restart the server service application without shutdown the controller. This is useful to set new configuration files or a new key modified by an administration session.

Table 24. RESTART

Command	RESTART
Response	OK – The restart process has begun.
Example	Send: RESTART Receive: OK

USR

The USR command retrieves the maximum number of users licensed to use the system at the same time. This command returns a fix string of 11 characters padded with zeros as follows: USERS 00000.

Table 25. USR

Command	USR
Response	USERS 00000 – The number of users.
Example	Send: USR Receive: USERS 00001

Chapter 3 – Configuration Data

The configuration data (naming sources, destinations, etc) can be accessed through the PIRC protocol using the GET and PUT commands. These files define the configuration of the PESA router being controlled through the PIRC.

Device.txt

This file is the main file for the configuration data. All data is maintained as ASCII strings. This file lists the product model on the first line. The next group of lines lists the number of router destinations, sources, and levels of control. Each line has a single number on it.

The last lines of the file are the names of the specific configuration tables.

```
Model <string>
NUMDST
NUMSRC
NUMLEV
Dst.txt
Src.txt
Lev.txt
Grp.txt
```

Dst.txt

This file lists the configuration data for destinations on the router. This is not a reserved filename. The filename is identified in the device.txt file. The file lists (in order) the destination number, basic status (used = 1, not used = 0), the destination string name, and the filename of the .GIF or .JPG image associated with the item.

NOTE

Images are not currently supported.

Since the file is space delimited, device names must be single word names, but may include characters such as hyphen (-) and underscore (_).

All destination names must be unique.

If a destination is named NULL, it will be treated as inactive by the applet. Status reports from PIRC server are permitted for the destination, but no graphical representations will be provided.

```
1 1 VTR-1 vtr.jpg
2 1 TAPE_RM_103 tape_player.jpg
3 1 TAPE_RM_101 tape_2.gif
4 1 TAPE_RM_102 tape_2.gif
5 0 VTR-4 images/vtr.jpg
6 1 VTR-2 vtr.jpg
7 1 NULL NULL
8 1 NULL NULL
```

Src.txt

The source configuration table has the same format as the destination configuration file.

All source names must be unique.

Lev.txt

The lev.txt file characterizes the levels of control for the system. It has the same basic format as the dst.dat file (number, on/off, name, image).

All level names must be unique.

```
1 1 AUDIO-L audio.jpg
2 1 AUDIO-R audio.jpg
3 1 DIGITAL-1 digital.jpg
4 1 COMPOSITE_VIDEO analog.gif
```

Grp.txt

The grp.txt file characterizes the groups for the system. It is required that group 0 be reserved as CUSTOM (i.e. BREAK-AWAY). It is required that group 1 be reserved as ALL (i.e. TAKE-ALL). Since groups 0 and 1 are required, they are NOT included in the grp.txt file.

Each line includes the group number, the group name, the group image, and the complete list of levels. The number of levels in each line MUST be the same as NUMLEV in the device.txt file.

```
2 DIGITAL digital.gif  1 1 1 0
3 ANALOG analog.gif 1 1 0 1
```

The file is interpreted to mean that all “1” levels must be from the same source to be considered a match for the group.

Password.txt

This file must be saved on the root of the controller where is NOT accessible through the Web Browser.

```
Username password
Username password
```

Security.txt

This file lists the privileges for each source, destination, and level as those privileges are assigned to each user login. This file should be regarded as a “grant permission” file only. If a particular destination, source, or level is NOT listed (or covered with a grant ALL=999), then there is not permission for that particular destination, source, or level.

Therefore, if a user appears in the password.txt file and can log in, but the user is not listed in the security.txt file, that user has NO privileges to control the switch. This also implies that if the security.txt file is missing or has been corrupted, no users will have privileges to control the switch.

This file is NOT accessible through the Web Browser.

To grant permission to a user all sources, destinations, or levels – regardless of the number of items, use the number 999 for the item. Specifying all levels (e.g. USER LEV 999) does NOT imply that all sources and all destinations have also been granted. Each item type (DST, SRC, LEV) is treated independently.

The following example grants permission to user “Username” for destinations 1 and 4 only. No other destinations have permission for this user. “Username” also has been granted permission for sources 1, 2, and 3. Levels 1, 2, 3 have also been granted, using the special number “999”, which means ALL. NO OTHER PERMISSIONS ARE IMPLIED.

```
Username DST 001
Username DST 004
Username SRC 001
Username SRC 002
Username SRC 003
Username LEV 999
```

Chapter 4 – System Architecture and Status Cache

The controller unit maintains a cached status of the switch. A complete matrix is maintained in memory on the PIRC server unit. The PIRC server cache is maintained such that the switch status is always current. Since it is "current", the return to the client from the controller will be the values from the cache.

Cache Matrix

The cache is made up of two 2-dimensional matrices.

Table 26. Switch Connectivity Matrix

DST	LEV 1	LEV 2	LEV 3	LEV 4
1	2	2	2	2
2	5	0	1	1
3	0	0	0	2
4	5	5	0	5

Table 27. Lock Status Cache

DST	LCK
1	0
2	1
3	13
4	0

The DST column lists the destination numbers.

The LCK column is a Boolean for lock status (0 – not locked). Positive number is the user id who owns the lock.

The LEV columns list the sources that define the input for that level, for that destination. A value of 0 means no connection.

Notion of a Group

The PIRC protocol contains an item that is referred to as a group of levels. The group is a named (numbered) list of levels that have relevance to the system installation.

For instance, in a system with 8 levels, the Group "ALL" would mean levels 1 through 8, inclusive. Group "Digital", however, may only include levels 1,2,5,6,7,8. Group "Analog" may include levels 1,2,3,4. And Group "Breakaway" is a custom list of levels for a particular switch, and is determined on a specific connection basis. Group "Breakaway" is number 0.

It is expected that most connections will be "ALL" i.e., all levels of control.

Groups are defined in the controller configuration (CFG) file.

Revision History

Rev.	Date	Description	By
1.0	02-01-00	Initial Release	R. Hormigo
1.1	04-05-00	Added PING, RESTART, CLOSE, BYE, USR, and KEY commands.	R. Hormigo
1.2	06-16-00	Reformatted document for in-house use.	D. Bailey
A	06-29-00	Reformatted document for publication per ECO-3693.	G. Tarlton
B	03-06-01	Deleted Printing Specification per ECO CE00113.	G. Tarlton

PESA

Switching
Systems