HomePortal® Intelligent Gateway CLI Reference Guide

Firmware Version: 9.3.1.10

Notice to Users

2WIRE PROVIDES NO WARRANTY WITH REGARD TO THIS MANUAL, THE SOFTWARE, OR OTHER INFORMATION CONTAINED HEREIN AND HEREBY EXPRESSLY DISCLAIMS ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE WITH REGARD TO THIS MANUAL, THE SOFTWARE, OR SUCH OTHER INFORMATION. IN NO EVENT SHALL 2WIRE, INC. BE LIABLE FOR ANY INCIDENTAL, CONSEQUENTIAL, OR SPECIAL DAMAGES, WHETHER BASED ON TORT, CONTRACT, OR OTHERWISE, ARISING OUT OF OR IN CONNECTION WITH THIS MANUAL, THE SOFTWARE, OR OTHER INFORMATION CONTAINED HEREIN OR THE USE THEREOF.

2Wire, Inc. reserves the right to make any modification to this manual or the information contained herein at any time without notice. The software described herein is governed by the terms of a separate user license agreement.

Updates and additions to software may require an additional charge. Subscriptions to online service providers may require a fee and credit card information. Financial services may require prior arrangements with participating financial institutions.

6242010

5100-000923-000

Contents

About This Guide

The *HomePortal® Intelligent Gateway CLI Reference Guide* is designed to serve as a reference to configure the 2Wire gateway that uses the 9.3.1.5 firmware, through the Command Line Interface (CLI). This guide contains the following chapters:

Chapter 1: Overview on page 1 provides you a general understanding of the CLI, command types, gateway features, etc.

Chapter 2: Launching the Gateway on page 5 describes how to launch the CLI. It also explains the steps for operating the CLI, viewing the help, and the CLI command tree.

Chapter 3: Global Commands on page 8 explains the global commands along with their respective description.

Chapter 4: Configuration Commands on page 11 explains the configuration commands along with their respective description, command syntax, and parameters.

Chapter 5: Show Commands on page 239 explains the show commands along with their respective description, command syntax, and parameters.

Audience

This guide is intended for use by:

- End Users
- Sales Engineers
- Support Staff
- Service Provider Technicians

Document Layout

The Configuration Commands chapter in this document consists of the configuration commands for each CLI module. Configuration commands have:

- **Description**: Provides detailed explanation/purpose of the command.
- **Parent**: Provides the navigation of the command.
- **Syntax**: Provides the command structure.
- **Parameter Description**: Provides command parameters description in the tabular format.
- **Example**: Provides an example on the command usage with the possible values of the parameters.

Note	Command syntax, parameters description, and example/s are present only for child commands, and not for major commands and command nodes.

This structure helps you navigate through the commands in a simple manner.

The Show Commands chapter also has a similar structure as the Configuration Commands chapter, except for examples, as it merely displays the configured parameters for each module.

Supported Hardware Platforms

The following hardware platforms are supported in the current release:

- 5011NV
- 5012NV

Style Conventions

The following style conventions are used in this guide:

Note Notes contain incidental information about the subject. In this guide, they are used to provide additional information about the product and to call attention to exceptions.

Caution notes identify information that helps prevent damage to hardware or loss of data.

Warning notes identify information that helps prevent injury or death.

Typographical Conventions

Convention	Used For
Blue Text	Cross references
Bold	Interface elements that are clicked or selected
Italic	Emphasis, book titles, variables, list terms
`Monospace`	Command syntax and code
`*Monospace Italic*`	Variables within command syntax and code

Related Documents

In addition to this guide, the HomePortal Intelligent Gateway Software documentation library includes:

Agile Part Number	Description
5100-000900-000	HomePortal® 5011NV/5012NV Intelligent Gateway Installation Guide
5100-000899-000	HomePortal® Intelligent Gateway 9.3.1.5 Configuration Guide

Support

Technical support is available from the 2Wire Website: http://support.2wire.com/index.php.

CHAPTER 1

Overview

This chapter provides a general overview of the gateway CLI and contains the following sub-sections:

What is Gateway CLI?

2Wire's gateway is a simplistic solution that is used by home-users, Small Office/Home Office (SOHO), and small business markets. You can configure the gateway using the Graphical User Interface (GUI) or Command Line Interface (CLI). 2Wire's gateway is equipped with a host of security and firewall features for fast and secured access to the Internet. 2Wire's gateway consists of popular open source network stacks and NP Linux (refer figure 1: Gateway Layers) and is bundled with NP BloX (CLI and Web management interfaces) to provide you with rapid management capabilities. You can configure your network by setting up LAN and WAN interfaces, provide various types of firewall settings, configure administration features such as backup and restore, and provide class-based queuing for the network traffic. It also facilitates you to configure various VoIP features such as interfaces, call settings, quality, codecs, logs etc.

Gateway Layers

The figure below displays the gateway layers:

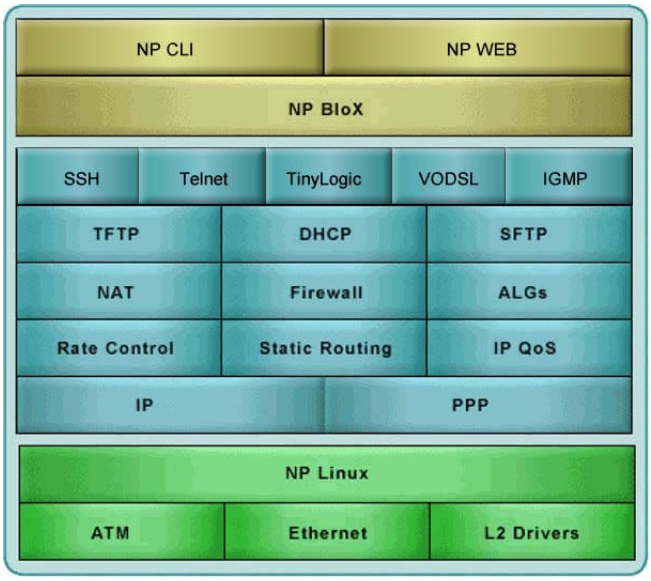

Figure 1: Gateway Layers

Gateway Features

2Wire's gateway supports the networking and security features to give you reliable and secure networking experience. 2Wire's gateway provides the following features:

- Security
  - Time-based Firewall policies to allow/deny access as per pre-defined time periods.
  - Host based and application level Firewall Policies.
- NAT/NAPT Support
  - Fully functional NAT/NAPT based on RFC 1631.
  - Application Level Gateway (ALG) support for all well-known protocols (such as FTP, H323, and SIP).
  - DMZplus for automatic WAN IP address assignment to a local computer.
- Network Protocol Support
  - IP address allocation through DHCP server and client configuration.
  - Support for ATM UNI, UBR, VBRnrt, VBRrt, CBR.
  - Support for up to four ATM PVCs in any configuration.
  - Compatibility with IPv4, TCP, UDP, ARP, ICMP, IPv6.
- VoIP
  - VoIP features such as interfaces, call settings, quality, codecs, logs, Realtime Transport Protocol (RTP), Session Description Protocol (SDP), and Session Initiation Protocol (SIP).
- Wireless
  - Wireless Multi-media (WMM) to prioritize multimedia data transfers through the network.
  - 802.1x authentication and 802.11e prioritization wireless draft standard support.
  - Station association feature for the wireless network to establish a communication link with the base station.
  - Support for all security protocols such as WPA PSK, WPA EAP/w, TKIP and AES.
  - Support for WPA/WPA2 encryption key for personal and enterprise systems (this feature also includes extended security features such as TKIP/CCMP [AES] and 802.1x).
  - Digital certificates to provide industry standard authentication.
  - Wireless networking for the flexibility to create AP to Client, AP to AP, or Client to Client networks.
  - Radius integration and MAC filtering.
  - Multiple SSID support.
- Diagnostics and Management Tools
  - Diagnostic network utility tool with a collection of generic utilities, for day-to-day management of the system and network. The tools can be used to troubleshoot, and also to debug connectivity issues, packet loss, and latency in a LAN environment.
  - TR-069 support for automating the installation and configuration of gateways from the LAN side, as well as for configuring the CPE via the ACS from the WAN side.
- Web Remote Access
  - Fast and easy access to the HomePortal network remotely using a standard Web browser, an Internet connection, and network password.
- Quality of Service (QoS)
  - QoS features such as policies, priority queuing, shaping, and management to effectively manage available Internet bandwidth.
- VLAN
  - VLAN feature to optimize sparse network resources by creating multiple sub-LANs within a LAN.
- UPnP
  - UPnP service configuration with TR-064 support.
- MAC Address Cloning
  - Cloning the MAC address of a target computer for testing, snooping, and more.

Gateway in a Networking Environment

The figure below demonstrates 2Wire's gateway in a networking environment:

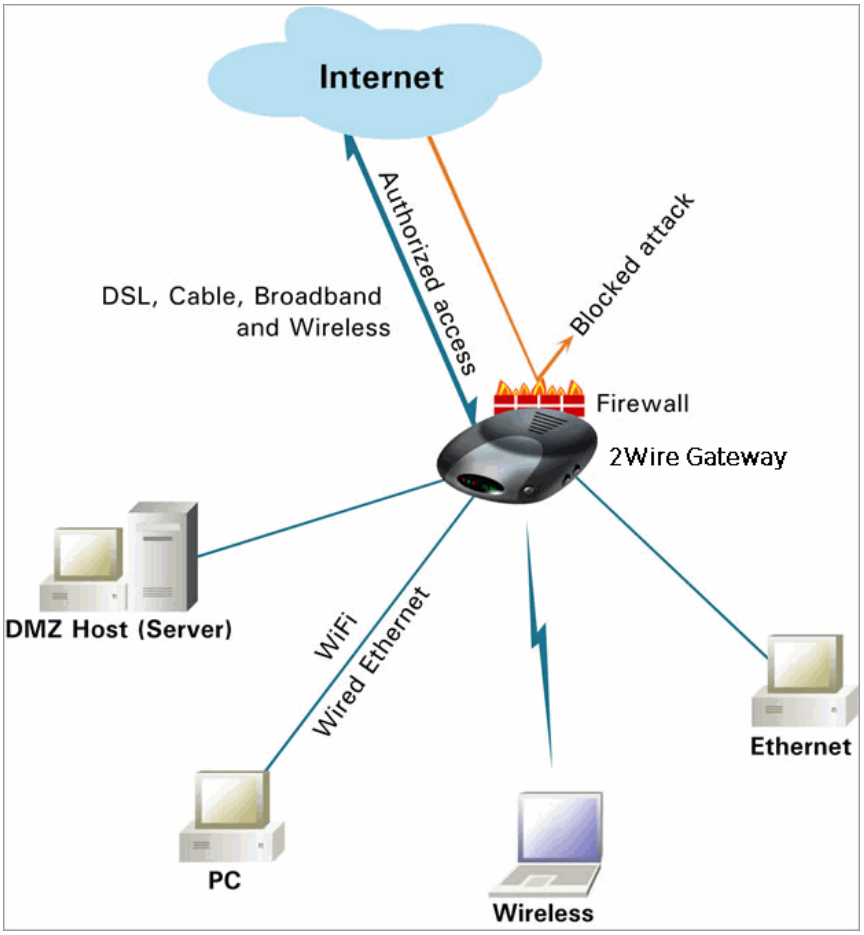

Figure 2: 2Wire Gateway in a Networking Environment

Gateway Command Types

The structure of the CLI commands is similar to a tree. There are modules that define a set of commands. In turn modules can be defined in parent modules. There are major commands that can be defined in modules. These major commands in turn can have commands and other major commands defined in them.

Command Nodes (Modules)

Command nodes are a collection of commands, major commands and modules themselves. Every module consists of the ROOT module. Below this ROOT module there are other modules. Command nodes do not affect any backend operation, as they do not have any function associated with them. When you enter a module on the command line, the CLI displays all the commands defined in it with the help '?' command.

Major Commands

Major commands are similar to the command nodes (modules). They differ in that they can define parameters like commands. On executing a major command, the CLI enters that major command mode. Under the major command there can be subcommands and child major commands.

Commands

Commands form the main part of the CLI engine. The commands accept parameters and pass them to the associated callback function. This makes the callback function perform desired operations based on the user inputs. Commands can be divided into groups based on the type of operation they perform, or based on the type of subsystem they will operate on. Each group can be defined as a module as described above. Commands can be executed only from the module where they have been defined. If there are two modules ‘mod1’ and ‘mod2’, then on entering ‘mod1’, CLI will allow execution of commands available only in ‘mod1’. To execute ‘mod2’ commands, the user must enter the ‘mod2’ module.

CHAPTER 2

Launching the Gateway

This chapter describes how to access and operate the CLI interface as well as view the help. It also explains the CLI tree structure.

Note To launch the CLI, you require the IP address of the gateway.

Accessing CLI

Once the gateway is installed, reboot the device and enter the login and password as *root*. This takes you to the # prompt. You must type the kcli command to get the kcli prompt as shown below:

```
#kcli <enter>
```

Note You can connect the gateway by using the RJ45/Ethernet cable or RS-232/Serial cable.

Operating CLI

You can invoke the global commands menu and perform various activities on the CLI, such as configure the commands, view the parameters for the configured commands, show/save/load history, go to previous module, logout, etc.

To invoke the global commands menu, type the following command:

```
#kcli> ?
```

This lists all the global commands that can be executed.

To enter the configuration menu, type the following command:

```
#kcli> config <enter>
```

To view the config module list:

```
config> ?
```

This lists all the gateway modules that can be configured.

To enter the show menu for viewing the configured command parameters for various modules, type the following at the kcli prompt:

```
#kcli> show <enter>
```

To view the configuration of each module:

```
show> <modulename> <enter>
```

The following figure displays the list of global commands:

```
kcli>

config           - Configure NPGateway parameters
show             - Show NPGateway parameters
history          - Show / Save / Load history
alias            - Show defined aliases / Add an alias for a command
exec-replay      - Replay commands from the file
exit             - Exit from the current node and go to parent
where            - Show the path of the current module from the root
logout           - Log out from the current Session
cli-settings     - Configure / Show CLI settings
tree             - Show module tree under the current module
set-timeout      - Set the inactivity timeout to 10 seconds
shell-escape     - Escape to the shell
!                - Escape to the shell
previous-module  - Go to the previous module
alias-file       - Save current aliases to file / Load aliases from file
event            - Command to register/unregister/block/unblock event

kcli>
```

Figure 3: Global Commands

The following figure displays the list of modules:

```
config>

admin-tools      - Configuration options
system           - System configuration
wireless         - Wireless Configuration
firewall         - Firewall Configuration
nat              - Nat Configuration
pppoe            - Configure PPP Over Ethernet Service
pppoa            -
diagnostic       - Network Diagnostic Utilities
upnp             - UPNP Device Configuration
tr64             - UPnP change tr64mode
igmp             - host list configuration
qos              -
if               - Interface configuration
dsl              -
dhcp             - DHCP Server Configuration
dns              -
vlan             - VLAN configuration
bridge           - Bridge configuration
usrmgmt          -
swupgrade        -
topology         - host list configuration
tr69             -
nptr98           -
voip             -
tr111part1       -
exit             - Exit from the current node and go to parent
where            - Show the path of the current module from the root
logout           - Log out from the current Session
cli-settings     - Configure / Show CLI settings
tree             - Show module tree under the current module
set-timeout      - Set the inactivity timeout to 10 seconds
shell-escape     - Escape to the shell
!                - Escape to the shell
previous-module  - Go to the previous module
alias-file       - Save current aliases to file / Load aliases from file
event            - Command to register/unregister/block/unblock event

config>
```

Figure 4: Module List

Viewing CLI Tree

You can view the command tree by entering the tree command at the root level (kcli prompt), configuration level (config prompt), or module level. This displays the complete command tree nested under the current command mode. The following figure displays the command tree for the Firewall module:

Figure 5: Command Tree

Viewing CLI Help

To view the help of any module, command, or parameter you must type ? after the module name/command/parameter.

Note The command including a space before ? indicates the listing of commands in the module, whereas if you type ? without space after the command name, it displays the help for that command, that is context sensitive help.

To view the help of a module:

```
config> firewall? <enter>
```

To view the commands and nested parameters:

```
config> firewall ? <enter>
```

CHAPTER 3

Global Commands

Global commands are exactly the same as regular CLI commands. The regular CLI commands are executed within the command nodes where it is defined. Global commands are available at all command nodes and thus can be executed in any module of the CLI. This chapter explains the global commands of the gateway CLI.

config

Description

The `config` command takes you to configuration mode to configure the parameters for the listed modules.

Parent

kcli

show

Description

The `show` command takes you to show mode to view the configured parameters for the listed modules.

Parent

kcli

history

Description

The `history` command displays the command history of the current CLI session, saves it, or loads the command history from a file. This command is useful for keeping track of command activity in a particular CLI session, as well as compare it with any previous sessions. The displayed history includes the command name and time stamp.

Parent

kcli

Parameter Description

Parameter	Description
save-to-file	Save the current CLI session history to a file. Enter the file name in which you want the history to be saved.
load-from-file	Load the command history from a previous CLI session saved in a file. Enter the file name to display the history in the current CLI session.

exit

Description

The `exit` command exits you from the current node and takes you to the parent node.

Parent

kcli

where

Description

The `where` command displays the current module path starting from the root node.

Parent

kcli

logout

Description

The `logout` command takes you to the # prompt.

Parent

kcli

cli-settings

Description

The `cli-settings` command allows you to view and/or configure the CLI settings with respect to the MORE feature. When enabled, the MORE feature displays the long command output part by part in the shell, after a specific show command is executed. Just executing the `cli-settings` command at the prompt displays the current setting, that is, whether the MORE feature is enabled or disabled.

Parent

kcli

Parameter Description

Parameter	Description
more	The MORE feature displays the long command output part by part in the shell, after a specific show command is executed. It is useful for viewing the output of show commands, where the output is very long to view without having to scroll the shell.
enable	Enable the MORE feature to display the long command output part by part in the shell, after a specific command is executed.
disable	Disable the MORE feature to display the complete show command output in the shell, wherein you may require to scroll the output for viewing a specific part of the displayed command output.

tree

Description

The `tree` command displays the complete command tree nested under the current command node.

Parent

kcli

set-timeout

Description

The `set-timeout` command sets the shell inactive timeout to 10 seconds. So when the shell remains inactive for 10 seconds, the current CLI session is exited to display the shell prompt.

Parent

kcli

Note You may want to enable the always-save-running-config command in the admin-tools module, before executing the set-timeout command.

previous-module

Description

The `previous-module` command takes the prompt to the previous command node.

Parent

kcli

CHAPTER 4

Configuration Commands

This chapter lists the module name, configuration commands for each module, purpose of each command, and parent (command navigation). The command syntax followed by its parameter description are also added wherever applicable.

Admin-Tools Module

This section describes configuration commands for the admin-tools module. You can restore backup settings, save configuration files, restore configuration, delete backup files, and change profile names.

admin-tools

Description

The `admin-tools` command node allows you to enter the configuration mode to configure various types of saving, backup, and restore settings for the gateway.

Parent

kcli/config

settings

Description

The `settings` major command configures the backup settings, such as auto-saving the running configuration, and setting the backup history size.

Parent

kcli/config/admin-tools

history-size

Description

The `history-size` command enters the number of configuration backups to be saved. The history size denotes the number of backups to be created for the device configuration. For example, if you enter one (1) as the history size, then the device saves only the last configuration. If you enter four (4) as the history size, then the last four configuration settings are saved in separate files, which you can retrieve when required.

Parent

kcli/config/admin-tools/settings

Syntax

```
history-size < historysize integer >
```

Note If the history size is zero (0), then no backup of the running configuration is taken. Also the earlier backups, if any, are deleted when you set the history size to zero (0).

always-save-running-config

Description

The `always-save-running-config` command automatically saves the current configuration of the gateway device before you log out of the session. Once saved, this configuration is used/applied every time the device is rebooted. However, if the always-save-running-config feature is disabled, then the changes made in the current configuration are lost, when the device is rebooted.

Parent

kcli/config/admin-tools/settings

Syntax

```
always-save-running-config { enable | disable }
```

Parameter Description

Parameter	Description
enable	Enable this feature to auto-save the running configuration of the device.
disable	Disable this feature if you do not want to automatically save the running configuration of the device.

save

Description

The `save` command configures the settings for saving the configuration backup/s.

Parent

kcli/config/admin-tools

running-config

Description

The `running-config` command saves the current configuration of the device. The current configuration is referred to as the running configuration.

Parent

kcli/config/admin-tools/save

Syntax

```
running-config
```

to-history

Description

The `to-history` command specifies the file name in which the current configuration is to be saved.

Parent

kcli/config/admin-tools/save

Syntax

```
to-history filename < filename string > backupname < name string >
```

Parameter Description

Parameter	Description
filename	Enter a file name to save the current configuration.
backupname	Enter a name for the device configuration backup to be created.

Note You can create as many backup entities as specified while setting the history size. For example, if you have entered one (1) as history size, then only one (1) backup entity is created.

to-remote

Description

The `to-remote` command specifies the IP address of the remote machine where the backup is to be saved. It also configures the relevant parameters such as file name, protocol for the file transfer, and authentication details for remote login.

Parent

kcli/config/admin-tools/save

Syntax

```
to-remote filename < filename string > remote-path < path string > protocol < protocol
string > remote-server-IP < server ipaddress > [ user < user string > password < password
string > ]
```

Parameter Description

Parameter	Description
filename	Enter the name of the file to be saved on the remote machine. This file is in the zipped format.
remote-path	Enter the path on the remote machine where the file is to be saved.
protocol	Enter a protocol (such as SCP, TFTP, SFTP, etc.) to be used for the file transfer.
tftp	Select the TFTP service for file transfer.
remote-server-IP	Enter the IP address of the remote machine where the file is to be saved.
user	Enter the user name to authenticate the specifed remote server. Authentication is not required if you have selected the TFTP protocol for file transfer.
password	Enter the password of the specified user to authenticate the remote server.

Example

The following example command saves the backup file "backup1" on a remote TFTP machine having IP address 192.168.2.1 in the "root" directory on this TFTP server, with authentication details as admin (username) and admin (password):

```
#kcli> config admin-tools save to-remote filename backup1 remote-path tftp://192.168.2.1/
root protocol tftp remote-server_ip 192.168.2.1 user admin password admin <enter>
```

restore

Description

The `restore` command restores the previous configuration from default settings, history, or the remote machine.

Parent

kcli/config/admin-tools

factory-defaults

Description

The `factory-defaults` command restores the default factory settings of the device. Factory default settings are the settings that are pre-configured into the device, thus making it ready for initial deployment. You may want to restore the factory settings in case of network connectivity problems or browser-related issues. Restoring factory default settings deletes all the backups of the running configuration.

Parent

kcli/config/admin-tools/restore

Syntax

```
factory-defaults
```

Example

The following example command restores the default factory settings of the device:

```
#kcli> config admin-tools restore factory-defaults <enter>
```

from-history

Description

The `from-history` command restores the local configuration backup file/s stored on the device in the history folder. Enter the file name from which the configuration is to be restored.

Parent

kcli/config/admin-tools/restore

Syntax

```
from-history < backupname string >
```

Example

The following example command restores the local configuration backup file “backup1”:

```
#kcli> config admin-tools restore from-history backup1 <enter>
```

remote

Description

The `remote` command restores the configuration saved on a remote server.

Parent

kcli/config/admin-tools/restore

Syntax

```
remote remote-file < path string > protocol { tftp | file } remote-server-IP < server
ipaddress > [ username < user string > password < password string > ]
```

Parameter Description

Parameter	Description
remote-file	Enter the name of the backup file saved on the remote machine.
protocol	Enter a protocol (TFTP, SFTP, or SCP) for file transfer.
tftp	Select the TFTP service for the remote file transfer.
file	Select the file service for the remote file transfer.
remote-server-IP	Enter the IP address of the remote server where the file is saved.
username	Enter the user name to authenticate the specified remote server. Authentication is not required if the TFTP protocol is used for file transfer.
password	Enter the password of the specified user to authenticate the remote server.

Example

The following example command restores the configuration saved on a remote server:

```
#kcli> config admin-tools restore remote backup1 protocol tftp remoter-server-IP 10.2.3.4
username john password admin123 <enter>
```

delete_backup

Description

The `delete_backup` command deletes the existing backup file.

Parent

kcli/config/admin-tools

Syntax

```
{ backup_name < name string > }
```

Parameter Description

Parameter	Description
backup_name	Enter the name of the backup file to be deleted.

change-profile

Description

The `change-profile` command selects a profile from the available profiles list created for the device, such as dsl_routed, dsl_bridge, ethernet_routed, ethernet_bridge, dsl, and ethernet.

Parent

kcli/config/admin-tools

Syntax

```
change-profile { profile_name < name string > }
```

Parameter Description

Parameter	Description
profile_name	Select a profile by entering its name.

Bridge Module

This section describes configuration commands for the bridge module. You can add, modify, or delete bridge and bridgeport parameters on the gateway. A bridge is a way to connect two Ethernet segments together in a protocol independent way. Packets are forwarded based on Ethernet address, rather than IP address (like a router). Since forwarding is done at Layer 2, all protocols can go transparently through a bridge. In this module, you can configure the bridge settings in the CLI interface.

bridge

Description

The `bridge` command node allows you to enter the configuration mode to set various bridge parameters.

Parent

kcli/config

add

Description

The `add` major command adds a bridge to the network. A bridge is a way to connect two Ethernet segments together in a protocol independent way. Packets are forwarded based on Ethernet address, rather than IP address (like a router). Since forwarding is done at Layer 2, all protocols can go transparently through a bridge.

Parent

kcli/config/bridge

bridge

Description

The `bridge` command adds a bridge to the network by entering the bridge name.

Parent

kcli/config/bridge/add

Syntax

```
bridge < bridge_name string(1:32) > mac-assignment {enable {user-mac | port-mac } |
disable} [ hello-time < hello_time integer(1:4294967295) > ] [ bridge-priority <
bridge_priority integer(0:4294967295) > ] [ stp { yes | no } ] [ forward-delay <
forward_delay integer(1:4294967295) > ] [ max-age < max_age integer(1:4294967295) > ] [
ageing < ageing_time integer(1:4294967295) > ]
```

Parameter Description

Parameter	Description
bridge	Enter a name for the bridge you are adding.
mac-assignment	Set the status (enable or disable) of MAC address assignment to the bridge. Accordingly, either a user-defined MAC address will be assigned to the bridge or the system will automatically detect the MAC address of the interface to assign it to the bridge. This feature basically controls how and which MAC address should be configured for the bridge.
enable	Enable MAC address assignment to either specify the MAC address to be assigned to the bridge or to select a port to assign its MAC address to the bridge.
port-mac	Enter the port/interface name whose MAC address is to be assigned to the bridge.
user-mac	Enter the MAC address to be assigned to the bridge.
disable	Disable the MAC address assignment. The device internally detects the MAC address based on the ports added and assigns it to the bridge.
hello-time	Enter the hello time between 1 and 10 seconds for the hello packet. Periodically, a hello packet is sent out by the Root Bridge and the Designated Bridges. Hello packets are used to communicate information about the topology throughout the bridged LAN.
bridge-priority	Set a priority value for the bridge. The priority level can range from 0 to 65535, with 0 indicating high priority and 65535 indicating low priority. The priority number is used to queue traffic in the network as per the priority set for each bridge.
stp	Enable or disable STP for the bridge. Spanning Tree Protocol (STP) is a bridge-based system used to provide fault tolerance on networks. This protocol allows you to implement parallel paths for network traffic. It ensures that all the redundant paths are disabled when the main paths are operational, and all redundant paths are enabled if the main paths fail.
enable	Enable STP if you want the bridge entity being configured to be part of the STP protocol.
disable	Disable STP if you do not want the bridge entity being configured to be part of the STP protocol.
forward-delay	Set the forward delay time between 4 and 30 seconds. The default setting is 15 seconds. Forward delay is time spent in the Listening State and the Learning State before entering the Forwarding State. This delay is essential so that when a new bridge comes onto a busy network, it looks at the traffic state before participating.
max-age	Enter the maximum age timeout period between 6 and 40 seconds. If a bridge does not send out a hello packet for the specified maximum age period, it is assumed to be dead.
aging	Enter the ageing time in seconds. The ageing time is the number of seconds a MAC-address is kept in the forwarding database after receiving a packet from an interface.

Example

The following example adds a bridge instance called "bridge1" with priority 1, STP enabled, STP max age 20 seconds, STP forward delay of 15 seconds, aging time as 300 seconds, and STP hello time of 2 seconds. This way a logical bridge instance is created. Each of the bridge instance is represented by a new network interface and it acts as a container for the interfaces participating in the bridging.

```
#kcli> config bridge add bridge bridge1 mac-assignment disable stp yes bridge-priority 8
max-age 20 forward-delay 15 aging 300 hello-time 2 <enter>
```

Note You need at least one such logical bridge instance to perform any bridging.

bridgeport

Description

The `bridgeport` command adds and configures the port for a bridge connection. By adding a bridge port, you add network device/s to take part in the bridging of the selected bridge. All devices act as one network. The bridge takes a short period of time when a device port is added, to learn the Ethernet addresses on the segment, before it can start forwarding the packets. Deleting a bridge port takes the selected device (port) out of the bridge. For adding a bridge port, map an interface to the bridge port entity, and specify the path-cost and priority. Enter the interface name for the bridge connection.

Parent

kcli/config/bridge/add

Syntax

```
bridgeport < interface_name string(1:32) > bridge < bridge_name string(1:32) > [ path-cost
< path_cost integer > ] [ priority < port_priority integer > ]
```

Parameter Description

Parameter	Description
bridge	Enter the name of the bridge to which the device interface is to be mapped.
path-cost	Enter a numeric value to set the cost of receiving or sending data packets on this interface. Faster interfaces should have lower path costs.
priority	Enter a numeric value to set the interface priority. By changing the priority of the port, you can make it more or less likely to become the Root Port. The lower the number, the more likely the port will be the Root Port.

Example

The following example adds a bridgeport eth0 for the bridge "bridge1" having the path cost of 19 and port priority as 128:

```
#kcli> config bridge add bridgeport eth0 bridge bridge1 path-cost 19 priority 128 <enter>
```

Note It is not possible to add a device interface to multiple bridges or to add a bridge device to another bridge.

modify

Description

The `modify` major command modifies the configured bridge and bridge port parameters.

Parent

kcli/config/bridge

bridge

Description

The `bridge` command modifies the bridge settings. Enter the name of the configured bridge to be modified.

Parent

kcli/config/bridge/modify

Syntax

```
bridge < bridge_name string(1:32) > [ mac-assignment { { enable { user-mac mac < usermac
integer > } | { port-mac port < param integer > } } | { disable } } ] [ hello-time <
hello_time integer(1:4294967295) > ] [ bridge-priority < bridge_priority
integer(0:4294967295) > ] [ stp { yes | no } ] [ forward-delay < forward_delay
integer(1:4294967295) > ] [ max-age < max_age integer(1:4294967295) > ] [ ageing <
ageing_time integer(1:4294967295) > ]
```

Parameter Description

Parameter	Description
mac-assignment	Enable or disable the MAC address assignment to the bridge.
enable	Enable the MAC address assignment, if it is not already enabled.
port-mac	Enter the port or interface name whose MAC address is to be assigned to the bridge.
user-mac	Enter the MAC address to be assigned to the bridge.
disable	Disable the MAC address assignment, if it is not already disabled.
hello-time	Enter the new hello time in seconds for the specified bridge.
bridge-priority	Enter the new priority value for the bridge.
stp	Modify the STP status (enable or disable).
enable	Enable STP, if it is not already enabled.
disable	Disable STP, if it is not already disabled.
forward-delay	Enter the new forwarding delay time in seconds for the bridge.
max-age	Enter the new maximum message age time in seconds for the bridge.
aging	Enter the new aging time in seconds for the bridge.

bridgeport

Description

The `bridgeport` command modifies the configured bridge port settings.

Parent

kcli/config/bridge/modify

Syntax

```
bridgeport < interface_name string(1:32) > bridge < bridge_name string(1:32) > [ path-cost
< path_cost integer > ] [ priority < port_priority integer > ]
```

Parameter Description

Parameter	Description
bridge	Enter the name of the bridge to which the device interface is to be mapped.
path-cost	Enter the new path cost for the bridge port interface.
priority	Enter the new priority for the interface.

delete

Description

The `delete` major command deletes the bridge and bridge port entities from the network.

Parent

kcli/config/bridge

bridge

Description

The `bridge` command deletes the specified bridge entity. Enter the bridge name to be deleted.

Parent

kcli/config/bridge/delete

Syntax

```
bridge < bridge_name string(1:32) >
```

bridgeport

Description

The `bridgeport` command deletes the specified bridge port. Deleting a bridge port takes the specified device (port) out of the bridge. .

Parent

kcli/config/bridge/delete

Syntax

```
bridgeport interface_name < port_interface string(1:32) > bridge < bridge_name
string(1:32) >
```

Parameter Description

Parameter	Description
interface_name	Enter the interface name from which the bridge port is to be deleted.
bridge	Enter the bridge name from which the bridge port is to be deleted.

IGMP Module

This section describes the configuration commands for the IGMP module. You can configure various IGMP proxy related settings.

igmp

Description

The `igmp` command node allows you to configure various IGMP proxy related settings. Internet Group Management Protocol (IGMP) is used by IPv4 systems (hosts and routers) to report their IP multicast group memberships to neighboring multicast routers. Version 3 of IGMP adds support for source filtering, that is, the ability for a system to report interest in receiving packets only from specific source addresses, or from all but specific source addresses, sent to a particular multicast address. This information can be used by multicast routing protocols to avoid delivering multicast packets from specific sources to networks where there are no interested receivers. IGMP proxy is a daemon that acts as a proxy for multicast traffic flowing from downstream to upstream interface and vice versa. It enables the system to issue IGMP host messages on behalf of hosts that the system discovers through standard IGMP interfaces.

Parent

kcli/config

settings

Description

The `settings` command configures the IGMP proxy settings, such as compatibility version and immediate leave status (enable or disable).

Parent

kcli/config/igmp

compatibility-version

Description

The `compatibility-version` command allows the selection of a compatible version for the IGMPv1, IGMPv2, or IGMPv3 querier. For example, if an IGMPv2 host sends the join request, the gateway sends the query message using IGMP version 2 only, even if the querier compatibility version is set to v3 on the gateway.

Parent

kcli/config/igmp/settings

Syntax

```
compatibility-version { v1 | v2 | v3 }
```

Parameter Description

Parameter	Description
v1	Select IGMP version 1, if supported by the host.
v2	Select IGMP version 2, if supported by the host.
v3	Select IGMP version 3, if supported by the host.

immediate-leave

Description

The `immediate-leave` command enables or disables the querier immediate leave functionality. Immediate leave is a function associated with IGMP snooping or IGMP routing, whereby the switch or router stops sending the multicast stream immediately when receiving an IGMP leave for the last member on this requesting interface. This means without sending one or more group specific queries and waiting for its timeout, the router stops sending the multicast stream.

Parent

kcli/config/igmp/settings

Syntax

```
immediate-leave { enable | disable }
```

Parameter Description

Parameter	Description
enable	Enable the querier immediate leave functionality.
disable	Disable the querier immediate leave functionality.

Example

The following example command enables the querier immediate leave:

```
#kcli> config igmp settings immediate-leave enable <enter>
```

wan-fwd-addentry

Description

The `wan-fwd-addentry` adds a WAN forwarding rule for the tranmission of IGMP traffic to the WAN. Each of the rule entry specifies if an IGMP message is to be forwarded to the WAN or be droppped. Each IGMP message is matched with the each of these rules. If the message matches any of the rules that allow forwarding to the WAN, that message is forwarded to all of the associated interfaces. If the IGMP message matches with any of the rules that deny forwarding to the WAN, then that message is dropped.

Parent

kcli/config/igmp/settings

Syntax

```
wan-fwd-addentry group-address < group_address string > group-mask < group_mask string >
fwd-allow { True | False } fwd-interface < fwd_interface string >
```

Parameter Description

Parameter	Description
group-address	Enter the IP multicast group address for the WAN forwarding rule entry.
group-mask	Enter the IP multicast group subnet mask for the WAN forwarding rule entry.
fwd-allow	Allow or deny the transmission of the IGMP message matching the rule.
True	Select True to allow forwarding the IGMP message to the WAN, if it matches the rule.
False	Select False to deny the transmission of the IGMP message to the WAN, if it matches the rule.
fwd-interface	Enter the egress interfaces where the IGMP traffic is to be forwarded, only if the forwarding is set to true.

Example

The following example command adds the WAN forwarding rule entry:

```
#kcli> config igmp settings wan-fwd-addentry group-address 224.0.0.1 group-mask
224.0.0.255 fwd-allow True fwd-interface bb0 <enter>
```

wan-fwd-config

Description

The `wan-fwd-config` command allows or denies the transmission of the IGMP messages, that does not match any of the configured IGMP rules, to WAN.

Parent

kcli/config/igmp/settings

Syntax

```
wan-fwd-config { default-allow { True | False } default-interface < default_interface
string > }
```

Parameter Description

Parameter	Description
default-allow	Allow or deny the transmission of an IGMP message to the WAN.
True	Select True to allow the transmission of the IGMP traffic to the WAN.
False	Select False to block the IGMP traffic to be forwarded to the WAN.
default-interface	If the IGMP message transmission is allowed (True), enter the default egress interfaces where the IGMP traffic is to be forwarded to.

Example

The following example command allows the transmission of the WAN-destined IGMP messages to the specified interface:

```
#kcli> config igmp settings wan-fwd-config default-allow True default-inteface bb0 <enter>
```

wan-fwd-remove-entry

Description

The `wan-fwd-remove-entry` command deletes a WAN forwarding rule configured for the transmission of IGMP messages to the WAN.

Parent

kcli/config/igmp/settings

Syntax

```
wan-fwd-remove-entry group-address < group_address string > group-mask < group_mask string
> fwd-interface < fwd_interface string >
```

Parameter Description

Parameter	Description
group-address	Enter the IP multicast group address for the WAN forwarding rule entry.
group-mask	Enter the IP multicast group subnet mask for the WAN forwarding rule entry.
fwd-interface	Enter the egress interfaces where the IGMP traffic is to be forwarded.

enable

Description

The `enable` command enables the IGMP proxy on the network.

Parent

kcli/config/igmp

Syntax

```
enable proxy [ snooping { enable | disable } ]
```

Parameter Description

Parameter	Description
proxy	Enable the IGMP proxy.
snooping	Enable or disable the IGMP snooping on the gateway. IGMP snooping prevents LAN hosts from receiving traffic for a multicast group they have not explicitly joined.
enable	Enable IGMP snooping on the gateway. If enabled, it analyzes all the IGMP packets between the LAN hosts connected to the gateway and multicast routers on the network. When a gateway listens to an IGMP report from a host for a given multicast group, it adds the host port number to the multicast list of that group. Only this LAN host is allowed to receive traffic for the multicast group it has joined.
disable	Disable IGMP snooping on the gateway.

Example

The following example command enables the IGMP proxy on the network:

```
#kcli> config igmp enable proxy snooping enable <enter>
```

disable

Description

The `disable` command disables the IGMP proxy on the network.

Parent

kcli/config/igmp

Syntax

```
disable proxy
```

Parameter Description

Parameter	Description
proxy	Disable the IGMP proxy.

Firewall Module

This section describes configuration commands for the firewall module. You can configure various firewall settings like access control, DMZ, host filter, application level gateway, game, time based policy, content filter, service control, firewall security mode, custom message support for redirection, firewall logging, management service, tcp timeout, udp timeout, ignore icmp broadcast, ignore icmp bogus error, NAT, etc.

firewall

Description

The `firewall` command node allows you to enter the configuration mode to configure firewall settings through a host of functionalities for the network security. A firewall is a piece of hardware and/or software that functions in a networked environment to prevent communications forbidden by the security policy.

Parent

kcli/config

security-mode

Description

The `security-mode` major command configures the firewall security mode. Select a mode from the list (medium, maximum, or disable).

Parent

kcli/config/firewall

maximum

Description

The `maxiumum` command sets the maximum mode for firewall. In maximum mode, the access to external network is blocked completely by default. Hence, you need to configure all the mode-dependent firewall rules for allowing access to any sites or services.

Parent

kcli/config/firewall/security-mode

Syntax

```
maximum
```

medium

Description

The `medium` command sets the medium mode for firewall. In medium mode, the LAN hosts are allowed to access the external network. While configuring, you need to specify what sites/URLs should be blocked on the network, so that the LAN hosts are not able to access those.

Parent

kcli/config/firewall/security-mode

Syntax

```
medium
```

Note On change of modes between medium and maximum, only mode-dependent rules (control rules) get affected. If you change the firewall mode, then you have to re-configure the mode-dependent rules. But mode-independent rules, such as DMZ and port forwarding, are not affected.

disable

Description

The `disable` command de-activates the firewall service on the network. Thus, any configured firewall rules are not applied on the gateway device.

Parent

kcli/config/firewall/security-mode

Syntax

```
disable
```

stealth-mode

Description

The `stealth-mode` major command enables or disables the stealth mode in the firewall. When stealth mode is enabled, the device firewall does not return any information in response to queries regarding connection to the device network. That is, the gateway is not visible to any user on the network, in order to access it. This discourages hackers from further attempts at accessing the network.

Parent

kcli/config/firewall

status

Description

The `status` command enables or disables stealth mode in firewall for advanced network security. When enabled, it prevents public traffic from accessing the network, because it appears as though there is no active network to access. The intent is to make the device invisible to other public network devices.

Parent

kcli/config/firewall/stealth-mode

Syntax

```
status { enable | disable }
```

Parameter Description

Parameter	Description
enable	Enable the stealth mode in firewall to hide the gateway device from public network devices.
disable	Disable the stealth mode in firewall.

nat

Description

The NAT command node configures basic and advanced NATting on the gateway. Network Address Translation (NAT) enables multiple hosts on a private network to access the Internet using a single public IP address. It involves re-writing the source and/or destination addresses of IP packets as they pass through a router or firewall.

Parent

kcli/config

advance-natting

Description

The `advance-natting` command configures the advanced mode of NAT. Advanced NATting is recommended for expert users. Unlike basic mode, it allows user to configure interface on which NAT is to be enabled. User can configure NATting by identifying the WAN interface first. With advanced NATting, user can start NATting on multiple interfaces (LAN or WAN). In this mode, public IP NATting can be enabled or disabled.

Parent

kcli/config/nat

Syntax

```
advance-natting interface < ifname string > public-ip-natting { enable | disable } conenat
{ enable | disable }
```

Parameter Description

Parameter	Description
interface	Select the outgoing (WAN) interface for NATting. If you select an interface for NATting, only the traffic coming from that interface undergoes NATting on the outgoing interface (WAN). For the LANs, the router acts as forwarder. Enter the interface name on which you want to enable NAT.
public-ip-natting	Enable or disable NATting for public IP address. If enabled, the public IP NATting NATs all the packets having public IP addresses present on the LAN with the WAN IP address of the device. In other words, the public IP address is re-NATted with the WAN IP address of the device.
enable	Enable public IP NATing on the device.
disable	Disable public IP NATing on the device.
conenat	Enable or disable the cone NAT in the advanced NATting mode. Cone NAT maps all requests from the same internal IP address and port to the same external IP address and port. Furthermore, any external host can communicate with the internal host by sending a packet to the mapped external IP address and port. Cone NAT support is used in case of gaming protocols, where an external host can communicate with a LAN client on the mapped port.
enable	Enable cone NAT on the network to allow external hosts to initiate a session with a LAN host on the mapped port.
disable	Disable the cone NAT on the network.

Note A warning message is displayed to the user while enabling advanced NATting mode "This is an expert level configuration and user should be aware of consequences." Additionally, if the basic NATting mode is enabled and user tries to enable the advanced mode, an error message is displayed stating "Basic mode should be disabled first in order to enable advanced NATting mode."

Example

The following example command enables advanced NATting mode:

```
#kcli> config nat advance-natting interface bbo public-ip-natting enable conenat enable
<enter>
```

basic-natting

Description

The `basic-natting` command allows the gateway device to start NATting data packets from the LAN network to the identified WAN interface automatically. Basic NATting is the default NATting mode of the gateway device and is the most basic form of the NAT configurations. When the basic mode is enabled, the NAT module automatically identifies the WAN interface of the device and enables NAT on that particular interface. User can also enable or disable the public IP NATting in the basic mode.

Parent

kcli/config/nat

Syntax

```
basic-natting public-ip-natting { enable | disable } conenat { enable | disable }
```

Parameter Description

Parameter	Description
public-ip-natting	Enable or disable NATting for public IP address. If enabled, the public IP NATting NATs all the packets having public IP addresses present on the LAN with the WAN IP address of the device. In other words, the public IP address is re-NATted with the WAN IP address of the device. The traffic originated from the LAN workstation connected to the device and having public IP address is NATted at the WAN interface of the device.
enable	Enable public IP NATing on the device.
disable	Disable public IP NATing on the device.
conenat	Enable or disable the cone NAT in the basic NATting mode. Cone NAT maps all requests from the same internal IP address and port to the same external IP address and port. Furthermore, any external host can communicate with the internal host by sending a packet to the mapped external IP address and port. Cone NAT support is used in case of gaming protocols, where an external host can communicate with a LAN client on the mapped port.
enable	Enable cone NAT on the network to allow external hosts to initiate a session with a LAN host on the mapped port.
disable	Disable the cone NAT on the network.

Example

The following example command enables basic NATting mode:

```
#kcli> config nat basic-natting public-ip-natting enable conenat enable <enter>
```

no

Description

The no major command disables NAT service on the interfaces.

Parent

kcli/config/nat

advance-natting

Description

The `advance-natting` command under no disables advanced NATting on the device.

Parent

kcli/config/nat/no

Syntax

```
advance-natting interface < ifname string > public-ip-natting { enable | disable } conenat
{ enable | disable }
```

Parameter Description

Parameter	Description
interface	Select the interface on which advanced NATting is to be disabled.
public-ip-natting	Enable or disable NATting for public IP address. If enabled, the public IP NATting NATs all the packets having public IP addresses present on the LAN with the WAN IP address of the device. In other words, the public IP address is re-NATted with the WAN IP address of the device.
enable	Enable public IP NATing on the device.
diable	Disable public IP NATing on the device.
conenat	Enable or disable cone NAT.
enable	Enable cone NAT, if it is not already enabled.
disable	Disable cone NAT, if it is not already disabled.

basic-natting

Description

The `basic-natting` command disables basic NATting mode on the device. If this mode is disabled, the gateway will not NAT data packets from the LAN network to the identified WAN interface.

Parent

kcli/config/nat/no

Syntax

```
basic-natting public-ip-natting { enable | disable } conenat { enable | disable }
```

Parameter Description

Parameter	Description
public-ip-natting	Enable or disable NATting for public IP address. If enabled, the public IP NATting NATs all the packets having public IP addresses present on the LAN with the WAN IP address of the device. In other words, the public IP address is re-NATted with the WAN IP address of the device.
enable	Enable public IP NATing on the device.
disable	Disable public IP NATing on the device.
conenat	Enable or disable cone NAT.
enable	Enable cone NAT, if it is not already enabled.
disable	Disable cone NAT, if it is not already disabled.

logging

Description

The `logging` major command enables or disables the firewall logging on the network.

Parent

kcli/config/firewall

status

Description

The `status` command enables or disables the firewall logging on the gateway.

Parent

kcli/config/firewall/logging

Syntax

```
status { enable | disable }
```

Parameter Description

Parameter	Description
enable	Enable firewall logging to start logging firewall events on the device.
disable	Disable firewall logging if you do not want to log firewall events on the device.

access-control

Description

The `access-control` major command configures the gateway access conditions to fortify the network. This can be done by configuring rules related to port forwarding, proxies, and trusted clients.

Parent

kcli/config/firewall

no

Description

The no major command under access control deletes the various access control rules related to proxy, port-forwarding, trusted client, and trusted management client features.

Parent

kcli/config/firewall/access-control

proxy

Description

The `proxy` major command configures the proxy settings on the device in relation to HTTP, FTP, and custom ports. A proxy service enables a computer network to allow clients to make indirect network connections to other network services. A client connects to the proxy server and then requests a connection, file, or other resource available on a different server. The proxy provides the resource either by connecting to the specified server or by serving it from a cache.

Parent

kcli/config/firewall/access-control

proxy

Description

The `proxy` major command under no deletes a configured proxy rule from the gateway device.

Parent

kcli/config/firewall/access-control/no

http

Description

The `http` command configures the proxy protocol as HTTP.

Parent

kcli/config/firewall/access-control/proxy

Syntax

```
http { proxy-host-port < host ipaddr > } [ policy < pname string(0:20) > ]
```

Parameter Description

Parameter	Description
proxy-host-port	Enter the IP address of the host that will act as the proxy for the LAN workstation.
policy	Enter a policy name as appropriate, to attach it to the rule.

Example

The following example command configures the HTTP as proxy protocol:

```
#kcli> config firewall access-control proxy http proxy-host-port 10.2.3.4 policy policy1
<enter>
```

http

Description

The `http` command deletes a proxy rule having HTTP as its protocol.

Parent

kcli/config/firewall/access-control/no/proxy

Syntax

```
http { proxy-host-port < host ipaddr > } [ policy < pname string(0:20) > ]
```

Parameter Description

Parameter	Description
proxy-host-port	Enter the host IP address of the proxy rule that is to be deleted.
policy	Enter the policy name associated with the proxy rule that is to be deleted.

port

Description

The `port` command configures the proxy setting on a specified port number on the network. Enter the port number on which the proxy is to be set up.

Parent

kcli/config/firewall/access-control/proxy

Syntax

```
port { < inport integer > protocol { tcp | udp } proxy-host-port < host ipaddr > } [ policy
< pname string(0:20) > ]
```

Parameter Description

Parameter	Description
protocol	Select the proxy communication protocol as either TCP or UDP.
tcp	Select TCP as the communication protocol for the proxy on the specified port.
udp	Select UDP as the communication protocol for the proxy on the specified port.
proxy-host-port	Enter the IP address of the host that will act as the proxy for the LAN workstation.
policy	Enter a policy name as appropriate, to attach it to the rule.

Example

The following example command configures the port as proxy protocol:

```
#kcli> config firewall access-control proxy port 6000 protocol tcp proxy-host-port 10.2.3.4
policy policy1 <enter>
```

port

Description

The `port` command deletes a proxy rule configured on a custom port in the network. Enter the port number on which the proxy rule is configured.

Parent

kcli/config/firewall/access-control/no/proxy

Syntax

```
port { < inport integer > protocol { tcp | udp } proxy-host-port < host ipaddr > } [ policy
< pname string(0:20) > ]
```

Parameter Description

Parameter	Description
protocol	Select the communication protocol as either UDP or TCP of the proxy rule to be deleted.
tcp	Select TCP as the communication protocol of the proxy rule to be deleted.
udp	Select UDP as the communication protocol of the proxy rule to be deleted.
proxy-host-port	Enter the IP address of the host of the custom port proxy rule.
policy	Enter the policy name associated with the proxy rule to be deleted.

ftp

Description

The `ftp` command configures the proxy protocol as FTP.

Parent

kcli/config/firewall/access-control/proxy

Syntax

```
ftp { proxy-host-port < host ipaddr > } [ policy < pname string(0:20) > ]
```

Parameter Description

Parameter	Description
proxy-host-port	Enter the IP address of the host that will act as the proxy for the LAN workstation/s.
policy	Enter a policy name as appropriate, to attach it to the rule.

Example

The following example command configures the port as proxy protocol:

```
#kcli> config firewall access-control proxy ftp proxy-host-port 10.2.3.4 policy policy1
<enter>
```

ftp

Description

The `ftp` command deletes a proxy rule having FTP as its protocol.

Parent

kcli/config/firewall/access-control/no/proxy

Syntax

```
ftp { proxy-host-port < host ipaddr > } [ policy < pname string(0:20) > ]
```

Parameter Description

Parameter	Description
proxy-host-port	Enter the host IP address of the proxy rule that is to be deleted.
policy	Enter the policy name associated with the proxy rule to be deleted.

port-forward

Description

The `port-forward` command creates a list of target IP addresses where the respective network ports are to be forwarded.

Parent

kcli/config/firewall/access-control

Syntax

```
port-forward { { service { http | https | ftp | telnet | ssh } } | { custom_port < inport integer > [ port_range_end < port integer > ] protocol { tcp | udp } } } { { ipaddr < host ipaddr > { toport < dport integer > } } | { { mac < macaddress string > } { hostname < hostname string > } { toport < dport integer > } } } { description < desc string > } [ app_name < name string > ] [ policy < pname string(0:20) > ]
```

Parameter Description

Parameter	Description
service	Select the service type to be forwarded to specific destination IP addresses. The service type can be HTTP, HTTPS, FTP, TELNET, SSH, or even a custom port. Using the service type, the destination computer can connect to a specific machine.
http	Select HTTP traffic.
https	Select HTTPS traffic.
ftp	Select FTP traffic.
telnet	Select TELNET traffic.
ssh	Select SSH traffic.
custom_port	Enter a custom port number to forward it to the specific destination IP address.
port_range_end	Enter the port range end between 0 and 4294967295.
protocol	Select either the TCP or UDP communication protocol for the custom port.
tcp	Select the TCP communication protocol for the custom port.
udp	Select the UDP communication protocol for the custom port.
ipaddr	Enter the host name string where the specified port is to be forwarded.
toport	Enter the destination port where the traffic is to be forwarded.
mac	Enter the MAC address of the host for port forwarding.
hostname	Enter the host name to be used for port forwarding.
toport	Enter the destination port where the traffic is to be forwarded.
description	Enter the port forwarding description.
app_name	Enter the ALG name to add the application type for the specified port and protocol.
forward-host-port	Enter the destination IP address to which the traffic is to be forwarded to using the configured port.
description	Enter the host (destination) description. For instance, the computer name, which would help identify the port destination.
policy	Enter a policy name as appropriate, to attach it to the port forwarding rule.

Example

The following example command configures the port forwarding rule:

```
#kcli> config firewall access-control port-forward service ssh ipaddr 10.2.3.4 toport 6000
description ssh app_name SSH policy policy1 <enter>
```

Alternatively, you can configure the custom port forwarding rule using the custom_port option:

```
#kcli> config firewall access-control port-forward custom_port 6000 port_range_end 6100
protocol tcp ipaddr 10.2.3.4 toport 8080 description customRule app_name alg policy policy1
<enter>
```

port-forward

Description

The `port-forward` command under no deletes various port forwarding rules configured on the gateway device.

Parent

kcli/config/firewall/access-control/no

Syntax

```
port-forward { { service { http | https | ftp | telnet | ssh } } | { custom_port < inport integer > protocol { tcp | udp } } } { forward-host-port < host ipaddr > } [ policy < pname string(0:20) > ]
```

Parameter Description

Parameter	Description
service	Select the service to be deleted, which can be HTTP, HTTPS, FTP, TELNET, SSH, or a custom port.
http	Select HTTP service as the port to be deleted.
https	Select HTTPS service as the port to be deleted.
ftp	Select FTP service as the port to be deleted.
telnet	Select TELNET service as the port to be deleted.
ssh	Select SSH service as the port to be deleted.
custom_port	Enter the custom port number that has to be deleted.
protocol	Select the protocol of the port to be deleted.
tcp	Select TCP protocol, if the rule is configured using TCP.
udp	Select UDP protocol, if the rule is configured using UDP.
forward-host-port	Enter the destination (host) IP address of the port to be deleted.
policy	Enter the policy name of the port to be deleted.

trusted-client

Description

The `trusted-client` command adds a list of IP addresses within the LAN that can have unrestricted access to the Internet, irrespective of the firewall rules. Enter an IP address of a machine within the LAN to set it as the trusted LAN client.

Parent

kcli/config/firewall/access-control

Syntax

```
trusted-client < clientip ipaddr >
```

trusted-client

Description

The `trusted-client` command under no deletes the trusted client IP addresses. Enter the IP address of the trusted client to be deleted.

Parent

kcli/config/firewall/access-control/no

Syntax

```
trusted-client < clientip ipaddr >
```

trusted-management-client

Description

The `trusted-management-client` command configures the remote client IP addresses for remote device management. Enter the remote client IP address.

Parent

kcli/config/firewall/access-control

Syntax

```
trusted-mangement-client < remoteclientip ipaddr >
```

trusted-management-client

Description

The `trusted-management-client` command under no deletes the remote client IP address that is used for device management.

Parent

kcli/config/firewall/access-control/no

Syntax

```
trusted-mangement-client < remoteclientip ipaddr >
```

add-pf-app

Description

The `add-pf-app` command adds a user-defined application for port forwarding. To add an application, you can specify the application name and associated port and protocol information.

Parent

kcli/config/firewall/access-control/

Syntax

```
add-pf-app { profile-name < desc string > } { port_range_start < inport integer > {
port_range_end < port integer > } protocol { tcp | udp } } { toport < dport integer > } {
app_name < name string > }
```

Parameter Description

Parameter	Description
profile-name	Enter a user-defined profile name for the application to be added.
port_range_start	Enter the start port for the application.
port_range_end	Enter the end port for the application.
protocol	Select the protocol (TCP or UDP) for the application.
tcp	Select TCP protocol for the application.
udp	Select UDP protocol for the application.
toport	Enter a numeric value for destination port where the traffic is to be forwarded.
app_name	Enter the application name to be added for port forwarding with the specified port and protocol information.

Example

The following example command adds the profile "MyProfile" with the specified port and protocol for the application type "FTP":

```
#kcli> config firewall access-control add-pf-app profile-name MyProfile port_range_start
6000 port_range_end 6009 protocol tcp toport 2330 app_name FTP <enter>
```

del-pf-app

Description

The `del-pf-app` command deletes a user-defined application for port forwarding.

Parent

kcli/config/firewall/access-control/

Syntax

```
del-pf-app { profile-name < desc string > } { port_range_start < inport integer > {
port_range_end < port integer > } protocol { tcp | udp } } { toport < dport integer > } {
app_name < name string > }
```

Parameter Description

Parameter	Description
profile-name	Enter the profile name of the application to be deleted.
port_range_start	Enter the start port number for the application to be deleted.
port_range_end	Enter the end port number for the application to be deleted.
protocol	Select the protocol for the application to be deleted.
tcp	Select TCP if the application profile is configured using TCP protocol.
udp	Select UDP if the application profile is configured using UDP protocol.
toport	Enter the destination port for the application to be deleted.
app_name	Enter the name of the application to be deleted.

app-forward

Description

The `app-forward` command allows the Internet traffic to pass through the firewall to the specified LAN devices. Associate a desired application from the given list with the computer on the network by entering the MAC or IP address of the host.

Parent

kcli/config/firewall/access-control

Syntax

```
app-forward { { app-name < app string > } { { ip-addr < ip string > } | { { mac < macaddress string > } { hostname < hostname strring > } } } }
```

Parameter Description

Parameter	Description
app-name	Select an application from the given list that is to be hosted by the computer on the network.
ip-addr	Enter the IP address of the computer that hosts the specified application.
mac	Enter the MAC address of the computer that hosts the specified application.
hostname	Enter the host name for the specified MAC address.

Example

The following example command associates the Web Server application to the specified host IP address:

```
#kcli> config firewall access-control app-forward app-name Web Server ip-addr 192.168.1.2 <enter>
```

host-filter

Description

The `host-filter` major command selects specific internal and external hosts for blocking or allowing access to. For instance, you can block access to specific websites, computers in the LAN, or even a MAC address.

Parent

kcli/config/firewall

no

Description

The no major command deletes the various host filter rules configured on the gateway. For instance, you can unblock access to a specific site, internal host IP, or a MAC address, if the given rule is configured to block the access to that site, MAC address, or internal host.

Parent

kcli/config/firewall/host-filter

external-site

Description

The `external-site` command blocks access to the specific websites (URLs) from within the network. Enter the website name or IP address to be blocked or allowed.

Parent

kcli/config/firewall/host-filter

Syntax

```
external-site < siteaddr string > [ policy < pname string(0:20) > ]
```

Parameter Description

Parameter	Description
policy	Enter a policy name as appropriate, to attach it to the rule.

Note The host filter is a mode-dependent rule. If you set the firewall to maximum mode, the access to the external network is blocked completely, by default. Hence, you need to configure the host filter rule for allowing access. But if you set the firewall to medium mode, all the LAN workstation are allowed to access external network by default. Hence, the host filter rule is to be configured for blocking the access to the external network.

external-site

Description

The `external-site` command under no unblocks access to the specific website URLs. Enter the website name (URL) or IP address to be unblocked.

Parent

kcli/config/firewall/host-filter/no

Syntax

```
external-site < siteaddr string > [ policy < pname string(0:20) > ]
```

Parameter Description

Parameter	Description
policy	Enter the associated policy name.

internal-host

Description

The `internal-host` command selects hosts from within the network to block or allow access to.

Parent

kcli/config/firewall/host-filter

Syntax

```
internal-host host-name < host string > [ policy < pname string(0:20) > ]
```

Parameter Description

Parameter	Description
host-name	Enter the host name or IP address to be blocked or allowed.
policy	Enter a policy name as appropriate, to attach it to the rule.

internal-host

Description

The `internal-host` command under no unblocks access to internal hosts.

Parent

kcli/config/firewall/host-filter/no

Syntax

```
internal-host host-name < host string > [ policy < pname string(0:20) > ]
```

Parameter Description

Parameter	Description
host-name	Enter the host name or IP address to be unblocked, if the rule is configured to block the access to that particular host.
policy	Enter the associated policy name.

mac

Description

The `mac` command allows or blocks access to MAC address/es within the network. Enter the MAC address to be blocked or allowed.

Parent

kcli/config/firewall/host-filter

Syntax

```
mac < mac_address macaddr > [ policy < pname string(0:20) > ]
```

Parameter Description

Parameter	Description
policy	Enter a policy name as appropriate, to attach it to the rule.

mac

Description

The `mac` command under no unblocks access to specific MAC address/es. Enter the MAC address to be unblocked, if the given rule is configured to block the access to that MAC address.

Parent

kcli/config/firewall/host-filter/no

Syntax

```
mac < mac_address macaddr > [ policy < pname string(0:20) > ]
```

Parameter Description

Parameter	Description
policy	Enter the associated policy name.

expert-control

Description

The `expert-control` command adds expert control firewall rules. Here, the assumption is that the user is an expert and is well aware of the consequences of adding these rules. This feature facilitates the user to configure packet filtering rules for data packets passing through the device. This is a mode-dependent rule. Hence, while the firewall is in medium mode, the rules are to be configured to reject the data packets if matching the rule. Whereas in maximum mode, the rules are to be configured to accept the data packets if matching the rule.

Parent

kcli/config/firewall/host-filter

Syntax

```
expert-control { protocol < proto string > | tcp | any } { source-network < snet string > |
any } { destination-network < dnet string > | any } { source-port < sport integer > | any }
{ dest-port < dport integer > | any } { source-mac < smac string(11:20) > | any } { in-
interface < iiface string > | any } { out-interface < oiface string > | any } { packet-
length < pktlen integer > | any } { tcp-flags < tcpflag string > | any } target { accept |
drop | reject } traffic dest { input | forward }
```

Parameter Description

Parameter	Description
protocol	Select a protocol for the rule, either TCP or any.
tcp	Select TCP protocol to match data packets using TCP protocol.
any	Select any option for protocol to match any protocol for a given packet.
source-network	Enter the source network name or select any to match any source network.
any	Select any option for source network to match any source network for a given packet.
destination-network	Enter the destination network name or select any to match any destination network.
any	Select any option for destination network to match any destination network for a given packet. .
source-port	Enter the source port number or select any to match any source port.
any	Select any optionSelect any option for source port to match to match any source port for a given packet.
dest-port	Enter the destination port number or select any to match any destination port.
any	Select any option for destination port to match any destination port for a given packet.
source-mac	Enter the source MAC address or select any to match any MAC address.
any	Select any option for source MAC address to match any MAC address for a given packet.
in-interface	Enter the input interface name or select any to match any input interface.
any	Select any option for input interface to match any input interface for a given packet.
out-interface	Enter the output interface name or select any to match any output interface.
any	Select any option for output interface to match any output interface for a given packet.
packet-length	Enter the packet length integer value or select any to match any packet length.
any	Select any option to match any packet length for a given packet.
tcp-flags	Specify the TCP flags or select any to match any TCP flags. You can specify TCP flags only if the selected protocol is TCP. The first argument is the flags that are to be examined, written as a comma-separated list, and the second argument is a comma-separated list of flags that are to be set. For example,s SYN,ACK,FIN,RST SYN.
any	Select any option for TCP flags to match any flags for a given packet.
target	Select the target action to be taken on the data packet, accept, drop, or reject.
accept	Select accept to accept the data packet matching the rule.
drop	Select drop to drop the data packet matching the rule.
reject	Select reject to reject the data packet matching the rule.
traffic dest	Add rule in either input or forward chain.
input	Select input chain for data packets originating from the router. That is, if the destination address belongs to the router, the data packet is processed against the input chain.
forward	Select forward chain for data packets that pass through the router to other devices.

Example

The following example command configures the expert control rule. Here, protocol TCP is selected for any source and destination port, with source port 20 and destination port 30. The input interface is eth0 and output

interface is any. Packet length is specified as any. As the TCP protocol is selected, the TCP flags are specified (SYN,ACK SYN), wherein the first argument is the flags to be examined, written as comma-separated list, and the second argument is the comma-separated list of flags to be set. The target action for the matching data packet is "reject". That is, the data packet matching the configured rule is rejected by the gateway:

```
#kcli> config firewall host-filter expert-control protocol tcp source-network any
destination-network any source-mac any source-port 20 dest-port 30 in-interface eth0 out-
interface any packet-length any tcp-flags "SYN,ACK SYN" target reject traffic dest input
<enter>
```

Note Expert control rules are mode-dependent rules. Hence, upon changing the firewall mode, you need to re-configure these rules. For example, if firewall is in medium mode, the rules should be configured to drop the data packets that match the given rule. Whereas in maximum mode, the rules should be configured to accept the data packets that match the given rule.

expert-control

Description

The `expert-control` command under no deletes a configured expert control rule.

Parent

kcli/config/firewall/host-filter/no

Syntax

```
expert-control { protocol < proto string > | tcp | any } { source-network < snet string > |
any } { destination-network < dnet string > | any } { source-port < sport integer > | any }
{ dest-port < dport integer > | any } { source-mac < smac string(11:20) > | any } { in-
interface < iiface string > | any } { out-interface < oiface string > | any } { packet-
length < pktlen integer > | any } { tcp-flags < tcpflag string > | any } target { accept |
drop | reject } traffic dest { input | forward }
```

Parameter Description

Parameter	Description
protocol	Specify the protocol for the rule to be deleted.
tcp	Select TCP if the rule to be deleted is configured using TCP protocol.
any	Select any if the rule to be deleted is configured using any protocol.
source-network	Specify the source network for the rule to be deleted.
any	Select any if the rule to be deleted is configured using any source network.
destination-network	Specify the destination network for the rule to be deleted.
any	Select any if the rule to be deleted is configured using any destination network.
source-port	Specify source port for the rule to be deleted.
any	Select any if the rule to be deleted is configured using any source port.
dest-port	Specify the destination port for the rule to be deleted.
any	Select any if the rule to be deleted is configured using any destination port.
source-mac	Specify the source MAC address for the rule to be deleted.
any	Select any if the rule to be deleted is configured using any source MAC address.
in-interface	Specify the input interface for the rule to be deleted.
any	Select any if the rule to be deleted is configured using any input interface.
out-interface	Specify the output interface for the rule to be deleted.
any	Select any if the rule to be deleted is configured using any output interface.
packet-length	Specify the packet length for the rule to be deleted.
any	Select any if the rule to be deleted is configured using any packet length.
tcp-flags	Specify TCP flags for the rule to be deleted.
any	Select any if the rule to be deleted is configured using any TCP flag.
target	Select the action to be taken on the targeted data packet, accept, drop, or reject.
accept	Select accept, if the rule is configured using this action.
drop	Select drop, if the rule is configured using this action.
reject	Select reject, if the rule is configured using this action.
traffic dest	Specify the chain (input or forward) in which the rule is added.
input	Select input chain for data packets originating from the router.
forward	Select forward chain for data packets that pass through the router to other devices.

alg

Description

The `alg` major command enables or disables the ALG service for the services running on the network, such as, IPSec, L2TP, FTP, TFTP, SIP, etc. The ALG is a proxy server. It overcomes various connectivity problems presented by firewalls and NAT servers. The key advantage of the ALG Proxy architecture is that external devices do not connect directly to the private network and internal devices do not connect directly to the public network. Thus, it enhances the network security.

Parent

kcli/config/firewall

no

Description

The no major command under alg disables ALG for services like IPSec, PPTP, L2TP, FTP, TFTP. Disabling ALG disallows data packets or protocols on the network.

Parent

kcli/config/firewall/alg

enable

Description

The `enable` command activates the ALG for specific services like IPSec, L2TP, FTP, TFTP, SIP, etc.

Parent

kcli/config/firewall/alg

Syntax

```
enable { ipsec | pptp | l2tp | quake3 | tftp | ftp | rtsp | sip | h323 }
```

Parameter Description

Parameter	Description
ipsec	Allow ESP packets on the network.
pptp	Allow PPTP on the network, to provide the global standard for broadband services.
l2tp	Allow L2TP on the network.
quake3	Allow quake packets (useful for running multimedia applications) on the network.
tftp	Allow TFTP on the network, for transferring small files between hosts on a network. It uses UDP (port 69) as its transport protocol.
ftp	Allow FTP on the network.
rtsp	Allow RTSP on the network, to establish and control media sessions between end points.
sip	Allow SIP on the network, to initiate, modify and terminate an interactive user session involving multimedia elements.
h323	Allow H.323 ITU VoIP protocol to facilitate audio-visual communication sessions on the network.

Example

The following example command enables the SIP service:

```
#kcli> config firewall alg enable sip <enter>
```

enable

Description

The `enable` command under no disables the ALG service on the network.

Parent

kcli/config/firewall/alg/no

Syntax

```
enable { ipsec | pptp | l2tp | quake3 | tftp | ftp | rtsp | sip | h323 }
```

Parameter Description

Parameter	Description
ipsec	Disallow ESP packets on the network.
pptp	Disallow the PPTP protocol on the network.
l2tp	Disallow L2TP on the network.
quake3	Disallow quake packets on the network.
tftp	Disallow TFTP on the network.
ftp	Disallow FTP on the network.
rtsp	Disallow RTSP on the network.
sip	Disallow SIP on the network.
h323	Disallow H.323 ITU VoIP protocol on the network.

default-config

Description

The `default-config` major command enables or disables the default services on the gateway, such as HTTP, SSH, TELNET, FTP, TFTP, DNS, etc.

Parent

kcli/config/firewall

no

Description

The `no` major command under default-config disables the specified default services on the gateway, such as HTTP, FTP, TFTP, TELNET.

Parent

kcli/config/firewall/default-config

enable

Description

The `enable` command activates the specified service/s on the gateway. Enter the service name from the available list of services.

Parent

kcli/config/firewall/default-config

Syntax

```
enable < servicename string >
```

enable

Description

The `enable` command under no disables the default services available on the network. Enter the service name to disable it on the network.

Parent

kcli/config/firewall/default-config/no

Syntax

```
enable < service string >
```

game

Description

The `game` major command enables or disables the games available on the WAN side game server. If you enable a game, the LAN user is able to connect to the WAN-side game server.

Parent

kcli/config/firewall

no

Description

The `no` major command under game disables games available on the WAN-side game server.

Parent

kcli/config/firewall/game

enable

Description

The `enable` command activates games on the WAN server, which lets a LAN workstation user connect to the WAN-side game server. Enter the game name from the list to enable it.

Parent

kcli/config/firewall/game

Syntax

```
enable < gamename string >
```

Note You can configure the games only if the firewall is in maximum mode.

enable

Description

The `enable` command under no disables games service on the WAN server, such that a LAN user cannot connect to the WAN-side game server. Enter the game name from the available list.

Parent

kcli/config/firewall/game/no

Syntax

```
enable < game string >
```

time-based-policy

Description

The `time-based-policy` major command creates time-based policies for various firewall rules. Here, you can configure schedules and assign these schedules to the configured policies. Time-based policy is a management tool to execute the policies defined for firewall on the specified schedule.

Parent

kcli/config/firewall

create-schedule

Description

The `create-schedule` major command creates a time schedule that can be assigned to different policies. The schedule can be set on a daily, weekly, or monthly basis.

Parent

kcli/config/firewall/time-based-policy

daily

Description

The `daily` command creates a daily time schedule.

Parent

kcli/config/firewall/time-based-policy/create-schedule

Syntax

```
daily schedule-name < name string(0:20) > start-time < stime string(0:20) > end-time <
etime string(0:20) >
```

Parameter Description

Parameter	Description
schedule-name	Enter a name for the schedule to be created.
start-time	Enter the start time in hh:mm (24-hour) format.
end-time	Enter the end time in hh:mm (24-hour) format.

Example

The following example command creates a schedule called "daily" that is to be associated with an existing policy. This policy will then be executed every day on the time specified in its associated schedule. In this example, the policy will be executed everyday from 03:00 PM to 04:00 PM:

```
#kcli> config firewall time-based-policy create-schedule daily schedule-name daily start-time 15:00 end-time 16:00 <enter>
```

week-days

Description

The `week-days` command creates a weekly time schedule, which gets implemented on all or specific week days.

Parent

kcli/config/firewall/time-based-policy/create-schedule

Syntax

```
week-days < wdays string(0:20) > schedule-name < name string(0:20) > start-time < stime string(0:20) > end-time < etime string(0:20) >
```

Parameter Description

Parameter	Description
schedule-name	Enter a name for the schedule to be created.
start-time	Enter the start time in hh:mm (24-hour) format.
end-time	Enter the end time in hh:mm (24-hour) format.

Example

The following example command creates a schedule called "weekly". This schedule is to be then associated with an existing policy. This policy will be executed every week on Monday (specified week day is 1, that is Monday) from 10:00 AM to 11:00 AM:

```
#kcli> config firewall time-based-policy create-schedule week-days 1 schedule-name weekly start-time 10:00 end-time 11:00 <enter>
```

monthly

Description

The `monthly` command configures a monthly time schedule. You can set the month/s (January to December) as well as the number of days in the specified month/s for the schedule to be implemented. Enter the number of

months in a range of 1-12, where 1 represents January, 2 represents February, etc. For example, for a period running from March to June, enter 3-6 as the value for specifying months.

Parent

kcli/config/firewall/time-based-policy/create-schedule

Syntax

```
monthly < mday string(0:20) > days < days string(0:20) > schedule-name < name string(0:20)
> start-time < stime string(0:20) > end-time < etime string(0:20) >
```

Parameter Description

Parameter	Description
days	Enter the days of the month (range 1-31). For example, to setup the schedule for the first 15 days of a given month, enter 1-15 as the value.
schedule-name	Enter a name for the schedule to be created.
start-time	Enter the start time in hh:mm (24-hour) format.
end-time	Enter the end time in hh:mm format.

delete-schedule

Description

The `delete-schedule` command deletes a configured time-based schedule. Enter the schedule name to be deleted.

Parent

kcli/config/firewall/time-based-policy

Syntax

```
delete-schedule < name string(0:20) >
```

Note Before deleting a schedule, you need to unassign the policy associated with that schedule by executing the "unschedule-policy" command. If you try to delete a schedule that has a policy associated with it, the error "Policy attached to schedule" is displayed.

create-policy

Description

The `create-policy` command creates a new policy which you can assign to one or multiple time schedules and rules (such as port forwarding, proxy, and allowed services, MAC addresses, sites) to implement the new policy. Enter the name of the policy to be created.

Parent

kcli/config/firewall/time-based-policy

Syntax

```
create-policy < name string(0:50) >
```

Example

The following example command creates a policy called "browsing". You can further assign time schedules to this policy to determine what time of day/week/month this policy is to be executed:

```
#kcli> config firewall time-based-policy create-policy browsing <enter>
```

delete-policy

Description

The `delete-policy` command deletes a policy entity from the gateway configuration. If you delete a policy, the associated rules/schedule will no longer get triggered in the network. Enter the policy name to be deleted.

Parent

kcli/config/firewall/time-based-policy

Syntax

```
delete-policy < name string(0:20) >
```

Note Before deleting a policy, ensure the policy is not associated with any schedule. If so, unassign the policy associated with the schedule using the "unschedule-policy" command. If you try to delete a policy that is associated with a schedule, an error is displayed stating "Policy attached to schedule".

schedule-policy

Description

The `schedule-policy` command associates a policy to a particular schedule. You can assign specific schedules to the configured policies to execute the policies on the set schedules. Note that you can use this command to associate only existing policies and schedules. In other words, you cannot create new policies or schedules by using this command. Enter an existing policy name to assign a schedule to.

Parent

kcli/config/firewall/time-based-policy

Syntax

```
schedule-policy < pname string(0:20) > schedule-name < sname string(0:20) >
```

Parameter Description

Parameter	Description
schedule-name	Enter an existing schedule name to assign it to the specified policy.

Example

The following example command associates the existing schedule called "daily" to the existing policy called "browsing". This policy will be executed everyday on the time specified in the "daily" schedule:

```
#kcli> config firewall time-based-policy schedule-policy browsing schedule-name daily
<enter>
```

unschedule-policy

Description

The `unschedule-policy` command unassigns a policy from a schedule. As a result, the policy can no longer be executed as per the previously associated schedule. Enter the policy name to unassign the schedule from.

Parent

kcli/config/firewall/time-based-policy

Syntax

```
unschedule-policy < pname string(0:20) > schedule-name < sname string(0:20) >
```

Parameter Description

Parameter	Description
schedule-name	Enter an existing schedule name to unassign the policy from.

contentfilter

Description

The `contentfilter` major command adds configures content filter rules for different content types. Content filter is a robust content security solution for the network using which you can practically filter any type of malicious content that may prove to be a threat for your network security. The content types, which you can filter out, include keyword names, files (.exe, .zip), viruses, and various protocols.

Parent

kcli/config/firewall

add

Description

The `add` command adds a content filter rule (content type and action to be taken) for the data packets received by the gateway. While configuring these rules, you need to specify the content type, such as keyword, file, virus, or protocol, and specify an action to be taken for the given content type, such as accept, reject or drop. Accordingly, the gateway takes the appropriate action when it encounters that type of content.

Parent

kcli/config/firewall/contentfilter

Syntax

```
type { { keyword name < name string(1:50) > action { accept | drop | reject | logaccept |
logreject | logdrop } match { contains } } | { file name < name string(0:50) > action {
accept | drop | reject | logaccept | logreject | logdrop } } | { protocol name < name
string(0:50) > action { accept | drop | reject | logaccept | logreject | logdrop } } | {
virus name < name string(0:50) > action { accept | drop | reject | logaccept | logreject |
logdrop } } } [ policy < pname string(0:20) > ]
```

Parameter Description

Parameter	Description
type	Select the content type with which the rule is configured, keyword, file, protocol or virus.
keyword	Select keyword as the content type for the content filter rule.
name	Enter the name string for the content type. For instance, if the content type is "keyword," then the name can be "Yahoo." The specified action will be on all the content having the word Yahoo in it.
action	Select an action the gateway should take when it encounters the specified content type.
accept	Select this option to accept the data packets of the specified content type.
drop	Select this option to drop the data packets of the specified content type.
reject	Select this option to reject the data packets of the specified content type.
logaccept	Select this action to make a log entry of the selected content type and accept that at the same time.
logreject	Select this action to make a log entry of the selected content type and reject that at the same time.
logdrop	Select this action to make a log entry of the selected content type and drop that at the same time.
match	Set the type of match for the rule.
contains	Select this option to match any criteria of the configured rule for the specified content type.
file	Select file as the content type. You can any of the well-known file types, such as exe, flash, gif, html, jpeg, ogg, pdf, perl, postscript, rar, rpm, rtf, tar, and zip.
name	Enter the file type from the given list, for which you want to configure the rule.
action	Select an action the gateway should take when it encounters the specified content type.
accept	Select this option to accept the data packets of the specified content type.
drop	Select this option to drop the data packets of the specified content type.
reject	Select this option to reject the data packets of the specified content type.
logaccept	Select this action to make a log entry of the selected content type and accept that at the same time.
logreject	Select this action to make a log entry of the selected content type and reject that at the same time.
logdrop	Select this action to make a log entry of the selected content type and drop that at the same time.
protocol	Select protocol as the content type. You can specify any of the well-known protocols.
name	Enter the protocol name from the given list.
action	Select an action the gateway should take when it encounters the specified content type.
accept	Select this option to accept the data packets of the specified content type.
drop	Select this option to drop the data packets of the specified content type.
reject	Select this option to reject the data packets of the specified content type.
logaccept	Select this action to make a log entry of the selected content type and accept that at the same time.
logreject	Select this action to make a log entry of the selected content type and reject that at the same time.
logdrop	Select this action to make a log entry of the selected content type and drop that at the same time.

Parameter	Description
virus	Select virus as the content type. You can specify a virus type, code_red or nimda.
name	Enter the virus name from the given list.
action	Select an action the gateway should take when it encounters the specified content type.
accept	Select this option to accept the data packets of the specified content type.
drop	Select this option to drop the data packets of the specified content type.
reject	Select this option to reject the data packets of the specified content type.
logaccept	Select this action to make a log entry of the selected content type and accept that at the same time.
logreject	Select this action to make a log entry of the selected content type and reject that at the same time.
logdrop	Select this action to make a log entry of the selected content type and drop that at the same time.
policy	Enter a policy name as appropriate, to attach it to the rule.

Example

The following example command creates a content filter rule having "keyword" as content type (for example, yahoo). Whenever a data packet is received matching this criteria, the specified action is taken. In this case, a log entry is made and the packet is rejected. This filter works on the specified time, during the day/week/month mentioned in the associated policy called "browsing":

```
#kcli> config firewall contentfilter add type keyword name yahoo action logreject match
contains policy browsing <enter>
```

matchpackets

Description

The `matchpackets` command specifies the number of packets that has to match the incoming data packets for the rule to execute. If the incoming data packets are in excess of 10, then the rule cannot be implemented.

Parent

kcli/config/firewall/contentfilter

Syntax

```
matchpackets < number integer >
```

remove

Description

The `remove` command deletes a configured content filter rule.

Parent

kcli/config/firewall/contentfilter

Syntax

```
remove type { keyword | file | protocol | viurs } name < name string(0:50) > [ policy <
pname string(0:20) > ]
```

Parameter Description

Parameter	Description
type	Select the content type with which the rule is configured, namely keyword, file, protocol or virus.
keyword	Select keyword as content type type, if the rule is configured for the keyword content type.
file	Select file as content type, if the rule is configured for the file content type.
protocol	Select protocol as the content type, if the rule is configured for the protocol-based content type.
virus	Select virus as the content type, if the rule is configured for the virus content type.
name	Enter the content name.
policy	Enter the associated policy name.

service-control

Description

The `service-control` major command allows or blocks various services on the network, such as ping, IPSec and PPTP tunnel, HTTP, HTTPS, FTP, TELNET, web proxy, and custom port.

Parent

kcli/config/firewall

no

Description

The no major command blocks a service from being accessed on the network, such that a LAN workstation cannot access an external service. By blocking the protocols or services that are highly susceptible to external attacks, you can make the network more secure. Services that you can block include ping, IPSec and PPTP tunneling, FTP, HTTP, HTTPS, TELNET, port, and web-proxy.

Parent

kcli/config/firewall/service-control

ping

Description

The `ping` command allows running ping service on the network.

Parent

kcli/config/firewall/service-control

Syntax

```
ping [ policy < pname string(0:20) > ]
```

Parameter Description

Parameter	Description
policy	Enter a policy name as appropriate, to attach it to the rule.

Note The service control is a mode-dependent rule. If you set firewall to maximum mode, the access to the external network is blocked completely, by default. Hence, you need to configure the services for allowing access to. But while the firewall is in medium mode, all the LAN workstations are allowed to access external network by default. Hence, the service control rule is to be configured for blocking the access, wherein you select the services that are to be blocked on your network.

ping

Description

The `ping` command blocks the ping service from running on the network.

Parent

kcli/config/firewall/service-control/no

Syntax

```
ping [ policy < pname string(0:20) > ]
```

Parameter Description

Parameter	Description
policy	Enter the associated policy name.

ipsec-tunnel

Description

The `ipsec-tunnel` command allows IPSec tunneling on the network.

Parent

kcli/config/firewall/service-control

Syntax

```
ipsec-tunnel [ policy < pname string(0:20) > ]
```

Parameter Description

Parameter	Description
policy	Enter a policy name as appropriate, to attach it to the rule.

ipsec-tunnel

Description

The `ipsec-tunnel` command blocks the IPsec tunneling on the network.

Parent

kcli/config/firewall/service-control/no

Syntax

```
ipsec-tunnel [ policy < pname string(0:20) > ]
```

Parameter Description

Parameter	Description
policy	Enter the associated policy name.

pptp-tunnel

Description

The `pptp-tunnel` command allows PPTP tunneling on the network.

Parent

kcli/config/firewall/service-control

Syntax

```
pptp-tunnel [ policy < pname string(0:20) > ]
```

Parameter Description

Parameter	Description
policy	Enter a policy name as appropriate, to attach it to the rule.

pptp-tunnel

Description

The `pptp-tunnel` command blocks the PPTP tunneling on the network.

Parent

kcli/config/firewall/service-control/no

Syntax

```
pptp-tunnel [ policy < pname string(0:20) > ]
```

Parameter Description

Parameter	Description
policy	Enter the associated policy name.

ftp

Description

The `ftp` command allows running FTP service on the network.

Parent

kcli/config/firewall/service-control

Syntax

```
ftp [ policy < pname string(0:20) > ]
```

Parameter Description

Parameter	Description
policy	Enter a policy name as appropriate, to attach it to the rule.

ftp

Description

The `ftp` command blocks the FTP service from running on the network.

Parent

kcli/config/firewall/service-control/no

Syntax

```
ftp [ policy < pname string(0:20) > ]
```

Parameter Description

Parameter	Description
policy	Enter the associated policy name.

http

Description

The `http` command allows running HTTP service on the network.

Parent

kcli/config/firewall/service-control

Syntax

```
http [ policy < pname string(0:20) > ]
```

Parameter Description

Parameter	Description
policy	Enter a policy name as appropriate, to attach it to the rule.

http

Description

The `http` command blocks the HTTP service from running on the network.

Parent

kcli/config/firewall/service-control/no

Syntax

```
http [ policy < pname string(0:20) > ]
```

Parameter Description

Parameter	Description
policy	Enter the associated policy name.

https

Description

The `https` command allows running HTTPS service on the network.

Parent

kcli/config/firewall/service-control

Syntax

```
https [ policy < pname string(0:20) > ]
```

Parameter Description

Parameter	Description
policy	Enter a policy name as appropriate, to attach it to the rule.

https

Description

The `https` command blocks the HTTPS service from running on the network.

Parent

kcli/config/firewall/service-control/no

Syntax

```
https [ policy < pname string(0:20) > ]
```

Parameter Description

Parameter	Description
policy	Enter the associated policy name.

web-proxy

Description

The `web-proxy` command allows running web proxy service on the network.

Parent

kcli/config/firewall/service-control

Syntax

```
web-proxy [ policy < pname string(0:20) > ]
```

Parameter Description

Parameter	Description
policy	Enter a policy name as appropriate, to attach it to the rule.

web-proxy

Description

The `web-proxy` command blocks web proxy service on the network.

Parent

kcli/config/firewall/service-control/no

Syntax

```
web-proxy [ policy < pname string(0:20) > ]
```

Parameter Description

Parameter	Description
policy	Enter the associated policy name.

telnet

Description

The `telnet` command allows running TELNET service on the network.

Parent

kcli/config/firewall/service-control

Syntax

```
telnet [ policy < pname string(0:20) > ]
```

Parameter Description

Parameter	Description
policy	Enter a policy name as appropriate, to attach it to the rule.

telnet

Description

The `telnet` command blocks the TELNET service from running on the network.

Parent

kcli/config/firewall/service-control/no

Syntax

```
telnet [ policy < pname string(0:20) > ]
```

Parameter Description

Parameter	Description
policy	Enter the associated policy name.

port

Description

The `port` command allows access to the custom port on the network. Enter the custom port number.

Parent

kcli/config/firewall/service-control

Syntax

```
port < inport string(0:20) > protocol { tcp | udp | tcpudp } [ policy < pname string(0:20)
> ]
```

Parameter Description

Parameter	Description
protocol	Select the communication protocol used for the port, TCP or UDP.
tcp	Select TCP as the port protocol.
udp	Select UDP as the port protocol.
tcpudp	Select both the TCP and UDP as the port protocol.
policy	Enter a policy name as appropriate, to attach it to the rule.

Example

The following example command allows the access to the specified port:

```
#kcli> config firewall service-control port 6000 protocol tcp policy policy1 <enter>
```

port

Description

The `port` command blocks a custom port from being accessed in the network. Enter the custom port number.

Parent

kcli/config/firewall/service-control/no

Syntax

```
port < inport integer > protocol { tcp | udp } [ policy < pname string(0:20) > ]
```

Parameter Description

Parameter	Description
protocol	Select the communication protocol used for the port, TCP or UDP.
tcp	Select TCP as the port protocol.
udp	Select UDP as the port protocol.
tcpudp	Select both TCP and UDP as the port protocols.
policy	Enter the associated policy name.

custom-message

Description

The `custom-message` major command configures a customized message for blocked sites. When a user tries to access a bocked site, the custom message is flashed, instead of the standard message.

Parent

kcli/config/firewall

status

Description

The `status` command under custom-message enables or disables the custom message when a user tries to access blocked sites.

Parent

kcli/config/firewall/custom-message

Syntax

```
status { enable | disable }
```

Parameter Description

Parameter	Description
enable	Enable custom message support.
disable	Disable custom message support.

message

Description

The `message` command allows you to enter the message string to be displayed when the user attempts to access a blocked site.

Parent

kcli/config/firewall/custom-message

Syntax

```
message < message string(1:1000) >
```

Example

The following example command adds the specified custom message string to be displayed to the user:

```
#kcli> config firewall custom-message “access denied” <enter>
```

mgmt-service

Description

The `mgmt-service` major command configures management services, such as HTTP, HTTPS, SSH, Telnet, SNMP or custom service) and the clients (LAN/WAN/both) that can access the device using that service.

Parent

kcli/config/firewall

add

Description

The `add` command adds a management service on the network.

Parent

kcli/config/firewall/mgmt-service

Syntax

```
{ port < inport integer > protocol { tcp | udp } source { lan | wan | lanwan } description
< desc string > }
```

Parameter Description

Parameter	Description
port	Select a port for the management service to be added, such as HTTP, HTTPS, SNMP, Telnet, SSH or specify a custom port.
protocol	Select a protocol for the management service, TCP or UDP.
tcp	Select TCP protocol.
udp	Select UDP protocol.
source	Specify the management source for the service, LAN, WAN, or both. Accordingly, only LAN, only WAN or both the clients will be able to access the device using the specified management service.
lan	Select LAN as management source. In this case, only LAN clients will be able to access the device for management using the specified service.
lanwan	Select LAN and WAN both as management source. In this case, both the LAN as well as WAN clients will be able to access the device for management using the specified service.
wan	Select WAN as management source. In this case, only WAN-side users (lying outside the LAN) will be able to access the device for management using the specified service.
description	Enter the service description.

Example

The following example command adds the specified management service on the network:

```
#kcli> config firewall mgmt-service add port 6000 protocol tcp source lanwan description
mgmtService <enter>
```

modify

Description

The `modify` command modifies the management service details, such as port, protocol and description.

Parent

kcli/config/firewall/mgmt-service

Syntax

```
{ rule-id < rid integer > port < inport integer > protocol { tcp | udp } source { lan | wan
| lanwan } description < desc string > }
```

Parameter Description

Parameter	Description
rule-id	Enter the management service rule ID number.
port	Modify management service port by entering new port number.
protocol	Modify management service protocol.
tcp	Select TCP protocol.
udp	Select UDP protocol.
source	Modify management source.
lan	Select LAN as management source.
lanwan	Select LAN and WAN both as management source.
wan	Select WAN as management source.
description	Modify service description.

delete

Description

The `delete` command deletes the selected management service. Thus, it ceases to be available to LAN, WAN, or both clients for accessing the device for management.

Parent

kcli/config/firewall/mgmt-service

Syntax

```
{ port < inport integer > protocol { tcp | udp } source { lan | wan | lanwan } description
< desc string > }
```

Parameter Description

Parameter	Description
port	Enter the port number for the management service to be deleted.
protocol	Specify the protocol for the management service to be deleted.
tcp	Select TCP if the service is configured using TCP protocol.
udp	Select UDP if the service is configured using UDP protocol.
source	Specify the management source for the service to be deleted.
lan	Select LAN if the service is configured using LAN management source.
lanwan	Select LAN and WAN if the service is configured using LAN and WAN both as management source.
wan	Select WAN if the service is configured using WAN management source.
description	Enter the service description.

dmz

Description

The `dmz` major command sets the IP of the host that acts as the port-forwarded DMZ host. A Demilitarized Zone (DMZ) host is a computer or a small sub-network that sits between a trusted internal network, such as a

corporate private LAN, and a non-trusted external network, such as the Internet. DMZ is used to secure an internal network from external access. So all the incoming or outgoing traffic is routed through this DMZ host.

Parent

kcli/config/firewall

no

Description

The `no` major command under DMZ deletes a DMZ host, such that the specified computer ceases to be a DMZ host.

Parent

kcli/config/firewall/dmz

host

Description

The `host` command sets up a computer as the DMZ host. Enter the host IP address or name of a computer in the LAN to set it as DMZ host.

Parent

kcli/config/firewall/dmz

Syntax

```
host < dmzhost string >
```

host

Description

The `host` command under the no module deletes the DMZ host by entering its name or IP address.

Parent

kcli/config/firewall/dmz/no

Syntax

```
host < dmzhost string >
```

ignore-icmp-bogus-error

Description

The `ignore-icmp-bogus-error` command enables or disables this feature on the network, so that ICMP error responses can be ignored or accepted by the device. The Internet Control Message Protocol (ICMP) is mainly used by the operating systems of the networked computers to send error messages. For example, an error message may indicate that a requested service is not available or that a host or router could not be reached.

Parent

kcli/config/firewall

Syntax

```
ignore-icmp-bogus-error { enable | disable }
```

Parameter Description

Parameter	Description
enable	Enable the ignore-icmp-bogus-error feature, so that the device can ignore the IGMP error responses.
disable	Disable the ignore-icmp-bogus-error feature, so that the device can accept the IGMP error responses.

ignore-icmp-broadcast

Description

The `ignore-icmp-broadcast` command enables or disable the ignore-icmp-broadcast feature, so that ICMP broadcast packets can be ignored or accepted by the device.

Parent

kcli/config/firewall

Syntax

```
ignore-icmp-broadcast { enable | disable }
```

Parameter Description

Parameter	Description
enable	Enable the ignore-icmp-broadcast feature, so that the device can ignore the ICMP broadcast packets.
disable	Disable the ignore-icmp-broadcast feature, so that the device can accept the ICMP broadcast packets.

tcp-timeout

Description

The `tcp-timeout` command sets the TCP timeout period for connections tracked by the netfilter conntrack (connection tracking) tool. Enter the TCP timeout period in seconds.

Parent

kcli/config/firewall

Syntax

```
tcp-timeout < time integer >
```

udp-timeout

Description

The `udp-timeout` command sets the UDP timeout period for connections tracked by the netfilter conntrack (connection tracking) tool. Enter the UDP timeout period in seconds.

Parent

kcli/config/firewall

Syntax

```
udp-timeout < time integer >
```

VLAN Module

This section describes configuration commands for the VLAN module. You can add or remove ports, add or remove VLANs, and set ingress or egress map for configuring qos.

vlan

Description

The `vlan` command node allows you to enter the configuration mode to configure the VLAN settings on the network. VLAN (or virtual LAN), is a method of creating independent logical networks within a physical network. It optimizes sparse network resources by creating multiple sub-LANs within a LAN. When a VLAN is created, users have the ability to create smaller broadcast domains within a layer 2 switched inter-networks by assigning different ports on the switch to different sub-networks. Further, you can assign different priorities for incoming and outgoing data on the various VLAN ports through the Quality of Service (QoS) settings.

Parent

kcli/config

portconfig

Description

The `portconfig` major command configures the port settings for the VLAN. It includes adding or deleting VLANs and their respective ports.

Parent

kcli/config/vlan

Syntax

```
portconfig
```

addport

Description

The `addport` command assigns a port (of an interface) to the VLAN entity.

Parent

kcli/config/vlan/portconfig

Syntax

```
addport { interface < interface_name string(1:32) > } { vlanid < vlanid integer(2:4094) > }
{ tagtype { untagged | tagged | custom } } { vlanifname < vlan_if_name string(1:32) > } {
adminstate { enable | disable }
```

Parameter Description

Parameter	Description
interface	Enter the interface name to be added to the VLAN.
vlanid	Enter the VLAN ID to be assigned to the port or interface.
untagged	Mark the port as "untagged." The untagged port has a single VLAN ID and cannot be assigned to other VLANs. Here, all the data packets are accepted that do not have an ID of any specific VLAN.
tagged	Mark the port as "tagged". The tagged port can be assigned to multiple VLANs. Here, only the data packets with the said VLAN ID tag are accepted.
custom	Mark the port as custom port. The data packets are marked with the specified VLAN ID.
vlanifname	Provide a name for the VLAN. The interface you have specified for VLAN is renamed to this new name, keeping the interface configuration as is.
adminstate	Enable or disable the VLAN interface state.
enable	Enable VLAN to activate it.
disable	Disable VLAN if you do not want to use it. The VLAN is deleted from the interface options.

Example

The following example command adds a custom port of the eth0 interface. This port has the VLAN ID 50 that is defined by the user.

```
#kcli> config vlan portconfig addport interface eth0 vlanid 50 tagtype custom vlanifname
abc1 adminstate enable <enter>
```

removeport

Description

The `removeport` command deletes an assigned port from an interface belonging to the VLAN. The said port ceases to be part of the VLAN.

Parent

kcli/config/vlan/portconfig

Syntax

```
removeport interface < interface_name string(1:32) > vlanid < vlanid integer(2:4094) >
vlanifname < vlan_if_name Enter vlan if name >
```

Parameter Description

Parameter	Description
interface	Enter the interface name to be deleted.
vlanid	Enter the VLAN ID number of the VLAN to be deleted.
vlanifname	Enter the new name of the VLAN interface you want to delete, with which the VLAN is renamed in the "addport" command.

modifyport

Description

The `modifyport` command modifies the admin state of the port by enabling or disabling it.

Parent

kcli/config/vlan/portconfig

Syntax

```
modifyport vlanifname < vlan_if_name integer > [ adminstate { enable | disable }
]
```

Parameter Description

Parameter	Description
vlanifname	Enter the VLAN interface name to which the port is assigned.
adminstate	Enable or disable the admin state of the port.
enable	Enable the port admin state.
disable	Disable the port admin state.

addvlan

Description

The `addvlan` command adds a VLAN to the network.

Parent

kcli/config/vlan/portconfig

Syntax

```
addvlan vlan_name < vlanname string > vlanid < vlanid integer >
```

Parameter Description

Parameter	Description
vlan_name	Enter an appropriate name for the VLAN. Any alpha-numeric value is acceptable, including an underscore (_), but not a hyphen (-).
vlanid	Enter an ID number for the given VLAN name. A VLAN ID (identifier) is a piece of required header information for the VLAN topology.

Example

The following example adds a VLAN called "management_vlan" with the VLAN ID 50:

```
#kcli> config vlan portconfig addvlan vlan_name management_vlan vlanid 50 <enter>
```

removevlan

Description

The `removevlan` command deletes a VLAN by its VLAN ID. The said VLAN thus ceases to be part of the network.

Parent

kcli/config/vlan/portconfig

Syntax

```
removevlan vlanid < vlanid integer >
```

Parameter Description

Parameter	Description
vlanid	Enter the VLAN ID number of the VLAN you want to delete.

qosconfig

Description

The `qosconfig` major command enables you to prioritize the incoming and outgoing traffic on the VLAN ports.

Parent

kcli/config/vlan

Syntax

```
qosconfig
```

set-ingress-map

Description

The `set-ingress-map` command configures the priority settings for the incoming traffic. Thus, you can optimize the network resources by assigning different priorities for the various VLAN ports.

Parent

kcli/config/vlan/qosconfig

Syntax

```
set-ingress-map vlanid < vlanid integer > vlanport < port string(1:32) > skbpriority <
skbprio integer > vlan_qos < qos integer(0:7) >
```

Parameter Description

Parameter	Description
vlanid	Enter the VLAN ID number on which the ingress QoS is to be set.
vlanport	Enter the VLAN port number for which the ingress QoS is to be set.
skbpriority	Enter the SKB priority value (integer) for the incoming data. The Socket Buffer (SKB) priority is mapped to the VLAN QoS priority value, wherein the network applications can distinguish between the data packets having different priorities. This is useful for bandwidth control and data filtering.
vlan_qos	Enter the VLAN QoS priority value for the incoming data between 0 and 7.

Example

The following example adds an ingress map for eth0 port having VLAN ID as 50. This map has the socket buffer priority as 1 and QoS priority as 4:

```
#kcli> config vlan qosconfig set-ingress-map vlanid 50 vlanport eth0 skbpriority 1 vlan_qos
4 <enter>
```

set-egress-map

Description

The `set-egress-map` command configures the priority settings for the outgoing traffic. Thus, you can optimize the network resources by assigning different priorities for the various VLAN ports.

Parent

kcli/config/vlan/qosconfig

Syntax

```
set-egress-map vlanid < vlanid integer > vlanport < port string > skbpriority < skbprio
integer > vlan_qos < qos integer(0:7) >
```

Parameter Description

Parameter	Description
vlanid	Enter the VLAN ID number on which the egress QoS is to be set.
vlanport	Enter the VLAN port number for which the egress QoS is to be set.
skbpriority	Enter the SKB priority value (integer) for the incoming data. The Socket Buffer (SKB) priority is mapped to the VLAN QoS priority value, wherein the network applications can distinguish between the data packets having different priorities. This is useful for bandwidth control and data filtering.
vlan_qos	Enter the VLAN QoS priority value for the outgoing data between 0 and 7.

Example

The following example adds an egress map for eth0 port having VLAN ID as 50. This map has the socket buffer priority as 1 and QoS priority as 4:

```
#kcli> config vlan qosconfig set-egress-map vlanid 50 vlanport eth0 skbpriority 1 vlan_qos
4 <enter>
```

PPPoA Module

This section describes configuration commands for the PPPoA module. You can configure the PPPoA session parameters, delete an existing PPPoA session etc.

pppoa

Description

The PPPoA command node allows you to enter the configuration mode for PPPoA. Point-to-Point Protocol over ATM (PPPoA) is a network protocol for encapsulating PPP frames in ATM AAL5. It is used mainly with cable modem, DSL and ADSL services. It offers standard PPP features such as authentication, encryption, and compression. If it is used as the connection encapsulation method on an ATM based network, it can reduce overhead slightly in comparison to PPPoE. It also avoids the issues related to having a MTU lower than that of standard Ethernet transmission protocols. It also supports the encapsulation types such as VC-MUX and LLC based.

Parent

kcli/config

set

Description

The `set` command configures the PPPoA session parameters.

Parent

kcli/config/pppoa

Syntax

```
set interface < interface string(1:32) > { default_params } | { session { enable | disable
} } | { config_params [ username < username string(1:32) > password < password string(6:32)
> ] [ defaultroute { enable | disable } ] [ usepeerdns { enable | disable } ] [ encryption
{ none | all | mppe } ] [ compression { none | all | vj } ] [ authentication { none | all |
```

```
pap | chap | papOrchap | msChap | msChapv2 | eapMD5 } ] [ lcpechointerval < lcpechointerval
integer(1:65535) > ] [ lcpechoretry < lcpechoretry integer(1:65535) > ] [ mtu < mtu
integer(1480:1500) > ] [ sessionmode { onDemand | keepAlive | manual } ] [ idleDisconnect <
idleDisconnect integer(0:65535) > ] [ autoDisconnect < autoDisconnect integer(0:65535) > ]
[ maxFailAttempt < maxFailAttempt integer(1:65535) > ] }
```

Parameter Description

Parameter	Description
interface	Specify the DSL interface on which PPPoA is to be enabled.
default_params	Select the default parameters for establishing a PPPoA session, if you do not want to configure the session using the custom parameters.
session	Enable or disable the PPPoA session status.
enable	Enable the PPPoA session to activate it.
disable	Disable the PPPoA session.
config_params	Configure the custom parameters for PPPoA session.
username	Configure the user name on the device to authenticate the PPPoA session on the access server.
password	Enter password for the above user name.
defaultroute	Enable or disable adding the default route for the PPPoA configuration. This parameter gives you the choice of routing data through the PPPoA protocol as well as the physical interface.
enable	Enable the default route to set the access server IP address as the default route gateway.
disable	Disable the default route feature, if you do not want to set the access server IP address as the default route on the network.
usepeerdns	Specify whether the device should receive the DNS server IP address from the access server along with the PPP IP address by enabling or disabling the user peer DNS feature.
enable	Enable the user peer DNS feature, so that the device requests for the DNS server address along with the PPPoA session initiation.
disable	Disable the user peer DNS feature, so that the device does not query the access server for the DNS server address.
encryption	Select the PPP encryption protocol to be used between the WAN device and ISP POP. The options are none, all, or MPPE.
none	Select none, if you do not want to use any PPP encryption protocol.
all	Select all to use any PPP encryption protocol.
mppe	Select MPPE to set Microsoft Point-to-Point Encryption (MPPE) protocol.
compression	Select the PPP compression protocol to be used between the WAN device and ISP POP.
none	Select none, if you do not want to use any PPP compression protocol.
all	Select all to use any PPP compression protocol.
vj	Select vj to use Van Jacobson (VJ) compression protocol.
authentication	Select the PPP authentication protocol to be used between the WAN device and ISP POP.
none	Select none, if you do not want to use any PPP authentication protocol.
all	Select all to use any PPP authentication protocol.
pap	Select pap to use Password Authentication Protocol (PAP).
chap	Select chapto use Challenge-Handshake Authentication Protocol (CHAP).
papOrchap	Select PAP or CHAP authentication protocol.
msChap	Select msChap to use Microsoft Challenge Handshake Authentication Protocol (MSCHAP).
msChapv2	Select msChapv2 to use MSCHAPv2 authentication protocol.
eapMD5	Select eapMD5 to use Extensible Authentication Protocol-Message-Digest algorithm 5 (EAP-MD5).
lcpechointerval	Set the LCP time interval between 1 and 65535 seconds. This is the interval between the Link Control Protocol (LCP) echo requests.

Parameter	Description
lcpechoretry	Enter the number of LCP echo retries (between 1 and 65535) within an echo period.
mtu	Enter the MTU size (between 1480 and 1500 bytes) to be used for the session. Maximum Transmission Unit (MTU) is the largest packet size allowed to be passed over the interface.
sessionmode	Select any of the available PPP session modes, onDemand, keepAlive, or manual.
onDemand	Select the onDemand PPP session mode. This option disconnects the PPPoE connection whenever the Internet idle time (no data transfer is taking place) exceeds the specified time. However, once the data transfer resumes through the PPPoE interface, the connection is automatically re-established.
keepAlive	Select the keepAlive PPP session mode. This option keeps the PPPoE connection always ON, irrespective of the presence of the data traffic.
manual	Select the manual session mode. In this mode, if the session is terminated, it has to be re-established manually when there is data to be exchanged. That is, the session will not get activated automatically, even if there is data traffic.
idleDisconnect	Set the idle time (in seconds) for the session. If the session mode is onDemand or manual, the session is disconnected automatically after the specified idle timeout. Default value is 1200 seconds. Entering a value of 0 (zero) indicates that the connection is not to be shut down automatically.
autoDisconnect	Set the automatic session disconnection period (in seconds). If this value is specified (for onDemand or manual session modes), the session is terminated once the auto disconnect time is lapsed, even if there is data traffic to be exchanged. Entering a value of 0 (zero) indicates that the connection is not to be shut down automatically.
maxFailAttempt	Set the maximum number of attempts (between 1 and 65535) for the device to re-establish the session, before the session is finally terminated. The max fail attempt value should not be 0 (zero).

Example

The following example starts the PPPoA session on eth0 interface:

```
#kcli> config pppoa set interface eth0 session <enter>
```

Alternatively, you can select the `config_params` option to configure PPPoA session parameters:

```
#kcli> config pppoa set interface eth0 config_params username admin password admin
defaultroute enable usepeerdns enable encryption mppe compression vj authentication eapMD5
lcpechointerval 300 lcpechoretry 3 mtu 1480 maxFailAttemp 3 sessionmode keepAlive
idleDisconnect 1200 autoDisconnect 10 <enter>
```

delete

Description

The `delete` command deletes an existing PPPoA session.

Parent

kcli/config/pppoa

Syntax

```
delete interface < interface string(1:32) >
```

Parameter Description

Parameter	Description
interface	Specify the DSL interface, on which the PPPoA session is enabled.

PPPoE Module

This section describes configuration commands for the PPPoE module. You can configure the Point-to-Point Protocol over Ethernet (PPPoE) session parameters, and enable or disable the PPPoE service on the network.

pppoe

Description

The PPPoE command node allows you to configure the PPPoE service, used for accessing the Internet.

Parent

kcli/config

set

Description

The `set` command starts or stops the PPPoE service on the device.

Parent

kcli/config/pppoe

Syntax

```
set interface < interface string(1:32) > { default_params } | { config_params username <
username string(1:32) > password < password string(6:32) > [ baudrate < baudrate
integer(0:2147483648) > ] [ acname < acname string > ] [ mtu < mtu integer(1480:1500) > ] [
tcpmss < tcpmss integer(1412:1460) > ] [ serviceid < serviceid string(1:32) > ] [
sessionMode { { onDemand idletimeout < idletimeout integer > } | { keepAlive } } ] [
authProtocol { pap | chap | chapOrpap | msChap | msChapV2 | eapMD5 } ] [ script < script
string > ] } | [ lcpechointerval < lcpechointerval integer(1:65535) > ] | [ lcpechoretry <
lcpechoretry integer(1:65535) > ] | { session { enable | disable } }
```

Parameter Description

Parameter	Description
interface	Enter the Ethernet interface name on which the PPPoE service is to start.
default_params	Select the default parameters for establishing a PPPoE session, if you do not want to configure the session using custom parameters.
config_params	Configure the PPPoE parameters for establishing a session.
username	Enter the user name as provided by the ISP to authenticate the PPPoE session.
password	Enter the password to authenticate the given PPPoE user name.
baudrate	The baud rate is the number of symbols transferred per second. Enter the baud rate for TTY devices (in seconds).
serviceid	Enter the service identification name as provided by the ISP.
acname	Enter the access concentrator name as provided by the ISP. A concentrator is used by the ISP to enable modem dialing. A concentrator provides communication capability between many low-speed, usually asynchronous channels and one or more high-speed, usually synchronous channels.
session	Enable (start) or disable (stop) the PPPoE session.
enable	Enable the session to start the PPPoE service.
disable	Disable the session to stop the PPPoE service.
mtu	Enter the MTU size (between 1480 and 1500 bytes) to be used for the session. Maximum Transmission Unit (MTU) is the largest packet size allowed to be passed over the interface.
tcpmss	Enter the TCP MSS integer value (between 1412 and 1460 bytes). Maximum segment size (MSS) is the largest amount of data (in bytes) to be handled by the device as a single, unfragmented piece.
defaultroute	Enable or disable the default route addition setting for the PPPoE configuration. This parameter gives you the choice of routing data through the PPPoE protocol as well as the physical interface.
enable	Enable the default route feature to set the PPPoE interface as the default route on the network.
disable	Disable the default route feature, if you do not want to set the PPPoE interface as the default route on the network.
sessionMode	Select the PPPoE session mode, onDemand or keepAlive.
onDemand	Select the onDemand PPP session mode. This option disconnects the PPPoE connection whenever the Internet idle time (no data transfer is taking place) exceeds the specified time. However, once the data transfer resumes through the PPPoE interface, the connection is automatically re-established.
idletimeout	Specify a timeout value (in seconds) for the "on demand" feature of the PPPoE connection. So, the PPPoE connection will be disconnected immediately after the specified seconds.
keepAlive	Select the keepAlive PPP session mode. This option keeps the PPPoE connection always ON, irrespective of the presence of the data traffic.
authProtocol	Select the protocol to be used for PPPoE session authentication.
pap	Select pap to use Password Authentication Protocol (PAP).
chap	Select chap to use Challenge-Handshake Authentication Protocol (CHAP).
chapOrpap	Select PAP or CHAP authentication protocol.
msChap	Select msChap to use Microsoft Challenge Handshake Authentication Protocol (MSCHAP).
msChapV2	Select msChapv2 to use Extensible Authentication Protocol-Message-Digest algorithm 5 (EAP-MD5).
eapMD5	Select eapMD5 to use EAP-MD5 authentication protocol.

Parameter	Description
script	**Note** This parameter is used only for internal purpose. No user action is required as far as configuration of the same is concerned. Hence, no description required for this parameter.
lcpechointerval	Set the LCP time interval between 1 and 65535 seconds. This is the interval between the Link Control Protocol (LCP) echo requests.
lcpechoretry	Enter the number of LCP echo retries (between 1 and 65535) within an echo period.

Example

The following example command starts the PPPoE session on bb0 interface using the default parameters:

```
#kcli> config pppoe set interface bb0 default_params <enter>
```

Alternatively, you can select the config_params option to configure various PPPoE session parameters:

```
#kcli> config pppoe set interface bb0 config_params username admin password admin mtu 1480
tcpmss 1412 defaultroute enable acname abc servicedi service1 sessionMode keepAlive
authProtocol msChap lcpechointerval 300 lcpechoretry 3 <enter>
```

backoff

Description

The backoff command configures backoff parameters to be used by PPP daemon in case of connection failure. When the gateway receives a receipt of authentication failure while trying to establish a PPP session, this exponential backoff mechanism is used to limit the repeated attempts to reconnect.

Parent

kcli/config/pppoe

Syntax

```
backoff settings < settings string(1:32) >
```

Parameter Description

Parameter	Description
settings	Set the backoff values by entering a string in the format of a:b:c,d:e:f. Here, a and d are the number of retry attempts, b and e are delay in seconds between successive connection attempts, and c and f are delay in minutes before starting the next sequence of connection attempts. For example, 3:30:5,3:30:10,3:30:20, etc.

set-default-domain

Description

The `set-default-domain` command sets a default domain. If the PPPoE user credentials do not contain a domain name, and if the default domain appending is enabled, this default domain name is appended to the specified PPPoE user. Enter the default domain to be appended.

Parent

kcli/config/pppoe

Syntax

```
set-default-domain < domain_name string >
```

default-domain-appending

Description

The `default-domain-appending` command enables or disables the default domain appending for the PPPoE user. If enabled, the user name is checked for the presence of the domain name. If the domain name is not provided by the PPPoE user, the default domain is appended automatically for that user. If default domain appending is disabled, the PPPoE user name is not appended with the default domain name.

Parent

kcli/config/pppoe

Syntax

```
default-domain-appending < status string >
```

allowed-domain-separator

Description

The `allowed-domain-separator` command adds the separator between PPPoE user name and domain name. The allowed domain separator is @. For instance, username@domain.com. Enter the domain separator.

Parent

kcli/config/pppoe

Syntax

```
allowed-domain-separator < separator string >
```

Wireless Module

This section describes configuration commands for the wireless module. You can configure various wireless settings for interface, radio, turbo-mode, multiple-SSID, etc.

wireless

Description

The `wireless` command node allows you to enter the configuration mode to configure various wireless settings for interface, radio, SSID, security mode etc.

Parent

kcli/config

interface

Description

The `interface` major command configures the wireless parameters specific to interfaces, such as the current SSID, interface mode (master or managed), wireless standard being used and the security parameters set. Enter the interface name to configure its parameters.

Parent

kcli/config/wireless

Syntax

```
interface < interface string(1:16) >
```

Example

The following example command allows the configuration of the wifi0 wireless interface:

```
#kcli> config wireless interface wifi0 <enter>
```

Proceed to set the various parameters of this interface, such as SSID, admin state, DTIM period, and WMM.

commit

Description

The `commit` command applies changes to the selected wireless interface.

Parent

kcli/config/wireless/interface

Syntax

```
commit
```

Example

The following example applies the changes to the wifi0 interface:

```
#kcli> config wireless interface wifi0 commit <enter>
```

ssid

Description

The `ssid` command sets the SSID for the specified wireless interface. Service Set Identifier (SSID) is the name designated for a specific wireless LAN. Enter the SSID value between 1 and 32 characters.

Parent

kcli/config/wireless/interface

Syntax

```
ssid < ssid string(1:32) >
```

Example

The following example command sets the SSID "npgw1" for the wifi0 interface on your network:

```
#kcli> config wireless interface wifi0 ssid npgw1 <enter>
```

Note The SSID value is space and case sensitive. You can enter an alphanumeric value of up to 32 characters.

admin-state

Description

The `admin-state` command enables or disables the admin state.

Parent

kcli/config/wireless/interface

Syntax

```
admin-state { up | down }
```

Parameter Description

Parameter	Description
up	Select the up option to run the interface.
down	Select the down option, if you do not want the interface to run.

Example

The following example command enables the admin state on the wifi0 interface:

```
#kcli config wireless interface wifi0 admin-state up <enter>
```

80211n-protection-type

Description

The `802.11n-protection-type` command sets the 802.11n protection type (none, rts, or cts2self). RTS/CTS (Request to Send/Clear to Send) is the mechanism used by 802.11 wireless networking protocol to reduce frame collisions introduced by the hidden terminal problem.

Parent

kcli/config/wireless/interface

Syntax

```
80211n-protection-type { none | rts | cts2self }
```

Parameter Description

Parameter	Description
none	Select none as the 802.11n protection type.
rts	Select RTS as the 802.11n protection type.
cts2self	Select cts2self as the 802.11n protection type.

Example

The following example command sets the cts2self protection type for the wifi0 interface:

```
#kcli> config wireless interface wifi0 80211n-protection-type cts2self <enter>
```

dtim-period

Description

The `ditm-period` command sets the DTIM period for the wireless interface. A Delivery Traffic Indication Message (DTIM) is a countdown mechanism that informs clients of the next window for listening to broadcast and multicast messages. When the Access Point (AP) has buffered the broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. The AP clients listen to the beacons and are awakened to receive the broadcast and multicast messages. Enter the DTIM period value between 1 and 65535 (in seconds).

Parent

kcli/config/wireless/interface

Syntax

```
dtim-period < dtimperiod integer >
```

Example

The following example command sets the DTIM period of 3 seconds for the wifi0 interface:

```
#kcli> config wireless interface wifi0 dtim-period 3 <enter>
```

erp-protection-type

Description

The `erp-protection-type` command sets the ERP protection type (none, RTS, or cts2self).

Parent

kcli/config/wireless/interface

Syntax

```
erp-protection-type { none | rts | cts2self }
```

Parameter Description

Parameter	Description
none	Select none as ERP protection type.
rts	Select RTS as ERP protection type.
cts2self	Select cts2self as ERP protection type.

Example

The example command sets the RTS ERP protection type for the wifi0 interface:

```
#kcli> config wireless interface wifi0 erp-protection-type rts <enter>
```

reliable-multicast

Description

The `reliable-multicast` command enables or disables the reliable multicast on the wireless interface.

Parent

kcli/config/wireless/interface

Syntax

```
reliable-multicast { disable | enable }
```

Parameter Description

Parameter	Description
disable	Disable reliable multicast on the wireless interface.
enable	Enable reliable multicast on the wireless interface. It provides a reliable sequence of packets to multiple recipients simultaneously, making it suitable for applications like multi-receiver file-transfer.

Example

The following example command enables the reliable multicast status on the wifi0 interface:

```
#kcli> config wireless interface wifi0 reliable-multicast enable <enter>
```

wps-admin-state

Description

The `wps-admin-state` command sets the WPS admin state (up or down) for the wireless interface.

Parent

kcli/config/wireless/interface

Syntax

```
wps-admin-state { down | up }
```

Parameter Description

Parameter	Description
down	Select down to disable the WPS on the wireless interface.
up	Select up to enable the WPS on the wireless interface.

Example

The following example command enables the WPS admin state on the wifi0 interface:

```
#kcli> config wireless interface wifi0 wps-admin-state up <enter>
```

rate

Description

The `rate` command selects a transfer rate between the client (station) and the AP.

Parent

kcli/config/wireless/interface

Syntax

```
rate { auto | { fixed < rate integer(1:1000) > } }
```

Parameter Description

Parameter	Description
auto	Select the auto option to enable the device to set the transfer rate automatically.
fixed	Select the fixed option to set the transfer rate. Enter an integer between 1 and 1000 for the rate value.

Example

The following example command allows the device to set the transfer rate between the client and the AP automatically:

```
#kcli> config wireless interface wifi0 rate auto <enter>
```

hw-mode

Description

The `hw-mode` command specifies the hardware mode for the radio interface. The available hardware mode options are 802.11a, 802.11b and 802.11g that refer to the wireless interface support for the respective standards. Select a hardware mode for the radio interface.

Parent

kcli/config/wireless/interface

Syntax

```
hw-mode { b | g | bg | abg | na | ng | nbg | nabg }
```

Parameter Description

Parameter	Description
b	Set the mode to 80.11b (also referred to as 802.11 High Rate or Wi-Fi). This is an extension to 802.11 that applies to the wireless LANS and provides 11 Mbps transmission (with a fallback to 5.5, 2 and 1 Mbps) in the 2.4 GHz channel.
g	Set the mode to 802.11g. This applies to the wireless LANs and provides 20+ Mbps transmission in the 2.4 GHz channel.
g	Set the mode to 802.11g. This applies to the wireless LANs and provides 20+ Mbps transmission in the 2.4 GHz channel.
bg	Set the mode to 802.11b/g.
abg	Set the mode to 802.11a/b/g.
na	Set the mode to 802.11na. 802.11n is a newer standard of WiFi LAN, subsequent to standards 802.11a, 802.11b and 802.11g.
ng	Set the mode to 802.11ng.
nbg	Set the mode to 802.11nb/ng.
nabg	Set the mode to 802.11na/nbg.

Example

The following example command sets the hardware mode to 802.11g:

```
#kcli> config wireless interface wifi0 hw-mode g <enter>
```

bridge-mode

Description

The `bridge-mode` command enables or disables the bridge mode for the wireless interface.

Parent

kcli/config/wireless/interface

Syntax

```
bridge-mode { disable | { enable < bridgename string(1:32) > } }
```

Parameter Description

Parameter	Description
disable	Disable the bridge mode.
enable	Enable the bridge mode. Enter the bridge name to which the interface is added.

Example

The following example command adds the wifi0 interface to the bridge "bridge1":

```
#kcli> config wireless interface wifi0 bridge-mode enable bridge1 <enter>
```

channel

Description

The `channel` command sets the channel for the wireless interface. Channel is the frequency to be used for the media access.

Parent

kcli/config/wireless/interface

Syntax

```
channel { auto | { fixed < channel_value integer(1:100) > } }
```

Parameter Description

Parameter	Description
auto	Select the auto option, if you want the device to automatically select the channel.
fixed	Select the fixed mode to define the channel frequency to be used. Enter an integer between 1 and 100 for the channel value.

Example

The following example command sets the fixed mode having the channel frequency of 6:

```
#kcli> config wireless interface wifi0 channel fixed 6 <enter>
```

regulatory-domain

Description

The `regulatory-domain`command sets the regulatory domain code. Enter the code value between 1 and 100.

Parent

kcli/config/wireless/interface

Syntax

```
regulatory-domain < rgdomain integer(1:100) >
```

Example

The following example command sets the regulatory domain code to 10:

```
#kcli> config wireless interface wifi0 regulatory-domain 10 <enter>
```

country-code

Description

The `country-code` command sets the country code for the wireless interface. Enter the country code value between 0 and 999.

Parent

kcli/config/wireless/interface

Syntax

```
country-code < ccode integer(0:999) >
```

Example

The following example command sets the country code value to 112:

```
#kcli> config wireless interface wifi0 country-code 112 <enter>
```

antenna-diversity

Description

The `antenna-diversity` command enables or disables the antenna diversity property. Selecting the enable option allows the antenna to automatically switch to other antenna having better signals.

Parent

kcli/config/wireless/interface

Syntax

```
antenna-diversity { enable | disable }
```

Parameter Description

Parameter	Description
enable	Enable antenna diversity for the radio interface to switch to the antenna having better signals.
disable	Disable antenna diversity for the radio interface.

Example

The following example command enables the antenna diversity to switch to the antenna transreceiving better signals:

```
#kcli> config wireless interface wifi0 antenna-diversity enable <enter>
```

rx-antenna

Description

The `rx-antenna` command sets the Rx antenna for the wireless interface. Rx stands for the wireless message integrity code receiver.

Parent

kcli/config/wireless/interface

Syntax

```
rx-antenna { auto | one | two }
```

Parameter Description

Parameter	Description
auto	Select the auto option to automatically identify the Rx antenna for receiving the transmission.
one	Select one for Rx antenna.
two	Select two for Rx antenna.

Example

The following example command allows the device to identify the Rx antenna automatically for receiving the transmission:

```
#kcli> config wireless interface wifi0 rx-antenna auto <enter>
```

tx-antenna

Description

The `tx-antenna` command sets the Tx antenna for the wireless interface. Tx stands for the wireless message integrity code transmitter.

Parent

kcli/config/wireless/interface

Syntax

```
tx-antenna { auto | one | two }
```

Parameter Description

Parameter	Description
auto	Select the auto option to automatically identify the Tx antenna for transmission.
one	Select one for Tx antenna.
two	Select two for Tx antenna.

Example

The following example command sets antenna one for Tx antenna:

```
#kcli> config wireless interface wifi0 tx-antenna one <enter>
```

preamble-type

Description

The `preamble-type` command sets the preamble type for the wireless interface. The preamble type defines the length of the CRC block for communication between the AP and the roaming wireless adapters. Ensure selection of the appropriate preamble type.

Parent

kcli/config/wireless/interface

Syntax

```
tx-antenna { auto | one | two }
```

Parameter Description

Parameter	Description
long	Select long as preamble type.
short	Select short as preamble type.

Example

The following example command sets the preamble type as long:

```
#kcli> config wireless interface wifi0 preamble-type long <enter>
```

mode

Description

The `mode` major command sets an operation mode (AP or client) for the selected wireless interface. In the AP mode (also called the master mode) the device controls association of the stations to the box. Whereas in the client mode (also called the managed mode), the box is able to connect to another AP.

Parent

kcli/config/wireless/interface

Syntax

```
mode
```

Note If you select the client mode, ensure that you have set the radio interface to the "managed" mode for the client mode to take effect.

ap

Description

The `ap` major command allows you to enter the configuration mode for the wireless interface. In the AP mode (also called the master mode) the device controls association of the stations to the box.

Parent

kcli/config/wireless/interface/mode

Syntax

```
ap master
```

Parameter Description

Parameter	Description
master	Configure the parameters for the master mode of the selected interface.

security-mode

Description

The `security-mode` major command configures the security settings for the master mode.

Parent

kcli/config/wireless/interface/mode/ap

Syntax

```
security-mode
```

key-management

Description

The `key-management` command sets the authentication mode for key management, open or restricted.

Parent

kcli/config/wireless/interface/mode/ap/security-mode

Syntax

```
key-management { open | restricted }
```

Parameter Description

Parameter	Description
open	Select the open key authentication. With this mode, the client device can complete the authentication and associate with the AP. However, the use of WEP prevents the client from sending data to and receiving data from the AP, unless the client has the correct WEP key.
restricted	Select the restricted key authentication. With this mode, the AP sends the client device a challenge text packet that the client must encrypt with the correct WEP key and return to the AP. If the client has the wrong key or no key, the authentication fails and the client is not allowed to associate with the AP. Restricted key authentication is not considered secure, because a hacker who detects both the clear-text challenge and the same challenge encrypted with a WEP key, can decipher the WEP key.

Example

The following example command sets the open key authentication:

```
#kcli config wireless interface wifi0 mode ap master security-mode key-management open
<enter>
```

default-key-mode

Description

The `default-key-mode` default-key-mode command enables or disables the default wireless security key.

Parent

kcli/config/wireless/interface/mode/ap/security-mode

Syntax

```
default-key-mode { enable | disable }
```

Parameter Description

Parameter	Description
enable	Enable the default wireless security key.
disable	Disable the default wireless security key.

Example

The following example command enables the default key mode:

```
#kcli> config wireless interface wifi0 mode ap master security-mode default-key-mode enable
<enter>
```

wep

Description

The wep command sets the WEP security mode. WEP is the oldest encryption method for wireless networks. It encrypts the traffic on the network and hence a hacker cannot understand the transmitted data. A key or password is required to decrypt this data at the receiving end. This security mode encrypts the data using 40 bits of the secret WEP key and random 24 bits.

Parent

kcli/config/wireless/interface/mode/ap/security-mode

Syntax

```
wep { [ key-length { { 64 { [ wep-key1 { ascii | hex } < wepkey1 string(1:32) > ] [ wep-key2
{ ascii | hex } < wepkey2 string(1:32) > ] [ wep-key3 { ascii | hex } < wepkey3
string(1:32) > ] [ wep-key4 { ascii | hex } < wepkey4 string(1:32) > ] } } | { 128 { [ wep-
key1 { ascii | hex } < wepkey1 string(1:32) > ] [ wep-key2 { ascii | hex } < wepkey2
string(1:32) > ] [ wep-key3 { ascii | hex } < wepkey3 string(1:32) > ] [ wep-key4 { ascii |
hex } < wepkey4 string(1:32) > ] } } } ] [ { default-key1 | default-key2 | default-key3 |
default-key4 } ] }
```

Parameter Description

Parameter	Description
key-length	Set the WEP key length, 128-bit or 64-bit. Keys are used to control the operation of a cipher so that only the correct key can convert an encrypted text to plain text. The key length is a measure of the number of possible keys which can be used in a cipher and is usually specified in bits. The key length is critical in determining the susceptibility of a cipher to exhaustive search attacks. A key should be large enough to repel a brute force attack (possible against any encryption algorithm).
64	Set the WEP key length to 64 (bits).
wep-key1	Set the WEP key 1 in either ASCII or hex.
ascii	Set the key in ASCII (5 values).
hex	Set the key in hex (10 values).
wep-key2	Set the WEP key 2.
ascii	Set the key in ASCII (5 values).
hex	Set the key in hex (10 values).
wep-key3	Set the WEP key 3.
ascii	Set the key in ASCII (5 values).
hex	Set the key in hex (10 values).
wep-key4	Set the WEP key 4.
ascii	Set the key in ASCII (5 values).
hex	Set the key in hex (10 values).
128	Set the WEP key length to 128 (bits).
wep-key1	Set the WEP key 1 in either ASCII or hex.
ascii	Set the key in ASCII (5 values).
hex	Set the key in hex (10 values).
wep-key2	Set the WEP key 2.
ascii	Set the key in ASCII (5 values).
hex	Set the key in hex (10 values).
wep-key3	Set the WEP key 3.
ascii	Set the key in ASCII (5 values).
hex	Set the key in hex (10 values).
wep-key4	Set the WEP key 4.
ascii	Set the key in ASCII (5 values).
hex	Set the key in hex (10 values).
default-key1	Set the WEP key 1 as default key.
default-key2	Set the WEP key 2 as default key.
default-key3	Set the WEP key 3 as default key.
default-key4	Set the WEP key 4 as default key.

Example

The following example command sets the WEP key authentication with a key length of 128 bits in ASCII:

```
#kcli config wireless interface wifi0 mode ap master security-mode wep key-length 128 ascii
wep-key1 secretwepkey1 <enter>
```

You can set all the four WEP keys and finally select one of them to set it as default key. For example:

```
#kcli> config wireless interace wlan0 mode ap master security-mode wep defaultkey1 <enter>
```

Note The values of the WEP keys are:
64-bit hex key: 10 hexadecimal digits, for example, secretkey1.
64-bit ASCII key: 5 characters, for example, pjohn.
128-bit hex key: 26 hexadecimal digits, for example, abcde1234567890abcde1234567890123456.
128-bit ASCII key: 13 characters, for example, secretwepkey1.

wpa2

Description

The `wpa2` command configures the WPA2 security mode. The WPA2 mode is the advanced version of the WPA and aims at solving many security issues that the WPA poses. It uses an AES encryption algorithm unlike WAP that uses the RC4 encryption algorithm.

Parent

kcli/config/wireless/interface/mode/ap/security-mode

Syntax

```
wpa2 { enc-type tkip | aesCcmp | both } [ primary-radius { authserver < ip_address
ipaddress > } { authport < port integer > } { authsecret < secret string > } ] [ secondary-
radius { authserver < ip_address ipaddress > } { authport < port integer > } { authsecret <
secret string > } ] [ primary-radius-acct { acctserver < ip_address ipaddress > } {
acctport < port integer > } { acctsecret < secret string > } ] [ secondary-radius-acct {
acctserver < ip_address ipaddress > } { acctport < port integer > } { acctsecret < secret
string > } ]
```

Parameter Description

Parameter	Description
enc-type	Select the encryption type, TKIP, AESCCMP or both, for the WPA2 security mode. Encryption type is the algorithm to be used for encrypting the data transmitted between the AP and the client.
tkip	Select TKIP as encryption type. Temporal Key Integrity Protocol (TKIP) is a security protocol used in Wi-Fi protected access and is designed to replace WEP without replacing the legacy hardware.
aesCcmp	Select AESCCMP as encryption type. Advanced Encryption Standard-Counter Mode (AES) is a symmetric 128-bit block data encryption technique that works at multiple network layers simultaneously. In Cipher Block Chaining Message Authentication Code Protocol (CCMP), unlike TKIP, key management and message integrity is handled by a single component built around AES.
both	Use both TKIP and AESCCMP encryption types.
primary-radius	Configure the primary RADIUS authentication server. Remote Authentication Dial-In User Service (RADIUS) is an authentication and accounting system used by many ISPs. While dialing the ISP you must enter your user name and password. This information is passed to a RADIUS server, which verifies whether the information is correct and then authorizes the access to the ISP server. WPA/WPA2 is designed for use with an IEEE 802.1X authentication server, which distributes different keys to each user.
authserver	Enter the IP address of the primary authentication server.
authport	Enter the primary server port number.
authsecret	Enter a string value for the authentication secret.
secondary-radius	Configure the secondary RADIUS server.
authserver	Enter the IP address of the secondary authentication server.
authport	Enter the secondary server port number.
authsecret	Enter a string value for the authentication secret.
primary-radius-acct	Configure the primary RADIUS accounting server.
acctserver	Enter the IP address of the primary accounting server.
acctport	Enter the port number for the primary accounting server.
acctsecret	Enter a string value for the authentication secret.
secondary-radius-acct	Configure the secondary RADIUS accounting server.
acctserver	Enter the IP address of the secondary accounting server.
acctport	Enter the port number for the secondary accounting server.
acctsecret	Enter a string value for the authentication secret.

Example

The following example command sets the WPA2 authentication mode with the specified details of encryption type, primary RADIUS server, and primary accounting server:

```
#kcli> config wireless interface wifi0 mode ap master security-mode wpa2 enc-type both
primary-radius authserver 10.0.0.1 authport 1812 authsecret secret1 primary-radius-acct
acctserver 10.0.1.2 acctport 46 acctsecret acctsecret1 <enter>
```

Note The accounting server fields are optional for both the primary as well as secondary RADIUS server configuration.

wpa

Description

The wpa configures the WPA security mode. Wi-Fi Protected Access (WPA), a new security standard built upon WEP, is an encryption method used to encrypt the traffic on the network. It provides more advanced protection to the traffic than WEP. It works with Pre-Shared Key (PSK) to decrypt the transmitted data at the receiving end. Also as per WPA, it is mandatory to enter enter a user name and password before connecting to the wireless network.

Parent

kcli/config/wireless/interface/mode/ap/security-mode

Syntax

```
wpa { enc-type tkip | aesCcmp | both } [ primary-radius { authserver < ip_address ipaddress
> } { authport < port integer > } { authsecret < secret string > } ] [ secondary-radius {
authserver < ip_address ipaddress > } { authport < port integer > } { authsecret < secret
string > } ] [ primary-radius-acct { acctserver < ip_address ipaddress > } { acctport <
port integer > } { acctsecret < secret string > } ] [ secondary-radius-acct { acctserver <
ip_address ipaddress > } { acctport < port integer > } { acctsecret < secret string > } ]
```

Parameter Description

Parameter	Description
enc-type	Select the encryption type, TKIP, AESCCMP or both, for the WPA security mode. Encryption type is the algorithm to be used for encrypting the data transmitted between the AP and the client.
tkip	Select Temporal Key Integrity Protocol (TKIP) as encryption type. TKIP is a security protocol used in Wi-Fi protected access and is designed to replace WEP without replacing the legacy hardware.
aesCcmp	Select AESCCMP as encryption type. Advanced Encryption Standard-Counter Mode (AES) is a symmetric 128-bit block data encryption technique that works at multiple network layers simultaneously. In Cipher Block Chaining Message Authentication Code Protocol (CCMP), unlike TKIP, key management and message integrity is handled by a single component built around AES.
both	Use both TKIP and AESCCMP encryption types.
primary-radius	Configure the primary RADIUS authentication server. Remote Authentication Dial-In User Service (RADIUS) is an authentication and accounting system used by many ISPs. While dialing the ISP you must enter your user name and password. This information is passed to a RADIUS server, which verifies whether the information is correct and then authorizes the access to the ISP server. WPA/WPA2 is designed for use with an IEEE 802.1X authentication server, which distributes different keys to each user.
authserver	Enter the IP address of the primary authentication server.
authport	Enter the primary server port number.
authsecret	Enter a string value for the authentication secret.
secondary-radius	Configure the secondary RADIUS server.
authserver	Enter the IP address of the secondary authentication server.
authport	Enter the secondary server port number.
authsecret	Enter a string value for the authentication secret.
primary-radius-acct	Configure the primary RADIUS accounting server.
acctserver	Enter the IP address of the primary accounting server.
acctport	Enter the port number for the primary accounting server.
acctsecret	Enter a string value for the authentication secret.
secondary-radius-acct	Configure the secondary RADIUS accounting server.
acctserver	Enter the IP address of the secondary accounting server.
acctport	Enter the port number for the secondary accounting server.
acctsecret	Enter a string value for the authentication secret.

Example

The following example command sets the WPA authentication mode with the specified details of encryption type, primary RADIUS server, and primary accounting server:

```
#kcli> config wireless interface wifi0 mode ap master security-mode wpa enc-type tkip
primary-radius authserver 10.0.0.1 authport 1812 authsecret secret1 primary-radius-acct
acctserver 10.0.1.2 acctport 46 acctsecret acctsecret1 <enter>
```

Note The accounting server fields are optional for both the primary as well as secondary RADIUS server configuration.

wpa-psk

Description

The `wpa-psk` command configures the WPA-PSK security mode. Wi-Fi Protected Access-Pre-shared Key (WPA-PSK) is based on the WEP and requires a key to be entered on both the access point and the client. In order to connect to the network, same key is required for the AP and the client. WpaPsk uses a pass-phrase that is between 8 to 63 characters and provides 128-bit encryption to further secure the wireless network.

Parent

kcli/config/wireless/interface/mode/ap/security-mode

Syntax

```
wpa-psk { { wpa-passphrase < wpspass string(1:32) > } | { wpa-hex < wpahex hex(64:64) > } }
```

Parameter Description

Parameter	Description
wpa-passphrase	Enter a pass-phrase string between 8 to 63 characters for the WPA-PSK security mode.
wpa-hex	Enter a pass-phrase hexadecimal value for the WPA-PSK security mode.

Example

The following example command sets the WPA-PSK security mode with the specified WPA passphrase and the AESCCMP encryption type:

```
#kcli> config wireless interface wifi0 mode ap master security-mode wpa-psk wpa-passphrase
wpapp enc-type aesCcmp <enter>
```

wpa2-psk

Description

The `wpa2-psk` command configures the WPA2-PSK security mode that is based on the WPA-PSK.

Parent

kcli/config/wireless/interface/mode/ap/security-mode

Syntax

```
wpa2-psk { { wpa2-passphrase < wpspass string(1:32) > } | { wpa2-hex < wpahex hex(64:64) >
} }
```

Parameter Description

Parameter	Description
wpa2-passphrase	Enter the pass-phrase for WPA2-PSK mode.
wpa2-hex	Enter a pass-phrase hexadecimal value for the WPA2-PSK security mode.

Example

The following example command sets the WPA2-PSK security mode with the specified WPA2 passphrase and both the AESCCMP and TKIP encryption types:

```
#kcli> config wireless interface wifi0 mode ap master security-mode wpa2-psk wpa2-hex
wpa2hex enc-type both <enter>
```

wpa-psk-mixed

Description

The `wpa-psk-mixed` command configures the WPA and WPA-PSK mixed mode.

Parent

kcli/config/wireless/interface/mode/ap/security-mode

Syntax

```
{ { wpa-mixed-passphrase < wpapass string(8:63) > } | { wpa-mixed-hex < wpahex hex(64:64) >
} } { enc-type tkip | aesCcmp | both }
```

Parameter Description

Parameter	Description
wpa-mixed-passphrase	Enter the pass-phrase for WPA-PSK mixed mode.
wpa-mixed-hex	Enter a pass-phrase hexadecimal value for the WPA-PSK mixed mode.
enc-type	Select the encryption type, TKIP, AESCCMP or both, for the WPA-PSK mixed mode. Encryption type is the algorithm to be used for encrypting the data transmitted between the AP and the client.
tkip	Select TKIP as encryption type. Temporal Key Integrity Protocol (TKIP) is a security protocol used in Wi-Fi protected access and is designed to replace WEP without replacing the legacy hardware.
aesCcmp	Select AESCCMP as encryption type. Advanced Encryption Standard-Counter Mode (AES) is a symmetric 128-bit block data encryption technique that works at multiple network layers simultaneously. In Cipher Block Chaining Message Authentication Code Protocol (CCMP), unlike TKIP, key management and message integrity is handled by a single component built around AES.
both	Use both TKIP and AESCCMP encryption types.

Example

The following example command sets the WPA-PSK mixed security mode with the specified WPA-PSK passphrase with the TKIP encryption types:

```
#kcli config wireless interface wifi0 mode ap master security-mode wpa-psk-mixed wpa-mixed-
passphrase mixedpp enc-type tkip <enter>
```

wpa-mixed

Description

The `wpa-mixed` command configures the WPA mixed mode. This mode is the combination of WPA and WPA2 security modes.

Parent

kcli/config/wireless/interface/mode/ap/security-mode

Syntax

```
{ enc-type tkip | aesCcmp | both } [ primary-radius { authserver < ip_address ipaddress > }
{ authport < port integer > } { authsecret < secret string > } ] [ secondary-radius {
authserver < ip_address ipaddress > } { authport < port integer > } { authsecret < secret
string > } ] [ primary-radius-acct { acctserver < ip_address ipaddress > } { acctport <
port integer > } { acctsecret < secret string > } ] [ secondary-radius-acct { acctserver <
ip_address ipaddress > } { acctport < port integer > } { acctsecret < secret string > } ]
```

Parameter Description

Parameter	Description
enc-type	Select the encryption type, TKIP, AESCCMP or both, for the WPA security mode. Encryption type is the algorithm to be used for encrypting the data transmitted between the AP and the client.
tkip	Select TKIP as encryption type. Temporal Key Integrity Protocol (TKIP) is a security protocol used in Wi-Fi protected access and is designed to replace WEP without replacing the legacy hardware.
aesCcmp	Select AESCCMP as encryption type. Advanced Encryption Standard-Counter Mode (AES) is a symmetric 128-bit block data encryption technique that works at multiple network layers simultaneously. In Cipher Block Chaining Message Authentication Code Protocol (CCMP), unlike TKIP, key management and message integrity is handled by a single component built around AES.
both	Use both TKIP and AESCCMP encryption types.
primary-radius	Configure the primary RADIUS authentication server. Remote Authentication Dial-In User Service (RADIUS) is an authentication and accounting system used by many ISPs. While dialing the ISP you must enter your user name and password. This information is passed to a RADIUS server, which verifies whether the information is correct and then authorizes the access to the ISP server. WPA/WPA2 is designed for use with an IEEE 802.1X authentication server, which distributes different keys to each user.
authserver	Enter the IP address of the primary authentication server.
authport	Enter the primary server port number.
authsecret	Enter a string value for the authentication secret.
secondary-radius	Configure the secondary RADIUS server.
authserver	Enter the IP address of the secondary authentication server.
authport	Enter the secondary server port number.
authsecret	Enter a string value for the authentication secret.
primary-radius-acct	Configure the primary RADIUS accounting server.
acctserver	Enter the IP address of the primary accounting server.
acctport	Enter the port number for the primary accounting server.
acctsecret	Enter a string value for the authentication secret.
secondary-radius-acct	Configure the secondary RADIUS accounting server.
acctserver	Enter the IP address of the secondary accounting server.
acctport	Enter the port number for the secondary accounting server.
acctsecret	Enter a string value for the authentication secret.

Example

The following example command sets the WPA mixed authentication mode with the specified details of encryption type, primary RADIUS server, and primary accounting server:

```
#kcli> config wireless interface wifi0 mode ap master security-mode wpa-mixed enc-type tkip
primary-radius authserver 127.0.0.1 authport 1812 authsecret secret1 primary-radius-acct
acctserver 127.0.1.2 acctport 46 acctsecret acctsecret1 <enter>
```

Note The accounting server fields are optional for both the primary as well as secondary RADIUS server configuration.

none

Description

The `none` command disables any encryption set on the wireless network.

Parent

kcli/config/wireless/interface/mode/ap/security-mode

Syntax

```
none
```

Example

The following example command sets no encryption type for the master mode:

```
#kcli> config wireless interface wifi0 mode ap master security-mode none <enter>
```

commit

Description

The `commit` command applies the changes to the selected interface.

Parent

kcli/config/wireless/interface/mode/ap

Syntax

```
commit
```

Example

The following example command applies the changes done in the AP mode to the wifi0 interface:

```
#kcli> config wireless interface wifi0 mode ap master commit <enter>
```

ssid-in-beacon

Description

The `ssid-in-beacon` command enables or disables the SSID broadcast in beacon.

Parent

kcli/config/wireless/interface/mode/ap

Syntax

```
ssid-in-beacon { enable | disable }
```

Parameter Description

Parameter	Description
enable	Enable the SSID broadcast in beacon, if you want the broadcast to be discovered by the stations.
disable	Disable the SSID broadcast to prevent the broadcast of the device be discovered by any stations/clients. Only clients that know the SSID of the device can connect to it, by explicitly setting the SSID to connect to their wireless setting.

Example

The following example command enables the SSID broadcast in beacon. If enabled, the SSID broadcast is discovered by the stations:

```
#kcli> config wireless interface wifi0 mode ap master ssid-in-beacon enable <enter>
```

beacon-interval

Description

The `beacon-interval` command specifies the beacon interval value (in milliseconds). Beacons are packets sent by an AP to synchronize a wireless network. Enter the beacon interval value between 1 and 1000 milliseconds. The recommended value is 100.

Parent

kcli/config/wireless/interface/mode/ap

Syntax

```
beacon-interval < bintval integer(1:256) >
```

Example

The following example command sets the beacon interval to 100 milliseconds. Thus, before a station enters the power save mode, it will wait for 100 milliseconds (time between beacon transmissions) to know when to wake up to receive the beacon:

```
#kcli> config wireless interface wifi0 mode ap master beacon-interval 100 <enter>
```

tx-power-limit

Description

The `tx-power-limit` enables or disables the Tx antenna power limit feature. You can also set the value for the same. Tx stands for the wireless message integrity code transmitter.

Parent

kcli/config/wireless/interface/mode/ap

Syntax

```
tx-power-limit { disable | { enable power < tx_pw integer(1:100) > } }
```

Parameter Description

Parameter	Description
enable	Disable Tx antenna.
disable	Enable Tx antenna.
power	Enter the Tx antenna power limit value between 1 and 100.

Example

The following example command enables the Tx antenna power limit feature. Here, the power limit is 100:

```
#kcli> config wireless interface wifi0 mode ap master tx-power-limit enable power 100
<enter>
```

ack-timeout

Description

The `ack-timeout` command sets the acknowledgement timeout period. Ack timeout is the delay that is expected before the AP receives an acknowledgement for the associated station. A value of 0 causes the station to continuously get disassociated and request for an association. Enter the acknowledgement timeout value between 1 and 100 milliseconds.

Parent

kcli/config/wireless/interface/mode/ap

Syntax

```
ack-timeout < acktimeout integer(1:100) >
```

Example

The following example command sets the delay period before the acknowledgement is received from the associated station for 100 milliseconds:

```
#kcli> config wireless interface wifi0 mode ap master ack-timeout 100 <enter>
```

rts-threshold

Description

The `rts-threshold` command sets the RTS threshold value for the wireless interface. Request to Send (RTS) controls the data packet size threshold. Enter the RTS threshold value (in bytes). If you encounter an inconsistent data flow, only minor modifications to the value range between 256 and 2432 (in bytes) are recommended.

Parent

kcli/config/wireless/interface/mode/ap

Syntax

```
rts-threshold { off | < rts integer(1:255) > }
```

Parameter Description

Parameter	Description
off	Disable the RTS threshold.

Example

The following example command sets the RTS threshold value to 2346 bytes:

```
#kcli config wireless interface wifi0 mode ap master rts-threshold 2346 <enter>
```

frag-threshold

Description

The `frag-threshold` command sets the fragmentation threshold value for the data packets. A packet exceeding the size limit specified by the network medium is broken into serveral segments. The fragmentation threshold defines the number of bytes used for the fragmentation boundary for directed messages. If you experience a high packet error rate, you may slightly decrease the fragmentation value within the value range of 1500 to 2346. Setting the fragmentation value too low, while the packet error rate is low, may result in a poor wireless performance. Lowering the threshold adds protocol overhead and reduces protocol efficiency. Enter the fragmentation threshold value in bytes.

Parent

kcli/config/wireless/interface/mode/ap

Syntax

```
frag-threshold { off | < frag integer(256:2346) > }
```

Parameter Description

Parameter	Description
off	Disable the fragmentation threshold.

Example

The following example command sets the fragmentation threshold value to 2346 bytes:

```
#kcli config wireless interface wifi0 mode ap master fragmentation-threshold 2346 <enter>
```

80211e

Description

The `80211e` command enables or disables the 802.11e Prioritization for the wireless interface. 802.11e Prioritization is a wireless draft standard that defines a set of Quality of Service enhancements for LAN applications, in particular the 802.11 Wi-Fi standard. This standard is considered of critical importance for delay-sensitive applications, such as Voice over Wireless IP and Streaming Multimedia. The protocol enhances the IEEE 802.11 Media Access Control (MAC) layer.

Parent

kcli/config/wireless/interface/mode/ap

Syntax

```
80211e { enable | disable }
```

Parameter Description

Parameter	Description
enable	Enable the 802.11e Prioritization to prioritize the voice data. This causes the VoIP packets (SIP protocol and RTP/RTCP) to have priority over the other web traffic such as FTP and HTTP.
disable	Disable 802.11e Prioritization to deactivate the voice data.

Example

The following example command enables the 802.11e voice prioritization. As a result, the VoIP packets will be given priority over the other web traffic:

```
#kcli> config wireless interface wifi0 mode ap master 80211e enable <enter>
```

client

Description

The `client` command sets the client mode for the specified wireless interface.

Parent

kcli/config/wireless/interface/mode

Syntax

```
client
```

Parameter Description

Parameter	Description
managed	Select the managed (client) mode. In the client mode, the box is able to connect to another AP.

Note If you select the client mode, ensure that you have set the radio interface to managed mode for the client mode to take effect.

security-mode

Description

The `security-mode` major command configures the security settings for the managed/client mode. The major command sets the WPS configuration for the wireless interface. Wi-Fi Protected Setup (WPS) is a standard for easy and secure establishment of a wireless home network. This protocol simplifies the process of configuring security on the wireless network.

Parent

kcli/config/wireless/interface/mode/client

Syntax

```
security-mode
```

key-management

Description

The `key-management` command sets the authentication mode for key management, open or restricted.

Parent

kcli/config/wireless/interface/mode/client/security-mode

Syntax

```
key-management { open | restricted }
```

Parameter Description

Parameter	Description
open	Select the open key authentication. With this mode, the client device can complete the authentication and associate with the AP. However, the use of WEP prevents the client from sending data to and receiving data from the AP, unless the client has the correct WEP key.
restricted	Select the restricted key authentication. With this mode, the AP sends the client device a challenge text packet that the client must encrypt with the correct WEP key and return to the AP. If the client has the wrong key or no key, the authentication fails and the client is not allowed to associate with the AP. Restricted key authentication is not considered secure, because a hacker who detects both the clear-text challenge and the same challenge encrypted with a WEP key, can decipher the WEP key.

Example

The following example command sets open key authentication for client mode:

```
#kcli> config wireless interface wifi0 mode client managed security-mode key-management
open <enter>
```

wpa-psk

Description

The `wpa-psk` command configures the WPA-PSK security mode. Wi-Fi Protected Setup-Pre-shared Kdy (WPA-PSK) is based on the WEP and requires a key to be entered on both the access point and the client. This key must be the same on both, only then you are allowed to connect to the network. WPA-PSK uses a pass-phrase that is between 8 to 63 characters and provides 128-bit encryption to further secure the wireless network.

Parent

kcli/config/wireless/interface/mode/client/security-mode

Syntax

```
wpa-psk { { wpa-passphrase < wpspass string(1:32) > } | { wpa-hex < wpahex hex(64:64) > } }
```

Parameter Description

Parameter	Description
wpa-passphrase	Enter a pass-phrase string between 8 to 63 characters for the WPA-PSK security mode.
wpa-hex	Enter a pass-phrase hexadecimal value for the WPA-PSK security mode.

Example

The following example command sets the WPA-PSK security mode with the specified WPA passphrase and the AESCCMP encryption type:

```
#kcli> config wireless interface wifi0 mode client managed security-mode wpa-psk wpa-passphrase wpapp enc-type aesCcmp <enter>
```

wpa2-psk

Description

The `wpa2-psk` command configures the WPA2-PSK security mode that is based on the WPA-PSK.

Parent

kcli/config/wireless/interface/mode/client/security-mode

Syntax

```
wpa2-psk { { wpa2-passphrase < wpspass string(1:32) > } | { wpa2-hex < wpahex hex(64:64) > } }
```

Parameter Description

Parameter	Description
wpa2-passphrase	Enter the pass-phrase for WPA2-PSK mode.
wpa2-hex	Enter a pass-phrase hexadecimal value for the WPA2-PSK security mode.

Example

The following example command sets the WPA2-PSK security mode with the specified WPA2 passphrase and both the AESCCMP and TKIP encryption types:

```
#kcli> config wireless interface wifi0 mode client managed security-mode wpa2-psk wpa2-hex wpa2hex enc-type both <enter>
```

wep

Description

The `wep` command configures the WEP security mode. WEP is the oldest encryption method for the wireless network. It encrypts the traffic on the network so that a hacker can not understand the transmitted data. A key or password is required to decrypt this data at the receiving end. This security mode encrypts the data using 40 bits of the secret WEP key and random 24 bits.

Parent

kcli/config/wireless/interface/mode/client/security-mode

Syntax

```
wep { [ key-length { { 64 { [ wep-key1 { ascii | hex } < wepkey1 string(1:32) > ] [ wep-key2 { ascii | hex } < wepkey2 string(1:32) > ] [ wep-key3 { ascii | hex } < wepkey3 string(1:32) > ] [ wep-key4 { ascii | hex } < wepkey4 string(1:32) > ] } } | { 128 { [ wep-key1 { ascii | hex } < wepkey1 string(1:32) > ] [ wep-key2 { ascii | hex } < wepkey2 string(1:32) > ] [ wep-key3 { ascii | hex } < wepkey3 string(1:32) > ] [ wep-key4 { ascii | hex } < wepkey4 string(1:32) > ] } } } ] [ { default-key1 | default-key2 | default-key3 | default-key4 } ] }
```

Parameter Description

Parameter	Description
key-length	Set the WEP key length, 128-bit or 64-bit. Keys are used to control the operation of a cipher so that only the correct key can convert an encrypted text to plain text. The key length is a measure of the number of possible keys which can be used in a cipher and is usually specified in bits. The key length is critical in determining the susceptibility of a cipher to exhaustive search attacks. A key should be large enough to repel a brute force attack (possible against any encryption algorithm).
64	Set the WEP key length to 64 (bits).
wep-key1	Set the WEP key 1 in either ASCII or hex.
ascii	Set the key in ASCII (5 values).
hex	Set the key in hex (10 values).
wep-key2	Set the WEP key 2.
ascii	Set the key in ASCII (5 values).
hex	Set the key in hex (10 values).
wep-key3	Set the WEP key 3.
ascii	Set the key in ASCII (5 values).
hex	Set the key in hex (10 values).
wep-key4	Set the WEP key 4.
ascii	Set the key in ASCII (5 values).
hex	Set the key in hex (10 values).
128	Set the WEP key length to 128 (bits).
wep-key1	Set the WEP key 1 in either ASCII or hex.
ascii	Set the key in ASCII (5 values).
hex	Set the key in hex (10 values).
wep-key2	Set the WEP key 2.
ascii	Set the key in ASCII (5 values).
hex	Set the key in hex (10 values).
wep-key3	Set the WEP key 3.
ascii	Set the key in ASCII (5 values).
hex	Set the key in hex (10 values).
wep-key4	Set the WEP key 4.
ascii	Set the key in ASCII (5 values).
hex	Set the key in hex (10 values).
default-key1	Set the WEP key 1 as default key.
default-key2	Set the WEP key 2 as default key.
default-key3	Set the WEP key 3 as default key.
default-key4	Set the WEP key 4 as default key.

Example

The following example command sets WEP key authentication with a key length of 128 bits in ASCII:

```
#kcli> config wireless interface wifi0 mode client managed security-mode wep key-length 128
ascii wep-key1 defaultwepkey1 <enter>>
```

Note The values of the WEP keys are:
64-bit hex key: 10 hexadecimal digits, for example, secretkey1.
64-bit ASCII key: 5 characters, for example, pjohn.
128-bit hex key: 26 hexadecimal digits, for example, abcde1234567890abcde1234567890123456.
128-bit ASCII key: 13 characters, for example, secretwepkey1.

wpa2

Description

The `wpa2` command configures the WPA2 security mode. WPA2 is the advanced version of WPA security mode.

Parent

kcli/config/wireless/interface/mode/client/security-mode

Syntax

```
wpa2 certificate-description < description string(1:32) > { enc-type tkip | aesCcmp | both
}
```

Parameter Description

Parameter	Description
enc-type	Select the encryption type, TKIP, AESCCMP or both, for the WPA security mode. Encryption type is the algorithm to be used for encrypting the data transmitted between the AP and the client.
tkip	Select TKIP as encryption type. Temporal Key Integrity Protocol (TKIP) is a security protocol used in Wi-Fi protected access and is designed to replace WEP without replacing the legacy hardware.
aesCcmp	Select AESCCMP as encryption type. Advanced Encryption Standard-Counter Mode (AES) is a symmetric 128-bit block data encryption technique that works at multiple network layers simultaneously. In Cipher Block Chaining Message Authentication Code Protocol (CCMP), unlike TKIP, key management and message integrity is handled by a single component built around AES.
both	Use both TKIP and AESCCMP encryption types.

Example

The following example command sets the WPA2 authentication mode with the specified encryption type:

```
#kcli> config wireless interface wifi0 mode client managed security-mode wpa2 enc-type both
<enter>
```

wpa

Description

The `wpa` command configures the WPA security mode. Wi-Fi Protected Access (WPA), a new security standard build upon WEP, is an encryption method used to encrypt the traffic on the network and provides more advanced protection to the traffic than WEP. It works with Pre-Shared Key (PSK) to decrypt the transmitted data at the receiving end. It also makes it mandatory that you enter a user name and password before connecting to the wireless network.

Parent

kcli/config/wireless/interface/mode/client/security-mode

Syntax

```
wpa certificate-description < description string(1:32) > { enc-type tkip | aesCcmp | both }
```

Parameter Description

Parameter	Description
certificate-description	Enter the WPA-EAP certificate description for the client.
enc-type	Select the encryption type, TKIP, AESCCMP or both, for the WPA security mode. Encryption type is the algorithm to be used for encrypting the data transmitted between the AP and the client.
tkip	Select TKIP as encryption type. Temporal Key Integrity Protocol (TKIP) is a security protocol used in Wi-Fi protected access and is designed to replace WEP without replacing the legacy hardware.
aesCcmp	Select AESCCMP as encryption type. Advanced Encryption Standard-Counter Mode (AES) is a symmetric 128-bit block data encryption technique that works at multiple network layers simultaneously. In Cipher Block Chaining Message Authentication Code Protocol (CCMP), unlike TKIP, key management and message integrity is handled by a single component built around AES.
both	Use both TKIP and AESCCMP encryption types.

Example

The following example command sets the WPA authentication mode with the specified encryption type:

```
#kcli> config wireless interface wifi0 mode client managed security-mode wpa enc-type tkip
<enter>
```

none

Description

The `none` command sets no encryption on the wireless network.

Parent

kcli/config/wireless/interface/mode/client/security-mode

Syntax

```
none
```

Example

The following example command sets no encryption type for the master mode:

```
#kcli> config wireless interface wifi0 mode client managed security-mode none <enter>
```

commit

Description

The `commit` command applies the changes to the selected interface.

Parent

kcli/config/wireless/interface/mode/client/security-mode

Syntax

```
commit
```

Example

The following example command applies the changes done in the client mode to the wifi0 interface:

```
#kcli> config wireless interface wifi0 mode client managed commit <enter>
```

wps

Description

The `wps` major command sets the WPS configuration for the wireless interface. Wi-Fi Protected Setup (WPS) is a standard for easy and secure establishment of a wireless home network. This protocol simplifies the process of configuring security on the wireless network.

Parent

kcli/config/wireless/interface

Syntax

```
wps
```

config-method

Description

The `config-method` command sets the configuration method (PIN or PBC) to enable WPS on the wireless network.

Parent

kcli/config/wireless/interface/wps

Syntax

```
config-method { { pin < pin integer(00000000:99999999) > } | pbc }
```

Parameter Description

Parameter	Description
pin	Select the PIN method for WPS. For usability and security of the wireless network, WPS implements the PIN method that enables user to establish a home network. PIN is the Personal Identification Number method, in which a PIN has to be taken either from a sticker lable or from the web interface of the WPS device. This PIN is then entered in the AP or client WPS device to connect. Enter the 8-digit PIN to activate WPS using PIN configuration method.
pbc	Select the Push Button Configuration (PBC) method, in which user pushes a button (either an actual or virtual one) on the registrar (usually the AP) and on the enrollee (a laptop, cell phone etc.). The WPS then connects to the correct AP and retrieves the encryption settings.

Example

The following example command sets the PIN configuration method using the 8-digit PIN number (94339898) to enable WPS on the wifi0 interface:

```
#kcli> config wireless interface wifi0 wps config-method 94339898 <enter>
```

wmm

Description

The `wmm` command configures the WMM parameters for the selected wireless interface. The Wireless Multimedia (WMM) feature helps you to control the multimedia traffic on the shared network connections. The gateway device follows the WMM specification standards, which are implementations of a subset of the 802.11e features. Enable or disable the WMM on the wireless interface.

Parent

kcli/config/wireless/interface

Syntax

```
wmm { enable | disable }
```

Parameter Description

Parameter	Description
enable	Enable WMM to use the multimedia over the wireless network.
disable	Disable WMM on the network.

Example

The following example command enables the WMM on the wifi0 interface:

```
#kcli> config wireless interface wifi0 wmm <enter>
```

accesscategory

Description

The `accesscatagory` major command sets the access category for multimedia content for the wireless interface. The voice and video (VO and VI) type of access category fall under high-priority traffic whereas best effort and background (BE and BK) type of data is considered medium priority by the wireless network.

Parent

kcli/config/wireless/interface/wmm

Syntax

```
accesscategory
```

Example

The following example command sets various WMM access category parameters such as BE, BK, VI, and VO:

```
#kcli wireless interface wifi0 wmm accesscategory <enter>
```

BE

Description

The BE command sets the best effort category for the wireless interface. In a best effort network, all users obtain best effort service, that is, they obtain unspecified variable bit rate and delivery time, depending on the current traffic load.

Parent

kcli/config/wireless/interface/wmm/accesscategory

Syntax

```
BE [ aifsn < beaifsn integer > ] [ cwmax < becwmax integer > ] [ cwmin < becwmin integer > ] [ txoplimit < betxlimit integer > ] [ acm { enable | disable } ] [ ack { noAck | immediateAck } ]
```

Parameter Description

Parameter	Description
aifsn	Set the AIFS period for BE. The back-off timing for each access category consists of a fixed period called the Arbitrary Inter-Frame Space (AIFS) Number. This is followed by a random period called the Contention Window. Enter AIFS number for BE.
cwmax	Set the upper limit for the doubling of the random back-off. Contention window refers to the random back-off timer used by the AP. The period set through the contention window minimum and the contention window maximum is the wait time period for the AP before attempting to access a channel again. If the AP fails to transfer the data frame in the first random back-off time, then it increments the re-try counter and keeps doubling the random back-off window. Enter the contention window maximum size.
cwmin	Set the contention window minimum size. The contention window minimum size is the upper limit used by the AP for the initial back-off wait time.
txoplimit	Set the transmission opportunity limit for the 802.11g hardware mode. Transmission opportunity (TXOP) is the time period used by the multimedia stations to transmit the packets on to the wireless network. Enter the TXOP limit.
acm	Enable or disable the ACM property for BE category. Access Control Mandatory (ACM) indicates whether admission control is mandatory for the Access Category.
enable	Enable ACM if you want to make the admission control mandatory for the BE access category.
disable	Disable ACM if you do not want to make the admission control mandatory for the BE access category.
ack	Set the acknowledgement policy (noAck, or immediateAck). This refers to the acknowledgment by the receiver after it receives the multimedia packets from the wireless interface.
noAck	Set the acknowlegement policy to noAck, if you do not want to get the acknowledgement of multimedia packets.
immediateAck	Set the acknowlegement policy to immediately receive the acknowledgement of multimedia packets from the receiver.

Example

The following example command sets specified parameters for the BE access category:

```
#kcli> config wireless interface wifi0 wmm accesscategory BE aifsn 1024 cwmax 1024 cwmin 1024 txoplimit 1024 acm enable ack immediateAck <enter>
```

BK

Description

The BK command sets the background category for the WMM. The background processes may refer to daemon processes that offer services like web pages serving, e-mail transferring, time synchronization, and other similar services.

Parent

kcli/config/wireless/interface/wmm/accesscategory

Syntax

```
BK [ aifsn < bkaifsn integer > ] [ cwmax < bkcwmax integer > ] [ cwmin < bkcwmin integer > ] [ txoplimit < bktxlimit integer > ] [ acm { enable | disable } ] [ ack { noAck | immediateAck } ]
```

Parameter Description

Parameter	Description
aifsn	Set the AIFS period for BK. The back-off timing for each access category consists of a fixed period called the Arbitrary Inter-Frame Space (AIFS) Number. This is followed by a random period called the Contention Window. Enter AIFS number for BK.
cwmax	Set the upper limit for the doubling of the random back-off. Contention window refers to the random back-off timer used by the AP. The period set through the contention window minimum and the contention window maximum is the wait time period for the AP before attempting to access a channel again. If the AP fails to transfer the data frame in the first random back-off time, then it increments the re-try counter and keeps doubling the random back-off window. Enter the contention window maximum size.
cwmin	Set the contention window minimum size. The contention window minimum size is the upper limit used by the AP for the initial back-off wait time.
txoplimit	Set the transmission opportunity limit for the 802.11g hardware mode. Transmission opportunity (TXOP) is the time period used by the multimedia stations to transmit the packets on to the wireless network. Enter the TXOP limit.
acm	Enable or disable the ACM property for BK category. Access Control Mandatory (ACM) indicates whether admission control is mandatory for the Access Category.
enable	Enable ACM if you want to make the admission control mandatory for the BK access category.
disable	Disable ACM if you do not want to make the admission control mandatory for the BK access category.
ack	Set the acknowledgement policy (noAck, or immediateAck). This refers to the acknowledgment by the receiver after it receives the multimedia packets from the wireless interface.
noAck	Set the acknowlegement policy to noAck, if you do not want to get the acknowledgement of multimedia packets.
immediateAck	Set the acknowlegement policy to immediately receive the acknowledgement of multimedia packets from the receiver.

Example

The following example command sets the specified parameters for the BK access category:

```
#kcli> config wireless interface wifi0 wmm accesscategory BK aifsn 1024 cwmax 1024 cwmin 1024 txoplimit 1024 acm enable ack noAck <enter>
```

VI

Description

The `VI` command sets the video category for the WMM.

Parent

kcli/config/wireless/interface/wmm/accesscategory

Syntax

```
VI [ aifsn < viaifsn integer > ] [ cwmax < vicwmax integer > ] [ cwmin < vicwmin integer > ] [ txoplimit < vitxlimit integer > ] [ acm { enable | disable } ] [ ack { noAck | immediateAck } ]
```

Parameter Description

Parameter	Description
aifsn	Set the AIFS period for VI. The back-off timing for each access category consists of a fixed period called the Arbitrary Inter-Frame Space (AIFS) Number. This is followed by a random period called the Contention Window. Enter AIFS number for BE.
cwmax	Set the upper limit for the doubling of the random back-off. Contention window refers to the random back-off timer used by the AP. The period set through the contention window minimum and the contention window maximum is the wait time period for the AP before attempting to access a channel again. If the AP fails to transfer the data frame in the first random back-off time, then it increments the re-try counter and keeps doubling the random back-off window. Enter the contention window maximum size.
cwmin	Set the contention window minimum size. The contention window minimum size is the upper limit used by the AP for the initial back-off wait time.
txoplimit	Set the transmission opportunity limit for the 802.11g hardware mode. Transmission opportunity (TXOP) is the time period used by the multimedia stations to transmit the packets on to the wireless network. Enter the TXOP limit.
acm	Enable or disable the ACM property for VI category. Access Control Mandatory (ACM) indicates whether admission control is mandatory for the Access Category.
enable	Enable ACM if you want to make the admission control mandatory for the VI access category.
disable	Disable ACM if you do not want to make the admission control mandatory for the VI access category.
ack	Set the acknowledgement policy (noAck, or immediateAck). This refers to the acknowledgment by the receiver after it receives the multimedia packets from the wireless interface.
noAck	Set the acknowlegement policy to noAck, if you do not want to get the acknowledgement of multimedia packets.
immediateAck	Set the acknowlegement policy to immediately receive the acknowledgement of multimedia packets from the receiver.

Example

The following example command sets the specified parameters for the VI access category:

```
#kcli> config wireless interface wifi0 wmm accesscategory VI aifsn 1024 cwmax 1024 cwmin 1024 txoplimit 1024 acm enable ack noAck <enter>
```

VO

Description

The VO command sets the voice category for the WMM.

Parent

kcli/config/wireless/interface/wmm/accesscategory

Syntax

```
VO [ aifsn < voaifsn integer > ] [ cwmax < vocwmax integer > ] [ cwmin < vocwmin integer > ] [ txoplimit < votxlimit integer > ] [ acm { enable | disable } ] [ ack { noAck | immediateAck } ]
```

Parameter Description

Parameter	Description
aifsn	Set the AIFS period for VO. The back-off timing for each access category consists of a fixed period called the Arbitrary Inter-Frame Space (AIFS) Number. This is followed by a random period called the Contention Window. Enter AIFS number for BE.
cwmax	Set the upper limit for the doubling of the random back-off. Contention window refers to the random back-off timer used by the AP. The period set through the contention window minimum and the contention window maximum is the wait time period for the AP before attempting to access a channel again. If the AP fails to transfer the data frame in the first random back-off time, then it increments the re-try counter and keeps doubling the random back-off window. Enter the contention window maximum size.
cwmin	Set the contention window minimum size. The contention window minimum size is the upper limit used by the AP for the initial back-off wait time.
txoplimit	Set the transmission opportunity limit for the 802.11g hardware mode. Transmission opportunity (TXOP) is the time period used by the multimedia stations to transmit the packets on to the wireless network. Enter the TXOP limit.
acm	Enable or disable the ACM property for VO category. Access Control Mandatory (ACM) indicates whether admission control is mandatory for the Access Category.
enable	Enable ACM if you want to make the admission control mandatory for the VO access category.
disable	Disable ACM if you do not want to make the admission control mandatory for the VO access category.
ack	Set the acknowledgement policy (noAck, or immediateAck). This refers to the acknowledgment by the receiver after it receives the multimedia packets from the wireless interface.
noAck	Set the acknowlegement policy to noAck, if you do not want to get the acknowledgement of multimedia packets.
immediateAck	Set the acknowlegement policy to immediately receive the acknowledgement of multimedia packets from the receiver.

Example

The following example command sets the specified parameters for the VO access category:

```
#kcli> config wireless interface wifi0 wmm accesscategory VO aifsn 1024 cwmax 1024 cwmin 1024 txoplimit 1024 acm enable ack immediateAck <enter>
```

commit

Description

The `commit` command applies the changes to the selected interface.

Parent

kcli/config/wireless/interface/wmm/accesscategory

Syntax

```
commit
```

Example

The following example command applies the configured accesss category settings on the wifi0 interface:

```
#kcli> config wireless interface wifi0 wmm accesscategory commit <enter>
```

state

Description

The `state` command sets the WMM state on the wireless interface. Wireless Multimedia (WMM) feature helps you to control the multimedia traffic on the shared network connections.

Parent

kcli/config/wireless/interface/wmm

Syntax

```
state { enable | disable } [ uapsd { enable | disable } ]
```

Parameter Description

Parameter	Description
enable	Enable the WMM on the interface if you want to use the multimedia over the wireless network.
disable	Disable the WMM on the interface.
uapsd	Set the status of UAPSD on the wireless network. Unscheduled Automatic Power Save Delivery (UAPSD) is a feature of Wi-Fi devices that allows them to save power. UAPSD is also known as WMM power save.
enable	Enable UAPSD on the wireless network to activate the automatic power save delivery.
disable	Disable UAPSD to de-activate the automatic power save delivery.

Example

The following example command enables the WMM state on the wifi0 interface, and it also enables the UAPSD on the wifi0 interface to activate the automatic power save delivery:

```
#kcli> config wireless interface wifi0 wmm state enable uapsd enable <enter>
```

mac-acl

Description

The `mac-acl` major command sets the MAC address ACL type (blacklist, whitelist, open). MAC Address Access Control List (MAC-ACL) is a type of security feature commonly used by wireless networks. MAC-ACL restricts clients from accessing network depending upon the specified list type.

Parent

kcli/config/wireless/interface

Syntax

```
mac-acl
```

acl-type

Description

The `acl-type` command sets the ACL type for MAC address filtering, blacklist, whitelist or open.

Parent

kcli/config/wireless/interface/mac-acl

Syntax

```
acl-type { open | whitelist | blacklist }
```

Parameter Description

Parameter	Description
open	Select open to disable the MAC address filtering.
whitelist	The whitelist, also known as the Positive Security Model, is defined as deny all, allow a few. That is, deny all traffic and allow only the defined acceptable traffic. The MAC address/s that you specify under whitelist can have access to the network.
blacklist	The blacklist or the Negative Security Model is defined as allow all, deny a few. That is, allow all the traffic except for the defined bad traffic. The MAC address that you specify under blacklist is denied access to the network.

Example

The following example command sets the whitelist ACL type for MAC filtering. Thus, the MAC address mentioned under whitelist can have access to your network:

```
#kcli> config wireless interface wifi0 mac-acl acl-type whitelist <enter>
```

acl-addmac

Description

The `acl-addmac` command adds the MAC address to the Access Control List (ACL) that is either whitelist or blacklist. Enter the MAC address to add it to the ACL.

Parent

kcli/config/wireless/interface/mac-acl

Syntax

```
acl-addmac < mac_address macaddr >
```

Example

The following example command adds the specified MAC address to the ACL. This MAC address is then added to the whitelist or blacklist:

```
#kcli> config wireless interface wifi0 acl-addmac 00:b4:c7:37:e9:12 <enter>
```

acl-delmac

Description

The `acl-delmac` command deletes the MAC address from ACL. Enter the MAC address to be deleted.

Parent

kcli/config/wireless/interface/mac-acl

Syntax

```
acl-delmac < mac_address macaddr >
```

radio

Description

The `radio` major command configures the radio interface parameters such as mode (master, managed, master and managed, WDS, and Ad-hoc), admin state, channel and channel policy, hardware mode (802.11a, 802.11b and 802.11g) and country code. Enter the radio interface name to configure it.

Parent

kcli/config/wireless

Syntax

```
radio < radio strng(1:16) >
```

Example

The following example command allows you to enter the configuration mode for setting the radio configuration parameters on wlan0 interface:

```
#kcli> config wireless radio wlan0 <enter>
```

admin-state

Description

The `admin-state` command enables or disables the admin state of the radio interface.

Parent

kcli/config/wireless/radio

Syntax

```
admin-state { up | down }
```

Parameter Description

Parameter	Description
up	Select the up option to enable the admin state and run the interface.
down	Select the down option, if you do not want the interface to run. This disables the admin state of that interface.

Example

The following example command enables the admin state on the wlan0 radion interface:

```
#kcli> config wireless radio wlan0 admin-state up <enter>
```

regulatory-domain

Description

The `regulatory-domain` command sets the regulatory domain code. Enter the code value between 1 and 100.

Parent

kcli/config/wireless/radio

Syntax

```
regulatory-domain < rgdomain integer(1:100) >
```

Example

The following example command sets the regulatory domain code to 10 on the wlan0 radio interface:

```
#kcli> config wireless radio wlan0 regulatory-domain 10 <enter>
```

country-code

Description

The `country-code` command sets the country code for the interface. Enter the country code value between 0 and 999.

Parent

kcli/config/wireless/radio

Syntax

```
country-code < ccode integer(0:999) >
```

Example

The following example command sets the country code value to 112 for the wlan0 radio interface:

```
#kcli> config wireless radio wlan0 country-code 112 <enter>
```

antenna-diversity

Description

The `antenna-diversity` command enables or disables the antenna diversity property. Selecting the enable option allows the antenna to automatically switch to other antenna having better signals.

Parent

kcli/config/wireless/radio

Syntax

```
antenna-diversity { enable | disable }
```

Parameter Description

Parameter	Description
enable	Enable antenna diversity for the radio interface to switch to the antenna having better signals.
disable	Disable antenna diversity for the radio interface.

Example

The following example command enables the antenna diversity to switch to the antenna transreceiving better signals:

```
#kcli> config wireless radio wlan0 antenna-diversity enable <enter>
```

rx-antenna

Description

The `rx-antenna` command sets the Rx antenna for the wireless interface. Rx stands for the wireless message integrity code receiver.

Parent

kcli/config/wireless/interface

Syntax

```
rx-antenna { auto | one | two }
```

Parameter Description

Parameter	Description
auto	Select the auto option to automatically identify the Rx antenna for receiving the transmission.
one	Select one for Rx antenna.
two	Select two for Rx antenna.

Example

The following example command allows the device to identify the Rx antenna automatically for receiving the transmission:

```
#kcli> config wireless radio wlan0 rx-antenna auto <enter>
```

tx-antenna

Description

The `tx-antenna` command sets the Tx antenna for the wireless interface. Tx stands for the wireless message integrity code transmitter.

Parent

kcli/config/wireless/interface

Syntax

```
tx-antenna { auto | one | two }
```

Parameter Description

Parameter	Description
auto	Select the auto option to automatically identify the Tx antenna for transmission.
one	Select one for Tx antenna.
two	Select two for Tx antenna.

Example

The following example command sets antenna one for Tx antenna:

```
#kcli> config wireless radio wlan0 tx-antenna one <enter>
```

hw-mode

Description

The `hw-mode` command sets the hardware mode for the radio interface. The available hardware mode options are 802.11b and 802.11g that refer to the wireless interface support for the respective standards. Select a hardware mode for the radio interface.

Parent

kcli/config/wireless/radio

Syntax

```
hw-mode { b | g }
```

Parameter Description

Parameter	Description
b	Select the 80.11b mode (also referred to as 802.11 High Rate or Wi-Fi). This is an extension to 802.11 that applies to wireless LANS and provides 11 Mbps transmission (with a fallback to 5.5, 2 and 1 Mbps) in the 2.4 GHz channel.
g	Select the 802.11g mode. This applies to wireless LANs and provides 20+ Mbps transmission in the 2.4 GHz channel.

Example

The following example command sets the hardware mode to 802.11g:

```
#kcli> config wireless radio wlano hw-mode g <enter>
```

channel

Description

The `channel` command sets the channel policy to either fixed or auto. Channel is the route that a message follows, as it is transmitted between a communication source and a receiver. It defines a portion of the radio spectrum the radio interface uses for transmitting and receiving the data.

Parent

kcli/config/wireless/radio

Syntax

```
channel { auto | { fixed < channel_value integer(1:100) > } }
```

Parameter Description

Parameter	Description
auto	Select the auto option, if you want the device to automatically select the channel.
fixed	Select the fixed mode to define the channel frequency to be used and enter an integer for the channel value.

Example

The following example command sets the fixed mode for the wlan0 radio interface having the channel frequency of 6:

```
#kcli> config wireless radio wlan0 channel fixed 6 <enter>
```

mode

Description

The `mode` command allows you to select the wireless mode for the radio interface, AP (master), client (managed), AP and client (master and managed), WDS or ad-hoc.

Parent

kcli/config/wireless/radio

Syntax

```
mode { ap | client | ap-and-client | wds | adhoc }
```

Parameter Description

Parameter	Description
ap	Select the AP mode. In this mode a central Access Point, known as master, decides the hopping sequence.
client	Select the client mode. This mode always has a central authority in the form of an access point. Any communication happens through this central AP acting as an arbitrator in the network.
ap-and-client	Select the AP and client mode. This mode has attributes of both, master as well as managed mode.
wds	Select the WDS mode. Wireless Distribution System (WDS) mode enables Access Points to communicate with one another in order to extend the range of a wireless network.
adhoc	Select the ad-hoc mode. This provides an informal way of creating a wireless network between two or more computers without the need for a centralized AP.

Example

The following example command sets the AP and client mode having the attributes of both the master and managed modes for the wlan0 radio interface:

```
#kcli> config wireless radio wlan0 mode ap-and-client <enter>
```

ack-timeout

Description

The `ack-timeout` command sets the acknowledgement timeout period (in milliseconds) for the radio interface. Ack timeout is the delay that is expected before the AP receives an acknowledgment for the associated station. Setting the value to 0 causes the station to continuously get disassociated and request for an association.

Parent

kcli/config/wireless/radio

Syntax

```
ack-timeout < acktimeout integer(1:100) >
```

Example

The following example command sets the delay period before the acknowledgement is received from the associated station for 100 milliseconds:

```
#kcli> config wireless radio wlan0 mode ap master ack-timeout 100 <enter>
```

commit

Description

The `commit` command applies the changes to the radio interface.

Parent

kcli/config/wireless/radio

Syntax

```
commit
```

Example

The following example command applies the changes to the wlan0 radio interface:

```
#kcli> config wireless radio wlan0 commit <enter>
```

multiple-ssid

Description

The `multiple-ssid` command configures the multiple SSID for the selected radio interface. Service Set Identifier (SSID) is a unique identifier used by the wireless networking devices to establish and maintain a wireless connection.

Parent

kcli/config/wireless

Syntax

```
multiple-ssid radio < radio string >
```

Parameter Description

Parameter	Description
radio	Enter a radio interface name to configure multiple SSID for it.

add-ssid

Description

The `add-ssid` command adds the multiple SSID value on the radio interface.

Parent

kcli/config/wireless

Syntax

```
add-ssid < ssid string >
```

Example

The following example command adds the multiple SSID value (npgw) on the wlan0 radio interface:

```
#kcli> config wireless multiple-ssid radio wlan0 add-ssid npgw <enter>
```

del-ssid

Description

The `del-ssid` command deletes the multiple SSID. Enter the SSID to be deleted.

Parent

kcli/config/wireless

Syntax

```
del-ssid < ssid string >
```

pki-import

Description

The `pki-import` command configures the PKI parameters such as PKI description, certificate authority (CA) certificate name, client certificate name, client key file name and client secret to import the PKI certificate for the wireless network security. The Public Key Infrastructure (PKI) is part of the cryptography protocol that acts as a certification authority and also is an arrangement that is used widely for secure electronic communication. The gateway device uses EAP-TLS security as one of the wireless client security modes.

Parent

kcli/config/wireless

Syntax

```
pki-import import-cert server-type { tftp | http } server < server string(1:32) > [ server-path < path string(1:32) > ] certificate-description < description string(1:32) > ca-certificate < ca_certificate_file string(1:32) > client-certificate < client_certificate string(1:32) > client-private-key < private_key_file string(1:32) > private-key-password < password string >
```

Parameter Description

Parameter	Description
import-cert	Import the PKI certificate stored on the server (HTTP or TFTP).
server-type	Select the server type where the PKI certificate is stored, either TFTP or HTTP.
tftp	Select TFTP if the PKI certificate is stored on the TFTP server.
http	Select HTTP if the PKI certificate is stored on the HTTP server.
server	Enter the name or IP address of the server where the certificate is stored.
server-path	Enter the parth on the server where the certificates are stored.
certificate-description	Enter the description of the certificate to be imported.
ca-certificate	Enter the name of the CA certificate file stored on the server.
client-certificate	Enter the name of the client certificate file stored on the server.
client-private-key	Enter the name of the client private key file.
private-key-password	Enter the client private key password.

Example

The following example command imports the PKI certificates from the specified location on the HTTP server:

```
#kcli> config wireless pki-import import-cert server-type http server 192.168.0.1 server-path /root/ certificate-description pkicertificate ca-certificate caCert.pem client-certificate clientCert.pem client-private-key clientKey.pem private-key-password secret
<enter>
```

Note For creating the CA certificates use the OpenSSL utility. It is an open source implementation of the SSL and TLS protocols.

pki-remove

Description

The `pki-remove` command deletes the PKI information from the system.

Parent

kcli/config/wireless

Syntax

```
pki-remove certificate-description < description string >
```

Parameter Description

Parameter	Description
certificate-description	Enter the description of the certificate information to be deleted.

turbo-mode

Description

The `turbo-mode` command enables or disables the turbo mode for the wireless interface. Turbo mode allows transmission on two channels, which improves the data transfer rate (up to 72 Mbps).

Parent

kcli/config/wireless

Syntax

```
turbo-mode interface < interface string > { enable | disable }
```

Parameter Description

Parameter	Description
interface	Specify the interface on which you want to set the turbo mode.
enable	Enable turbo mode to increase the data transfer rate.
disable	Disable turbo mode.

Example

The following example command enables the turbo mode on the wifi0 interface:

```
#kcli> config wireless turbo-mode interface wifi0 enable <enter>
```

Software Upgrade Module

This section describes configuration commands for the software upgrade module. You can upgrade the current version of the gateway by specifying the firmware location (where the upgrade image is stored).

swupgrade

Description

The `swupgrade` command node allows you to upgrade the current version of gateway. The software upgrade can be performed from a local or remote location.

Parent

kcli/config

url

Description

The `url` command sets the location of the firmware from where it has to be upgraded. Enter the URL string where the upgrade image is stored. The available service is HTTP for which you need to authenticate by providing the user name and password.

Parent

kcli/config/swupgrade

Syntax

```
url < url string > [ mode { sync | async } ] [ username < uname string > password < pass string > ]
```

Parameter Description

Parameter	Description
mode	Select a mode for software upgrade, synchronous or asynchronous.
sync	Select the synchronous mode, if you do not want to run other applications and command prompt while software upgrade is in progress.
async	Select asynchronous mode, if you want to use command prompt while software upgrade is in progress. Software upgrade will run in background in this case.
username	Enter the user name to authenticate.
password	Enter the password for the specified user name to authenticate.

Example

The following example command sets the firmware location for upgrade:

```
#kcli> config swupgrade url http://10.32.2.21/swupgrade.img. mode sync username john password admin <enter>
```

clear-history

Description

The `clear-history` command clears the history of entire software upgrade log.

Parent

kcli/config/swupgrade

Syntax

```
clear-history
```

Topology Module

This section describes configuration commands for the topology module. You configure and view the LAN hosts on the network and their respective settings.

topology

Description

The `topology` command node allows you to enter the configuration mode for setting various parameters regarding the network topology, that is, the LAN hosts.

Parent

kcli/config

host_list

Description

The `host_list` command refreshes or clears the list of LAN hosts. You can also set the time interval (in minutes) for refreshing the host list.

Parent

kcli/config/topology

Syntax

```
host_list { refresh } | { clear } | { set_refresh_interval < refresh_time integer > } | {
set_time_limit < time_limit integer > }
```

Parameter Description

Parameter	Description
refresh	Refresh the host list.
clear	Clear the host list.
set_refresh_interval	Set the refresh time interval in minutes after which the host list is refreshed. Default value is 5 minutes.
set_time_limit	Set the time limit (in days) for which the inactive host/s should remain in the database. After the time limit is exceeded, the inactive host is automatically removed from the topology host list. Default value is 7 days.

UPnP Module

This section describes configuration commands for the UPnP module. You can enable or disable UPnP device, add/remove/blacklist LAN clients, enable or disable read-only access for TR-064 service.

upnp

Description

The UPnP commmand node allows you to enter the configuration mode for setting the UPnP parameters. Universal Plug and Play (UPnP) is a networking architecture for automatically configuring devices, discovering services, and providing peer-to-peer data transfer over an IP network. It works with wired or wireless networks and can be supported on any operating system. It also supports device-driver independence and zero-configuration networking, which implies automatic installation.

Parent

kcli/config

enable

Description

The `enable` command activates the UPnP service on the network.

Parent

kcli/config/upnp

Syntax

```
enable [ setlanif-upnp < name string(1:50) > ]
```

Parameter Description

Parameter	Description
setlaninf-upnp	Enter the LAN interface on which the UPnP service is to be enabled.

Example

The following example command sets the LAN interface eth0 as the UPnP-enabled interface:

```
#kcli> config upnp enable setlaninf-upnp eth0 <enter>
```

disable

Description

The `disable` command deactivates the UPnP service on the network.

Parent

kcli/config/upnp

Syntax

```
disable
```

blacklist

Description

The `blacklist` major command sets the IP address/es of the the LAN host/s that are to be blocked from accessing the device using the UPnP service.

Parent

kcli/config/upnp

add

Description

The `add` command configures a rule for UPnP implementation.

Parent

kcli/config/upnp

Syntax

```
add protocol-name < name string(0:50) > internalclient < name ipaddr > externalport <
port_no integer(1:32627) > internalport < port_no integer(1:32627) > portdesc < description
string(1:50) > portlease < leaseduration integer(1:32627) > portstatus { enable | disable }
```

Parameter Description

Parameter	Description
protocol-name	Enter the name of the protocol to be forwarded to the specified port on the configured internal client.
internalclient	Internal client is the LAN workstation or device, where the service is to be forwarded. Enter the IP address of the internal client where the port is to be forwarded.
externalport	Enter the external port number.
internalport	The internal port is the port on the configured internal client. The incoming request is to be forwarded to this port. Enter the internal port number.
portdesc	Port mapping is the process where packets arriving to a particular IP address/port can be translated and thus redirected to a different IP/port. This functionality is a way to create a persistent passage through NAT. Port mapping is only necessary for incoming connections, not for the returning traffic. Enter the port mapping description, such as SSH, FTP, TelNet, etc. for the UPnP rule.
portlease	Enter the port lease duration (in minutes).
portstatus	Enable or disable the port mapping for the UPnP rule.
enable	Enable port mapping to map the protocol port on the gateway to the configured internal host.
disable	Disable port mapping on the network.

Example

The following example command configures the UPnP rule on the gateway:

```
#kcli> config upnp protocol-name http internalclient 192.168.1.2 externalport 2660
internalport 8080 portdesc ssh portlease 10 portstatus enable <enter>
```

remove

Description

The `remove` command deletes an existing UPnP rule.

Parent

kcli/config/upnp

Syntax

```
remove protocol-name < name string(0:50) > internalclient < name ipaddr > externalport <
port_no integer(1:32627) > internalport < port_no integer(1:32627) >
```

Parameter Description

Parameter	Description
protocol-name	Enter the protocol name for the rule to be deleted.
internalclient	Enter the name or IP address of the internal client configured for the rule to be deleted.
externalport	Enter the external port number for the rule to be deleted.
internalport	Enter the internal port number for the internal client configured for the rule to be deleted.

log

Description

The `log` command enables or disables the logging for the UPnP service.

Parent

kcli/config/upnp

Syntax

```
log { enable | disable }
```

Parameter Description

Parameter	Description
enable	Enable UPnP logging to log the UPnP related actions and events.
disable	Disable UPnP logging, if you do not want to log UPnP related actions and events.

port_forwarding

Description

The `port_forwarding` command enables or disables port forwarding for UPnP. Port forwarding allows remote computers (such as public machines on the Internet) to connect to a specific computer within a private LAN. For example, running a public HTTP server within a private LAN (port 80), or permitting FTP access to hosts on a private LAN from the Internet (port 21).

Parent

kcli/config/upnp

Syntax

```
port_forwarding { enable | disable }
```

Parameter Description

Parameter	Description
enable	Enable port forwarding for UPnP to allow communications by external hosts using the service provided in the LAN (HTTP, FTP, SSH etc.)
disable	Disable port forwarding for UPnP, so that the external connections are no longer permitted within the LAN.

read-access

Description

The `read-access` command enables or disables read-only access to the management applications using the UPnP service actions.

Parent

kcli/config/upnp

Syntax

```
read-access { enable | disable }
```

Parameter Description

Parameter	Description
enable	Enable the read-only access for UPnP service. If enabled, the management applications can only read the UPnP data, but cannot modify it.
disable	Disable the read-only access for UPnP service. If disabled, the management applications can both read and modify the UPnP data.

stealth_mode

Description

The `stealth_mode` command enables or disables the stealth mode for UPnP.

Parent

kcli/config/upnp

Syntax

```
stealth_mode { enable | disable }
```

Parameter Description

Parameter	Description
enable	Enable stealth mode by restarting the UPnP service. When UPnP stealth mode is enabled, the UPnP service does not advertise or listen on multicast. Clients need to communicate with the gateway using unicast and must know the gateway address/ URL.
disable	Disable stealth mode for UPnP service. If disabled, the clients are able to communicate with the gateway device without knowing the actual IP address or URL.

request-limit

Description

The `request-limit` command modifies the number of SSDP packets accepted by the UPnP service per minute. Enter the number of packets between 0 and 32627.

Parent

kcli/config/upnp

Syntax

```
request-limit < limit integer(0:32627) >
```

enable

Description

The `enable` command activates the TR-064 service on the network.

Parent

kcli/config/tr64

Syntax

```
enable [ setlanif-tr64 < name string(1:50) > ]
```

Parameter Description

Parameter	Description
setlaninf-tr64	Set the LAN interface on which the TR-064 service is to be enabled.

Example

The following example command sets the LAN interface eth0 as the TR-064-enabled interface:

```
#kcli> config tr64 enable setlaning-tr64 eth0 <enter>
```

disable

Description

The `disable` command deactivates the TR-064 service on the network.

Parent

kcli/config/tr64

Syntax

```
Disable
```

blacklist

Description

The `blacklist` command sets the IP address/es of the the LAN host/s that are to be blocked from accessing the device using TR-064 service.

Parent

kcli/config/tr64

add

Description

The `add` command blacklists the LAN hosts and blocks them from accessing the TR-064-enabled devices on the network.

Parent

kcli/config/tr64/blacklist

Syntax

```
internalclient < name ipaddr >
```

Parameter Description

Parameter	Description
internalclient	Enter the IP address of the LAN host.

Example

The following example command adds the internal LAN host 192.168.1.0 to the blacklist. As a result, this LAN host will be denied access to the TR-064 enabled device:

```
#kcli> config tr64 blacklist add internalclient 192.168.1.0 <enter>"
```

delete

Description

The `delete` command deletes the LAN host from the blacklist.

Parent

kcli/config/tr64/blacklist

Syntax

```
internalclient < name ipaddr >
```

Parameter Description

Parameter	Description
internalclient	Enter the IP address of the LAN host to be deleted from the blacklist.

read-access

Description

The `read-access` command enables or disables read-only access to the management applications using the TR-064 service actions.

Parent

kcli/config/tr64

Syntax

```
read-access { enable | disable }
```

Parameter Description

Parameter	Description
enable	Enable the read-only access for the TR-064 service. If enabled, the management applications can read the TR-069 data, but cannot modify it.
disable	Disable the read-only access for TR-064 service. If disabled, the management applications can both read and modify the TR-064 data.

Example

The following example command enables the read-only access for TR-064 service. As a result, the LAN device can only view the TR-064 configuration:

```
#kcli> config tr64 read-access enable <enter>
```

User Management Module

This section describes configuration commands for the user management module. You can configure and manage the users of your device. In other words, you can add or delete the users, edit user password, and other relevant user information for the device.

usrmgmt

Description

The `usrmgmt` command node allows you to enter the configuration mode to configure and manage the users of the device. You can add or delete the users, edit user password and other relevant user information for the device.

Parent

kcli/config

add-user

Description

The `add-user` command adds a new user on the device.

Parent

kcli/config/usrmgmt

Syntax

```
add-user { user-name < usrname string(2:50) > } { password-type { blank | default | { custom { passwd < passwd password(6:50) > } { confirm-passwd < confrmpasswd password(6:50) > } [ password-hint < hint string(0:100) > ] } } } { type { { admin { role < role string(2:50) > } } | samba | ftp } } [ usr-description < usrdesc string(5:500) > ] [ e-mail < email string(5:50) > ] [ useraddress < usraddr string(5:500) > ]
```

Parameter Description

Parameter	Description
user-name	Enter the name of the user to be added.
password	Enter the password for the new user.
password-type	Select a password type, blank, default, or custom, for the new password.
blank	Select the password type blank. This does not require setting up a password for the specified user.
default	Select the default password type. This sets the default password for the specified user.
custom	Select the custom password type to be able to enter a password for the specified user. The user needs to change the default password to set it as the custom password.
confirm-password	Re-enter the password to confirm.
password-hint	Provide a hint for the new password.
type	Select a type for the new user, admin, samba or FTP.
admin	Select admin as user type.
role	Select a role for the new user. Select guest to provide restricted access, su (superuser) to provide complete read-write access, techsupport for technical support, or administrator for administrator user.
samba	Select samba as user type.
ftp	Select ftp as user type.
user-description	Enter the description for the new user (use double quotes to include spaces).
e-mail	Enter the new user's e-mail address.
useraddress	Enter the new user's address.

Example

The following example command adds a new user john with the specified parameters to the network:

```
#kcli> config usrmgmt add-user user-name john passwd abcd confirm-password abcd type samba usr-description sambauser email john@abc.org useraddress john"mainstreet"fairfax"pa
<enter>
```

Note Use double quotes to include spaces while entering the description, e-mail address and address of the new user. Also, do not type special characters while entering the password for the new user.

delete-user

Description

The `delete-user` command deletes the user on the device.

Parent

kcli/config/usrmgmt

Syntax

```
delete-user { user-name < usrname string(2:50) > }
```

Parameter Description

Parameter	Description
user-name	Enter the name of the user to be deleted.

change-password

Description

The `change-password` command changes the password of the specified user.

Parent

kcli/config/usrmgmt

Syntax

```
change-password { user-name <  usname string(2: 50) > } { password-type { blank | default |
{ custom { { new-password < newpasswd password(6:50) > } { confirm-password < conpasswd
password(6:50) > } [ password-hint < hint string(0:100) > ] } } } [ old-password < passwd
password(1:50) > ] }
```

Parameter Description

Parameter	Description
user-name	Enter the user name whose password is to be changed.
password-type	Select a password type, blank, default, or custom, for the new password.
blank	Select the password type blank. This does not require setting up a password for the specified user.
default	Select the default password type. This sets the default password for the specified user.
custom	Select the custom password type to be able to enter a password for the specified user. The user needs to change the default password to set it as the custom password.
new-password	Enter the new password for the specified user.
confirm-password	Re-enter the new password to confirm.
password-hint	Provide a hint for the new password.
old-password	Enter the old password for the specified user.

Note To enter securely, press *Enter* after the old-password, new-password, and confirm-password keywords. Also, do not insert extra white spaces, tabs or new line characters while changing the user password.

edit-user-info

Description

The `edit-user-info` command modifies the user details such as user role, e-mail address, description and address.

Parent

kcli/config/usrmgmt

Syntax

```
edit-user-info { username < usrname string(2:50) > } [ role < role string(2:50) > ] [ usr-description < usrdesc string(5:500) > ] [ e-mail < email string(5:50) > ] [ useraddress < usraddr string(5:500) > ]
```

Parameter Description

Parameter	Description
username	Enter the user name whose details are to be modified.
role	Enter the role of the specified user.
user-description	Enter the description for the specified user.
e-mail	Enter the e-mail address of the specified user.
useraddress	Enter the user address.

Note Use double quotes to include spaces while entering the description and address for the user. Also, do not type special characters other than @ while entering the email address of the user.

passwordEGST

Description

The `passwordEGST` command enables or disables the password Embedded Gateway Support Tool (EGST) function. If enabled, the user attempt to access the Internet is intercepted by the gateway. It provides a HURL page to the user to set or change the password before accessing the Internet.

Parent

kcli/config/usrmgmt

Syntax

```
passwordEGST { enable | disable }
```

Parameter Description

Parameter	Description
enable	Enable the password EGST function.
disable	Disable the password EGST function.

password-required

Description

The `password-required` command enables or disables the requirement of a password to be set to change the user management settings.

Parent

kcli/config/usrmgmt

Syntax

```
password-required { true | false }
```

Parameter Description

Parameter	Description
true	Enable the requirement of a password. If enabled, the users that have the password type as blank or default, must set or change the password for getting access to Internet. Once the new password is saved, the user is not prompted for a password while accessing Inernet.
false	Disable the requirement of a password.

reset-password

Description

The `reset-password` command resets the password for the specified user.

Parent

kcli/config/usrmgmt

Syntax

```
reset-password { user-name < usname string(2:50) > } { key-provided < keyprovided
password(8:10) > } { new-password < newpasswd password(6:50) > } { confirm-password <
conpasswd password(6:50) > } [ password-hint < hint string(0:100) > ]
```

Parameter Description

Parameter	Description
user-name	Enter the name of the user whose password is to be reset.
key-provided	Reset the password by providing any of the two keys: the default WEP key mentioned on the device, or you can obtain the key by calling the 2Wire helpdesk. Enter this key to reset the password.
new-password	Enter the new password for the specified user.
confirm-password	Re-enter the password to confirm.
password-hint	Provide a hint for the new password.

Note To enter securely, press Enter after the new-password, and confirm-password keywords.

Diagnostic Module

This section describes configuration commands for the diagnostic module. You can configure diagnostic parameters like download, upload, UDP Echo Server, ping, traceroute, nslookup, etc. The ping service in Diagnostic lets you know whether a host on the network is active/reachable, the trace route service helps you reach a particular host or network, and the NS lookup service resolves an IP address for a host name or resolves a host name for an IP address.

diagnostic

Description

The `diagnostic` command node allows you to enter the configuration mode for setting the diagnostics services for diagnosing network connection issues. These services are ping, trace route and NS lookup.

Parent

kcli/config

downloadconfig

Description

The `downloadconfig` command configures the download parameters to perform a download on gateway. You can configure interface, ethernet priority, DSCP, and URL of the source.

Parent

kcli/config/diagnostic

interface

Description

The `interface` command configures the IP layer interface parameters to perform the download.

Parent

kcli/config/diagnostic/downloadconfig

Syntax

```
interface < interfacename string > [ ethernetPriority < ethernetpriority integer(0:7) > ] [
DSCP < dscpvalue integer(0:63) > ] [ downloadURL < downloadURL string > ]
```

Parameter Description

Parameter	Description
ethernetPriority	Enter the ethernet priority for marking packets transmitted during download. Value ranges from 0 to 7.
DSCP	Enter the DiffServ value for marking packets transmitted during download. Value ranges from 0 to 63.
downloadURL	Enter the URL of the gateway to perform the download.

Example

The following example command configures the interface for the download configuration:

```
#kcli> config diagnostic downloadconfig interface eth0 ethernetPriority 1 DSCP 21
downloadURL ftp.2wire.com <enter>
```

start

Description

The `start` command starts the data download on the gateway.

Parent

kcli/config/diagnostic/downloadconfig

Syntax

```
start
```

UDPEchoServerConfig

Description

The `UDPEchoServerConfig` command configures the UDP Echo Server for echo services such as path continuity and integrity verification. With UDP Echo server, you can send and receive data packets from source address to destination address. With UDP Echo Plus server, you achieve improved monitoring capabilities, such as packet's sequence number, sequence number of incrementing packet count, reception time of echo request packet, forwarding time of echo response packet, and number of locally dropped echo response packets. You must enable the source/destination server, and then configure interface, source IP address, destination IP address and UDP port.

Parent

kcli/config/diagnostic

config

Description

The `config` command configures UDP echo server for echo services such as path continuity and integrity verification. You must enable the server, and then configure interface, source IP address, and UDP port.

Parent

kcli/config/diagnostic/UDPEchoServerConfig

Syntax

```
config interface < interfacename string(0:32) > source-ip-addr < sipaddr string(0:35) >
UDPPort < udpport integer >
```

Parameter Description

Parameter	Description
interface	Enter the IP layer interface name, which is used by the gateway to listen and receive echo request.
source-ip-addr	Enter the IP address of the UDP echo server.
UDPPort	Enter the UDP port number that is used by the gateway for listening and responding to echo requests.

Example

The following example command configures the UDP Echo server:

```
#kcli> config diagnostic UDPEchoServerConfig config interface eth0 source-ip-addr
192.168.1.254 UDPPort 137 <enter>
```

UDPEchoPlusServer

Description

The `UDPEchoPlusServer` command enables or disables the UDP Echo plus server.

Parent

kcli/config/diagnostic/UDPEchoServerConfig

enable

Description

The `enable` command enables the UDP Echo plus server for improved monitoring capabilities of echo services.

Parent

kcli/config/diagnostic/UDPEchoServerConfig/UDPEchoPlusServer

Syntax

```
enable
```

disable

Description

The `disable` command disables the UDP Echo plus server.

Parent

kcli/config/diagnostic/UDPEchoServerConfig/UDPEchoPlusServer

Syntax

```
disable
```

UDPEchoServer

Description

The `UDPEchoServer` command enables or disables the UDP Echo server.

Parent

kcli/config/diagnostic/UDPEchoServerConfig

enable

Description

The `enable` command enables the UDP Echo server.

Parent

kcli/config/diagnostic/UDPEchoServerConfig/UDPEchoServer

Syntax

```
enable
```

disable

Description

The `disable` command disables the UDP Echo server.

Parent

kcli/config/diagnostic/UDPEchoServerConfig/UDPEchoServer

Syntax

```
disable
```

uploadconfig

Description

The `uploadconfig` command configures the upload parameters to perform a upload on destination server from gateway. You must configure interface, ethernet priority, DSCP, and URL of destination server.

Parent

kcli/config/diagnostic

interface

Description

The `interface` command configures the interface to perform an upload. Enter the IP layer interface name.

Parent

kcli/config/diagnostic/uploadconfig

Syntax

```
interface < interfacename string > [ ethernetPriority < ethernetpriority integer(0:7) > ] [
DSCP < dscpvalue integer(0:63) > ] [ uploadURL < uploadURL string > ]
```

Parameter Description

Parameter	Description
ethernetPriority	Enter the ethernet priority for marking packets transmitted in the upload. Value ranges from 0 to 7.
DSCP	Enter the DiffServ value for marking packets transmitted in the upload. Value ranges from 0 to 63.
uploadURL	Enter the URL for the gateway to perform the upload

Example

The following example command configures the interface for the upload configuration:

```
#kcli> config diagnostic uploadconfig interface eth0 ethernetPriority 3 DSCP 23 uploadURL
ftp1.2wire.com <enter>
```

start

Description

The `start` command activates the uploading of the information packets on the gateway.

Parent

kcli/config/diagnostic/uploadconfig

Syntax

```
start
```

ping

Description

The `ping` major command starts or stops the ping service on the network. The Packet InterNet Groper (Ping) service is used for tests and measurements of the Internet system and client nets. It sends various types of probe packets, and processes the reply from the target receiver to know whether the target receiver is active on the network or not.

Parent

kcli/config/diagnostic

Syntax

```
ping
```

start

Description

The `start` command enables a new ping to verify whether the device is functional (from an external network/WAN).

Parent

kcli/config/diagnostic/ping

Syntax

```
start { host-address < hostaddr string > } [ ping-count < count integer(1:50) > ] [ packet-size < packetsize integer > ]
```

Parameter Description

Parameter	Description
host-address	Enter the name or IP address of the target host to ping.
ping-count	Enter the number of echo requests to send to the host. Value ranges from 1 to 50.
packet-size	Enter the packet size in bytes. This results in a total packet size of the packet size value plus 8 extra bytes for the ICMP header.

stop

Description

The `stop` command disables the previously fired ping command.

Parent

kcli/config/diagnostic/ping

Syntax

```
stop
```

traceroute

Description

The `traceroute` command starts or stops the trace route feature on the network. This feature determines the specific route followed by packets across an IP network. This helps identify routing problems or firewalls that may be blocking access to a site.

Parent

kcli/config/diagnostic

start

Description

The `start` command enables the trace route service on the network.

Parent

kcli/config/diagnostic/traceroute

Syntax

```
start { host-address < hostaddr string > } [ max-hops < maxhops integer > ]
```

Parameter Description

Parameter	Description
host-address	Enter the name or IP address of the target host.
max-hops	Enter the maximum number of hops that trace route utility should take before stopping. Value ranges from 2 to 65535.

stop

Description

The `stop` command disables the previously fired trace route command.

Parent

kcli/config/diagnostic/traceroute

Syntax

```
stop
```

nslookup

Description

The `nslookup` command starts or stops the NS lookup service on the network. This service looks up an IP address or an Fully Qualified Domain Name (FQDN) of a host on the network. When you use this feature, a DNS is queried for the name or IP address.

Parent

kcli/config/diagnostic

Syntax

```
nslookup
```

start

Description

The `start` command enables the NS lookup service.

Parent

kcli/config/diagnostic/nslookup

Syntax

```
start { host-address < hostaddr string > }
```

Parameter Description

Parameter	Description
host-address	Enter the name or IP address of the target host.

stop

Description

The `stop` command disables the previously fired NS lookup command.

Parent

kcli/config/diagnostic/nslookup

Syntax

```
stop
```

System Module

This section describes configuration commands for the system module. You can set the system parameters like date, time, domain name, log-persistency, ntpserver, captive-portal, syslog, timezone, host name, auto updation of DNS, tftp server location, etc. Here you can provide various types of settings that are mandatory to configure NP Gateway in order to make it functional.

system

Description

The `system` command node allows you to enter the configuration mode for basic device settings. Here you can provide various types of settings that are mandatory to configure the gateway in order to make it functional. The settings include date, time, NTP server, domain, syslog, and DNS.

Parent

kcli/config

syslog

Description

The `syslog` command major command configures the system log service. You can enable or disable the syslog service, set its size (in KB), and configure remote logging too.

Parent

kcli/config/system

service

Description

The `service` command enables or disables the system logging service.

Parent

kcli/config/system/syslog

Syntax

```
service { enable | disable }
```

Parameter Description

Parameter	Description
enable	Enable the system logging service to monitor critical system events and configuration changes made on the system.
disable	Disable the syslog service to stop system logging.

size

Description

The `size` command sets the maximum size of the log file that the gateway device should maintain before creating a new log file.

Parent

kcli/config/system/syslog

Syntax

```
size < max_log_size integer(1:500) > [ num-rotated-logs < num_rotated_logs integer(0:99) > ]
```

Parameter Description

Parameter	Description
max-log-size	Enter the maximum size (in kilobytes) of the log file that the gateway device should maintain. Value ranges from 1KB to 500KB.
num-rotated-logs	Enter the number the log files are rotated, when they reach a certain trigger size. Enter a numeric value (Default=1, Max=99, Purge=0) to indicate the number of related logs.

Example

The following example command configures the syslog file size:

```
#kcli> config system syslog size 25 num-rotated-logs 56 <enter>
```

remote-logging

Description

The `remote-logging` command maintains log files on a remote machine. Additionally, you have the option to enable or disable logging on the local machine.

Parent

kcli/config/system/syslog

Syntax

```
remote-logging { { enable < server string(1:32) > [ port < port integer > ] [ local-logging
{ enable | disable } ] } | disable }
```

Parameter Description

Parameter	Description
enable	Enable the remote logging service, and enter the remote syslog host name or IP address.
port	Enter the remote syslog server port number.
disable	Disable the remote logging service.
local-logging	Enable or disable the local logging. If enabled, you can keep a backup of the log files.
enable	Enable the local logging to keep a backup of the log files.
disable	Disable the local logging.

Example

The following example command enables the remote logging service:

```
#kcli> config system syslog remote-logging enable 192.168.0.15 port 514 local-logging
enable <enter>
```

klog

Description

The `klog` command enables or disables the klog service and sets the file size (in Kilobytes). Klog is a system daemon which intercepts and logs Linux kernel messages.

Parent

kcli/config/system

Syntax

```
klog
```

log-level

Description

The `log-level` command configures the maximum size of the klog file that the gateway device should maintain, before creating a new klog file. Enter the file size (in kilobytes). Value ranges from 1 to 8.

Parent

kcli/config/system/klog

Syntax

```
log-level < log-level integer(1:8) >
```

service

Description

The `service` command enables or disables the klog service.

Parent

kcli/config/system/klog

Syntax

```
service { enable | disable }
```

Parameter Description

Parameter	Description
enable	Enable the klog service to log Linux kernel messages.
disable	Disable the klog service to deactivate logging of Linux kernel messages.

date

Description

The `date` command sets the device date in the mm-dd-yyyy format.

Parent

kcli/config/system

Syntax

```
date < date string(10:10) >
```

Note The date value is taken as the default date by the device for executing all date-dependent commands, if any.

time

Description

The `time` command sets the device time in the HH:MM:SS format.

Parent

kcli/config/system

Syntax

```
time < time-str string(8:8) >
```

Note The time value is taken as the default time by the device for executing all time-dependent commands, if any.

ntpserver

Description

The `ntpserver` command enables or disables the Network Time Protocol (NTP) server. If enabled, the device date and time are retrieved from the configured NTP server's system time. If you configure this service, then enter the NTP server name or IP address.

Parent

kcli/config/system

Syntax

```
ntpserver { < server string(1:32) > enable } | { disable }
```

Parameter Description

Parameter	Description
enable	Enable the NTP server. Now, the gateway fetches the date and time values from the NTP server.
primary	Enter the primary server IP address. This is the location from where the NTP server fetches the date and time.
secondary	Enter the secondary server IP address. This is location from where the NTP server fetches the date and time if the primary server is down.
tertiary	Enter the tertiary server IP address. This is location from where the NTP server fetches the date and time if the secondary server is down.
fourth	Enter the fourth server IP address. This is location from where the NTP server fetches the date and time if the tertiary server is down.
fifth	Enter the fifth server IP address. This is location from where the NTP server fetches the date and time if the fourth server is down.
interval	Set the time interval in hours after which the NTP server updates the time of the gateway device.
disable	Disable the NTP server to manually set the device date and time.

Note In case the NTP server is enabled, the device date and time is retrieved and synchronized from the specified NTP server. This overwrites any manually set device date and time.

timezone

Description

The `timezone` command sets the NTP server's time zone to be configured for the gateway device. You need to select a time zone from the available list that are specified in the configured NTP server.

Parent

kcli/config/system

Syntax

```
timezone { { (GMT-12:00) International Date Line West | (GMT-11:00) Midway Island, Samoa |
(GMT-10:00) Hawaii | (GMT-09:00) Alaska | (GMT-08:00) Pacific Time - US and Canada; Tijuana
| (GMT-07:00) Arizona | (GMT-07:00) Chihuahua, La Paz, Mazatlan | (GMT-07:00) Mountain Time
- US and Canada | (GMT-06:00) Central America | (GMT-06:00) Central Time - US and Canada |
```

```
(GMT-06:00) Guadalajara, Mexico City, Monterrey | (GMT-06:00) Saskatchewan | (GMT-05:00)
Bogota, Lima, Quito | (GMT-05:00) Eastern Time - US and Canada | (GMT-05:00) Indiana (East)
| (GMT-04:00) Atlantic Time - Canada | (GMT-04:00) Caracas, La Paz | (GMT-04:00) Santiago |
(GMT-03:30) Newfoundland | (GMT-03:00) Brasilia | (GMT-03:00) Buenos Aires, Georgetown |
(GMT-03:00) Greenland | (GMT-02:00) Mid-Atlantic | (GMT-01:00) Azores | (GMT-01:00) Cape
Verde Is. | (GMT) Casablanca, Monrovia | (GMT) Greenwich Mean Time : Dublin, Edinburg,
Lisbon, London | (GMT+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna | (GMT+01:00)
Belgrade, Bratislava, Budapest, Ljubljana, Prague | (GMT+01:00) Brussels, Copenhagen,
Madrid, Paris | (GMT+01:00) Sarajevo, Skopje, Warsaw, Zagreb | (GMT+01:00) West Central
Africa | (GMT+02:00) Athens, Beirut, Istanbul, Minsk | (GMT+02:00) Bucharest | (GMT+02:00)
Cairo | (GMT+02:00) Harare, Pretoria | (GMT+02:00) Helsinki, Kyiv, Riga, Sofia, Tallinn,
Vilnius | (GMT+02:00) Jerusalem | (GMT+03:00) Baghdad | (GMT+03:00) Kuwait, Riyadh |
(GMT+03:00) Moscow, St. Petersburg, Volgograd | (GMT+03:00) Nairobi | (GMT+03:30) Tehran |
(GMT+04:00) Abu Dhabi, Muscat | (GMT+04:00) Baku, Tbilisi, Yerevan | (GMT+04:30) Kabul |
(GMT+05:00) Ekaterinburg | (GMT+05:00) Islamabad, Karachi, Tashkent | (GMT+05:30) Chennai,
Kolkata, Mumbai, New Delhi | (GMT+05:45) Kathmandu | (GMT+06:00) Almathy, Novosibirsk |
(GMT+06:00) Astana, Dhaka | (GMT+06:00) Sri Jayawardenepura | (GMT+06:30) Rangoon |
(GMT+07:00) Bangkok, Hanoi, Jakarta | (GMT+07:00) Krasnoyarsk | (GMT+08:00) Beijing,
Chongging, Hong Kong, Urumgi | (GMT+08:00) Irkutsk, Ulaan Bataar | (GMT+08:00) Kuala
Lumpur, Singapore | (GMT+08:00) Perth | (GMT+08:00) Taipei | (GMT+09:00) Osaka, Sappora,
Tokyo | (GMT+09:00) Seoul | (GMT+09:00) Yakutsk | (GMT+09:30) Adelaide | (GMT+09:30) Darwin
| (GMT+10:00) Brisbane | (GMT+10:00) Canberra, Melbourne, Sydney | (GMT+10:00) Guam, Port
Moresby | (GMT+10:00) Hobart, Tasmania | (GMT+10:00) Vladivostok | (GMT+11:00) Magadan,
Solomon Is., New Caledonia | (GMT+12:00) Auckland, Wellington | (GMT+12:00) Fiji,
Kamchatka, Marshall Is. | (GMT+13:00) Nuku'alofa } } | { adjust-for-daylight-savings {
(GMT-12:00) International Date Line West | (GMT-11:00) Midway Island, Samoa | (GMT-10:00)
Hawaii | (GMT-09:00) Alaska | (GMT-08:00) Pacific Time - US and Canada; Tijuana | (GMT-
07:00) Arizona | (GMT-07:00) Chihuahua, La Paz, Mazatlan | (GMT-07:00) Mountain Time - US
and Canada | (GMT-06:00) Central America | (GMT-06:00) Central Time - US and Canada | (GMT-
06:00) Guadalajara, Mexico City, Monterrey | (GMT-06:00) Saskatchewan | (GMT-05:00) Bogota,
Lima, Quito | (GMT-05:00) Eastern Time - US and Canada | (GMT-05:00) Indiana (East) | (GMT-
04:00) Atlantic Time - Canada | (GMT-04:00) Caracas, La Paz | (GMT-04:00) Santiago | (GMT-
03:30) Newfoundland | (GMT-03:00) Brasilia | (GMT-03:00) Buenos Aires, Georgetown | (GMT-
03:00) Greenland | (GMT-02:00) Mid-Atlantic | (GMT-01:00) Azores | (GMT-01:00) Cape Verde
Is. | (GMT) Casablanca, Monrovia | (GMT) Greenwich Mean Time : Dublin, Edinburg, Lisbon,
London | (GMT+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna | (GMT+01:00)
Belgrade, Bratislava, Budapest, Ljubljana, Prague | (GMT+01:00) Brussels, Copenhagen,
Madrid, Paris | (GMT+01:00) Sarajevo, Skopje, Warsaw, Zagreb | (GMT+01:00) West Central
Africa | (GMT+02:00) Athens, Beirut, Istanbul, Minsk | (GMT+02:00) Bucharest | (GMT+02:00)
Cairo | (GMT+02:00) Harare, Pretoria | (GMT+02:00) Helsinki, Kyiv, Riga, Sofia, Tallinn,
Vilnius | (GMT+02:00) Jerusalem | (GMT+03:00) Baghdad | (GMT+03:00) Kuwait, Riyadh |
(GMT+03:00) Moscow, St. Petersburg, Volgograd | (GMT+03:00) Nairobi | (GMT+03:30) Tehran |
(GMT+04:00) Abu Dhabi, Muscat | (GMT+04:00) Baku, Tbilisi, Yerevan | (GMT+04:30) Kabul |
(GMT+05:00) Ekaterinburg | (GMT+05:00) Islamabad, Karachi, Tashkent | (GMT+05:30) Chennai,
Kolkata, Mumbai, New Delhi | (GMT+05:45) Kathmandu | (GMT+06:00) Almathy, Novosibirsk |
(GMT+06:00) Astana, Dhaka | (GMT+06:00) Sri Jayawardenepura | (GMT+06:30) Rangoon |
(GMT+07:00) Bangkok, Hanoi, Jakarta | (GMT+07:00) Krasnoyarsk | (GMT+08:00) Beijing,
Chongging, Hong Kong, Urumgi | (GMT+08:00) Irkutsk, Ulaan Bataar | (GMT+08:00) Kuala
Lumpur, Singapore | (GMT+08:00) Perth | (GMT+08:00) Taipei | (GMT+09:00) Osaka, Sappora,
Tokyo | (GMT+09:00) Seoul | (GMT+09:00) Yakutsk | (GMT+09:30) Adelaide | (GMT+09:30) Darwin
| (GMT+10:00) Brisbane | (GMT+10:00) Canberra, Melbourne, Sydney | (GMT+10:00) Guam, Port
Moresby | (GMT+10:00) Hobart, Tasmania | (GMT+10:00) Vladivostok | (GMT+11:00) Magadan,
Solomon Is., New Caledonia | (GMT+12:00) Auckland, Wellington | (GMT+12:00) Fiji,
Kamchatka, Marshall Is. | (GMT+13:00) Nuku'alofa } }
```

Parameter Description

Parameter	Description
(GMT-12:00) International Date Line West	Set the required time zone for the gateway device. The date and time thus displayed will be as per the set time zone.
(GMT-11:00) Midway Island, Samoa	
(GMT-10:00) Hawaii	
(GMT-09:00) Alaska	
(GMT-08:00) Pacific Time - US and Canada; Tijuana	
(GMT-07:00) Arizona	
(GMT-07:00) Chihuahua, La Paz, Mazatlan	
(GMT-07:00) Mountain Time - US and Canada	
(GMT-06:00) Central America	
(GMT-06:00) Central Time - US and Canada	
(GMT-06:00) Guadalajara, Mexico City, Monterrey	
(GMT-06:00) Saskatchewan	
(GMT-05:00) Bogota, Lima, Quito	
(GMT-05:00) Eastern Time - US and Canada	
(GMT-05:00) Indiana (East)	
(GMT-04:00) Atlantic Time - Canada	
(GMT-04:00) Caracas, La Paz	
(GMT-04:00) Santiago	
(GMT-03:30) Newfoundland	
(GMT-03:00) Brasilia	
(GMT-03:00) Buenos Aires, Georgetown	
(GMT-03:00) Greenland	
(GMT-02:00) Mid-Atlantic	
(GMT-01:00) Azores	
(GMT-01:00) Cape Verde Is.	
(GMT) Casablanca, Monrovia	
(GMT) Greenwich Mean Time : Dublin, Edinburg, Lisbon, London	
(GMT+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna	
(GMT+01:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague	

Parameter	Description
(GMT+01:00) Brussels, Copenhagen, Madrid, Paris	
(GMT+01:00) Sarajevo, Skopje, Warsaw, Zagreb	
(GMT+01:00) West Central Africa	
(GMT+02:00) Athens, Beirut, Istanbul, Minsk	
(GMT+02:00) Bucharest	
(GMT+02:00) Cairo	
(GMT+02:00) Harare, Pretoria	
(GMT+02:00) Helsinki, Kyiv, Riga, Sofia, Tallinn, Vilnius	
(GMT+02:00) Jerusalem	
(GMT+03:00) Baghdad	
(GMT+03:00) Kuwait, Riyadh	
(GMT+03:00) Moscow, St. Petersburg, Volgograd	
(GMT+03:00) Nairobi	
(GMT+03:30) Tehran	
(GMT+04:00) Abu Dhabi, Muscat	
(GMT+04:00) Baku, Tbilisi, Yerevan	
(GMT+04:30) Kabul	
(GMT+05:00) Ekaterinburg	
(GMT+05:00) Islamabad, Karachi, Tashkent	
(GMT+05:30) Chennai, Kolkata, Mumbai, New Delhi	
(GMT+05:45) Kathmandu	
(GMT+06:00) Almathy, Novosibirsk	
(GMT+06:00) Astana, Dhaka	
(GMT+06:00) Sri Jayawardenepura	
(GMT+06:30) Rangoon	
(GMT+07:00) Bangkok, Hanoi, Jakarta	
(GMT+07:00) Krasnoyarsk	
(GMT+08:00) Beijing, Chongging, Hong Kong, Urumgi	
(GMT+08:00) Irkutsk, Ulaan Bataar	
(GMT+08:00) Kuala Lumpur, Singapore	
(GMT+08:00) Perth	

Parameter	Description
(GMT+08:00) Taipei	
(GMT+09:00) Osaka, Sappora, Tokyo	
(GMT+09:00) Seoul	
(GMT+09:00) Yakutsk	
(GMT+09:30) Adelaide	
(GMT+09:30) Darwin	
(GMT+10:00) Brisbane	
(GMT+10:00) Canberra, Melbourne, Sydney	
(GMT+10:00) Guam, Port Moresby	
(GMT+10:00) Hobart, Tasmania	
(GMT+10:00) Vladivostok	
(GMT+11:00) Magadan, Solomon Is., New Caledonia	
(GMT+12:00) Auckland, Wellington	
(GMT+12:00) Fiji, Kamchatka, Marshall Is.	
(GMT+13:00) Nuku'alofa	
adjust-for-daylight-savings	
(GMT-12:00) International Date Line West	
(GMT-11:00) Midway Island, Samoa	
(GMT-10:00) Hawaii	
(GMT-09:00) Alaska	
(GMT-08:00) Pacific Time - US and Canada; Tijuana	
(GMT-07:00) Arizona	
(GMT-07:00) Chihuahua, La Paz, Mazatlan	
(GMT-07:00) Mountain Time - US and Canada	
(GMT-06:00) Central America	
(GMT-06:00) Central Time - US and Canada	
(GMT-06:00) Guadalajara, Mexico City, Monterrey	
(GMT-06:00) Saskatchewan	
(GMT-05:00) Bogota, Lima, Quito	
(GMT-05:00) Eastern Time - US and Canada	
(GMT-05:00) Indiana (East)	
(GMT-04:00) Atlantic Time - Canada	

Parameter	Description
(GMT-04:00) Caracas, La Paz	
(GMT-04:00) Santiago	
(GMT-03:30) Newfoundland	
(GMT-03:00) Brasilia	
(GMT-03:00) Buenos Aires, Georgetown	
(GMT-03:00) Greenland	
(GMT-02:00) Mid-Atlantic	
(GMT-01:00) Azores	
(GMT-01:00) Cape Verde Is.	
(GMT) Casablanca, Monrovia	
(GMT) Greenwich Mean Time : Dublin, Edinburg, Lisbon, London	
(GMT+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna	
(GMT+01:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague	
(GMT+01:00) Brussels, Copenhagen, Madrid, Paris	
(GMT+01:00) Sarajevo, Skopje, Warsaw, Zagreb	
(GMT+01:00) West Central Africa	
(GMT+02:00) Athens, Beirut, Istanbul, Minsk	
(GMT+02:00) Bucharest	
(GMT+02:00) Cairo	
(GMT+02:00) Harare, Pretoria	
(GMT+02:00) Helsinki, Kyiv, Riga, Sofia, Tallinn, Vilnius	
(GMT+02:00) Jerusalem	
(GMT+03:00) Baghdad	
(GMT+03:00) Kuwait, Riyadh	
(GMT+03:00) Moscow, St. Petersburg, Volgograd	
(GMT+03:00) Nairobi	
(GMT+03:30) Tehran	
(GMT+04:00) Abu Dhabi, Muscat	
(GMT+04:00) Baku, Tbilisi, Yerevan	
(GMT+04:30) Kabul	
(GMT+05:00) Ekaterinburg	

Parameter	Description
(GMT+05:00) Islamabad, Karachi, Tashkent	
(GMT+05:30) Chennai, Kolkata, Mumbai, New Delhi	
(GMT+05:45) Kathmandu	
(GMT+06:00) Almathy, Novosibirsk	
(GMT+06:00) Astana, Dhaka	
(GMT+06:00) Sri Jayawardenepura	
(GMT+06:30) Rangoon	
(GMT+07:00) Bangkok, Hanoi, Jakarta	
(GMT+07:00) Krasnoyarsk	
(GMT+08:00) Beijing, Chongging, Hong Kong, Urumgi	
(GMT+08:00) Irkutsk, Ulaan Bataar	
(GMT+08:00) Kuala Lumpur, Singapore	
(GMT+08:00) Perth	
(GMT+08:00) Taipei	
(GMT+09:00) Osaka, Sappora, Tokyo	
(GMT+09:00) Seoul	
(GMT+09:00) Yakutsk	
(GMT+09:30) Adelaide	
(GMT+09:30) Darwin	
(GMT+10:00) Brisbane	
(GMT+10:00) Canberra, Melbourne, Sydney	
(GMT+10:00) Guam, Port Moresby	
(GMT+10:00) Hobart, Tasmania	
(GMT+10:00) Vladivostok	
(GMT+11:00) Magadan, Solomon Is., New Caledonia	
(GMT+12:00) Auckland, Wellington	
(GMT+12:00) Fiji, Kamchatka, Marshall Is.	
(GMT+13:00) Nuku'alofa	

reboot

Description

The `reboot` command restarts the device immediately.

Parent

kcli/config/system

Syntax

```
reboot
```

Note Before rebooting the device, you may want to save the current configuration through the admin-tools module (in case the "always-save" option is disabled).

domain

Description

The `domain` command specifies a domain name, which can be part of a website, URL or an email address. It is then looked up into the DNS, which communicates to the workstation of the IP address/es corresponding to that name. Enter the domain name of the device.

Parent

kcli/config/system

Syntax

```
domain < domain-str string(1:64) >
```

host

Description

The `host` command sets the host name for the gateway device. Enter the host name that is used to identify the device on the network.

Parent

kcli/config/system

Syntax

```
host < host-str string(1:64) >
```

dns

Description

The `dns` command configures the primary and secondary DNS IP address/es. DNS hosting means that a carrier has a server that resolves the requests for a customer's domain name to the appropriate IP address, or vice versa.

Parent

kcli/config/system

Syntax

```
dns [ primary [ ip < pri_dns ipaddr(0:255) > ] | [ disable-primary ] ] [ secondary [ ip <
sec_dns ipaddr(0:255) > ] | [ disable-secondary ] ] [ tertiary [ ip < ter_dns ipaddr(0:255)
> ] | [ disable-tertiary ] ]
```

Parameter Description

Parameter	Description
primary	Set the primary DNS server that acts as the most authoritative server for a particular domain.
ip	Enter a DNS server IP to set it as the primary DNS.
disable-primary	Disable the primary DNS.
secondary	Set the secondary DNS server that acts as a backup server for a particular domain in case the primary DNS server is not reachable.
ip	Enter a DNS server IP to set it as the secondary DNS.
disable-secondary	Disable the secondary DNS.
tertiary	Set the tertiary DNS server acts as a backup server for a particular domain in case the secondary DNS server is not reachable.
ip	Enter a DNS server IP to set it as the tertiary DNS.
disable-tertiary	Disable the tertiary DNS.

Example

The following example command configures DNS service on the server:

```
#kcli> config system dns primary ip 198.41.0.4 secondary ip 204.74.112.1 tertiary ip
207.142.131.234 <enter>
```

auto-update-DNS

Description

The `auto-update-DNS` command automatically updates the DNS information. DNS is a system that stores information associated with domain names in a distributed database on networks, such as the Internet. It associates many types of information with domain names, but most importantly, it provides the IP address associated with the domain name.

Parent

kcli/config/system

Syntax

```
auto-update-DNS { enable | disable }
```

Parameter Description

Parameter	Description
enable	Enable the auto update DNS service. If enabled, the new DNS information is retrieved from the ISP and the existing DNS entries that are statically set, are overwritten. For the auto update DNS service to function properly, the WAN address mode should be set to DHCP, PPPoE, PPTP or L2TP.
disable	Disable the auto update DNS service.

Note Configure the ISP mode on the network for the auto update DNS service to take effect.

service

Description

The `service` command enables or disables the specified service on the device.

Parent

kcli/config/system

Syntax

```
service { syslog | snmp | web-server | ssh | telnet | ftp | cron } { { enable [ port < port integer > ] } | { disable } }
```

Parameter Description

Parameter	Description
syslog	Enable or disable the syslog service on the gateway device.
snmp	Enable or disable the SNMP service on the gateway device.
web-server	Enable or disable the Web server on the gateway device.
ssh	Enable or disable the SSH service on the gateway device.
telnet	Enable or disable the TelNet service on the gateway device.
ftp	Enable or disable the FTP service on the gateway device.
cron	Enable or disable the CRON service on the gateway device.
tftp	Enable or disable the TFTP service on the gateway device.
enable	Enable the specified service on the gateway device.
port	Enter the port number on which the service is to be enabled.
default-port	Use the default port on which the service is to be enabled.
disable	Disable the specified service on the gateway device.

Example

The following example command enables SNMP service on the default port:

```
#kcli> config system service snmp enable default-port <enter>
```

logs

Description

The `logs` command deletes all the log files present on the gateway.

Parent

kcli/config/system

Syntax

```
logs clear
```

Parameter Description

Parameter	Description
clear	Delete the log files on the device.

day-light-saving

Description

The `day-light-saving` command configures the day light saving feature on the gateway device.

Parent

kcli/config/system

Syntax

```
day-light-saving { user-defined { startdate < date string > [ starttime < time string > ] }
{ enddate < date string > [ endtime < time string > ] } } | { standard }
```

Parameter Description

Parameter	Description
standard	Select the standard day light saving configuration option. The settings in this case are as per the OS configuration.
user-defined	Select the customized day light saving option that allows you to define date and time.
startdate	Enter the date on which you want to start the day light saving on the device. The format has to be in MM.D.W., where MM=month, D=day of the week (0 being Sunday), and w=week of the month.
starttime	Enter the day light saving start time in HH:MM:SS format.
enddate	Enter the date on which you want to end the day light saving on the device. The format has to be in MM.D.W., where MM=month, D=day of the week (0 being Sunday), and w=week of the month.
endtime	Enter the day light saving end time in HH:MM:SS format.

Example

The following example command configures day light settings on the gateway device:

```
#kcli> config system day-light-saving user-defined startdate 05.2.2 starttime 07:00:00
enddate 6.2.2 endtime 15:00:00 <enter>
```

Note While configuring the day light saving, note that only the NTP server (if configured and enabled) settings take effect.

mail

Description

The `mail` command configures the mail system log feature on the device. You can also mail the log files to the intended recipient.

Parent

kcli/config/system

Syntax

```
mail { set_mail_params [ domain_name < domainname string > ] [ mail_server < servername string > ] [ subject < sub string > ] [ send_from < email_add string > ] [ username < user string > ] [ password < pass string > ] [ send_to < email string > ] } | { mail_syslog }}
```

Parameter Description

Parameter	Description
mail_syslog	Send the system log files to the recipient through e-mail.
set_mail_params	Configure the e-mail parameters to send the system log files to the intended recipient. Here, you can set the mail server, sender/recipient e-mail address, etc.
domain_name	Enter the domain name for the SMTP server. For example, yahoo.com.
mail_server	Enter the server name or IP address of the mail server. For example, mail.yahoo.com.
subject	Enter the subject line of the syslog mail.
send_from	Enter the sender's e-mail address.
username	Enter the user name of the sender so as to authenticate the same on the server.
password	Enter the password to authenticate the sender's user name.
send_to	Enter the recipient's e-mail address.

Example

The following example command configure the mail system on the gateway device:

```
#kcli> config system mail set_mail_params domain_name a1b2c3 mail_server exchange.2wire.com subject logfiles send_from abc@2wire.com username abc password 2wire send_to xyz@2wire.com
```

captive-portal

Description

The `captive-portal` command enables or diables captive-portal on LAN. Captive portal is the configured redirect URL where the user is redirected, regardless of the website user is trying to access.

Parent

kcli/config/system

Syntax

```
captive-portal { { enable [ redirect-url < redirecturl string >  ] [ allowed-ip-list < allowediplist string > ] } | { disable } }
```

Parameter Description

Parameter	Description
enable	Enable the captive portal.
redirect-url	Enter the redirect URL, if the user is not to be redirected to the specified redirect URL.
allowed-ip-list	Enter comma-separated list of IP addresses where the HTTP (port 80) traffic must be permitted.
disable	Disable captive portal.

Example

The following example command configures the captive-portal and IP addresses that are excluded from getting redirected:

```
#kcli> config system captive-portal enable redirect-url www.2wire.com allowed-ip-list
192.168.0.15,192.168.0.25 <enter>
```

log-persistency

Description

The `log-persistency` command saves the files in the /var/log/ directory across reboots.

Parent

kcli/config/system

Syntax

```
log-persistency { enable | disable }
```

Parameter Description

Parameter	Description
enable	Enable to save the Var directory log files.
disable	Disable to delete the Var directory log files everytime the system reboots.

tftp-Server-Location

Description

The `tftp-server-Location` command configures the location for the TFTP server on the gateway device. You can use this location to upload and download files on the gateway device.

Parent

kcli/config/system

Syntax

```
tftp-Server-Location < directory_location string(1:64) >
```

onetime-redirect

Description

The `onetime-redirect` command enables or disables the one-time redirect. If enabled, whenever the CPE is bootstrapped for the first time, it is redirected to the specified redirect URL before the user start browsing the Internet. Once the redirection is successful for the first time, the user is not redirected again the next time onwards.

Parent

kcli/config/system

Syntax

```
onetime-redirect { { enable [ redirect-url < redirecturl string > ] } | { disable } }
```

Parameter Description

Parameter	Description
enable	Enable the one-time redirect.
redirect-url	Enter the one-time redirect URL where the user is to be redirected, when the device is bootstrapped for the first time.
disable	Disable the one-time redirect.

crashdumpinfo

Description

The `crashdumpinfo` command deletes the system crashdump information.

Parent

kcli/config/system

Syntax

```
crashdumpinfo { clear }
```

Parameter Description

Parameter	Description
clear	Delete the system crashdump information.

DHCP Module

This section describes the DHCP module configuration commands. In this module, you can configure vendor information, DNS parameters, MAC entries, host entries, etc.

dhcp

Description

The `dhcp` command node allows you to enter the configuration mode for setting the DHCP server parameters. Dynamic Host Configuration Protocol (DHCP) is a client-server networking protocol that provides a mechanism

for allocation of IP addresses to clients. You can configure the DHCP server to assign IP addresses dynamically to the LAN hosts. When you select the DHCP mode for dynamically assigning an IP address to the device, the WAN interface of the device becomes the DHCP client and obtains an IP address from the DHCP server.

Parent

kcli/config

vendor

Description

The `vendor` command node adds or deletes a vendor in the vendor database.

Parent

kcli/config/dhcp

add

Description

The `add` command adds a vendor to the vendor database.

Parent

kcli/config/dhcp/vendor

Syntax

```
add { vendor < vendorname string > }
```

Parameter Description

Parameter	Description
vendor	Enter a vendor name that is used as an identification for the vendor in the vendor database. Enter an alphanumeric value to indicate the vendor name.

Example

The following example command adds a vendor to the vendor database:

```
#kcli> config dhcp vendor add vendor a1b2c3 <enter>
```

delete

Description

The `delete` command deletes vendor from the vendor database.

Parent

kcli/config/dhcp/vendor

Syntax

```
delete { vendor < vendorname string > }
```

Parameter Description

Parameter	Description
vendor	Enter the vendor name to be deleted from the database.

dns

Description

The `dns` command node adds, modifies, or removes hostentry and macentry. Domain Name System (DNS) translates domain names (computer host names) to IP addresses.

Parent

kcli/config

macentry

Description

The `macentry` command node adds, modifies, or deletes the MAC entries. MAC entry or Media Access Control (MAC) address is the physical address of any device on the network, such as the NIC in a computer. The MAC address, which is made up of two equal parts, is 6 bytes long. The first 3 bytes identify the company that made the NIC. The second 3 bytes are the serial number of the NIC itself.

Parent

kcli/config/dns

add

Description

The `add` command adds the MAC address entries. It maps a MAC address to an IP address by adding a record. When a LAN device with mapped MAC address requests for an IP address, then the DHCP server assigns the mapped IP address to that device.

Parent

kcli/config/dns/macentry

Syntax

```
add { mac < macaddress macaddr > } { ip < ipaddress ipaddr > } { hostname < host string > }
[ dmzplus { enable | disable } ]
```

Parameter Description

Parameter	Description
mac	Enter the MAC address of the device to be configured on the DHCP server.
ip	Enter the static IP address that must be assigned to the device.
hostname	Enter the hostname of the device to be configured on the DHCP server.
dmzplus	Enable or disable the DMZplus environment on the network. If enabled, the DMZ host must renew the IP address assigned by the gateway. After renewing the IP address, the traffic directed to the gateway WAN IP address is received by the DMZ host interface connected to the gateway. DMZPlus is useful when configuring customized firewalls on the WAN.
enable	Enable DMZ configuration on the network.
disable	Disable DMZ configuration on the network.

Example

The following example command adds the Mac entry to the DHCP server:

```
#kcli> config dns macentry add mac 01-23-45-67-89-ab ip 192.168.1.162 hostname xyz dmzplus
enable <enter>
```

modify

Description

The `modify` command edits the static IP or hostname of the configured MAC address on the DHCP server.

Parent

kcli/config/dns/macentry

Syntax

```
modify { mac < macaddress macaddr > } [ ip < ipaddress ipaddr > ] [ hostname < host string
> ] [ { dmzvalue { enable | disable } } ]
```

Parameter Description

Parameter	Description
mac	Specify the MAC address of the device whose IP address or host name is to be modified.
ip	Enter the modified static IP address to be assigned to the device.
hostname	Enter a new value to indicate the hostname to be assigned to the device.
dmzvalue	Modify DMZPlus mode status.
enable	Enable the DMZ mode if it is not already enabled.
disable	Disable the DMZ mode if it is not already disabled.

remove

Description

The `remove` command deletes the MAC address entry from the DHCP server.

Parent

kcli/config/dns/macentry

Syntax

```
remove { mac < macaddress macaddr > }
```

Parameter Description

Parameter	Description
mac	Specify the MAC address to be deleted.

hostentry

Description

The `hostentry` command node adds, modifies, or deletes the host entries. Hostentry or Hostname is a unique name by which a network-attached device is known on the network.

Parent

kcli/config/dns

add

Description

The `add` command adds the DNS host entries. Host entry or hostname is a unique name by which a network-attached device is known on the network. The add command adds entries of the devices that are configured statically on the LAN and have valid IP address in the same network range as configured on the DHCP server.

Parent

kcli/config/dns/hostentry

Syntax

```
add { hostname < host string > } { ip < ipaddress ipaddr > }
```

Parameter Description

Parameter	Description
hostname	Enter an alphanumeric value for the host name.
ip	Enter the IP address of the network device.

Example

The following example command adds the hostname to the network device on the DHCP server:

```
#kcli> config dns hostentry add hostname a1b2c3 ip 192.168.1.164 <enter>
```

modify

Description

The `modify` command edits the hostname of the network device on the DHCP server.

Parent

kcli/config/dns/hostentry

Syntax

```
modify { rulenumber < rule integer > } [ ip < ipaddress ipaddr > ] [ hostname < host string > ]
```

Parameter Description

Parameter	Description
rulenumber	Enter the rule number that is used as an ID by the DHCP server for authentication.
ip	Enter the new IP address of the network device.
hostname	Enter new alphanumeric value for the host name.

remove

Description

The `remove` command removes a hostname entry of the network device from the DHCP server.

Parent

kcli/config/dns/hostentry

Syntax

```
remove { rulenumber < rule integer > }
```

Parameter Description

Parameter	Description
rulenumber	Enter the rule number that is used as an ID by the DHCP server for authentication.

domainentry

Description

The `domainentry` command node adds, modifies, or deletes the domain entries.

Parent

kcli/config/dns

add

Description

The `add` command adds the domain-based static DNS entries.

Parent

kcli/config/dns/domainentry

Syntax

```
add { domain < domainname string(1:256) > } { interface < ifname string(1:32) > } { mode { auto | manual } } [ primary < primary string(7:15) > ] [ secondary < secondary string(7:15) > ] { fallback { enable | disable } } { status { enable | disable } }
```

Parameter Description

Parameter	Description
domain	Enter an aphanumeric domain name for the DNS entry.
interface	Enter the interface name on which primary and secondary DNS servers can be added.
mode	Select a mode from the available options, auto or manual. Mode indicates the way the DNS servers are obtained for the said domain.
auto	Select the auto mode to use the default DNS servers for the specified interface.
manual	Select the manual mode to manually configure the DNS servers.
primary	Enter the primary DNS server IP address.
secondary	Enter the secondary DNS server IP address.
fallback	Enable or disable the fallback feature.
enable	Enable the fallback feature to send any query for the specified domain to the default servers in case of failure.
disable	Disable fallback feature if you do not want to use the default servers for name resolution.
status	Enable or disable the DNS domain name entry.
enable	Enable the domain name entry, if you want to use it for name resolution purpose.
disable	Disable the domain name entry, if you do not want to use it for name resolution purpose. Disabling the entry does not delete it, but it is still present on the network for later use.

Example

The following example command adds the domain-based static DNS entry named 2wire.com:

```
#kcli> config dns domainentry add domain 2wire.com interface bb1 mode auto fallback enable status enable <enter>
```

modify

Description

The `modify` command edits the domain-based static DNS entry parameters.

Parent

kcli/config/dns/domainentry

Syntax

```
modify { domain < domainname string(1:256) > } [ interface < ifname string(1:32) > ] [ mode { auto | manual } ] [ primary < primary string(7:15) > ] [ secondary < secondary string(7:15) > ] [ fallback { enable | disable } ] [ status { enable | disable } ]
```

Parameter Description

Parameter	Description
domain	Enter the domain name to be modified.
interface	Modify the interface for the primary and secondary DNS servers. Enter a new server name.
mode	Select the mode to obtain the DNS servers.
auto	Select auto mode if it is not already selected. Now the default DNS servers are used for the specified interface.
manual	Select manual mode if it is not already selected. Now you can manually configure the DNS servers.
primary	Modify the primary DNS server IP address.
secondary	Modify the secondary DNS server IP address.
fallback	Modify the status of the fallback feature.
enable	Enable the fallback feature if it is not already enabled. Now, any query for the said domain is sent to the default servers in case of failure.
disable	Disable the fallback feature if it is not already disabled.
status	Modify the status of the domain name entry.
enable	Enable the domain name entry if it is not already enabled.
disable	Disable the domain name entry if it is not already disabled. Now, the entry is only de-activated, but not deleted from the DNS database.

remove

Description

The `remove` command deletes a domain-based static DNS entry.

Parent

kcli/config/dns/domainentry

Syntax

```
remove { domain < domainname string(1:256) > }
```

Parameter Description

Parameter	Description
domain	Enter the domain name to be deleted.

pool

Description

The `pool` command adds a new IP address pool for the DHCP server. You can also modify or delete an existing pool.

Parent

kcli/config/dhcp

add

Description

The `add` command adds a new IP address pool for the DHCP server.

Parent

kcli/config/dhcp/pool

Syntax

```
add interface < ifname string(1:32) > entry < precedence int > min < addr ipaddr > max <
addr ipaddr > [ vendor < id string(1:256) > ] status { enable | disable }
```

Parameter Description

Parameter	Description
interface	Enter the interface name for which the pool is to be used.
entry	Enter the precedence of the pool entry. For example, entering 1 (one) provides the pool entry the highest precedence.
min	Specify the first IP address in the pool to be assigned by the DHCP server.
max	Specify the last IP address in the pool to be assigned by the DHCP server.
vendor	Specify the vendor ID to associate it with the pool. A LAN host obtains the IP address from the pool associated with that vendor.
status	Enable or disable the pool.
enable	Enable the pool to use it for IP address allocation.
disable	Disable the pool. If disabled, no IP address is to be allocated from this pool.

Example

The following example command configures the lease period and default network type for the DHCP server:

```
#kcli> config dhcp pool add interface eth0 entry 1 min 192.168.1.64 max 192.168.1.143
vendor a1b2c3 status enable <enter>
```

modify

Description

The `modify` command modifies the configuration of an existing IP address pool to be assigned by the DHCP server.

Parent

kcli/config/dhcp/pool

Syntax

```
modify interface < ifname string(1:32) > entry < precedence int > { [ min < addr ipaddr > ]
[ max < addr ipaddr > ] } [ vendor < id string(1:256) > ] [ status { enable | disable } ]
```

Parameter Description

Parameter	Description
interface	Modify the interface for which the IP address pool is to be used. Enter the new interface name.
entry	Modify the pool entry number so as to change its location in the pools table.
min	Modify the first IP address in the pool to be assigned by the DHCP server.
max	Modify the last IP address in the pool to be assigned by the DHCP server.
vendor	Modify the vendor specified for the pool. Enter the new vendor ID for the pool.
status	Modify the pool status.
enable	Enable the pool to use it for IP address assignment.
disable	Disable the pool, if you do not want to use it for IP address assignment.

remove

Description

The `remove` command deletes an existing IP address pool.

Parent

kcli/config/dhcp/pool

Syntax

```
remove interface < ifname string(1:32) > entry < precedence int >
```

Parameter Description

Parameter	Description
interface	Enter the interface name specified for the IP address pool to be deleted.
entry	Enter the entry number for the pool to be deleted.

vid

Description

The `vid` command node adds or deletes a vendor ID in the vendor database.

Parent

kcli/config/dhcp

add

Description

The `add` command adds a new vendor ID to the vendor database.

Parent

kcli/config/dhcp/vid

Syntax

```
add vendor < id string(1:256) > mode { exact | prefix | suffix | substring } script < path string(1:256) > interfaces < iflist string(1:256) >
```

Parameter Description

Parameter	Description
vendor	Enter the vendor ID name string between 1 and 256 characters.
mode	Select the mode for comparing the vendor ID with the actual vendor ID.
exact	Select exact if the configured and actual vendor ID strings should match exactly.
prefix	Select prefix if the actual vendor ID string can be prefixed to the configured vendor ID string, while ensuring that both the vendor IDs have the matching attributes.
suffix	Select suffix if the actual vendor ID string can be suffixed after the configured vendor ID string, while ensuring that both the vendor IDs have the matching attributes.
substring	Select substring, if the actual vendor ID is a substring of the configured vendor ID while matching their attributes.
script	Enter the script path for executing vendor specific configuration, such as QoS and firewall rules when the client acquires or releases IP addresses.
interfaces	Add a comma-separated list of interfaces through which the LAN clients using the specified vendor ID are allowed to resolve the DNS queries.

Example

The following example command adds a vendor ID to the vendor database:

```
#kcli> config dhcp vendor a1b2c3 mode exact script /mnt/rw/HSI.sh interfaces bb0,bb1
<enter>
```

expired-leases-status

Description

The `expired-leases-status` command enables or disables the display of the expired DHCP client leases. The lease period is the time (in seconds) for which the DHCP allocates an IP address to a DHCP client. Before the leases expire, the DHCP clients are expected to renew the leases in order to continue to use the allocated IP addresses.

Parent

kcli/config/dhcp

Syntax

```
expired-leases-status { enable | disable }
```

Parameter Description

Parameter	Description
enable	Enable the expired leases status to view the expired DHCP client leases.
disable	Disable the expired leases status to hide the expired DHCP client leases.

server

Description

The `server` command enables or disables the DHCP server on the LAN interface of the device.

Parent

kcli/config/dhcp

Syntax

```
server { enable | disable } [ dns-proxy { enable | disable } ]
```

Parameter Description

Parameter	Description
enable	Enable the DHCP server on the network.
disable	Disable the DHCP server on the network.
dns-proxy	Enable or disable the DNS proxy.
enable	Enable the DNS proxy service. If enabled, any DNS request is proxied to the device and is resolved by the DNS proxy. If the DNS resolution is not present in DNS cache of the device, the request goes to the public DNS server configured on the device.
disable	Disable the DNS proxy service.

Example

The following example command enables the DHCP server and DNS proxy service on the network:

```
#kcli> config dhcp server enable dns-proxy enable <enter>
```

server-params

Description

The `server-params` command configures the DHCP server parameters.

Parent

kcli/config/dhcp

Syntax

```
server-params { { lease-period < lease_interval integer(60:60) > } | { default-network-type
{ private | public-proxied | public-routed } } }
```

Parameter Description

Parameter	Description
lease-period	Set the DHCP lease period in seconds. The lease period is the time for which the DHCP allocates an IP address to a DHCP client. Before the leases expire, the DHCP clients are expected to renew the leases in order to continue to use the allocated IP addresses. Enter the DHCP lease period between 60 and 86400 seconds.
default-network-type	Select a network type to be used as default network, private, public-proxied or public-routed.
private	Select the private network as default network type.
public-proxied	Select the public-proxied as default network type. This method allows the subnet mask of the public IP addresses provisioned on the primary broadband connection to be statically assigned or DHCP distributed to the specific LAN devices. IP addresses obtained from this subnet are not NATted by the device.
public-routed	Select the public-routed as default network type. This is similar to public proxied subnet, except that this mode allows a different supplementary network to be specified on the LAN. You can specify the IP address and subnet mask.

Example

The following example command configures the lease period and default network type for the DHCP server:

```
#kcli> config dhcp server-params lease-period 86400 default-network-type public-proxied
<enter>
```

network-disable

Description

The `network-disable` command disables the specified network type.

Parent

kcli/config/dhcp

Syntax

```
network-disable network-type { public-proxied | public-routed }
```

Parameter Description

Parameter	Description
network-type	Select the network type to disable it.
public-proxied	Select the public-proxied network type to disable it.
public-routed	Select the public-routed network type to disable it.

network-enable

Description

The `network-enable` command selects the default IP address allocation pool for the DHCP server.

Parent

kcli/config/dhcp

Syntax

```
network-enable network-type { { public-proxied { interface < interface_name string(1:32) > usable-subnet-mask < usable_mask ipaddr > lease-period < lease_interval integer > } } | { public-routed { interface-name < ifname string(0:32) > gateway < gwaddr ipaddr > subnet-mask < subnet_mask ipaddr > lease-period < lease_interval integer > } } }
```

Parameter Description

Parameter	Description
network-type	Select the network type for IP address allocation. The options are public-proxied and public-routed.
public-proxied	Select the public-proxied network type. You can enter the subnet mask as provided by the ISP. Based on the subnet mask addressing, the gateway determines the number of public IP addresses. These are the broadband IP addresses that are statically assigned or dynamically distributed to the LAN clients. IP addresses obtained from this subnet are not NATted by the device.
interface	Enter the public-proxied interface name.
usable-subnet-mask	Enter a usable subnet mask.
public-routed	Select the public-routed network type. This mode allows a different supplementary network to be specified on the LAN. You can specify the desired IP address and subnet mask.
interface-name	Enter the public-routed interface name.
gateway	Specify the gateway IP address, if the network type is public-routed.
subnet-mask	Specify the subnet mask, if the network type is public-routed.
lease-period	Enter the lease period, during when the interface is available for the application. Value ranges from 60 to 86400.

Example

The following example command sets the public-proxie network type for IP address allocation:

```
#kcli> config dhcp network-enable network-type public-proxied interface bb1 usable-subnet-mask 255.255.255.0 lease-period 86400 <enter>
```

option60

Description

The `option60` command selects the public-proxied network type for IP address allocation: allows DHCP relay to direct the client traffic to a specific DHCP server that provides dedicated service required by a DHCP client like Internet access or IPTV service.

Parent

kcli/config/dhcp

Syntax

```
option60 { enable | disable }
```

Parameter Description

Parameter	Description
enable	Enable the Option60 service on your network.
disable	Disable the Option60 service on your network.

optiontr111

Description

The `optiontr111` command enables or disables the vendor-specific information DHCP option TR-111. It allows an ACS managing a device to identify the associated gateway through which thats device is connected. The device identity and gateway identity information exchanged via DHCP is contained within the vendor-specific Information DHCP Option TR-111. This DHCP option is defined to allow vendor-specific information from multiple distinct organizations, where the specific organization is explicitly identified via an IANA Enterprise Number.

Parent

kcli/config/dhcp

Syntax

```
optiontr111 { enable | disable }
```

Parameter Description

Parameter	Description
enable	Enable the Option TR-111 service on the network.
disable	Disable the Option TR-111 service on the network.

self-address-mode

Description

The `self-address-mode` command allows the gateway to use Address Resolution Protocol (ARP) for assigning itself an available IP address from the pool. Self addressing is active only when DHCP server is disabled.

Parent

kcli/config/dhcp

Syntax

```
self-address-mode status { { enable [ self-address-string < selfaddressstring string > ] }
| disable }
```

Parameter Description

Parameter	Description
status	Enable or disable the self addressing mode.
enable	Enable the self addressing mode to obtain an available IP address, if the DHCP server is disabled.
self-address-string	Enter the comma-separated list of IP addresses and IP address range using hyphen. For example, 192.168.1.254, 192.168.1.63, 192.168.1.253-192.168.1.1.
disable	Disable the self addressing mode, if you want to dynamically assign the IP address to the device.

Example

The following example command enables the self addressing mode on the gateway device:

```
#kcli> config dhcp self-address-mode status enable self-address-string 192.168.1.254,
192.168.1.63, 192.168.1.253-192.168.1.1. <enter>
```

QoS Module

This section describes configuration commands for the Quality of Service (QoS) module. You can set various QoS parameters such as default queue, state, classification, etc.

qos

Description

The `qos` command node allows you to enter the configuration mode for setting the QoS parameters. QoS in networking applications is defined as the ability to guarantee pre-defined levels of performance for various applications sharing the same network bandwidth. The level of performance can be parameterized by bit rate, latency, jitter, error rate, etc. The performance guarantees can be prioritized and can vary in nature across applications. When implemented as a feature in networking applications, QoS refers to the ability to control resources such as network bandwidth rather than the actual quality of service achieved by the applications. Given the mix of traffic that flows through the Internet, QoS guarantees become crucial for enabling a good user experience for real time applications such as streaming media, Voice over IP (VoIP), Internet Protocol Television (IPTV), etc. QoS is not only required in Internet backbones and service provider networks, but is also essential in access devices such as CPE. QoS is used to assign different priorities for incoming and outgoing data on the various VLAN ports.

Parent

kcli/config

classification

Description

The `classification` major command configures the traffic classification parameters for classifying the data traffic arriving on the network. Classification checks the data traffic on the interface it arrives on. The classification can be carried out on the basis of several packet characteristics, such as protocol, port number, source or destination address, 802.1p value, incoming interface.

Parent

kcli/config/qos

add

Description

The `add` command adds various classification parameters to check the data traffic on the network. Any combination of classifiers can be used to identify a data flow.

Parent

kcli/config/qos/classification

Syntax

```
add { classifyAny | { [ sourceip < ip string > ] [ sourcemask < mask string > ] [ sourcemac
< mac string > ] [ { [ protocol < protocol integer > ] | [ [ tcp-flags < flags string > ] [
sourceport < port integer > [ sportrange < port integer > ] protocol { tcp | udp } ] [
destport < port integer > [ dportrange < port integer > ] protocol { tcp | udp } ] ] } ] [
destinterface < destiface string > ] [ destip < ip string > ] [ destmask < mask string > ]
[ match_8021p < pvalue integer(0:7) > match_vlanport < vport string > ] [ match_dscp < dscp
integer > ] [ interface { local | < iface string > } ] [ pktlen < length integer > [
pktlenrange < length integer > ] ] } } { [ [ fwmark < fwmark integer > ] [ to_queue <
queueid integer > ] [ to_interface < iface string > [ masquerade { { True [ to_port < port
string > ] } | False } ] [ set_vlanqos < qosvalue interger > ] ] [ set_dscp < dscpvalue
integer(0:63) > ] ] }
```

Parameter Description

Parameter	Description
classifyAny	Select classifyAny option to classify any data packet.
sourceip	Classify and mark the data traffic on the ingress interface based on the source IP address. Enter the source IP address.
sourcemask	Classify and mark the data traffic on the ingress interface based on the source netmask. Enter the source netmask value.
sourcemac	Classify and mark the data traffic on the ingress interface based on the source MAC address. Enter the source MAC address.
protocol	Classify and mark the data traffic on the ingress interface based on the protocol. Enter the protocol number.
sourceport	Classify and mark the data traffic on the ingress interface based on the source port. Enter the source port number.
sportrange	Enter the source port range.
protocol	Select the protocol (TCP or UDP) for the specified source port range.
tcp	Select the TCP protocol.
udp	Select the UDP protocol.
destport	Classify and mark the data traffic on the ingress interface based on the destination port. Enter the destination port number.
dportrange	Enter the destination port range.
tcp-flags	Specify the TCP flags. Note that you can specify TCP flags only if the selected protocol is TCP. For example, SYN,ACK,FIN,RST SYN. The first argument is the flags that should be examined, written as a comma-separated list, and the second argument is a comma-separated list of flags to be set.
destinterface	Classify and mark the data traffic based on the destination interface.
protocol	Select the protocol (TCP or UDP) for the specified destination port range.
tcp	Select the TCP protocol.
udp	Select the UDP protocol.
destip	Classify and mark the data traffic on the ingress interface based on the destination IP address. Enter the destination IP address.
destmask	Classify and mark the data traffic on the ingress interface based on the destination netmask. Enter the destination netmask value.
match_8021p	Match the 802.1p value. It is a 3-bit value in the VLAN header to indicate prioritization. It provides priority levels ranging from 0 to 7 (that is, a total of 8 levels), with level 7 representing the highest priority. This permits packets to cluster and form different traffic classes. Thus, when network congestion occurs, packets having higher priorities will receive preferential treatment while low priority packets will be kept on hold. Enter the 802.1p value to be matched to the data packets between 0 and 7.
match_vlanport	Enter the VLAN port for VLAN ID on which the check is to be performed.
match_dscp	Classify and mark the data traffic based on the DSCP value. Differentiated Services Code Point (DSCP) is a field in the header of IP packets for packet classification purposes (used especially for controlling the bandwidth).
interface	Enter the interface on which the data traffic classification is to be performed.
local	Classify and mark the data traffic generated locally.
pktlen	Classify and mark the data traffic based on the packet length.
pktlenrange	Enter the maximum packet length range.
to_queue	Classify and mark the data traffic to a particular queue. Enter the queue ID.
masquerade	Start masquerading for VLAN. Masquerading is source NATting the outbound traffic.

Parameter	Description
True	Enable masquerade to a port, if you want to use the device as NATter. It allows internally connected computers that do not have one or more registered public IP addresses to communicate to the Internet via the device's public IP address.
to_port	Enter the outgoing port or interface name to which source NATting is to be done.
False	Disable masquerade, if you do not want to use the device as NATter.
set_vlanqos	Classify and mark the data traffic based on the VLAN QoS (802.1p) value. The 802.1p sets a 3-bit value in the VLAN header to indicate prioritization. This 3-bit value provides priority levels ranging from 0 to 7 (that is, a total of 8 levels), with level 7 representing the highest priority. This permits packets to cluster and form different traffic classes. Thus, when network congestion occurs, packets having higher priorities will receive preferential treatment while low priority packets will be kept on hold.
to_interface	Classify the data packet to the outgoing interface. Enter the interface name.
set_dscp	Set DSCP value for the data packet. Differentiated Services Code Point (DSCP) is a field in the header of IP packets for packet classification purposes (used especially for controlling the bandwidth). Enter DSCP value between 1 and 63.
fwmark	Set the firewall mark for the classified packets. Enter a numeric value for the firewall mark.

Example

The following example classifies any data packets having any combination of classifiers:

```
#kcli> config qos classification add classifyAny set_dscp 7 <enter>
```

Alternatively, you can specify the classifiers to identify the matching data flow. For instance, the following example command sets the classification for checking data packets matching the specified criteria:

```
#kcli> config qos classification add sourceip 192.168.1.2 sourcemask 255.255.255.1
sourcemac 10:c4:31:a2:08 sourceport 21 sportrange 80 protocol tcp tcp-flags SYN,ACK,
interface local pktlen 987 pktlenrange 1028 destip 10.29.1.35 destinterface abc1 destport
6000 dportrange 6600 protocol udp destmask 255.255.255.0 match_8021p 6 match_vlanport 6100
match_dscp 8979 to_queue 543 to_interface abc2 set_vlanqos 6 set_dscp 63 fwmark 400 <enter>
```

delete

Description

The `delete` command deletes a classification entry. It can be deleted using the classification ID or the associated parameters.

Parent

kcli/config/qos/classification

Syntax

```
delete { [ classificationid < id integer > ] | [ { classifyAny | { [ sourceip < ip string >
] [ sourcemask < mask string > ] [ sourcemac < mac string > ] [ { [ protocol < protocol
integer > ] | [ [ tcp-flags < flags string > ] [ sourceport < port integer > [ sportrange <
port integer > ] protocol { tcp | udp } ] [ destport < port integer > [ dportrange < port
integer > ] protocol { tcp | udp } ] ] } ] [ destinterface < destiface string > ] [ destip
< ip string > ] [ destmask < mask string > ] [ match_8021p < pvalue integer(0:7) >
match_vlanport < vport string > ] [ match_dscp < dscp integer > ] [ interface { local | <
iface string > } ] [ pktlen < length integer > [ pktlenrange < length integer > ] ] } } { [
[ to_queue < queueid integer > ] [ { [ masquerade { { True [ to_port < port string > ] } |
False } ] [ set_vlanqos < qosvalue interger > ] ] | [ to_interface < interface string > ] }
] [ set_dscp < dscpvalue integer(0:63) > ] ] } ] }
```

Parameter Description

Parameter	Description
classificationid	Enter the ID of the classification to be deleted.
classifyAny	Select classifyAny option to classify any data packet.
sourceip	Enter the source IP address of the data traffic.
sourcemask	Enter the source netmask of the data traffic.
sourcemac	Enter the source MAC address.
protocol	Enter the protocol number.
sourceport	Enter the source port number.
sportrange	Enter the source port range.
protocol	Select the protocol (TCP or UDP) for the specified source port range.
tcp	Select the TCP protocol.
udp	Select the UDP protocol.
destport	Enter the destination port number.
dportrange	Enter the destination port range.
tcp-flags	Enter the TCP flags.
destinterface	Enter the destination interface name.
protocol	Select the protocol (TCP or UDP) for the specified destination port range.
tcp	Select the TCP protocol.
udp	Select the UDP protocol.
destip	Enter the destination IP address.
destmask	Enter the destination netmask value.
match_8021p	Enter the 802.1p value to be matched to the data packets between 0 and 7.
match_vlanport	Enter the VLAN port for VLAN ID on which the check is to be performed.
match_dscp	Enter the DSCP value.
interface	Enter the interface on which the data traffic classification is to be performed.
local	Select the locally generated traffic.
pktlen	Enter the packet length value.
pktlenrange	Enter the maximum packet length range.
to_queue	Enter the queue ID.
masquerade	Start masquerading for VLAN.
True	Enable masquerade to a port.
to_port	Enter the outgoing port or interface name to which source NATting is to be done.
False	Disable masquerade, if you do not want to use the device as NATter.
set_vlanqos	Enter the VLAN QoS (802.1p) value.
to_interface	Enter the outgoing interface name.
set_dscp	Enter the DSCP value (between 1 and 63) for the data packet.
fwmark	Enter a numeric value for the firewall mark.

set

Description

The `set` command enables or disables the classification state.

Parent

kcli/config/qos/classification

Syntax

```
set classificationid < id integer > state { enable | disable }
```

Parameter Description

Parameter	Description
classificationid	Enter the classification ID to set its state.
state	Enable or disable the specified classification.
enable	Enable the specified classification to apply its configurations to the matching data packets.
disable	Disable the specified classification if you do not want to apply its settings to the matching data packets.

queue

Description

The queue major command adds two types of transmit queues for traffic control, hardware queues and software queues. Each network interface in the system can have multiple transmit queues for traffic control. In case of software queues, any given interface can have a maximum of eight queues. In case of hardware queues, the WAN interface can have a maximum of eight queues per PVC in the DSL WAN addressing mode. Whereas the LAN interface can have up to four queues in the DSL and Ethernet WAN addressing mode. These interface queues can be configured under any one of the top-level Queuing Disciplines (qdisc), such as Hierarchical Token Bucket (HTB), Weighted Round Robin (WRR), and Weighted Fair Queue (WFQ).

Parent

kcli/config/qos

Syntax

```
queue
```

add

Description

The add command adds a transmit queue for traffic control.

Parent

kcli/config/qos/queue

Syntax

```
add queue { SP | WRR | WFQ } [ hw-queue DSL | Ethernet ] [ priority < prio integer > ] [ qinterface < interface string > ] [ rate < rate integer > ] [ shapingburst < shapingburst integer > ] [ weight < weight integer > ]
```

Parameter Description

Parameter	Description
queue	Select the queue type for determining the priority of the data packets. The queue types are Strict Priority (SP), Weighted Round Robin (WRR), and Weighted Fair Queuing (WFQ), each of which has a different purpose of queuing.
SP	Add a SP queue. The data packets queued in the SP are scheduled to be transmitted ahead of the packets queued in the rest of the queues.
WRR	Add a WRR queue. WRR scheduling prevents the low-priority queues from being completely neglected during the periods of high priority traffic. By using this scheduling, low-priority queues have the opportunity to transmit packets even though the high priority queues are not empty.
WFQ	Add a WFQ queue. WFQ is a packet scheduling technique that allows guaranteed bandwidth services. The purpose of WFQ is to let several sessions share the same link.
hw-queue	Select the hardware queue type, DSL or ETH (Ethernet.)
DSL	Select DSL as queue type, if the WAN addressing mode is DSL.
ETH	Select ETH (Ethernet) as queue type, if the WAN addressing mode is Ethernet.
priority	Select the priority for the queue. Enter the priority value between 0 and 7 (7 being the highest priority.)
qinterface	Enter the egress interface on which the queue is to be added.
rate	Configure traffic shaping by specifying the amount of bandwidth to be allocated to the logical interface. If the value is less than 100, it should be the percentage of the rate of the highest rate constrained layer over which the packet will travel on egress interface. If the value is greater than 100, it should be in bits per second. A value of -1 indicates no shaping.
shapingburst	The shaping burst size specifies how much traffic (in bytes) per burst can be sent within a given unit of time so as not to create scheduling concerns.
weight	Enter the queue weight. Setting the higher queue weight gives the queue a priority over the other queues with lower weights.

Example

The following example command adds a queue with SP priority on the eth0 interface of the device with the shaping rate as 200 bits/second and shaping burst size as 90 bytes:

```
#kcli>qos queue add queue SP hw-queue DSL priority 5 qinterface bb0 rate 200 shapingburst
90 weight 100 <enter>
```

Note To add or delete a queue, the queue state must be disabled.

set

Description

The `set` command enables or disables the specified queue.

Parent

kcli/config/qos/queue

Syntax

```
set queue < queueid integer > state { enable | disable }
```

Parameter Description

Parameter	Description
queue	Specify the queue ID to set its state.
state	Enable or disable the specified queue.
enable	Enable the queue to apply its configurations for determining the priority of the matching data packets.
disable	Disable the queue if you do not want to apply its settings for determining priority of the data packets.

delete

Description

The `delete` command deletes an existing queue.

Parent

kcli/config/qos/queue

Syntax

```
delete queue < queueid integer >
```

Parameter Description

Parameter	Description
queue	Enter the ID of the queue to be deleted.

state

Description

The `state` command enables or disables the QoS state on the network.

Parent

kcli/config/qos

Syntax

```
state { enable | disable }
```

Parameter Description

Parameter	Description
enable	Enable QoS to activate the queuing operations.
disable	Disable QoS.

Example

The following example command enables the QoS on the network for queuing operations:

```
#kcli> config qos state enable <enter>
```

default-queue

Description

The `default-queue` command sets the default queuing for data packets. If the packets do not classify into any of the custom queues, they must pass through the default queuing mechanism.

Parent

kcli/config/qos

Syntax

```
default-queue < queue_id integer >
```

Example

The following example command sets the default queue with queue ID 50:

```
#kcli> config qos default-queue 50 <enter>
```

TR-069V2 Module

This section describes configuration commands for the TR-069V2 module. You can configure the TR-069 protocol settings as laid by the DSL Forum.

tr69

Description

The `tr69` command node allows you to enter the configuration mode for setting the TR-069 protocol parameters. The TR-069 protocol is used for communication between the CPE device and the Auto-Configuration Server (ACS). This protocol helps in automating most of the tasks involved in remote CPE management.

Parent

kcli/config

device-info

Description

The `device-info` major command sets the device details, used by the ACS to communicate with the device. Majority of the information pertains to the device manufacturer.

Parent

kcli/config/tr69

Syntax

```
device-info
```

device-details

Description

The `device-details` command sets the specification version and provisioning code of the CPE device when the device was connected to the network for the first time.

Parent

kcli/config/tr69/device-info

Syntax

```
device-details [ spec-version < version string(0:0) > ] [ provisioning-code < code string(0:0) > ]
```

Parameter Description

Parameter	Description
spec-version	Enter the version of specification implemented by the device.
provisioning-code	Provisioning Code is the identifier of the primary service provider and other provisioning information, which may be used by the ACS to determine service provider specific customization and provisioning parameters. Enter a numeric value to indicate provisioning code.

Example

The following example command configures the device details:

```
#kcli> config tr69 device-info device-details spec-version 1.25 provisioning-code 5 <enter>
```

description

Description

The `description` command specifies the detailed device information that defines the objective and functionality of the device.

Parent

kcli/config/tr69/device-info

Syntax

```
description < describe string(0:0) > [ model-name < name string(0:0) > ]
```

Parameter Description

Parameter	Description
model-name	Enter the model name of the CPE.

manufacturer-info

Description

The `manufacturer-info` command sets the details of the device manufacturer.

Parent

kcli/config/tr69/device-info

Syntax

```
manufacturer-info [ manufacturer < string string(0:0) > ] [ manufacturer-OUI < oui
string(0:0) > ] [ product-class < class string(0:0) > ]
```

Parameter Description

Parameter	Description
manufacturer	Enter the device manufacturer's name.
manufacturer-OUI	Enter the OUI string-a six hexadecimal-digit value using all upper-case letters and any leading zeros. Manufacturer OUI refers to the Organizationally Unique Identifier (OUI) of the device manufacturer. .
product-class	Enter the product class name.

Example

The following example command configures the manufacturer information:

```
#kcli> config tr69 device-info manufacturer-info manufacturer 2wire manufacturer-OUI 525
product-class a1b2c3 <enter>
```

acs-url

Description

The `acs-url` command sets the URL for the CPE to connect to the ACS. Enter the URL string value.

Parent

kcli/config/tr69

Syntax

```
acs-url < url string(0:0) >
```

Example

The following example command configures the ACS URL:

```
#kcli> config tr69 acs-url www.2wire.com <enter>
```

kick-url

Description

The `kick-url` command configures the LAN accessible URL, using which you can start the CPE. Enter the URL string.

Parent

kcli/config/tr69

Syntax

```
kick-url < url string(0:0) > [ progress-url < url string(0:0) > ]
```

Parameter Description

Parameter	Description
progress-url	Enter the progress URL string. It displays the file download progress.

agent-status

Description

The `agent-status` command enables or disables the TR-Agent service on the CPE.

Parent

kcli/config/tr69

Syntax

```
agent-status { enable | disable }
```

Parameter Description

Parameter	Description
enable	Enable the TR-Agent service on CPE for the remote management of CPE by the ACS.
disable	Disable the TR-Agent service on CPE to disable remote management of CPE by the ACS.

certificate-info

Description

The `certificate-info` command configures the ACS certificate information.

Parent

kcli/config/tr69

Syntax

```
certificate-info [ certificate-path < path displaystring > ] [ certificate-file < file displaystring > ]
```

Parameter Description

Parameter	Description
certificate-path	Enter the path to save and access the certificate.
certificate-file	Enter the certificate file name.

Example

The following example command configures the certificate information:

```
#kcli> config tr69 certificate-info certificate-path /user/local/share/curl/ certificate-file cacert.pem <enter>
```

connection-request-info

Description

The `connection-request-info` command configures the ACS connection request parameters. This enables the ACS to send a connection request to the CPE.

Parent

kcli/config/tr69

Syntax

```
connection-request-info [ cr-url < url string(0:0) > ] [ username < username string(0:0) > ] [ password < passwd string > ]
```

Parameter Description

Parameter	Description
cr-url	Enter the URL string of the CPE where the ACS can send a CR.
username	Enter the CPE's user name for authenticating the connection request.
password	Enter the password for the specified connection request username.

Example

The following example command configures the connection request information:

```
#kcli> config tr69 connection-request-info username abc password a1b5c9 cr-url www.2wire.com <enter>
```

cpe-auth-params

Description

The `cpe-auth-params` command sets the authentication parameters to be used by the CPE to make a connection with the ACS. The parameters include login credentials, as also the basic and digest authentication methods.

Parent

kcli/config/tr69

Syntax

```
cpe-auth-params [ username < username string(0:0) > ] [ password < passwd string(0:0) > ] [
auth-method { Basic | Digest } ]
```

Parameter Description

Parameter	Description
username	Enter the user name to authenticate the CPE.
password	Enter the password for the user name.
auth-method	Select the authentication method to access CPE.
Basic	Select the basic authentication method. Enter the user name and password for this method.
Digest	Select the digest authentication method. Enter the user name and password for this method.

Example

The following example command configures the certificate request information:

```
#kcli> config tr69 cpe-auth-params username xyz password a1b5c9 auth-method Basic <enter>
```

periodic-inform

Description

The `periodic-inform` command configures various parameters of the perodic inform request, such as enabling periodic inform, periodic inform interval, and periodic inform reference time. This is to let the ACS know that the said CPE is active in the network.

Parent

kcli/config/tr69

Syntax

```
periodic-inform { [ true [ inform-interval < interval integer(0:0) > ] [ inform-time <
integer integer(0:0) > ] ] | false }
```

Parameter Description

Parameter	Description
true	Select true to enable periodic inform.
inform-interval	Enter the duration (in seconds) for the CPE to attempt connecting to ACS.
inform-time	Enter the absolute time (in seconds) for the CPE to initiate the inform method calls.
false	Select false to disable periodic inform.

request-download

Description

The `request-download` command configures the execution of request download RPC.

Parent

kcli/config/tr69

Syntax

```
request-download filetype { Firmware_upgrade | Web_content | Vendor_config_file } [
argument-name < name string(0:0) > ] [ argument-value < value string(0:0) > ]
```

Parameter Description

Parameter	Description
filetype	Configure the file types supported by TR-069 for download.
Firmware_upgrade	Request for download of firmware upgrade image for entire board.
Web_content	Request for download of Web UI packages.
Vendor_config_file	Request for download of vendor specific configuration packages.
argument-name	Enter an alphanumeric value for file argument name.
argument-value	Enter a numeric value for file argument value.

Example

The following example command configures the execution of request download:

```
#kcli> config tr69 request-download filetype Firmware_upgrade argument-name abc argument-
value 123 <enter>
```

upgrades-manage

Description

The `upgrades-manage` command determines whether the Management Interface (MI) other than ACS is allowed to upgrade the firmware.

Parent

kcli/config/tr69

Syntax

```
upgrades-manage { true | false }
```

Parameter Description

Parameter	Description
true	Select true to allow only the ACS to manage upgrades for the CPE. Other management interfaces are not allowed to upgrade the CPE.
false	Select false to enable ACS and other management interfaces to upgrade the CPE.

cwmpinterface

Description

The `cwmpinterface` command sets the WAN interface to be used for TR-069. Enter the WAN interface name.

Parent

kcli/config/tr69

Syntax

```
cwmpinterface < cwmpinterface string(0:0) >
```

tr69-remote-ui-config

Description

The `tr69-remote-ui-config` command enables or disables the remote access for the Technician Login interface for configuring the advanced gateway settings.

Parent

kcli/config/tr69

Syntax

```
tr69-remote-ui-config { [ true [ remote-ui-min-port < minport integer(0:65000) > ] [
remote-ui-max-port < maxport integer(0:65000) > ] [ max-session-no < maxsession
integer(0:65000) > ] ] | false }
```

Parameter Description

Parameter	Description
true	Enable the remote access for Technician Login interface.
remote-ui-min-port	Enter the minimum port range for remote access.
remote-ui-max-port	Enter the maximum port range for remote access.
max-session-no	Enter the maximum number of concurrent sessions.
false	Disable the remote access for Technician Login interface.

Example

The following example command configures the remote UI access parameters:

```
#kcli> config tr69 tr69-remote-ui-config true remote-ui-min-port 6000 remote-ui-max-port
6600 max-session-no 3 <enter>
```

Interface Module

This section describes configuration commands for the interface module. You can configure the LAN and WAN interfaces on your network.

if

Description

The `if` command node allows you to enter the configuration mode for setting the LAN and WAN interface parameters on the network.

Parent

kcli/config

route-add

Description

The `route-add` command configures the routes to other network devices. The user may add routing entries when required to add static routes to other network devices.

Parent

kcli/config/if

Syntax

```
route-add destination { { default } | { < dest-ip ipaddr > < dest-mask ipaddr > } } gw-addr
< gw-addr ipaddr > [ metric < metric integer > ]
```

Parameter Description

Parameter	Description
destination	Enter the destination IP address and subnet mask or set the default destination to capture all the IP addresses on the network. Destination address refers to the static IP address for a route, a machine or a subnet.
default	Select default for the destination route to capture all the IP addresses on the network.
gw-addr	Enter the IP address of the gateway to reach the destination. This is the gateway IP address of the static route.
metric	Enter a numeric value for the routing metric. This refers to the cost metric for the route. Metric is used for choosing among the multiple routes in the routing table that closely match the destination address of a packet being forwarded. The route with the lowest metric is chosen. The metric can reflect the number of hops, the speed of the path, path reliability, path bandwidth, MTU, or administrative properties.

Example

The following example command configures the route to other network devices:

```
#kcli> config if route-add destination 192.134.54.68 gw-addr 192.168.4.1 metric 16 <enter>
```

route-del

Description

The `route-del` command deletes the configured route.

Parent

kcli/config/if

Syntax

```
route-del destination { { default } | { < dest-ip ipaddr > < dest-mask ipaddr > } }
```

Parameter Description

Parameter	Description
destination	Enter the destination IP address of the route to be deleted.
default	Enter default if you have set the default destination to capture all the IP addresses in the network while configuring the routing parameters. Enter the destination IP address and network mask for the route to be deleted.

staticparams

Description

The `staticparams` command configures the parameters for the static WAN connection.

Parent

kcli/config/if

Syntax

```
staticparams ip < staticaddr ipaddr > netmask < mask ipaddr > gw < gwaddr ipaddr >
```

Parameter Description

Parameter	Description
ip	Enter the IP address required to connect to the WAN.
netmask	Enter the network mask for WAN connection.
gw	Enter the WAN router IP address.

Example

The following example command configures the status parameters for the interface:

```
#kcli> config if staticparams ip 192.168.10.88 netmask 255.255.255.0 gw 192.164.10.1
<enter>
```

wan-addrmode

Description

The `wan-addrmode` command configures the WAN addressing mode, PPPoE, PPPoA, DHCP, or static.

Parent

kcli/config/if

Syntax

```
wan-addrmode { pppoe | dhcp | static | pppoa | none } [ tunnel_mode { pptp | l2tp | none } ]
```

Parameter Description

Parameter	Description
pppoe	Select the PPPoE mode to get the IP address from a PPPoE server. Point-to-Point Protocol over Ethernet (PPPoE) is used for connecting the users on an Ethernet to the Internet through a common broadband medium, such as a single DSL line, wireless device or cable modem.
dhcp	Select the DHCP mode for dynamically assigning an IP address to the device. Dynamic Host Configuration Protocol (DHCP) is a client-server networking protocol that provides a mechanism for allocation of IP addresses to clients. With dynamic addressing, a device can have a different IP address every time it connects to the network.
static	Select the static mode to statically configure the device IP address.
pppoa	Select the PPPoA mode to get the IP address from the PPPoA server. Point-to-Point Protocol over ATM (PPPoA) is a network protocol for encapsulating PPP frames in ATM AAL5. It is used mainly with cable modem, DSL and ADSL services. It offers standard PPP features such as authentication, encryption, and compression. If it is used as the connection encapsulation method on an ATM based network, it can reduce overhead slightly in comparison to PPPoE. It avoids the issues related to the lower MTU as compared to the standard Ethernet transmission protocols. It also supports the encapsulation types, VC-MUX and LLC based.
none	Select the none option to switch between the WAN and LAN interfaces. If you do not use this option, the reset to LAN/WAN would not take place.
tunnel_mode	Select the tunnel mode for the WAN interface for added security, PPTP, L2TP or none. Setting tunnel wraps the entire IP packet inside a new IP packet and attaches a new IP header to it before tranmitting it through the public network. The destination address contained in the new header is an IPSec entity that unwraps the packet and sends it to its ultimate destination. Thus, tunneling hides the source and destination addresses before the data is sent through the insecure network. The receiving device recovers the hidden addresses and delivers the packet to its intended address.
pptp	Select PPTP as tunnel mode. Point-to-Point Tunneling Protocol (PPTP) is used for implementing VPNs. It provides the facility to dial in to the corporate network via Internet.
l2tp	Select L2TP as tunnel mode. Layer 2 Tunneling Protocol (L2TP) is a tunneling protocol used for supporting VPNs. It facilitates tunneling network traffic between two peers over Internet.
none	Select none if you do not want to set any tunneling mode on the network.

Example

The following example command configures the DHCP as WAN connection type:

```
#kcli> config if wan-addrmode dhcp tunnel_mode pptp <enter>
```

interface-state

Description

The `interface-state` command enables or disables the interface. Enter the interface name to set its status.

Parent

kcli/config/if

Syntax

```
interface-state < interface-name string(1:32) > { enable | disable | disableip | resetToLan
| resetToWan | resetToSecondaryWan }
```

Parameter Description

Parameter	Description
enable	Enable the specified interface.
disable	Disable the specified interface.
disableip	Remove the configured IP address of the specified interface.
resetToLan	If the specified interface is configured as WAN interface, then reset it as LAN interface.
resetToWan	If the specified interface is configured as LAN interface, then reset it as WAN interface.
resetToSecondaryWan	If the specified interface is configured as LAN interface, then reset it as secondary WAN interface.

Example

The following example command enables the interface state:

```
#kcli> config if interface-state bb0 enable <enter>
```

interface

Description

The `interface` command configures interface parameters such as IP address, netmask, broadcast address, or enable the DHCP client for dynamically obtaining the IP address from a DHCP server. Enter the interface name to configure its parameters.

Parent

kcli/config/if

Syntax

```
interface < interface_name string(1:32) > { dhcp_client { enable [ get_dns { enable |
disable } ] } | { none } } | { pppoe_client { enable | disable } } | { pppoa_client { enable
| disable } } | { { ip < ipaddress ipaddr > mask < netmask ipaddr > broadcast < broadcast
ipaddr > } [ gateway < gwaddr ipaddr > ] [ mtu < mtu integer > ] }
```

Parameter Description

Parameter	Description
ip	Enter the IP address of the interface.
dhcp_client	Start the DHCP client on the interface to get the IP address dynamically from the server.
enable	Enable the DHCP client on the interface.
get_dns	Enable DNS option to get the DNS information for the DHCP client from the server.
enable	Enable the DNS information for the interface.
disable	Disable the DNS information for the interface.
none	Select none if you do not want to start DHCP client on the interface.
pppoe_client	Start or stop PPPoE client on the specified interface.
enable	Select enable to start the PPPoE client on the specified interface.
disable	Select disable to stop the PPPoE client on the specified interface.
pppoa_client	Start or stop PPPoA client on the specified interface.
enable	Select enable to start the PPPoA client on the specified interface.
disable	Select disable to stop the PPPoA client on the specified interface.
mask	Enter the network mask for the interface.
broadcast	Enter the broadcast address for the interface.
gateway	Enter the gateway IP address.
mtu	Enter the MTU value for the interface. Maximum Transmission Unit (MTU) refers to the size (in bytes) of the largest packet that a given layer of a communication protocol can transmit. Any message larger than the specified MTU is divided into smaller packets before being sent.

Example

The following example command configures the DHCP type client interface:

```
#kcli> config if interface eth0 dhcp_client enable get_dns enable <enter>
```

clone_wanmac

Description

The `clone_wanmac` command configures the MAC address cloning feature. If enabled, it sets the router's WAN port MAC address to any computer on the network.

Parent

kcli/config/if

Syntax

```
clone_wanmac { mac_addr < mac macaddr > enable } | { disable }
```

Parameter Description

Parameter	Description
mac_addr	Enter the new MAC address for the WAN interface.
enable	Enable the MAC address to apply it on the WAN addressing mode change.
disable	Disable the MAC address cloning feature.

Example

The following example command enables the MAC address to apply it on the WAN addressing mode change:

```
#kcli> config if interface eth0 clone_wanmac 4c:00:10:c4:eb:06 enable <enter>
```

Note The addressing mode needs to be re-applied or changed to some other mode in order to apply the new MAC address to the interface.

def_mode

Description

The `def_mode` command sets the default mode (PPPoE, PPPoA, DCHP, or none) for the specified WAN access type (DSL or Ethernet).

Parent

kcli/config/if

dsl_iface

Description

The `dsl_iface` command sets the default WAN addressing mode for the DSL interface.

Parent

kcli/config/if/def_mode

Syntax

```
dsl_iface { none | dhcp | pppoe | pppoa }
```

Parameter Description

Parameter	Description
none	Select none if no default WAN addressing mode is to be set for the DSL interface.
dhcp	Select DHCP as default WAN addressing mode for the DSL interface. Now, whenever the WAN access type is changed to DSL, the WAN addressing mode applied is DHCP.
pppoe	Select PPPoE as default WAN addressing mode for the DSL interface. Now, whenever the WAN access type is changed to DSL, the WAN addressing mode applied is PPPoE.
pppoa	Select PPPoA as default WAN addressing mode for the DSL interface. Now, whenever the WAN access type is changed to DSL, the WAN addressing mode applied is PPPoA.

Example

The following example command sets DHCP as the default WAN addressing mode for the DSL interface:

```
#kcli> config if def_mode dsl_iface dhcp <enter>
```

eth_iface

Description

The `eth_iface` command sets the default WAN addressing mode for the Ethernet interface.

Parent

kcli/config/if/def_mode

Syntax

```
eth_iface { none | dhcp | pppoe | pppoa }
```

Parameter Description

Parameter	Description
none	Select none if no default WAN addressing mode is to be set for the Ethernet interface.
dhcp	Select DHCP as default WAN addressing mode for the Ethernet interface. Now, whenever the WAN access type is changed to Ethernet, the WAN addressing mode applied is DHCP.
pppoe	Select PPPoE as default WAN addressing mode for the Ethernet interface. Now, whenever the WAN access type is changed to Ethernet, the WAN addressing mode applied is PPPoE.
pppoa	Select PPPoA as default WAN addressing mode for the Ethernet interface. Now, whenever the WAN access type is changed to Ethernet, the WAN addressing mode applied is PPPoA.

Example

The following example command sets DHCP as the default WAN addressing mode for the Ethernet interface:

```
#kcli> config if def_mode eth_iface dhcp <enter>
```

stop-wan-service

Description

The `stop-wan-service` command stops the WAN addressing service that could be PPPoE, PPPoA, or DHCP, running on the primary broadband interface.

Parent

kcli/config/if

Syntax

```
stop-wan-service
```

wan-access-type

Description

The `wan-access-type` command configures the WAN access type, DSL, Ethernet or auto.

Parent

kcli/config/if

Syntax

```
wan-access-type { DSL | Ethernet | Auto }
```

Parameter Description

Parameter	Description
DSL	Select DSL as WAN access type. Enter the PVC values for the same.
Ethernet	Select Ethernet as WAN access type. With this option, you can create VLANs on the network.
Auto	Select auto as WAN access type to automatically detect the connection mode (Ethernet or DSL).

mdi_config

Description

The `mdi_config` command configures the MDI settings on the gateway. Here, you can specify different settings on each of the Ethernet ports. MDI/MDIX is a type of Ethernet port connection using twisted pair cabling. The MDI is the component of the media attachment unit that provides physical and electrical connection to the cabling medium. An MDIX (MDI crossover) is a version of MDI that enables connection between devices. MDI ports connect to MDIX ports via straight-through twisted pair cabling. Both the MDI-to-MDI and MDIX-to-MDIX connections use crossover twisted pair cabling.

Parent

kcli/config/if

Syntax

```
mdi_config port < number integer > state { auto | mdi | mdix }
```

Parameter Description

Parameter	Description
port	Specify the Ethernet LAN port number on which MDI is to be configured.
state	Select the state of MDI, auto (for detecting the cables automatically), MDI (straight cables), or MDIX (crossover cable).
Auto	Select auto for auto-detection of the cable type (MDI or MDIX). If this option is selected, the gateway automatically detects the transmit and receive pairs (MDI/MDIX) set on the Ethernet WAN interface and makes the swap internally.
mdi	Select MDI if the connection is via straight-through cable. This is the standard twisted pair Ethernet port (Medium Dependent Interface).
mdix	Select MDIX if the connection is via crossover cable. This is a version of MDI that enables connection between like devices used for crossover.

Example

The following example command configures the MDI settings:

```
#kcli> config if mdi_config port 2 state mdi <enter>
```

pppoe-relay-add

Description

The `pppoe-relay-add` command adds a PPPoE relay service on the gateway. You can specify the WAN and LAN interfaces for the PPPoE relay service. This is a user-space relay agent for PPPoE. It works in concert with the PPPoE client and server.

Parent

kcli/config/if

Syntax

```
pppoe-relay-add wan_interface < name string > lan_interfaces < lannames string > no-of-sessions < sessions integer > state { enable | disable }
```

Parameter Description

Parameter	Description
wan_interface	Enter the WAN interface name managed by PPPoE relay. The in and out requests are managed on this interface.
lan_interfaces	Enter the LAN interfaces that can use the PPPoE relay service. Only PPPoE clients are connected to these interfaces. Once a LAN interface is added, the connected clients can obtain IP address from the PPPoE server.
no-of-sessions	Enter the number of concurrent PPPoE sessions that are allowed through PPPoE relay service. Default value is 5000. The allowed range is 1 to 65534.
state	Enable or disable the PPPoE relay on the gateway.
enable	Enable the PPPoE relay to assign IP address to the LAN workstations running a PPPoE client.
disable	Disable the PPPoE relay.

Example

The following example command adds a WAN interface PPPoE relay on the device:

```
#kcli> config if pppoe-relay-add wan_interface bb1 lan_interfaces bb0,bb2 no-of-sessions 2
state enable <enter>
```

pppoe-relay-delete

Description

The `pppoe-relay-delete` command deletes the specified PPPoE relay.

Parent

kcli/config/if

Syntax

```
pppoe-relay-delete wan_interface < name string >
```

Parameter Description

Parameter	Description
wan_interface	Enter the WAN interface on which PPPoE relay is running.

pppoe-relay-modify

Description

The `pppoe-relay-modify` command modifies the configured PPPoE relay settings.

Parent

kcli/config/if

Syntax

```
pppoe-relay-modify wan_interface < name string > [ lan_interfaces < lannames string > ] [
no-of-sessions < sessions integer > ] [ state { enable | disable } ]
```

Parameter Description

Parameter	Description
wan_interface	Modify the WAN interface on which PPPoE relay is running. Enter the name of the new WAN interface.
lan_interfaces	Modify the LAN interfaces specified for PPPoE relay. Enter the new LAN interfaces names.
no-of-sessions	Modify the number of PPPoE sessions. Enter the new number for the same.
state	Modify the PPPoE relay state (enable or disable).
enable	Enable PPPoE relay if it is not already enabled.
disable	Disable PPPoE relay if it is not already disabled.

re-apply-wan-mode

Description

The `re-apply-wan-mode` command re-applies the WAN addressing mode, PPPoE, PPPoA, DHCP, static, or none.

Parent

kcli/config/if

Syntax

```
re-apply-wan-mode
```

auto-wan-addrmode

Description

The `auto-wan-addrmode` command enables the device to automatically select the WAN addressing mode (DHCP, PPPoE, PPPoA, or static).

Parent

kcli/config/if

Syntax

```
auto-wan-addrmode { enable | disable }
```

Parameter Description

Parameter	Description
enable	Select enable to automatically select the WAN addressing mode.
disable	Select disable if you want to manually configure the WAN addressing mode.

TR111Part1 Module

This section describes configuration commands of the TR111Part1 module. You can configure TR-111 to facilitate the identification of the associated gateway through the ACS, using the CPE WAN management protocol.

tr111part1

Description

The `tr111part1` command allows you to enter the configuration mode of TR-111 module. TR-111 is a CPE WAN management protocol that allows an ACS to identify the associated gateway.

Parent

kcli/config

manageable-device

Description

The `manageable-device` major command adds or deletes a device, managed by the TR-111 service, on the gateway. Specify the device details such as manufacturer OUI, product class, MAC address.

Parent

kcli/config/tr111part1

add

Description

The `add` command adds a device to be managed by the TR-111 service.

Parent

kcli/config/tr111part1/manageable-device

Syntax

```
add Manufacturer-OUI < oui string> Serial-Number < number string> Product-Class < class string> MAC-Addr < addr string>
```

Parameter Description

Parameter	Description
Manufacturer-OUI	Enter the OUI string, a six hexadecimal digit value using all upper-case letters and any leading zeros. OUI refers to the Organizationally Unique Identifier (OUI) of the device manufacturer.
Serial-Number	Enter the serial number of the device as provided to the gateway by the device.
Product-Class	Enter the product category name. This is the identifier of the product class, for which the device serial number applies as provided to the gateway by the device.
MAC-Addr	Enter the device MAC address.

Example

The following example command adds a device with the specified information to be managed by the TR-111 service:

```
#kcli> config tr111part1 manageable-device add Manufacturer-OUI 2wire Serial-Number 1234567890 Product-Class abc MAC-Addr 01:23:45:67:89:ab <enter>
```

delete

Description

The `delete` command deletes an existing device managed by the TR-111 service.

Parent

kcli/config/tr111part1/manageable-device

Syntax

```
delete MAC-Addr < addr string>
```

Parameter Description

Parameter	Description
MAC-Addr	Enter the MAC address of the device to be deleted.

manageable-device-notification-limit

Description

The `manageable-device-notification-limit` command sets the minimum time, in seconds, between active notifications requested by the ACS, when a device entry is added or removed. That is, the frequency (in seconds) of the active notifications resulting from addition or deletion of manageable devices. Enter the minimum notification time in seconds.

Parent

kcli/config/tr111part1

Syntax

```
manageable-device-notification-limit < limit integer>
```

DSL Module

This section describes configuration commands for the DSL module. You can set the DSL parameters like loop diagnostic state, auto-scanning, retrain, modulation type, interface, etc.

dsl

Description

The `dsl` command node allows you to enter the configuration mode to set various DSL parameters.

Parent

kcli/config

interface

Description

The `interface` major command configures the interface for DSL. Enter the interface name.

Parent

kcli/config/dsl

Syntax

```
interface < ifname string(1:32) >
```

atm-parameters

Description

The `atm-parameters` command configures the Asynchronous Transfer Mode (ATM) parameters like encapsulation, qos, peak-cell-rate, max-burst-size, and sustainable-cell-rate. ATM is a fast-packet, connection-oriented, and cell-switching technology for broadband signals. You can configure ATM parameters to enable the gateway to communicate with the DSLAM.

Parent

kcli/config/dsl/interface

Syntax

```
atm-parameters [ atm-encapsulation { bridged_llc | bridged_vcmux | routed_llc |
routed_vcmux } ] [ atm-qos { UBR | CBR | GFR | ABR | VBR } ] [ atm-peak-cell-rate <
atmprakcellrate integer > ] [ atm-max-burst-size < atmmaxburstsize integer > ] [ atm-
sustainable-cell-rate < sustainablecellrate integer > ]
```

Parameter Description

Parameter	Description
atm-encapsulation	Select the encapsulation of different protocols like Logical Link Control (LLC) and Virtual Channel Multiplex (VCMUX) in ATM cells. In LLC mode, a single virtual channel can be used by different protocols. In VCMUX mode, each protocol uses a separate virtual channel.
bridged_llc	Select bridged LLC mode, if the WAN addressing mode is PPPoE, DHCP, or static.
bridged_vcmux	Select bridged VCMUX mode, if the WAN addressing mode is PPPoE, DHCP, or static.
routed_llc	Select routed LLC mode, if the WAN addressing mode is PPPoA.
routed_vcmux	Select routed VCMUX mode, if the WAN addressing mode is PPPoA.
atm-qos	ATM QoS assures that data transfer speed is consistent. ATM generally operates at minimum access speeds of DS-1 (for example, T1 at 1.544 Mbps and E-1 at 2.048 Mbps) and DS-3 (for example, E-3 at 34.368 Mbps and T1 at 44.736 Mbps).
UBR	In case of Unspecified Bit Rate (UBR), the traffic is allocated to all remaining transmission capacity.
CBR	In case of Constant Bit Rate (CBR), a peak cell rate is specified, which is constant.
GFR	In case of Guaranteed Frame Rate (GFR), a class of traffic accesses the additional bandwidth dynamically as it becomes available to support non real-time application.
ABR	In case of Available Bit Rate (ABR), a minimum guaranteed rate is specified.
VBR	In case of Variable Bit Rate (VBR), an average cell rate is specified, which can peak at a certain level for a maximum interval before surfacing any issues.
atm-peak-cell-rate	Enter the ATM PCR value. ATM Peak Cell Rate (PCR) is the maximum transfer rate that the VC is permitted to transmit. Value ranges from 0 to 4294967295.
atm-max-burst-size	Enter a numeric value to indicate the ATM max burst size. ATM max burst size is the maximum number of sent at the peak cell rate for VC to calculate the Burst Tolerance for the channel. Value ranges from 0 to 4294967295.
atm-sustainable-cell-rate	Enter the ATM sustainable cell rate value. ATM sustainable cell rate is the mean transfer rate that the network guarantees to the VC. Value ranges from 0 to 4294967295.

Example

The following example command configures the ATM parameters of interface bb0:

```
#kcli> config dsl interface bb0 atm-parameters atm-encapsulation bridged_llc atm-qos UBR
atm-peak-cell-rate 15 atm-max-burst-size 16 atm-sustainable-cell-rate 17 <enter>
```

basic-config

Description

The `basic-config` command configures the basic interface parameters for DSL.

Parent

kcli/config/dsl/interface

Syntax

```
basic-config [ interface-config { enable | disable } ] [ link-type < linktype string > ] [ destination-address < ipaddress ipaddr > ] [ fcs-preserved { enable | disable } ] [ vc-searchlist < vcsearchlist string > ] [ default-pbit < def_pbit integer > ]
```

Parameter Description

Parameter	Description
interface-config	Enables or disables the DSL physical link.
enable	Enables DSL physical link.
disable	Disables DSL physical link.
link-type	Enter the link type for DSL connection. It refers to the complete stack of protocol used for this connection.
destination-address	Enter the destination address of PVC or SVC.
fcs-preserved	Enable or disable FCS preserved. Frame Check Sequence (FCS) indicates if a checksum is to be added in the ATM payload and is only applicable in the upstream direction.
enable	Enable FCS preserved.
disable	Disable FCS preserved.
vc-searchlist	Enter the comma-separated ordered list of VPI/VCI pairs to search, if a link using the destination address cannot be established. VC searchlist is used, when the CPE fails to establish a connection and the auto scanning is enabled. The device starts scanning the PVCs mentioned in the VC searchlist only for the first time.
default-pbit	Enter the default P-bit that should be used for parity checking. A Parity-bit (P-bit) is an error detectecting mechanism used against an array of data. It is an additional binary digit added to the group of bits forming a data packet. Every byte of data stored in the system memory contains 8 bits of actual data, each of them is either a one (1) or a zero (0). For example, 10110011 has 3 zeros and 5 one bits. Whereas the byte 00100100 has 6 zeros and 2 ones. That is, some bytes have an even number of ones (1) and some have odd number. If the data byte has an even number of ones, the parity bit added to the data packet is set to one (1), otherwise it is set to zero (0). When the data is transmitted, the binary digits sent must match the length of bits that the recipient is expecting. If the data is even and the data sent with its parity bit is odd, the data packet is rejected due to an error in parity.

Example

The following example command configures the basic parameters of interface bb0:

```
#kcli> config dsl interface bb0 basic-config interface-config enable link-type pppoa destination-address PVC:8/35 fcs-preserved enable vc-searchlist 0/35,0/36 default-pbit -2 <enter>
```

delete

Description

The `delete` command deletes the DSL link.

Parent

kcli/config/dsl/interface

Syntax

```
delete
```

auto-scanning

Description

The `auto-scanning` command configures the auto-scan function to negotiate the VPI/VCI and encapsulation type on the DSLAM device.

Parent

kcli/config/dsl

Syntax

```
auto-scanning { on | off }
```

Parameter Description

Parameter	Description
on	Enable the auto-scanning function to negotiate VPI/VCI and encapsulation type on the DSLAM device.
off	Disable the auto-scanning function to enforce the configured VPI/VCI and encapsulation type on the gateway.

annex_m

Description

The `annex-m` command expands the capability of pre-enabled annex_a installed on the gateway, thus resulting in higher bandwidths. The data rates can be approximately as high as 12 or 24 Mbit/s while downloading and 3 Mbit/s while uploading.

Parent

kcli/config/dsl

Syntax

```
annex_m { on | off }
```

Parameter Description

Parameter	Description
on	Enable the Annex M to support higher bandwidth on the gateway.
off	Disable the Annex M support on the gateway.

eoc-serial-number

Description

The `eoc-serial-number` command stores the serial number of the gateway in the non-volatile memory. This number is shared with the ATU-C or Original Equipment Manufacturer (OEM) through the xDSL embedded operations channel to support administration and maintenance activities. Enter the EOC serial number.

Parent

kcli/config/dsl

Syntax

```
eoc-serial-number < eoc_serial_number string(1:128) >
```

eoc-vendor-id

Description

The `eoc-vendor-id` command stores the vendor ID of the gateway in the non-volatile memory. This ID is shared with the ATU-C or Original Equipment Manufacturer (OEM) through the xDSL embedded operations channel to support administration and maintenance activities. Enter the EOC system vendor ID.

Parent

kcli/config/dsl

Syntax

```
eoc-vendor-id < eoc_vendor_id string(1:128) >
```

eoc-version

Description

The `eoc-version` command stores the firmware version of the gateway in the non-volatile memory. This version is shared with the ATU-C or Original Equipment Manufacturer (OEM) through the xDSL embedded operations channel to support administration and maintenance activities. Enter the EOC version of the system software.

Parent

kcli/config/dsl

Syntax

```
eoc-version < eoc_version string(1:128) >
```

loop-diagnostics-state

Description

The `loop-diagnostics-state` command configures the loop diagnostics for indicating availability of diagnostic data. Enter a alphanumeric value to indicate the loop diagnostics state.

Parent

kcli/config/dsl

Syntax

```
loop-diagnostics-state < loopdiagnostics string >
```

mode_adsl2

Description

The `mode_adsl2` command enables or disables the ADSL2 support. ADSL2 extends the capability of basic ADSL. The data rates can be approximately as high as 24Mb/s for downloading and 3.5Mb/s for uploading.

Parent

kcli/config/dsl

Syntax

```
mode_adsl2 { on | off }
```

Parameter Description

Parameter	Description
on	Enable the ADSL2 mode.
off	Disable the ADSL2 mode.

mode_adsl2plus

Description

The `mode_adsl2plus` command enables or disables the ADSL2+ support. ADSL2+ extends the capability of basic ADSL. The data rates can be approximately as high as 24 Mbit/s for downloading and up to 3.5 Mbit/s for uploading.

Parent

kcli/config/dsl

Syntax

```
mode_adsl2plus { on | off }
```

Parameter Description

Parameter	Description
on	Enable the ADSL2+ mode.
off	Disable the ADSL2+ mode.

mode_auto

Description

The `mode_auto` command enables or disables the automatic seletion of xDSL modem supported mode. If enabled, the gateway attempts to connect in a mode supported by the xDSL modem device. If disabled, the supported mode must be manually defined by the user.

Parent

kcli/config/dsl

Syntax

```
mode_auto { on | off }
```

Parameter Description

Parameter	Description
on	Enable the auto mode so that the DSL modem connects in any mode supported by the xDSL modem device.
off	Disable the auto mode, if you want to manually define the allowed modes.

mode_gdmt

Description

The `mode_gdmt` command enables or disables the G.DMT support. G.DMT full-rate ADSL expands the usable bandwidth of existing copper telephone lines by delivering high-speed data rates up to 12 Mbit/s for downloading and 1.3 Mbit/s for uploading.

Parent

kcli/config/dsl

Syntax

```
mode_gdmt { on | off }
```

Parameter Description

Parameter	Description
on	Enable the G.DMT mode.
off	Disable the G.DMT mode.

mode_glite

Description

The `mode_glite` command enables or disables the G.Lite support. Enabling G.Lite provides greater resistance to noise and tolerates longer loop lengths, thus minimizing bandwidth loss while the data is sent to the customer premises. G.Lite supports upto 1.5 Mbit/s download speeds.

Parent

kcli/config/dsl

Syntax

```
mode_glite { on | off }
```

Parameter Description

Parameter	Description
on	Enable the G.Lite mode.
off	Disable the G.Lite mode.

mode_t1413

Description

The `mode_t1413` command enables or disables the ANSI T1.413 support. ANSI T1.413 supports the DMT protocol, which is a full-rate implementation of ADSL. ANSI T1.413 defines the interaction and electrical characteristics requirements for the connection between the ISP and the gateway installed at customer premises.

Parent

kcli/config/dsl

Syntax

```
mode_t1413 { on | off }
```

Parameter Description

Parameter	Description
on	Enable the T1.413 mode.
off	Disable the T1.413 mode.

mode_VDSL2

Description

The `mode_VDSL2` command enables or disables the VDSL2 support. VDSL2 is an enhancement to G.993.1 (VDSL) that permits the transmission of asymmetric and symmetric aggregate data rates up to 200 Mbit/s on twisted pairs using a bandwidth of up to 30 MHz. VDSL2 is the newest and most advanced standard of DSL broadband wireline communications. Designed to support the wide deployment of Triple Play services such as voice, video, data, high definition television (HDTV), and interactive gaming. VDSL2 enables operators and carriers to gradually, flexibly, and cost efficiently upgrade existing xDSL infrastructure.

Parent

kcli/config/dsl

Syntax

```
mode_VDSL2 { on | off }
```

Parameter Description

Parameter	Description
on	Enable the VDSL2 mode.
off	Disable the VDSL2 mode.

modulation-type

Description

The `modulation-type` command sets the type of DSL mode. When set to auto, xDSL modes are controlled by the auto mode. To override the automatic mode control, set the modulation type to ADSL2+, ADSL2, or ADSL1.

Parent

kcli/config/dsl

Syntax

```
modulation-type { ADSL_2plus | ADSL2 | ADSL | Auto }
```

Parameter Description

Parameter	Description
ADSL_2plus	Set the ADSL2+ line to train in the ITU G.992.5 mode.
ADSL2	Set the ADSL2 line to train in the ITU G.992.5 mode.
ADSL	Set the ADSL line to train in the ITU G.992.5 mode.
Auto	Set the ADSL line to auto-negotiate the setting to match the setting of the DSL access multiplexer (DSLAM) that is centrally located.

Example

The following example command configures the modulation type:

```
#kcli> config dsl modulation-type ADSL_2plus <enter>
```

nlnm_threshold

Description

The `nlnm_threshold` command sets the NLNM threshold. Non-linear Noise Monitoring (NLNM) threshold is the number of tones with excessive non-linear noise that triggers flagging of unexpected line conditions, such as, missing phone filter.

Parent

kcli/config/dsl

Syntax

```
nlnm_threshold < nlnm_threshold string >
```

phy_r

Description

The `phy_r` command enables or disables the physical layer re-transmission feature. This feature is functional when ISPs devices relay signals that support Broadcom xDSL chips installed on the gateway at customer premises.

Parent

kcli/config/dsl

Syntax

```
phy_r { on | off }
```

Parameter Description

Parameter	Description
on	Enable the physical layer re-transmission.
off	Disable the physical layer re-transmission.

re_adsl

Description

The `re_adsl` command enables or disables the Reach Extended ADSL mode (also known as Annex L mode). This mode optimizes bit-loading between upstream and downstream ADSL2/2+ bands to allow the longest possible loop reach. It is enabled for ADSL2/2+ operation by default.

Parent

kcli/config/dsl

Syntax

```
re_adsl { on | off }
```

Parameter Description

Parameter	Description
on	Enable the Reach Extended ADSL mode.
off	Disable the Reach Extended ADSL mode.

retrain

Description

The `retrain` command initiates retrain, if there is a loss of margin messages during reception. When enabled, the interface retrains and resets its operational conditions till the link conditions change enough to warrant this.

Parent

kcli/config/dsl

Syntax

```
retrain { start }
```

Parameter Description

Parameter	Description
start	Start retraining.

sra

Description

The `sra` command enables or disables the SRA feature. The Seamless Rate Adaptation (SRA) controls the ADSL2 and ADSL2+ mode. It also allows the DSL framing parameters and rates to change in real-time (without re-training), if noise conditions on the line vary significantly.

Parent

kcli/config/dsl

Syntax

```
sra { on | off }
```

Parameter Description

Parameter	Description
on	Enable the SRA feature.
off	Disable the SRA feature.

sra_delay_pad

Description

The `sra_delay_pad` command enables or disables the optimized utilization of SRA delay time (only for ADSL2/2+ modes). If enabled, the feature facilitates implementation of the boost rates in lesser duration instead of using the available maximum delay time.

Parent

kcli/config/dsl

Syntax

```
sra_delay_pad { on | off }
```

Parameter Description

Parameter	Description
on	Enable the SRA delay feature to allow the modem to consume less delay than the default maximum delay time for SRA downshift.
off	Disable the SRA delay feature to use the default delay time.

statistics

Description

The `statistics` command resets the DSL link statistics. After rectifying the DSL link issues, you must reset the statistics to determine if the issues are resolved.

Parent

kcli/config/dsl

Syntax

```
statistics { reset }
```

Parameter Description

Parameter	Description
reset	Select reset to view the updated statistics.

VoIP Module

This section describes the VoIP module configuration commands. You can configure voice service, profile, and lines. You can also configure echo cancellation, SIP server parameters, faxT38 support, call transfer, call waiting, and QoS parameters.

voip

Description

The `voip` command node allows you to enter the configuration mode for setting the Voice over IP (VoIP) service parameters.

Parent

kcli/config

add-voice-service

Description

The `add-voice-service` command adds a new voice service.

Parent

kcli/config/voip

Syntax

```
add-voice-service voice-sevice < service integer(0:65535) >
```

Parameter Description

Parameter	Description
voice-service	Enter a voice service number for identification of the service. Each new voice service must have a unique identification number.

Example

The following example command creates a new voice service:

```
#kcli> config voip add-voice-service voice-service 1 <enter>
```

add-voice-profile

Description

The `add-voice-profile` command adds a new VoIP server profile. A VoIP server profile corresponds to one or more phone lines that share the same VoIP server configuration.

Parent

kcli/config/voip

Syntax

```
add-voice-profile voiceServiceNum < voiceServ integer(0:65535) > profileName < profName
string > [ sipServer < sip string > ] [ serviceProviderUrl < surl string > ]
```

Parameter Description

Parameter	Description
voiceServiceNum	Enter the the VoIP service identification number to add the VoIP server profile to the same.
profileName	Enter an alphanumeric value for the profile ID.
sipServer	Enter the SIP server IP address or resolved domain name address for associating it with the voice profile.
serviceProviderUrl	Enter the SIP service provider URL.

Example

The following example command creates the new voice profile "profile1" with the configured details:

```
#kcli> config voip add-voice-profile voiceServiceNum 1 profileName profile1 sipServer
10.0.0.3 serviceProviderUrl www.abc.com <enter>
```

add-line

Description

The `add-line` command adds a new phone line to an existing voice service profile.

Parent

kcli/config/voip

Syntax

```
add-line voiceService < voiceserv integer > profileId < profId integer > lineDirectory < lindir string > lineExtension < name integer > lineType { fxs | dect } username < name string > password < pass string > physical-port < pass string >
```

Parameter Description

Parameter	Description
voiceService	Enter the the VoIP service identification number on the device.
profileId	Enter the profile ID for the phone line. If two voice profiles are present on the device, one of these profiles (for example, profile1) is enabled and is the default profile used by both Line 1 and Line 2. Although, the second profile (profile2) can also be used by both the phone lines.
lineDirectory	Enter the phone number.
lineExtension	Enter the extension number for the phone line as provided by the ISP, for example, 5000.
lineType	Select the phone line type, Digital Enhanced Cordless Technology (DECT) or Foreign eXchange Subscriber (FXS).
fxs	Select FXS line type. In this case, the Foreign eXchange Subscriber (FXS) interface must be connected to the subscriber equipment (telephones, modems, or fax machines). The physical connectivity to the telephone is mandatory for the service to function.
dect	Select DECT line type. In this case, you need Digital Enhanced Cordless Technology (DECT) phone. DECT phones are different from the usual cordless phones because they allow you to use the Wi-Fi access point to connect to your gateway and configure VoIP connection.
username	Enter the user name as provided by the ISP.
password	Enter the password for the specified user as provided by the ISP.
physical-port	Enter the physical end point value or the port number on the splitter. If you are using a splitter and you have configured the details for P1/F1 port, then enter 1 as the physical end point value or port number.

Example

The following example command creates a new phone line with the configured details:

```
#kcli> config voip add-line voiceService 1 profileId 1 lineDirectory 1101 lineExtension 5000 lineType dect username tim password test1 physical-port 1 <enter>
```

del-voice-service

Description

The `del-voice-service` command deletes an existing voice service. As a result, all the configurations associated with that service are deleted.

Parent

kcli/config/voip

Syntax

```
del-voice-service voice-sevice < service integer(0:65535) >
```

Parameter Description

Parameter	Description
voice-sevice	Enter the the VoIP service identification number to be deleted.

delete-profile

Description

The `delete-profile` command deletes an existing voice service profile.

Parent

kcli/config/voip

Syntax

```
delete-profile voiceService < voiceserv integer(0:65535) > profileId < profId integer >
```

Parameter Description

Parameter	Description
voiceService	Enter the the associated VoIP service identification number.
profileId	Enter the profile ID to be deleted.

line-delete

Description

The `line-delete` command deletes a phone line from the voice service profile.

Parent

kcli/config/voip

Syntax

```
line-delete voiceService < voiceserv integer > profileId < profId integer > lineId < lindir integer >
```

Parameter Description

Parameter	Description
voiceService	Enter the the associated VoIP service identification number.
profileId	Enter the associated profile ID.
lineId	Enter the phone line ID to be deleted.

set-bband-interface

Description

The `set-bband-interface` command sets the broadband interface on which the VoIP service should be running.

Parent

kcli/config/voip

Syntax

```
set-bband-interface interface-name < name string >
```

Parameter Description

Parameter	Description
interface-name	Enter the broadband interface name on which VoIP service should be running.

Example

The following example command sets the bb1 interface for the VoIP service:

```
#kcli> config voip set-bband-interface-name bb1 <enter>
```

set-digit-map

Description

The `set-digit-map` command sets the digit map for the phone. The digit map controls the transmission of the dialed digit information. The string defines the criteria to be met as digits are collected before an outgoing request can be initiated. In other words, the digit map definition is used for defining the phone specific dialing behavior. A phone dial plan directs the phone to initiate a call when you have entered the complete number. If the phone digit map is defined incorrectly, the phone may start to dial before you are actually able to enter all the required digits.

Parent

kcli/config/voip

Syntax

```
set-digit-map voiceService < voiceserv integer(0:65535) > profileId < profId integer >
digitMap < digmap string >
```

Parameter Description

Parameter	Description
voiceService	Enter the the VoIP service identification number for the digit map.
profileId	Enter the voice profile ID for the digit map.
digitMap	Enter the digit map string for phone number identification. For example, [2-9]11|0T|011xxx.T|91[2-9]xxxxxxxxx|[1-8]xx.

Example

The following example command sets the digit map for the specified phone line:

```
#kcli> config voip set-digit-map voiceService 1 profileID profile1 digitMap [2-
9]11|0T|011xxx.T|91[2-9]xxxxxxxxx|[1-8]xx <enter>.
```

It means the following:

[2-9]11: 911 rule: x11 are dialled immediately (111 is covered below)

[1-8]xx 0T: Local operator rule: After dialing "0" (zero) the phone waits "T" seconds and then completes the call automatically

011xxx.T: International rule without prefix

91[2-9]xxxxxxxxx: LD rule with prefix

[1-8]xx: A regular 3 digit extension is dialed immediately (9 excluded as a prefix)

set-digitmap-enable

Description

The `set-digitmap-enable` command enables or disables the digit map for a specified voice service.

Parent

kcli/config/voip

Syntax

```
set-digitmap-enable voiceService < voiceserv integer(0:65535) > profileId < profId integer
> state { true | false }
```

Parameter Description

Parameter	Description
voiceService	Enter the voice service identification number to enable or disable the digit map of that phone line.
profileId	Enter the associated profile ID for the digit map.
state	Enable or disable the digit map of the specified phone line.
true	Select true to enable the digit map of the specified phone line.
false	Select false to disable the digit map of the specified phone line.

Example

The following example command enables the digit map for the specified voice service:

```
#kcli> config voip set-digitmap-enable voiceService 1 profileID profile1 state true <enter>
```

set-dtmf-method

Description

The `set-dtmf-method` command sets a method for passing the DTMF digits. The options are inband, rfc2833, and sipinfo. Dual Tone Multi Frequency (DTMF) signals are generated when you press an ordinary telephone's touch keys and are sent to the phone company for connecting an external number.

Parent

kcli/config/voip

Syntax

```
set-dtmf-method voiceService < voiceserv integer(0:65535) > profileId < profId integer >
DTMFMethod { inband | rfc2833 | sipinfo }
```

Parameter Description

Parameter	Description
voiceService	Enter the voice service identification number for which the DTMF method is to be used.
profileId	Enter the profile ID.
DTMFMethod	Select a method to pass the DTMF digits.
inband	Select the in-band method for voice communication. In-band means that the DTMF digits are in the normal audio frequency of the telephone. Inband digits are the signals sent on the telephone line before the PBX connects the calling party to the called party. These digits are not sent until the called party answers the phone.
rfc2833	Select the RFC2833 method for voice communication. Digits pressed by the user are sent to the other end via RTP packets. The format of these RTP packets is defined in the RFC 2833.
sipinfo	Select the SIP info method for voice communication. This method allows the carrying of session-related control information generated during the session. One example of such session control information is ISUP and ISDN signaling messages used for controlling telephony call services.

Example

The following example command sets the SIP info as DTMF method:

```
#kcli> config voip set-dtmf-method voiceService 1 profileID profile1 DTMFMethod inband
<enter>
```

set-echocancel

Description

The `set-echocancel` command removes echo from a VoIP call to improve voice quality. Echo cancellation also reduces bandwidth consumption because of its silence suppression technique.

Parent

kcli/config/voip

Syntax

```
set-echocancel voiceService < voiceserv integer(0:65535) > profileId < profId integer >
lineId < lindir integer > state { true | false }
```

Parameter Description

Parameter	Description
voiceService	Enter the voice service identification number to remove echo from that phone line.
profileId	Enter the voice profile ID.
lineId	Enter the phone line ID.
state	Enable or disable the echo cancellation for the specified phone line.
true	Select true to enable the echo cancellation.
false	Select false to disable the echo cancellation.

Example

The following example command enables the echo cancellation for VoIP service:

```
#kcli> config voip set-echocancel voiceService 1 profileID profile1 lineID 1 state true
<enter>
```

set-faxT38

Description

The `set-faxT38` command enables or disables the T.38 fax support on the network.

Parent

kcli/config/voip

Parameter Description

Parameter	Description
true	Select true to enable T.38 fax support to allow the gateway to permit faxes to be transported across IP network.
false	Select false to disable T.38 fax support, if you do not wish to permit faxes to be transported across IP network.
profileId	Enter the voice service profile ID to enable T.38 fax support on that profile.

Example

The following example command enables the T.38 fax service for VoIP:

```
#kcli> config voip set-faxT38 true profileId 1 <enter>
```

set-line-enable

Description

The `set-line-enable` command enables or disables the phone line.

Parent

kcli/config/voip

Syntax

```
set-line-enable voiceService < voiceserv integer(0:65535) > profileId < profId integer >
lineId < lindir integer > state { Enabled | Disabled }
```

Parameter Description

Parameter	Description
voiceService	Enter the associated voice service identification number.
profileId	Enter the associated voice profile ID.
lineId	Enter the phone line ID.
state	Enable or disable the specified phone line.
Enabled	Enable the specified phone line.
Disabled	Disable the said phone line.

Example

The following example command enables the specified phone line:

```
#kcli> config voip set-line-enable voiceService 1 profileID profile1 lineID 1 state Enabled
<enter>
```

set-line-username-password

Description

The `set-line-username-password` configures the SIP user name and password for the corresponding phone line.

Parent

kcli/config/voip

Syntax

```
set-line-username-password voiceService < voiceserv integer(0:65535) > profileId < profId
integer > lineId < lindir integer > username < name string > [ password < pass string > ]
```

Parameter Description

Parameter	Description
voiceService	Enter the associated voice service identification number.
profileId	Enter the profile ID.
lineId	Enter the phone line ID.
username	Enter the SIP user name for the specified phone line.
password	Enter the password for the specified SIP user.

Example

The following example command sets the SIP user john and the password for the same:

```
#kcli> config voip set-line-username-password voiceService 1 profileId profile1 lineID 1
username john password test1 <enter>
```

set-list-enable

Description

The `set-list-enable` command enables or disables the codecs list for a phone line.

Parent

kcli/config/voip

Syntax

```
set-list-enable voiceService < voiceserv integer(0:65535) > profileId < profId integer >
lineId < lindir integer > listId < listid integer(0:65535) > status { true | false }
```

Parameter Description

Parameter	Description
voiceService	Enter the associated voice service identification number.
profileId	Enter the associated voice profile ID.
lineId	Enter the phone line ID.
listId	Enter the list ID that you want to enable or disable.
status	Enable or disable the specified codec entry.
true	Select true to enable the specified codec list entry to be used for the phone line.
false	Select false to disable the specified codec list entry.

Example

The following example enables the specified codecs list for the phone line "phone1":

```
#kcli> config voip set-list-enable voiceService 1 profileId profile1 lineID 1 listID 60
status true <enter>
```

set-profile-enable

Description

The `set-profile-enable` command enables or disables the voice profile.

Parent

kcli/config/voip

Syntax

```
set-profile-enable voiceService < voiceserv integer(0:65535) > profileId < profId integer >
control { Enabled | Disabled }
```

Parameter Description

Parameter	Description
voiceService	Enter the voice service identification number.
profileId	Enter the ID of the voice profile that you want to enable or disable.
control	Enable or disable the specified voice profile.
Enabled	Enable the voice profile.
Disabled	Disable the voice profile.

Example

The following example command enables the specified voice profile:

```
#kcli> config voip set-profile-enable voiceService 1 profileId profile1 control Enabled
<enter>
```

set-profile-rtp-min-max

Description

The `set-profile-rtp-min-max` sets minimum and maximum Real-time Transport Protocol (RTP) port values for the specified voice profile.

Parent

kcli/config/voip

Syntax

```
set-profile-rtp-min-max voiceService < voiceserv integer(0:65535) > profileId < profId
integer > rtpPortMin < portmin integer > rtpPortMax < portmax integer >
```

Parameter Description

Parameter	Description
voiceService	Enter the associated voice service identification number.
profileId	Enter the voice profile ID.
rtpPortMin	Enter the minimum port value to be used for the incoming RTP streams for this voice profile.
rtpPortMax	Enter the maximum port value to be used for the incoming RTP streams for this voice profile.

Example

The following example command sets the minimum and maximum RTP port values for the voice profile:

```
#kcli> config voip set-profile-rtp-min-max voiceService 1 profileID profile1 rtpPortMin 1
rtpPortMax 3 <enter>
```

set-qos-params

Description

The `set-qos-params` command configures QoS on the router to prioritize the VoIP packets (SIP and RTP). Configure the QoS parameters for marking DSCP values of SIP and RTP packets.

Parent

kcli/config/voip

Syntax

```
set-qos-params voiceService < voiceserv integer(0:65535) > profileId < profId integer >
sip-dscp < sipdscp integer > rtp-dscp < rtpdscp integer >
```

Parameter Description

Parameter	Description
voiceService	Enter the associated voice service identification number.
profileId	Enter the voice profile ID.
sip-dscp	Enter the DSCP mark value for SIP packets.
trp-dscp	Enter the DSCP mark value for RTP packets.

Example

The following example command sets the SIP and RTP DSCP mark values for high priority (EF queue):

```
#kcli> config voip set-qos-params voiceService 1 profileID profile1 sip-dscp 46 rtp-dscp 46
<enter>
```

set-sip-svr

Description

The `set-sip-svr` command configures the SIP server settings. SIP is an application-layer control protocol that can establish, modify, or terminate multimedia sessions (conferences) such as Internet telephony calls. A SIP server is the main component of an IP PBX, dealing with the setup of all SIP calls in the network.

Parent

kcli/config/voip

Syntax

```
set-sip-svr voiceService < voiceServ integer(0:65535) > profileId < profId integer >
sipServerAddress < address string >
```

Parameter Description

Parameter	Description
voiceService	Enter the associated voice service identification number.
profileId	Enter the voice profile ID.
sipServerAddress	Enter the SIP server IP address.

Example

The following example command sets the minimum and maximum RTP port values for the voice profile:

```
#kcli> config voip set-sip-svr voiceService 1 profileID profile1 sipServerAddress
192.168.1.0 <enter>
```

reset-rtp-stats

Description

The `reset-rtp-stats` command resets the statistics of the cumulative calls for the active phone line.

Parent

kcli/config/voip

Syntax

```
reset-rtp-stats control { true }
```

Parameter Description

Parameter	Description
control	Enable the reset VoIP RTP statistics feature.
true	Select true to reset the VoIP RTP statistics.

set-line-call-transfer

Description

The `set-line-call-transfer` command enables or disables the call transfer feature for the specified phone line.

Parent

kcli/config/voip

Syntax

```
set-line-call-transfer voiceService < voiceserv integer(0:65535) > profileId < profId
integer > lineId < lindir integer > state { true | false }
```

Parameter Description

Parameter	Description
voiceService	Enter the voice service number for which the call transfer feature is to be activated.
profileId	Enter the associated profile ID.
lineId	Enter the phone line directory ID.
state	Enable or disable the call transfer feature.
true	Enable the call transfer feature.
false	Disable the call transfer feature.

Example

The following example command enables the call transfer feature for the specified phone line:

```
#kcli> config voip set-line-call-transfer voiceService 1 profileID 1 lineID 1 state true
<enter>
```

set-line-call-waiting

Description

The `set-line-call-waiting` command enables or disables the call waiting feature for the specified phone line.

Parent

kcli/config/voip

Syntax

```
set-line-call-waiting voiceService < voiceserv integer(0:65535) > profileId < profId
integer > lineId < lindir integer > state { true | false }
```

Parameter Description

Parameter	Description
voiceService	Enter the voice service number for which the call waiting is to be activated.
profileId	Enter the associated profile ID.
lineId	Enter the phone line directory ID.
state	Enable or disable the call waiting.
true	Enable the call waiting.
false	Disable the call waiting.

Example

The following example command enables the call waiting feature for the specified phone line:

```
#kcli> config voip set-line-call-waiting voiceService 1 profileID 1 lineID 1 state true
<enter>
```

CHAPTER 5

Show Commands

This chapter lists the module name, show commands for each module, purpose of each command, and parent (command navigation). The command syntax followed by its parameter description are also added wherever applicable.

Admin-Tools Module

This section describes show commands for the admin-tools module. You can view admin-tools parameters like profile details, transaction history, backup history, vendor config file list, etc.

admin-tools

Description

The `admin-tools` command node allows you to enter the view mode that displays the admin tools settings such as backup, restore, and history.

Parent

kcli/show

settings

Description

The `settings` command displays the configured backup and restore settings.

Parent

kcli/show/admin-tools

history-size

Description

The `history-size` command displays the number of backups specified during configuration of the history size.

Parent

kcli/show/admin-tools/settings

Syntax

```
history-size
```

always-save-runningconfig

Description

The `always-save-runningconfig` command displays whether saving the current configuration of the gateway is enabled or disabled.

Parent

kcli/show/admin-tools/settings

Syntax

```
always-save-runningconfig
```

transaction-size

Description

The `transaction-size` command displays the transaction size for locking in the AIM. It determines how many MIs can accept the lock.

Parent

kcli/show/admin-tools/settings

Syntax

```
transaction-size
```

backup-history

Description

The `backup history` command displays the configuration backup details such as backup file name, date and time when the backup file was created.

Parent

kcli/show/admin-tools

Syntax

```
backup-history
```

current-profile-name

Description

The `current-profile-name` command displays the current profile selected for the device.

Parent

kcli/show/admin-tools

Syntax

```
transaction-size
```

profiles

Description

The `profiles` command displays the available profiles on the device, such as dsl_routed, dsl_bridge, ethernet_routed, ethernet_bridge, dsl, and ethernet.

Parent

kcli/show/admin-tools

Syntax

```
profiles
```

transaction-history

Description

The `transaction-history` command displays the locking history. It displays MIs having locks, as also the MIs that have accepted the lock earlier and have now released the lock.

Parent

kcli/show/admin-tools

Syntax

```
transaction-history
```

vendor-config-file-list

Description

The `vendor-config-file-list` command displays the modules present on the device, for example, npconfig, npdsl, npif, etc.

Parent

kcli/show/admin-tools

Syntax

```
vendor-config-file-list
```

Bridge Module

This section describes show commands of the bridge module. You can view bridge entities, bridge port entities, and bridge forward database entries (lists the mac addresses and their respective state).

bridge

Description

The `bridge` command node allows you to enter the view mode that displays the bridge configuration, including bridge and bridge port entities, and bridge forward database entries that list the MAC addresses and their respective state.

Parent

kcli/show

bridge

Description

The `bridge` command displays the bridge configuration that includes the bridge name, priority, ageing time, hardware address, max age, etc. Enter the bridge name to view its configuration.

Parent

kcli/show/bridge

Syntax

```
bridge [ < bridge_name string(1:32) > ]
```

bridgeport

Description

The `bridgeport` command displays the bridge port configuration details for the respective interfaces.

Parent

kcli/show/bridge

Syntax

```
bridgeport [ < port_interface string(1:32) > ]
```

bridgefdb

Description

The `bridgefdb` command displays the forward database entries that list the MAC addresses and their respective state.

Parent

kcli/show/bridge

Syntax

```
bridgefdb [ bridge-name < bridge_name string(1:32) > ] [ port-number < port_number integer
> ]
```

Parameter description

Parameter	Description
bridge-name	Enter the name of the required bridge for viewing the forward database entries.
port-number	Enter the port number of the bridge.

IGMP Module

This section describes show commands of the IGMP module. You can view various IGMP settings, such as IGMP WAN forwarding entries, group and hosts statistics, downstream, and router interfaces.

igmp

Description

The `igmp` command node allows you to enter the show mode that displays the configured IGMP settings.

Parent

kcli/show

downstream-interfaces

Description

The `downstream-interfaces` command displays the downstream interfaces used for IGMP proxy.

Parent

kcli/show/igmp

Syntax

```
downstream-interfaces
```

exclude-sources

Description

The `exclude-sources` command displays the list of sources (unicast IP addresses). The multicast traffic coming only from these sources for a particular group (multicast IP address/es) is blocked and is not forwarded to the downstream network. This "Exclude" list is valid only if the filter mode for that group is set to "Exclude."

Parent

kcli/show/igmp

Syntax

```
exclude-sources
```

group-memberships

Description

The `group-memberships` command displays a list of hosts that have currently joined a particular group (multicast IP address/es) on the specified downstream interface.

Parent

kcli/show/igmp

Syntax

```
group-memberships
```

group-stats

Description

The `group-stats` command displays the statistics of the group, such as group address, number of joins and leaves on current day, and last report time.

Parent

kcli/show/igmp

Syntax

```
group-stats
```

include-sources

Description

The `include-sources` command displays a list of sources (unicast IP addresses). The multicast traffic coming only from these sources for a particular group (multicast IP address/es) is allowed. Traffic coming from any other sources is not forwarded to the downstream network. This "Include" list is valid only if the filter mode for that group is set to "Include."

Parent

kcli/show/igmp

Syntax

```
include-sources
```

multicast-groups

Description

The `multicast-groups` command displays the list of active multicast groups.

Parent

kcli/show/igmp

Syntax

```
multicast-groups
```

router-interfaces

Description

The `router-interfaces` command displays the list of downstream interfaces with corresponding multicast group and its filter mode (Exclude or Include).

Parent

kcli/show/igmp

Syntax

```
router-interfaces
```

settings

Description

The `settings` command displays the IGMP settings on the device, such as IGMP proxy state (enable or disable), client version, upstream interface name.

Parent

kcli/show/igmp

Syntax

```
settings
```

host-stats

Description

The `host-stats` command displays the IGMP host statistics, such as, host address, current and quarter hour start time, total number of joins and leaves, maximum delay in current day and in quarter hour.

Parent

kcli/show/igmp

Syntax

```
host-stats
```

igmp-wan-fwd-entries

Description

The `igmp-wan-fwd-entries` command displays the details of IGMP WAN forwarding rule entries, such as, multicast group address and subnet mask, forwarding status (True/False), and interface where the IGMP traffic is to be forwarded.

Parent

kcli/show/igmp

Syntax

```
igmp-wan-fwd-entries
```

Firewall Module

This section describes show commands of the firewall module. You can view firewall parameters like access control, log-status, udp-timeout settings, default configuation settings, filter types, service control settings, etc.

firewall

Description

The `firewall` command node allows you to enter the view mode that displays the various firewall configurations on the gateway.

Parent

kcli/show

dmz

Description

The `dmz` command displays the various hosts in DMZ.

Parent

kcli/show/firewall

Syntax

```
dmz
```

service-control

Description

The `service-control` command displays the list of blocked and allowed services on the gateway.

Parent

kcli/show/firewall

Syntax

```
service-control
```

security-mode

Description

The `security-mode` command displays the firewall security mode (medium, maximum or disabled).

Parent

kcli/show/firewall

Syntax

```
security-mode
```

alg

Description

The `alg` command displays the status (enabled or disabled) of various services on the gateway, such as, IPSEC, PPTP, TFTP, L2TP.

Parent

kcli/show/firewall

Syntax

```
alg
```

custom-message

Description

The `custom-message` command displays the custom message as well as its status (enabled or disabled).

Parent

kcli/show/firewall

Syntax

```
custom-message
```

access-control

Description

The `access-control` command node displays the various access control rules, including proxy, port-forwarding, trusted clients, and trusted remote clients.

Parent

kcli/show/firewall

proxy

Description

The `proxy` command displays the proxy servers available on the gateway. Details include the host IP, service, port number, protocol, and the associated policy name.

Parent

kcli/show/firewall/access-control

Syntax

```
proxy
```

port-forward

Description

The `port-forward` command displays the list of IP addresses where the traffic is to be forwarded, along with relevant details such as port, protocol, description, and assigned policy name.

Parent

kcli/show/firewall/access-control

Syntax

```
port-forward
```

trusted-client

Description

The `trusted-client` command displays the list of trusted client IP addresses.

Parent

kcli/show/firewall/access-control

Syntax

```
trusted-client
```

trusted-management-client

Description

The `trusted-management-client` command displays the trusted client IP addresses used for remote device management.

Parent

kcli/show/firewall/access-control

Syntax

```
trusted-management-client
```

app-forward

Description

The `app-forward` command displays the active and inactive applications on the network.

Parent

kcli/show/firewall/access-control

Syntax

```
app-forward { active-apps | inactive-apps } [ category { games | audio-video | servers |
mip | others | user-defined } ]
```

Parameter Description

Parameter	Description
active-apps	View the list of active applications.
inactive-apps	View the list of inactive applications.
category	Select the application category from the given list (audio-video, games, mip, others, servers, or user-defined) to view the list of application/s added under that particular category.
games	Select games category if the application belongs to the same.
audio-video	Select audio-video category if the application belongs to the same.
servers	Select servers category if the application belongs to the same.
mip	Select MIP category if the application belongs to the same.
others	Select others category if the application does not belong to any category available in the list.
user-defined	Select user-defined category if the application exists under the user-defined profile name.

user-apps

Description

The `user-apps` command displays the user-defined application/s on the network.

Parent

kcli/show/firewall/access-control

Syntax

```
user-apps
```

host-filter

Description

The `host-filter` command node displays the list of blocked websites, internal hosts, and MAC addresses.

Parent

kcli/show/firewall

external-site

Description

The `external-site` command displays the list of blocked external websites.

Parent

kcli/show/firewall/host-filter

Syntax

```
external-site
```

internal-host

Description

The `internal-host` command displays the list of blocked internal hosts.

Parent

kcli/show/firewall/host-filter

Syntax

```
internal-host
```

macs

Description

The `macs` command displays a list of blocked MAC addresses.

Parent

kcli/show/firewall/host-filter

Syntax

```
macs
```

expert-control

Description

The `expert-control` command displays the configured expert control (packet filtering) rules.

Parent

kcli/show/firewall/host-filter

Syntax

```
expert-control
```

nat

Description

The `nat` command node allows you to enter the view mode of NAT.

Parent

kcli/show

interfaces

Description

The `interfaces` command displays the list of NAT-enabled interfaces, as also the status of public IP NATting and the cone NAT on each of them.

Parent

kcli/show/nat

Syntax

```
interfaces
```

default-config

Description

The `default-config` major command allows you to enter the view mode of the firewall default configuration wherein you can view the list of enabled or disabled default services on the gateway.

Parent

kcli/show/firewall

service-status

Description

The `service-status` command displays the list of enabled or disabled services on the gateway. Services include HTTP, FTP, TFTP, TELNET, SSH, SNMP, etc.

Parent

kcli/show/firewall/default-config

Syntax

```
service-status
```

games-config

Description

The `games-config` major command allows you to enter the show mode for viewing status of available games on the WAN-side server.

Parent

kcli/show/firewall

games-status

Description

The `games-status` command displays the list of enabled or disabled games on the WAN-side server.

Parent

kcli/show/firewall/games-config

Syntax

```
games-status
```

time-based-policy

Description

The `time-based-policy` command node displays the time schedules on the gateway device. You can view the schedules, policies, as well as the list of associated schedules and policies.

Parent

kcli/show/firewall

policies

Description

The `policies` command displays the list of policies created on the device.

Parent

kcli/show/firewall/time-based-policy

Syntax

```
policies
```

schedule

Description

The `schedule` command displays the list of time schedules.

Parent

kcli/show/firewall/time-based-policy

Syntax

```
schedule
```

scheduled-policies

Description

The `scheduled-policies` command displays the list of policies and their associated schedules.

Parent

kcli/show/firewall/time-based-policy

Syntax

```
scheduled-policies
```

contentfilter

Description

The `contentfilter` major command displays the details of the content filter rules.

Parent

kcli/show/firewall

filters

Description

The `filters` command displays the filter settings for the available content types.

Parent

kcli/show/firewall/contentfilter

Syntax

```
filters [ type { keyword | file | protocol | virus } ]
```

Parameter Description

Parameter	Description
type	Select the content type.
keyword	Select keyword content type if the rule is configured using the same.
file	Select file content type if the rule is configured using the same.
protocol	Select protocol content type if the rule is configured using the same.
virus	Select virus content type if the rule is configured using the same.

matchpacket

Description

The `matchpacket` command displays the matched packets number.

Parent

kcli/show/firewall/contentfilter

Syntax

```
matchpacket
```

mgmt-service

Description

The `mgmt-service` command displays the management service source configuration.

Parent

kcli/show/firewall

Syntax

```
mgmt-service
```

logging-status

Description

The `logging-status` command displays the firewall logging status (enabled or disabled) on the network.

Parent

kcli/show/firewall

Syntax

```
logging-status
```

ignore-icmp-bogus-error

Description

The `ignore-icmp-bogus-error` command displays whether the ignore-icmp-bogus-error feature is enabled or disabled on the network.

Parent

kcli/show/firewall

Syntax

```
ignore-icmp-bogus-error
```

ignore-icmp-broadcast

Description

The `ignore-icmp-broadcast` command displays whether the ignore-icmp-broadcast feature is enabled or disabled on the network.

Parent

kcli/show/firewall

Syntax

```
ignore-icmp-broadcast
```

tcp-timeout

Description

The `tcp-timeout` command displays the TCP timeout period (in seconds) set on the gateway.

Parent

kcli/show/firewall

Syntax

```
tcp-timeout
```

udp-timeout

Description

The `udp-timeout` command displays the UDP timeout period (in seconds) set on the gateway.

Parent

kcli/show/firewall

Syntax

```
udp-timeout
```

block-invalid-ip

Description

The `block-invalid-ip` command displays the status of blocking invalid IP address feature (enabled or disabled).

Parent

kcli/show/firewall

Syntax

```
block-invalid-ip
```

block-invalid-mac

Description

The `block-invalid-mac` command displays the status of blocking invalid MAC address feature (enabled or disabled).

Parent

kcli/show/firewall

Syntax

```
block-invalid-mac
```

stealth-mode-status

Description

The `stealth-mode-status` command displays the status of stealth mode (enabled or disabled).

Parent

kcli/show/firewall

Syntax

```
stealth-mode-status
```

VLAN Module

This section describes show commands of the VLAN module. You can view ports, VLAN IDs, QoS settings, etc.

vlan

Description

The `vlan` command node allows you to enter the view mode that displays the VLAN configuration details, including ports, VLAN IDs, QoS settings, etc.

Parent

kcli/show

vlanport

Description

The `vlanport` command displays the port details of the configured VLANs.

Parent

kcli/show/vlan

Syntax

```
vlanport [ vlanid < vlanid integer > ]
```

Parameter Description

Parameter	Description
vlanid	Enter the ID of the VLAN whose port details you want to view.

vlans

Description

The `vlans` command displays all the configured VLANs' details. You can view the VLAN names and their respective IDs.

Parent

kcli/show/vlan

Syntax

```
vlans [ vlanid < vlanid integer > ]
```

Parameter Description

Parameter	Description
vlanid	Enter the ID of the VLAN whose details you want to view.

vlan-ingress-map

Description

The `vlan-ingress-map` command displays the ingress QoS settings (priority settings for incoming data) of the respective VLAN ports.

Parent

kcli/show/vlan

Syntax

```
vlan-ingress-map [ vlanid < vlanid integer > ] [ vlanport < port integer > ]
```

Parameters Description

Parameter	Description
vlanid	Enter the ID of the VLAN whose ingress QoS setting you want to view.
vlanport	Enter the port number of the VLAN whose ingress QoS setting you want to view.

vlan-egress-map

Description

The vlan-egress-map command displays the egress QoS settings (priority settings for outgoing data) of the respective VLAN ports.

Parent

kcli/show/vlan

Syntax

```
vlan-egress-map [ vlanid < vlanid integer > ] [ vlanport < port integer > ]
```

Parameter Description

Parameter	Description
vlanid	Enter the ID of the VLAN whose egress QoS setting you want to view.
vlanport	Enter the port number of the VLAN whose egress QoS setting you want to view.

PPPoA Module

This section describes show commands of the PPPoA module. You can view the configured parameters and status for PPPoA.

pppoa

Description

The pppoa command node allows you to enter the view mode that displays the configured PPPoA settings.

Parent

kcli/show

status

Description

The `status` command displays the PPPoA interface status (up or down).

Parent

kcli/show/pppoa

Syntax

```
status [ interface < interface string(1:32) > ]
```

Parameter Description

Parameter	Description
interface	Enter the name of the DSL interface on the network to view its status (up or down).

params

Description

The `params` command displays the configured PPPoA parameters, such as interface, authentication, compression, encryption type, session mode.

Parent

kcli/show/pppoa

Syntax

```
params [ interface < interface string(1:32) > ]
```

Parameter Description

Parameter	Description
interface	Enter the DSL interface name to view its parameters.

PPPoE Module

This section describes show commands of the PPPoE module. You can view the configured parameters and status for PPPoE.

pppoe

Description

The `pppoe` command node allows you to enter the view mode that displays various PPPoE parameters configured on the device.

Parent

kcli/show

status

Description

The `status` command displays the PPPoE session status (up or down).

Parent

kcli/show/pppoe

Syntax

```
status [ interface < interface string(1:32) > ]
```

Parameter Description

Parameter	Description
interface	Enter the PPPoE interface name on which PPPoE service is running.

config

Description

The `config` command displays the PPPoE configuration parameters including interface name, user name, password, MTU size, MSS size, service ID, etc.

Parent

kcli/show/pppoe

Syntax

```
config [ interface < interface string(1:32) > ]
```

Parameter Description

Parameter	Description
interface	Enter the PPPoE interface name to view its configuration.

backoff

Description

The `backoff` command displays the backoff settings.

Parent

kcli/show/pppoe

Syntax

```
backoff settings
```

Parameter Description

Parameter	Description
settings	View the backoff settings.

default-domain-append-status

Description

The `default-domain-append-status` command displays if appending the default domain to a PPPoE user name is enabled or disabled.

Parent

kcli/show/pppoe

Syntax

```
default-domain-append-status
```

default-domain

Description

The default-domain command displays the default domain set for the PPPoE user.

Parent

kcli/show/pppoe

Syntax

```
default-domain
```

allowed-domain-separator

Description

The `allowed-domain-separator` command displays the separator (@) for domain and user name.

Parent

kcli/show/pppoe

Syntax

```
allowed-domain-separator
```

Wireless Module

This section describes show commands of the wireless module. You can view the certificate information, list of wi-fi interfaces, list of radio interfaces, etc.

wireless

Description

The `wireless` allows you to enter the configuration mode that displays the wireless configuration details, such as PKI information, wireless interface configuration, radio interface configuration, multiple SSID, and AP mode configuration.

Parent

kcli/show

interface

Description

The `interface` command displays the configuraion of the selected wireless interface, which includes the current SSID, interface mode, wireless standard being used, and security parameters set. Enter the interface name to view its configuration.

Parent

kcli/show/wireless

Syntax

```
interface < ifname string(1:32) >
```

basic-config

Description

The `basic-config` command displays the basic configuration of the selected interface, including current SSID, hardware mode, channel policy, channel, admin status, interface mode and transfer rate between the client and the AP.

Parent

kcli/show/wireless/interface

Syntax

```
basic-config
```

security-config

Description

The `security-config` command displays the security configuration of the selected interface, including security mode, broadcast SSID status and MAC-ACL type.

Parent

kcli/show/wireless/interface

Syntax

```
security-config
```

advanced-config

Description

The `advanced-config` command displays the advanced configuration of the selected interface, including antenna transmit power, beacon interval, 802.11e prioritization status, acknowledgement timeout period, RTS threshold and fragmentation threshold.

Parent

kcli/show/wireless/interface

Syntax

```
advanced-config
```

wep-security-details

Description

The `wep-security-details` command displays the configured WEP security details for the selected interface, including the key length, default WEP key and additional WEP keys.

Parent

kcli/show/wireless/interface

Syntax

```
wep-security-details
```

wpa-security-details

Description

The `wpa-security-details` command displays the configured WPA security details such as shared key and encryption type.

Parent

kcli/show/wireless/interface

Syntax

```
wpa-security-details
```

ap-association-list

Description

The `ap-association-list` command displays the association list details such as the client MAC address, link quality, signal level and noise level.

Parent

kcli/show/wireless/interface

Syntax

```
ap-association-list
```

channel-list

Description

The `channel-list` command displays the channel list for the selected interface along with the channel details such as frequency and current status.

Parent

kcli/show/wireless/interface

Syntax

```
channel-list
```

clean-channel

Description

The `clean-channel` command displays the channel with least radio interference.

Parent

kcli/show/wireless/interface

Syntax

```
clean-channel
```

power-list

Description

The `power-list` command displays the list of supported power levels.

Parent

kcli/show/wireless/interface

Syntax

```
power-list
```

rate-list

Description

The `rate-list` command displays the list of transfer rates available between the client and the AP, along with the rate details such as transfer rate (in bits), rate description (Mb/sec) and current status.

Parent

kcli/show/wireless/interface

Syntax

```
rate-list
```

statistics

Description

The `statistics` command displays the statistics of the selected interface, including access point MAC address, link quality, signal level (in dBm), noise level (in dBm), number of missed beacons, etc.

Parent

kcli/show/wireless/interface

Syntax

```
statistics
```

wpa-radius-authenticator-details

Description

The `wpa-radius-authenticator-details` command displays WPA security mode details for the selected interface. This includes the authentication and accounting server configuration for the primary and secondary radius servers.

Parent

kcli/show/wireless/interface

Syntax

```
wpa-radius-authenticator-details
```

mac-acl

Description

The `mac-acl` command displays the MAC address/es along with their ACL type.

Parent

kcli/show/wireless/interface

Syntax

```
mac-acl
```

pki-description

Description

The `pki-desription` command displays all the imported PKIs. The information displayed includes PKI description, CA (certificate authority) certificate name, client certificate name, client key file name and client secret.

Parent

kcli/show/wireless/interface

Syntax

```
pki-description
```

scan-ap-list

Description

The `scan-ap-list` command displays details such as SSID, security settings, MAC AP address, configured channel, transmission frequency, link quality, signal level, noise level, mode, beacon interval, encryption key and bit rate per second of the available APs.

Parent

kcli/show/wireless/interface

Syntax

```
scan-ap-list
```

antenna-diversity

Description

The `antenna-diversity` command displays the antenna diversity status.

Parent

kcli/show/wireless/interface

Syntax

```
antenna-diversity
```

pki

Description

The `pki` command displays the configured PKI certificate information on the system.

Parent

kcli/show/wireless

Syntax

```
pki-description
```

Parameter Description

Parameter	Description
description	Enter the PKI description to view the certificate details.

wifi-interfaces

Description

The `wifi-interfaces` command displays the configured wireless interfaces on the network.

Parent

kcli/show/wireless

Syntax

```
wifi-interfaces
```

radio

Description

The `radio` command displays the configured radio interfaces on the network. It also displays the configured parameters for the selected interface, including mode (master/managed), hardware mode, channel and channel policy, and admin status.

Parent

kcli/show/wireless

Syntax

```
radio [ interface < if string(16:16) > ]
```

Parameter Description

Parameter	Description
interface	Enter the radio interface name to view its configuration.

multiple-ssid

Description

The `multiple-ssid` command displays the multiple SSID for the radio interface.

Parent

kcli/show/wireless

Syntax

```
multiple-ssid radio < radio string >
```

Parameter Description

Parameter	Description
radio	Enter the radio interface name to view the associated multiple SSID.

turbo-mode

Description

The `turbo-mode` command displays the status of the turbo mode on the wireless interface.

Parent

kcli/show/wireless

Syntax

```
turbo-mode
```

wmm

Description

The `wmm` command displays the WMM configuration settings, such as state, and selected access category (BE, BK, VI or VO) .

Parent

kcli/show/wireless/interface

Syntax

```
wmm
```

state

Description

The `state` command displays the WMM status (enabled or disabled) on the wireless interface.

Parent

kcli/show/wireless/interface/wmm

Syntax

```
state
```

accesscategory

Description

The `accesscategory` command displays the access category (BE, BK, VI or VO) for WMM and associated configuration settings (AIFSN, contention window maximum and minimum value, transmission opportunity time limit etc.)

Parent

kcli/show/wireless/interface/wmm

Syntax

```
accesscategory
```

BE

Description

The BE command in access category displays the BE (Best Effort) access category settings, such as AIFSN, contention window maximum and minimum value, transmission opportunity time limit etc.

Parent

kcli/show/wireless/interface/wmm/accesscategory

Syntax

```
BE
```

BK

Description

The BK command in accesscategory displays the BK (background) access category settings, such as AIFSN, contention window maximum and minimum value, transmission opportunity time limit etc.

Parent

kcli/show/wireless/interface/wmm/accesscategory

Syntax

BK

VI

Description

The VI command in accesscategory displays the VI (video) access category settings, such as AIFSN, contention window maximum and minimum value, transmission opportunity time limit etc.

Parent

kcli/show/wireless/interface/wmm/accesscategory

Syntax

VI

VO

Description

The VO command in accesscategory displays the VO (voice) access category settings, such as AIFSN, contention window maximum and minimum value, transmission opportunity time limit etc.

Parent

kcli/show/wireless/interface/wmm/accesscategory

Syntax

VO

Software Upgrade Module

This section describes show commands of the software upgrade module. You can view the upgrade status and history, and the details of the binary image used for upgrade.

swupgrade

Description

The swupgrade command node allows you to view the firmware version configuration details, which include the history of upgrades on the device, image details, and automatic upgrade settings.

Parent

kcli/show

image_info

Description

The `image_info` command displays the binary image details of the firmware upgrade, which include version number, release date, name, vendor, etc.

Parent

kcli/show/swupgrade

Syntax

```
image_info url < url string >
```

Parameter Description

Parameter	Description
url	Enter the URL string to view the firmware version details.

upgrade-status

Description

The `upgrade-status` command displays the current software upgrade status, such as, sw_success (upgrade is successful), sw_failed (upgrade failed), sw_not_running (no upgrade is currently in progress), or sw_in_progress (upgrade is currently in progress).

Parent

kcli/show/swupgrade

Syntax

```
upgrade-status
```

history

Description

The `history` command displays the firmware upgrade history, which includes the number of upgrades, time stamp, status, and message.

Parent

kcli/show/swupgrade

Syntax

```
history
```

Topology Module

This section describes show commands of the topology module. You can view the interface parameters, statistics, status, etc.

topology

Description

The `topology` command node allows you to enter the view mode that displays the interface parameters, statistics and status.

Parent

kcli/show

refresh_interval

Description

The `refresh_interval` command displays the refresh time interval in minutes.

Parent

kcli/show/topology

Syntax

```
refresh_interval
```

wan_arp_status

Description

The `wan_arp_status` command displays the Address Resolution Protocol (ARP) status on the WAN interface.

Parent

kcli/show/topology

Syntax

```
wan_arp_status
```

max_host_entries

Description

The `max_host_entries` command displays the maximum number of host entries to be scanned.

Parent

kcli/show/topology

Syntax

```
max_host_entries
```

time-limit

Description

The `time-limit` command displays the time limit set for inactive hosts. After the time limit is over, the inactive hosts are removed from the topology host list.

Parent

kcli/show/topology

Syntax

```
time-limit
```

host-list

Description

The `host-list` command displays the host list for a particular interface.

Parent

kcli/show/topology

Syntax

```
host-list [ interfacename < interface integer(0:32) > ]
```

Parameter Description

Parameter	Description
interfacename	Enter the interface name, for which the hosts are to be listed.

arp-cache

Description

The `arp-chache` command displays the MAC address/s and IP address/s of the devices on the network. The Address Resolution Protocol (ARP) cache is a table that stores mappings between Data Link Layer addresses (usually MAC addresses) and Network Layer addresses (usually IP addresses). The ARP cache is stored in the RAM by the operating system.

Parent

kcli/show/topology

Syntax

```
arp-cache
```

UPnP Module

This section describes show commands of the UPnP module. You can view the rules, status of UPnP and TR64, interface names of UPnP and TR64, blocked IPaddress in UPnP and TR64, etc.

rules

Description

The `rules` command displays the configured UPnP rules.

Parent

kcli/show/upnp

Syntax

```
rules
```

upnpstatus

Description

The `upnpstatus` command displays the UPnP service status (enabled or disabled) on the device.

Parent

kcli/show/upnp

Syntax

```
upnpstatus
```

upnplaninterface

Description

The `upnplaninterface` command displays the configured UPnP LAN interface name.

Parent

kcli/show/upnp

Syntax

```
upnplaninterface
```

tr64-blacklist

Description

The `tr64-blacklist` command displays the list internal hosts blacklisted from accessing the TR-064-enabled devices.

Parent

kcli/show/upnp

Syntax

```
tr64-blacklist
```

tr64laninterface

Description

The `tr64laninterface` command displays the available LAN interfaces on which TR-064 service is enabled.

Parent

kcli/show/upnp

Syntax

```
tr64laninterface
```

tr64-read-access

Description

The `tr64-read-access` command displays the status of the TR-064 read-only access (enabled or disabled) on the device.

Parent

kcli/show/upnp

Syntax

```
tr64-read-access
```

tr64status

Description

The `tr64status` command displays the TR-064 service status (enabled or disabled) on the device.

Parent

kcli/show/upnp

Syntax

```
tr64status
```

upnp-blacklist

Description

The `upnp-blacklist` command displays the list of internal hosts blacklisted from accessing the UPnP-enabled devices.

Parent

kcli/show/upnp

Syntax

```
upnp-blacklist
```

upnp-read-access

Description

The `upnp-read-access` command displays the status of the UPnP read-only access (enabled or disabled) on the device.

Parent

kcli/show/upnp

Syntax

```
upnp-read-access
```

logstatus

Description

The `logstatus` command displays the status of the UPnP logging (enabled or disabled).

Parent

kcli/show/upnp

Syntax

```
logstatus
```

port_forwarding

Description

The `port_forwarding` command displays the status of the port forwarding (enabled or disabled) for UPnP.

Parent

kcli/show/upnp

Syntax

```
port_forwarding
```

stealth_mode

Description

The `stealth_mode` command displays the status of the stealth mode (enabled or disabled.)

Parent

kcli/show/upnp

Syntax

```
stealth_mode
```

request-limit

Description

The `request-limit` command displays the number of packets accepted by the UPnP service per minute.

Parent

kcli/show/upnp

Syntax

```
request-limit
```

User Management Module

This section describes show commands of the user management module. You can view the user information and their roles.

usrmgmt

Description

The `usermgmt` command node allows you to enter the view mode that displays the network user details.

Parent

kcli/show

show-user-info

Description

The `show-user-info` command displays the details of the selected user, including description, e-mail address, address, user role and user type.

Parent

kcli/show/usrmgmt

Syntax

```
show-user-info { user-name < usrname string(2:50) > }
```

Parameter Description

Parameter	Description
iuser-name	Enter the name of the user to view the details.

show-all-user-info

Description

The `show-all-user-info` command displays the details of all the users available on the system.

Parent

kcli/show/usrmgmt

Syntax

```
show-all-user-info
```

roles

Description

The `roles` command displays all the user roles along with the associated permission IDs.

Parent

kcli/show/usrmgmt

Syntax

```
roles
```

passwordEGST

Description

The `passwordEGST` command displays whether the EGST password function is enabled or disabled.

Parent

kcli/show/usrmgmt

Syntax

```
passwordEGST
```

password-required

Description

The `password-required` command displays the status of the password required feature, enabled (true) or disabled (false).

Parent

kcli/show/usrmgmt

Syntax

```
password-required
```

Diagnostic Module

This section describes show commands of the diagnostic module. You can view the results of previously executed commands like nslookup, ping, and traceroute. Also, you can view the parameters of download, upload, and UDP Echo server.

diagnostic

Description

The `diagnostic` command allows you to enter the view mode that displays the configured network diagnostic utilities, such as ping, trace route, and NS lookup.

Parent

kcli/show

nslookup

Description

The `nslookup` command displays the output of NS Lookup service, such as server name, IP address along with the time stamp.

Parent

kcli/show/diagnostic

Syntax

```
nslookup
```

ping

Description

The `ping` command displays the output of previously executed ping command in the form of IP address or name of the target host, packets transmitted and lost along with the time stamp.

Parent

kcli/show/diagnostic

Syntax

```
ping
```

traceroute

Description

The `traceroute` command displays the output of previously executed trace route command in the form of IP address or name of the target host, number of hops taken along with the time stamp.

Parent

kcli/show/diagnostic

Syntax

```
traceroute
```

downloadconfig

Description

The `downloadconfig` command displays the configured downloadconfig parameters, such as download state, DownloadURL, DSCP, Ethernet priority, etc.

Parent

kcli/show/diagnostic

Syntax

```
downloadconfig
```

UDPEchoConfig

Description

The `UDPEchoConfig` command displays the configured parameters for UDPEchoConfig, such as UDP server status, UDP Plus server status, UDP Plus server supported, source IP address, and UDP server interface.

Parent

kcli/show/diagnostic

Syntax

```
UDPEchoConfig
```

uploadConfig

Description

The `uploadConfig` command displays the configured uploadconfig parameters, such as Ethernet priority, file length, UPLD BOM time, UPLD EOM time, and UPLD ROM time.

Parent

kcli/show/diagnostic

Syntax

```
uploadConfig
```

System Module

This section describes show commands of the system module. You can view information pertaining to syslog, system-info, time zone, NTP server, service status, captive portal, log persistency, mail config, first use date, etc.

system

Description

The `system` command node allows you to enter the view mode that displays the device configuration details. It includes information pertaining to syslog, time zone, NTP server, services status etc.

Parent

kcli/show

syslog

Description

The `syslog` major command displays the syslog parameter details related to remote logging, and system log.

Parent

kcli/show/system

system-log

Description

The `system-log` command displays the device log details, including the time stamp.

Parent

kcli/show/system/syslog

Syntax

```
system-log
```

remote-logging

Description

The `remote-logging` command displays the remote-logging server details, including server IP, service state, and remote server port number.

Parent

kcli/show/system/syslog

Syntax

```
remote-logging
```

settings

Description

The `settings` command displays the syslog settings, which include state, maximum file size and number of files to be maintained on the device.

Parent

kcli/show/system/syslog

Syntax

```
settings
```

filters

Description

The `filters` command displays the filter used for displaying logs.

Parent

kcli/show/system/syslog

Syntax

```
filters
```

log

Description

The `log` command displays the system logs.

Parent

kcli/show/system/syslog

Syntax

```
log filter < filter string(1:32) > priority { all | debug | info | notice | warn | err | crit | alert | emerg } offset < offset integer >
```

Parameter Description

Parameter	Description
filter	Enter the filter name for viewing logs.
priority	Select the priority filter for viewing logs.
all	Select all to view all logs.
debug	Select debug to view the debug or higher logs.
info	Select info to view the info or higher logs.
notice	Select notice to view the notice or higher logs.
warn	Select warn to view the warning or higher logs.
err	Select err to view the error or higher logs.
crit	Select crit to view the critical or higher logs.
alert	Select alert to view the alert or higher logs.
emerg	Select emerg to view the emergency or higher logs.
offset	Select offset to view the offset value for displaying logs. Enter the offset value for the log file.

system-group

Description

The `system-group` command displays the device details like host name, domain name, primary/secondary DNS IP address/es, date, time and total device running (up) time.

Parent

kcli/show/system

Syntax

```
system-group
```

timezone

Description

The `timezone` command displays the device time zone, and the status of the day light saving (enabled or disabled).

Parent

kcli/show/system

Syntax

```
timezone
```

ntpserver

Description

The `ntpserver` command displays the configured NTP server details, which include state and server name.

Parent

kcli/show/system

Syntax

```
ntpserver
```

system-info

Description

The `system-info` command displays the firmware version, serial number, device ID, and hardware version of the device.

Parent

kcli/show/system

Syntax

```
system-info
```

service-status

Description

The `service-status` command displays the state of the various configured services on the device.

Parent

kcli/show/system

Syntax

```
service-status
```

autoupdate-DNS-status

Description

The `autoupdate-DNS-status` command displays the status of the auto DNS update service (enabled or disabled) on the device.

Parent

kcli/show/system

Syntax

```
auto
```

day-light-saving

Description

The `day-light-saving` command displays the day light saving settings, which include start and end date, start and end time, and the type (standard or user-defined).

Parent

kcli/show/system

Syntax

```
day-light-saving
```

mail_config

Description

The `mail_config` command displays the mail syslog configuration, including the sender/recipient email address, subject, user name, SMTP server and domain.

Parent

kcli/show/system

Syntax

```
mail_config
```

captive-portal

Description

The `captive-portal` command displays the redirect URL, captive portal status (enabled or disabled), and allowed URL list.

Parent

kcli/show/system

Syntax

```
captive-portal
```

first-use-date

Description

The `first-use-date` command displays the date when the system connected to the Internet for first time after the firmware upgrade.

Parent

kcli/show/system

Syntax

```
first-use-date
```

klog-settings

Description

The `klog-settings` command displays the configured parameters for klog.

Parent

kcli/show/system

Syntax

```
klog-settings
```

log-persistency

Description

The `log-persistency` command displays whether the log persistency is enabled or disabled.

Parent

kcli/show/system

Syntax

```
log-persistency
```

tftp-Server-Directory-Location

Description

The `tftp-Server-Directory-Location` command displays the location of the directory used by the TFTP server on the gateway.

Parent

kcli/show/system

Syntax

```
tftp-Server-Directory-Location
```

onetime-redirect

Description

The `onetime-redirect` command displays the one-time redirect details, such as its status (enabled or disabled), redirect URL, and port.

Parent

kcli/show/system

Syntax

```
onetime-redirect
```

DNS-Communication

Description

The `DNS-Communication` command displays the status of the DNS server (up or down).

Parent

kcli/show/system

Syntax

```
DNS-Communication
```

crashdumpinfo

Description

The `crashdumpinfo` major command displays the system crash dump information, either full or summary.

Parent

kcli/show/system

Syntax

```
crashdumpinfo
```

full

Description

The `full` command under crashdumpinfo displays the complete record of the system memory at the time of kernel crash.

Parent

kcli/show/system/crashdumpinfo

Syntax

```
full
```

summary

Description

The `summary` command under crashdumpinfo displays the summary of crash dump, such as date, time, length, and cause of kernel crash.

Parent

kcli/show/system/crashdumpinfo

Syntax

```
summary
```

DHCP Module

This section describes show commands of the DHCP module. You can view server parameters, client lease information, expired lease status, option 60 status, vendor IDs, etc.

dhcp

Description

The `dhcp` command node allows you to enter the view mode that displays the configured DHCP parameters and lease information.

Parent

kcli/show

dns

Description

The `dns` command node displays the configured MAC entry and host entry details.

Parent

kcli/show

server-params

Description

The `server-params` command displays the configured server parameters, such as lease information, server status, and DNS proxy status.

Parent

kcli/show/dhcp

Syntax

```
server-params
```

expired-lease-status

Description

The `expired-lease-status` command displays the status (enabled or disabled) of the expired DHCP client lease.

Parent

kcli/show/dhcp

Syntax

```
expired-lease-status
```

client-leases

Description

The `client-leases` command displays the client lease information, that is the client's MAC address and the remaining lease period for the client.

Parent

kcli/show/dhcp

Syntax

```
client-leases
```

clients

Description

The `client` command displays the list of DHCP clients along with their respective IP addresses and vendor IDs.

Parent

kcli/show/dhcp

Syntax

```
interface
```

ip-option

Description

The `ip-option` command displays the status of the IP option (enabled or disabled).

Parent

kcli/show/dhcp

Syntax

```
ip-option
```

option60

Description

The `option60` command displays the status of the DHCP client to determine which dedicated service like Internet or IPTV service is accessed.

Parent

kcli/show/dhcp

Syntax

```
option60
```

optionTR111

Description

The `optionTR111` command displays the status of the optionTR111 feature to determine which devices have bypassed the gateway for connecting to the network.

Parent

kcli/show/dhcp

Syntax

```
optionTR111
```

public-private

Description

The `public-private` command displays the status of the public-proxied and public-routed interfaces (enabled or disabled) on the network.

Parent

kcli/show/dhcp

Syntax

```
public-private
```

pools

Description

The `pools` command displays the list of configured pools for DHCP client, along with the IP address range, respective vendor IDs, and DHCP interface/s.

Parent

kcli/show/dhcp

Syntax

```
pools
```

self-address-info

Description

The `self-address-info` command displays the DHCP server parameters, which include status (enable or disable), and IP address pool.

Parent

kcli/show/dhcp

Syntax

```
self-address-info
```

vendorids

Description

The `vendorids` command displays the vendor IDs associated with option 60 feature.

Parent

kcli/show/dhcp

Syntax

```
vendorids
```

vids

Description

The `vids` command displays the vendor IDs for whom option 60 feature is provided.

Parent

kcli/show/dns

Syntax

```
vids
```

QoS Module

This section describes show commands of the qos module. You can view the queue parameters, classification parameters, queue status, etc.

qos

Description

The `qos` command node allows you to enter the view mode that displays the QoS configuration.

Parent

kcli/show

classification

Description

The `classification` command displays the classification parameters.

Parent

kcli/show/qos

Syntax

```
classification [ cid < cid integer > ]
```

Parameter Description

Parameter	Description
cid	Enter the classification ID to view its parameters.

default-queue

Description

The `default-queue` command displays the default queue configured on the network. If the data packet does not classify into any of the custom queues, it must be passed through the default queue.

Parent

kcli/show/qos

Syntax

```
default-queue
```

queue

Description

The `queue` command displays the custom queues on the system.

Parent

kcli/show/qos

Syntax

```
queue [ queueid < qid integer > ]
```

Parameter Description

Parameter	Description
queueid	Enter the ID of the queue to view its details.

state

Description

The `state` command displays whether the queing is enabled or disabled.

Parent

kcli/show/qos

Syntax

```
state
```

TR-69v2 Module

This section describes show commands of the TR-69v2 module. You can view the device information, ACS URL string, ACS connection request information, CPE user name and password, kick URL string, and the periodic inform details.

tr69

Description

The `tr69` command node allows you to enter the view mode that displays the parameters of the TR-069 service.

Parent

kcli/show

device-info

Description

The `device-info` command displays the description and the model name of the CPE device.

Parent

kcli/show/tr69

Syntax

```
device-info
```

acs-url

Description

The `acs-url` command displays the ACS URL with which the CPE is managed.

Parent

kcli/show/tr69

Syntax

```
acs-url
```

connection-request-info

Description

The `connection-request-info` command displays the connection request information, that is, connection request URL and username.

Parent

kcli/show/tr69

Syntax

```
connection-request-info
```

cpe-auth-info

Description

The `cpe-auth-info` command displays the CPE user name used for authentication of the CPE while connecting to the ACS.

Parent

kcli/show/tr69

Syntax

```
cpe-auth-info
```

kick-url

Description

The `kick-url` command displays the LAN-accessible URL used to start the CPE.

Parent

kcli/show/tr69

Syntax

```
kick-url
```

acs-ip-list

Description

The `acs-ip-list` command displays the ACS IP address list.

Parent

kcli/show/tr69

Syntax

```
acs-ip-list
```

agent-status

Description

The `agent-status` command displays the flag that indicates the status of the TR-069 agent (enabled or disabled) in the current configuration.

Parent

kcli/show/tr69

Syntax

```
agent-status
```

certificate-info

Description

The `certificate-info` command displays the ACS certificate information, that is, SSL certificate file name and path.

Parent

kcli/show/tr69

Syntax

```
certificate-info
```

download-queue

Description

The `download-queue` command displays the information about the download queue.

Parent

kcli/show/tr69

Syntax

```
download-queue
```

periodic-inform-info

Description

The `periodic-inform-info` command displays the CPE periodic information, which includes the service status, interval, and time.

Parent

kcli/show/tr69

Syntax

```
periodic-inform-info
```

upgrades-managed

Description

The `upgrades-managed` command displays the status of the upgrades management by the ACS, true (enabled) or false (disabled).

Parent

kcli/show/tr69

Syntax

```
upgrades-managed
```

cwmpinterface

Description

The `cwmpinterface` command displays the WAN interface on which the TR-069 service is running.

Parent

kcli/show/tr69

Syntax

```
cwmpinterface
```

remote-ui-config

Description

The `remote-ui-config` command displays the remote UI configuration details such as maximum number of sessions, maximum and minimum port range, and status (enabled or disabled).

Parent

kcli/show/tr69

Syntax

```
remote-ui-config
```

Interface Module

This section describes show commands of the interface module. You can view interface statistics, WAN addressing mode, configured routes, etc.

if

Description

The `if` command node allows you to enter the view mode that displays the configured interface parameters, interface statistics, WAN addressing mode, and configured routes.

Parent

kcli/show

interface

Description

The `interface` command displays the details of the configured interfaces such as interface name, hardware address, IP address, network mask, broadcast address, MTU, and other related information. Enter the name of an interface to view its details.

Parent

kcli/show/if

Syntax

```
interface [ < interface string(1:32) > ]
```

interface-stats

Description

The `interface-stats` command displays the statistics of the specified interface. Enter the name of an interface to view its statistics.

Parent

kcli/show/if

Syntax

```
interface-stats [ < interface string(1:32) > ]
```

staticparams

Description

The `staticparams` command displays the configured WAN connection parameters.

Parent

kcli/show/if

Syntax

```
staticparams
```

route

Description

The `route` command displays the routes added on the gateway device.

Parent

kcli/show/if

Syntax

```
route [ destination { { default } | { < dest-ip ipaddr > < dest-mask ipaddr > } } ]
```

Parameter Description

Parameter	Description
destination	Enter the route destination IP address/es.
default	Select the default destination IP addresses on the network.

wanmac

Description

The `wanmac` command displays the hardware address and the status of the MAC address (whether the MAC address cloning for the WAN interface is enabled or disabled).

Parent

kcli/show/if

Syntax

```
wanmac
```

wan-mode

Description

The `wan-mode` command displays the WAN addressing mode along with other details such as WAN status, tunnel mode and tunnel status.

Parent

kcli/show/if

Syntax

```
wan-mode
```

mdi_config

Description

The `mdi_config` command displays the MDI configuration on the network in terms of port/s and the state (MDI, MDIX, or auto) on each of the ports.

Parent

kcli/show/if

Syntax

```
mdi_config [ port < portnum integer > ]
```

Parameter Description

Parameter	Description
port	Specify the port number on which the MDI is configured.

pppoe-relay-configuration

Description

The `pppoe-relay-configuration` command displays the PPPoE relay configuration in terms of inbound interface/s, number of concurrent sessions, and relay service status (enable or disable).

Parent

kcli/show/if

Syntax

```
pppoe-relay-configuration [ wan_interface < interface string > ]
```

Parameter Description

Parameter	Description
wan_interface	Enter the WAN interface name to view the PPPoE relay configuration.

wan-access-type

Description

The `wan-access-type` command displays the WAN addressing mode configured on the device in terms of WAN access type (auto, DSL, or Ethernet).

Parent

kcli/show/if

Syntax

```
wan-access-type
```

auto-wan-mode

Description

The `auto-wan-mode` command displays whether the auto WAN addressing mode is enabled or disabled.

Parent

kcli/show/if

Syntax

```
auto-wan-mode
```

def_mode

Description

The `def_mode` command displays the default mode configured for WAN access.

Parent

kcli/show/if

Syntax

```
def_mode
```

TR111Part1 Module

This section describes show commands of the TR111Part1 module. You can view information pertaining to the manageable devices.

tr111part1

Description

The `tr111part1` command node allows you to enter the show mode of the TR-111 module.

Parent

kcli/show

manageable-device-info

Description

The `manageable-device-info` command displays the notification limit (in seconds) and number of devices managed by the TR-111 service.

Parent

kcli/show/tr111part1

Syntax

```
manageable-device-info
```

manageable-devices

Description

The `manageable-device` command displays the details of the devices managed by the TR-111 service, such as manufacturer OUI, product class, and MAC address.

Parent

kcli/show/tr111part1

Syntax

```
manageable-devices [ IP-Addr < ip string> ]
```

Parameter Description

Parameter	Description
IP-Addr	Enter the IP address of the device.

DSL Module

This section describes show commands of the DSL module. You can view the tone settings, WAN interface parameters, loop diagnostic state, auto-scan status, etc.

dsl

Description

The `dsl` command node allows you to enter the view mode that displays the DSL parameters and their status.

Parent

kcli/show

tone

Description

The `tone` command displays the configured parameters for the types of tone, such as SNR-per-subcarrier, Bit-allocation-per-subcarrier, and gain-allocation-per-subcarrier.

Parent

kcli/show/dsl

bit-allocation-per-subcarrier

Description

The `bit-allocation-per-subcarrier` command displays the bit allocation per subcarrier.

Parent

kcli/show/dsl/tone

Syntax

```
bit-allocation-per-subcarrier
```

gain-allocationper-subcarrier

Description

The `gain-allocationper-subcarrier` command displays the gain allocation per subcarrier.

Parent

kcli/show/dsl/tone

Syntax

```
gain-allocationper-subcarrier
```

snr-per-subcarrier

Description

The `snr-per-subcarrier` command displays the signal-to-noise ratio per subcarrier.

Parent

kcli/show/dsl/tone

Syntax

```
snr-per-subcarrier
```

wan-interface-config

Description

The `wan-interface-config` command displays the configured parameters for WAN interface, such as general parameters, time parameters, and termination unit parameters.

Parent

kcli/show/dsl

interface

Description

The `interface` major command displays the DSL WAN interface configuration.

Parent

kcli/show/dsl/wan-interface-config

Syntax

```
interface < ifname string(1:32) >
```

general_params

Description

The `general_params` command displays the general parameters of the WAN interface, such as link status, modulation type, DSL modem version.

Parent

kcli/show/dsl/wan-interface-config/interface

Syntax

```
general_params
```

termination_unit_params

Description

The `termination_unit_params` command displays the termination unit parameters of the WAN interface, such as ATUR Vendor, ATUR Country, ATUR ANSISTD, ATUR ANSIREV, ATUC Vendor, ATUC Country, ATUC ANSISTD, and ATUC ANSIREV.

Parent

kcli/show/dsl/wan-interface-config/interface

Syntax

```
termination_unit_params
```

time-params

Description

The `time-params` command displays the time parameters of the WAN interface, such as Total Start, Show Time Start, Last Show Time Start, Current Day Start, and Quarter Hour Start.

Parent

kcli/show/dsl/wan-interface-config/interface

Syntax

```
time-params
```

interface

Description

The `interface` major command displays the interface name of the DSL link in use.

Parent

kcli/show/dsl

Syntax

```
interface < ifname string(1:32) >
```

atm-parameters

Description

The `atm-parameters` command displays the ATM parameter details of the DSL interface.

Parent

kcli/show/dsl/interface

Syntax

```
atm-parameters
```

atm-params-stats

Description

The `atm-params-stats` command displays DSL ATM parameter statistics of the DSL interface.

Parent

kcli/show/dsl/interface

Syntax

```
atm-params-stats
```

basic-config

Description

The `basic-config` command displays basic configuration details of DSL interface, such as the status of interface configuration (enable or disable), VC search list, destination address, and default P-bit.

Parent

kcli/show/dsl/interface

Syntax

```
basic-config
```

current-day-statistics

Description

The `current-day-statistics` command displays current day statistics of the DSL interface.

Parent

kcli/show/dsl/interface

Syntax

```
current-day-statistics
```

last-show-time-statistics

Description

The `last-show-time-statistics` command displays last show time statistics of the DSL interface.

Parent

kcli/show/dsl/interface

Syntax

```
last-show-time-statistics
```

quarter-hour-statistics

Description

The `quarter-hour-statistics` command displays quarter hour statistics of the DSL interface.

Parent

kcli/show/dsl/interface

Syntax

```
quarter-hour-statistics
```

show-time-statistics

Description

The `show-time-statistics` command displays total time statistics of the DSL interface.

Parent

kcli/show/dsl/interface

Syntax

```
show-time-statistics
```

total-statistics

Description

The `total-statistics` command displays total statistics of the DSL interface.

Parent

kcli/show/dsl/interface

Syntax

```
total-statistics
```

pvc-status

Description

The `pvc-status` command displays if the ATM circuit status is up or down.

Parent

kcli/show/dsl/interface

Syntax

```
pvc-status
```

auto-scanning

Description

The `auto-scanning` command displays the status of the auto-scanning, enabled (on) or disabled (off.)

Parent

kcli/show/dsl

Syntax

```
auto-scanning
```

auto-scan-status

Description

The `auto-scan-status` command displays whether the auto-scan has started or stopped.

Parent

kcli/show/dsl

Syntax

```
auto-scan-status
```

loop-diagnostics-state

Description

The `loop-diagnostics-state` command displays the configured value for the Loop diagnostics state.

Parent

kcli/show/dsl

Syntax

```
loop-diagnostics-state
```

driver_config

Description

The `driver_config` command displays the current state of all DSL configuration parameters.

Parent

kcli/show/dsl

Syntax

```
driver_config
```

time_since_last

Description

The `time_since_last` command displays the list of timers that measure the time transpired since the most recent event. The list covers only certain xDSL statistics parameters actually displayed in the detailed DSL statistics UI.

Parent

kcli/show/dsl

Syntax

```
time_since_last
```

VoIP Module

This section describes show commands of the VoIP module. You can view profiles, lines, codecs, and physical interfaces.

voip

Description

The `voip` command node allows you to enter the view mode that displays the VoIP service configuration.

Parent

kcli/show

bband-interface

Description

The `bband-interface` command displays the current WAN interface for VoIP.

Parent

kcli/show/voip

Syntax

```
bband-interface
```

capability

Description

The `capability` command displays the VoIP capability associated with the gateway device.

Parent

kcli/show/voip

Syntax

```
capability voiceService < service integer(0:65535) > capability < cap string >
```

Parameter Description

Parameter	Description
voiceService	Enter the associated voice service number.
capability	Enter the capability name to view its details.

codecs

Description

The `codecs` command displays the codecs associated with the specified capability.

Parent

kcli/show/voip

Syntax

```
codecs voiceService < service integer > [ codecId < id integer > ]
```

Parameter Description

Parameter	Description
voiceService	Enter the associated voice service number.
codecId	Enter the codec ID to view its details.

lineList

Description

The `lineList` command displays the list associated with the specified phone line.

Parent

kcli/show/voip

Syntax

```
lineList voiceService < service integer > voiceProfileId < profile integer > LineId <
directory integer > [ listId < id integer > ]
```

Parameter Description

Parameter	Description
voiceservice	Enter the associated voice service number.
voiceProfileId	Enter the voice profile ID number.
LineId	Enter the phone line ID.
listId	Enter the associated list ID.

physical-interfaces

Description

The `physical-interfaces` command displays the physical interfaces associated with the specified voice service.

Parent

kcli/show/voip

Syntax

```
physical-interfaces voiceService < service integer >
```

Parameter Description

Parameter	Description
voiceService	Enter the voice service number to view the physical interfaces associated with it.

voiceLine

Description

The `voiceLine` command displays the voice line configuration details, for example, line name, line status (enable or disable), line ID, line directory number, line type (dect or fxs).

Parent

kcli/show/voip

Syntax

```
voiceLine voiceService < service integer > voiceProfileId < profile integer > [ LineId < directory integer > ]
```

Parameter Description

Parameter	Description
voiceService	Enter the associated voice service identification number.
voiceProfileId	Enter the voice profile ID.
LineId	Enter the phone line ID to view its configuration.

voiceProfile

Description

The `voiceProfile` command displays the voice profile details, such as profile status (enable or disable), DTMF method used, digit map, signaling protocol.

Parent

kcli/show/voip

Syntax

```
voiceProfile [ voiceService < service integer > profileId < id integer > ]
```

Parameter Description

Parameter	Description
voiceService	Enter the associated voice service number.
profileId	Enter the voice profile ID number to view its details.

APPENDIX A

Glossary

Term	Description
Access Point (AP)	An Access Point is a hardware device or a computer's software that acts as a communication hub for users of a wireless device to connect to a wired LAN. APs are important for providing enhanced wireless security and for extending the physical range of service a wireless user has access to.
Advanced Encryption Standard (AES)	AES is a symmetric 128-bit block data encryption technique that works at multiple network layers simultaneously.
Aging Time	The aging time is the number of seconds a MAC-address will be kept in the forwarding database after having received a packet from a MAC address.
American Standard Code for Information Interchange (ASCII)	ASCII specifies a correspondence between the digital bit patterns and the symbols/ glyphs of a written language, thus allowing digital devices to communicate with each other and to process, store, and communicate character-oriented information. It uses a 7-bit code, meaning that it uses the bit patterns represented with seven binary digits (a range of 0 to 127 decimal) to represent character information.
Antenna Transmit Power	Antenna Transmit Power is the amount of power used by the wireless radio transceiver to send the signal out. Limiting antenna power can be useful for security purposes. The recommended value is 100 dB.
Application Level Gateway (ALG)	An ALG consists of a security component that augments a firewall or NAT employed in a computer network. It allows legitimate application data to pass through the security checks of the firewall that would have otherwise restricted the traffic for not meeting its limited filter criteria.
Asymmetric Digital Subscriber Line (ADSL)	ADSL is a high-speed Internet access service that utilizes existing copper telephones lines to send and receive data at speeds that far exceed conventional dial-up modems.
Asynchronous Transfer Mode (ATM)	ATM is a dedicated-connection switching technology that organizes digital data into 53-byte cell units and transmits them over a physical medium using digital signal technology. Individually, a cell is processed asynchronously relative to other related cells and is queued before being multiplexed over the transmission path.
Beacon Interval	Beacons are packets sent by an AP to synchronize a wireless network. Specify a beacon interval value between 1 and 1000 (milliseconds). The recommended value is 100.
Bridge	A bridge is a way to connect two Ethernet segments together in a protocol independent way. Packets are forwarded based on Ethernet address, rather than IP address (like a router since forwarding is done at Layer 2, all protocols can go transparently through a bridge.
Broadcast Address	Broadcast Address is an IP address that is used to deliver a message from one machine to all machines on a network.
Certificates	Certificates are digital signatures issued by a Certification Authority (CA). In NP Secure, certificates are used only when RSA Certificate is selected as the authentication mode, while configuring a connection. Note that the information entered in this screen is used for all the configured connections using certificate as the authentication information.
Certification Authority (CA) Certificate	In cryptography, a certificate authority or certification authority (CA) is an entity that issues digital certificates for use by other parties. It is an example of a trusted third party. CAs are characteristic of many public key infrastructure (PKI) schemes.
Channel	Channel is the route which a message follows, as it is transmitted between a communication source and a receiver. It defines a portion of the radio spectrum the radio interface uses for transmitting and receiving the data.
Contention Window	The Contention Window refers to the random back-off timer used by the AP. The period set through the contention window minimum and the contention window maximum is the wait time for the AP before attempting to access a channel again.
Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP)	CCMP is an IEEE 802.11i encryption protocol. It was created to replace, together with TKIP, the earlier insecure WEP protocol. CCMP uses the Advanced Encryption Standard (AES) algorithm. In the CCMP, unlike TKIP, key management and message integrity is handled by a single component built around AES.

Term	Description
Customer Premise Equipment (CPE)	CPE is any terminal and associated equipment and inside wiring located at a subscriber's premises and connected with a carrier's telecommunication channel(s) at the demarcation point. The demarcation point is a point established in a building or complex to separate customer equipment from telephone company equipment. CPE generally refers to telephones, DSL/cable modems, or set-top boxes for use with communication service providers' services.
Daylight Saving Time (DST)	The Daylight Saving Time, also know as summer time, is a commonly used time system for adjusting the official local time forward, usually by one hour, from its official standard time for the summer month.
Delivery Traffic Indication Message (DTIM) Period	A DTIM is a countdown mechanism informing clients of the next window for listening to broadcast and multicast messages. When the AP has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. The AP clients hear the beacons and awaken to receive the broadcast and multicast messages.
Demilitarized Zone (DMZ)	A DMZ PC is a computer or small sub-network that sits between a trusted internal network, such as a corporate private LAN and a non-trusted external network, such as the public Internet.
DHCP Client Lease	The length of time the IP address is available to the device it was assigned to. This time period is determined by the DHCP server.
Differentiated Services Code Point (DSCP)	The DSCP is a field in the header of IP packets for packet classification purposes (used especially for controlling bandwidth).
Digital Subscriber Line (DSL)	DSL is a family of technologies that provides digital data transmission over the wires of a local telephone network. In telecommunications marketing, the term Digital Subscriber Line is widely understood to mean Asymmetric Digital Subscriber Line (ADSL), the most commonly installed technical varieties of DSL. DSL service is delivered simultaneously with regular telephone on the same telephone line as it uses a higher frequency band that is separated by filtering.
Domain Name	Domain Name is a name that is entered into a computer as part of a website, other URL, or an email address. It is then looked up into the DNS, which communicates to the workstation of the IP addresses corresponding to that name.
Domain Name System (DNS)	The DNS is a system that stores information associated with domain names in a distributed database on networks, such as the Internet. The domain name system associates many types of information with domain names, but most importantly, it provides the IP address associated with the domain name.
Dynamic Domain Name System (DDNS)	The DDNS maps Internet domain names to IP addresses. Unlike DNS that works with static IP addresses only, DDNS works with dynamic IP addresses, for example the IP addresses assigned by an ISP or other DHCP server.
Dynamic Host Configuration Protocol (DHCP)	The DHCP is a set of rules used by a communications device (such as a computer, router or networking adapter) to allow the device to request and obtain an Internet address from a DHCP server which has a list of addresses available for assignments.
Dual Tone Multi Frequency (DTMF)	DTMF is the signal to the phone company that you generate when you press an ordinary telephone's touch keys. DTMF has generally replaced loop disconnect ("pulse") dialling. With DTMF, each key you press on your phone generates two tones of specific frequencies. So that a voice cannot imitate the tones, one tone is generated from a high-frequency group of tones and the other from a low frequency group.
Encryption Type	Encryption Type is the algorithm to be used for encrypting the data transmitted between the AP and the client. The value can be either tkip or aesCcmp.
File Transfer Protocol (FTP)	FTP is used for exchanging files over the Internet. FTP works in the same way as HTTP for transferring Web pages from a server to a user's browser and SMTP for transferring electronic mail across the Internet in that, like these technologies, FTP uses the Internet's TCP/IP protocols to enable data transfer. FTP is most commonly used to download a file from a server using the Internet or to upload a file to a server (for instance, uploading a Web page file to a server).
Firewall	A Firewall involves the hardware or software that attempts to protect a computer or network against malicious attacks. By acting as a wall between one network and another, it controls the flow of data and methods in which one network can connect to another to limit exposure.
Forwarding	Forwarding is the relaying of packets from one network segment to another by nodes in a computer network. The bridges forward packets according to a simple algorithm. Forwarding Table displays this information.

Term	Description
Fragmentation Threshold	When transmitting a packet over a network medium, sometimes the packet is broken into several segments, if the size of packet exceeds that allowed by the network medium. The Fragmentation Threshold defines the number of bytes used for the fragmentation boundary for directed messages. This value should remain at its default setting of 2346. If you experience a high packet error rate, you may slightly increase your "Fragmentation" value within the value range of 1500 to 2346. Setting the Fragmentation value too low may result in poor performance.
Hardware Mode	The wireless hardware mode is the wireless Data Link Protocol standard used. This can be 802.11a, 802.11b, or 802.11g (IEEE 802.11b, IEEE 802.11a, IEEE 802.11g).
Hexadecimal (Hex)	Hexadecimal is primarily used in computing to represent a byte, whose 256 possible values can be represented with only two digits in hexadecimal notation. Alternatively, representing a byte with 8-bit ASCII has a number of problems. First, there are unprintable control characters; second, ASCII itself stops at 7 bits with the remainder being system-specific extensions; and finally, even if all characters in the machine's set are displayable as something, neither users nor input methods are generally prepared to handle 256 unique characters.
Host Name	A host name is the unique name given to a machine (or a device) on a network. This host name is used to identify connected device or machine for various types of electronic communication.
ISP Mode	ISP Mode is a communication protocol followed by a service provider for its Internet service. The ISP Mode can be PPPoE, DHCP or static.
Layer 2 Tunneling Protocol (L2TP)	L2TP is an extension of the Point-to-Point Tunneling Protocol (PPTP) used by an ISP to enable the operation of a VPN over the Internet.
Lease Period	The Lease Period is the time for which the DHCP allocates an IP address to a DHCP client. Before the leases expire, the DHCP clients are expected to renew the leases in order to continue to use the allocated IP addresses.
Local Area Network (LAN)	LAN covers small area such as an office, a home, a building, or a college. LANs generally are based on switched Ethernet or Wi-Fi technology.
MAC Address Access List (MAC-ACL)	MAC-ACL is a type of security feature commonly used by wireless networks. Under this, the device creates and distributes a MAC-ACL to APs so that only authorized NICs can connect to the network.
Media Access Control (MAC) address	This is the physical address of any device, such as the NIC in a computer, on the network. The MAC address, which is made up of two equal parts, is 6 bytes long. The first 3 bytes identify the company that made the NIC. The second 3 bytes are the serial number of the NIC itself.
Multiple Service Set Identifier (SSID)	Multiple SSID is a unique identifier used by wireless networking devices to establish and maintain wireless connection.
Netmask	A netmask, also known as a subnet mask, or address mask, is a bitmask used to determine the subnet of the host.
Network Address Translation (NAT)	NAT is defined in RFC 1631. It was published in 1994, to solve the problem of IP address shortage. At the same time, it broke the peer-to-peer nature of the Internet by defining closed networks connecting through a Wireless, a NAT device. This is the way most enterprise and home networks connect to the Internet today. NAT is an Internet standard that enables a LAN to use one set of IP addresses for internal traffic and a second set of addresses for external traffic.
Network Time Protocol (NTP)	NTP is used for synchronizing the clocks over network. NTP is an Internet standard protocol (built on top of TCP/IP) that assures accurate synchronization to the millisecond of computer clock times in a network. Based on UTC, NTP synchronizes client workstation clocks to the U.S. Naval Observatory Master Clocks in Washington, DC and Colorado Springs CO. Running as a continuous background client program on a computer, NTP sends periodic time requests to servers, obtaining server time stamps and using them to adjust the client's clock. The latest version of NTP is defined in RFC 1305.
Non-linear Noise Monitoring (NLNM) Threshold	NLNM threshold is the number of tones with excessive non-linear noise that triggers flagging of unexpected line conditions, such as, missing phone filter.

Term	Description
OpenSSL Utility	This is an open source implementation of the SSL and the TLS protocols. The core library (written in the C programming language) implements the basic cryptographic functions and provides various utility functions. Wrappers allowing the use of the OpenSSL library in a variety of computer languages are available. Versions are available for most Unix based operating systems (including Solaris, Linux, Mac OS X and the four open source BSD operating systems) and also for Microsoft Windows.
Permanent Virtual Circuit (PVC)	A PVC is a fixed circuit that is defined in advance by a public network carrier (or a network manager on an internal network). The permanence of the line removes the setup overhead and improves performance. A PVC is used on a circuit that includes routers that must maintain a constant connection in order to transfer routing information in a dynamic network environment. Carriers assign PVCs to customers to reduce overhead and improve performance on their networks.
Point-to-Point Tunneling Protocol (PPTP)	PPTP is a method for implementing VPNs. As the Internet is essentially an open network, the PPTP is used for secure data transfer from a remote client to a private enterprise server.
Port Forwarding	Port forwarding is the act of forwarding a network port from one machine to another. One use of this technique is to allow an external user to reach a port on a private IP address (inside a LAN) from the outside via a NAT-enabled router.
Pre-shared Key (PSK)	Pre-shared Key (psk) is the authentication password key that the remote user needs to enter while establishing a connection with the local gateway.
Public Key Infrastructure (PKI) Pass Phrase	The PKI Pass Phrase is used to protect the private key information in certificates from unauthorized access.
Quality of Service (QoS)	The Quality of Service (QoS) feature allows you to measure network bandwidth, detect changing network conditions (such as congestion or availability of bandwidth), and prioritize traffic. For example, QoS can be applied to prioritize traffic for latency-sensitive applications (such as voice or video) and to control the impact of latency-insensitive traffic (such as bulk data transfers). QoS enables complex networks to control and predictably service a variety of networked applications and traffic types. Almost any network can take advantage of QoS for optimum efficiency, whether it is a small corporate network, an Internet service provider, or an enterprise network.
Real-time Transport Protocol (RTP)	The RTP defines a standardized packet format for delivering audio and video over the Internet. RTP is used extensively in communication and entertainment systems that involve streaming media, such as telephony, video teleconference applications and web-based push to talk features. For these it carries media streams controlled by H.323, MGCP, Megaco, SCCP, or Session Initiation Protocol (SIP) signaling protocols, making it one of the technical foundations of the Voice over IP industry. RTP is usually used in conjunction with the RTP Control Protocol (RTCP). While RTP carries the media streams (for example, audio and video) or out-of-band events signaling (DTMF in separate payload type), RTCP is used to monitor transmission statistics and Quality of Service (QoS) information. When both protocols are used in conjunction, RTP is usually originated and received on even port numbers, whereas RTCP uses the next higher odd port number.
Remote Authentication Dial-In User Service (RADIUS)	RADIUS is an authentication and accounting system used by many ISPs. When you dial in to the ISP you must enter your user name and password. This information is passed to a RADIUS server, which checks that the information is correct and then authorizes the access to the ISP system.
Routing Information Protocol (RIP)	RIP is a simple distance vector protocol. RIP uses static metrics to compare routes. The protocol is limited to networks whose longest path is 15 hops.
RSA Certificate Authentication	RSA Certificate authentication method requires an RSA Certificate issued by a Certificate Authority for NP Secure. If you wish to use this authentication method, you need to import the certificate information from a PKI server into NP Secure.
RTS Threshold	RTS stands for Request to Send. This parameter controls what size data packet the low level RF protocol issues to an RTS packet. If you encounter an inconsistent data flow, only minor modifications to the value range between 256 and 2432 are recommended. The recommended value for RTS Threshold is 2432.

Term	Description
Seamless Rate Adaptation (SRA)	SRA software allows modems to make seamless data transfer rate changes to avoid dropping a connection. Modems are affected by cross talk from adjacent lines, as well as by other interference such as temperature changes and radio signals. Any interference on the connection can cause a modem to retrain on another connection and drop the existing connection. SRA makes dynamic data transfer rate changes to accommodate temporary noise conditions on the line thus preventing dropped connections.
Session Initiation Protocol (SIP)	The SIP is an IETF-defined signaling protocol, widely used for controlling multimedia communication sessions such as voice and video calls over Internet Protocol (IP). The protocol can be used for creating, modifying and terminating two-party (unicast) or multiparty (multicast) sessions consisting of one or several media streams. The modification can involve changing addresses or ports, inviting more participants, adding or deleting media streams, etc. Other feasible application examples include video conferencing, streaming multimedia distribution, instant messaging, presence information, file transfer and online games.
Shared Key	The Shared Key is a password for your wireless interface that is only known to you. The value can be wpaPass (WPA Passphrase) or WPA-PSK Hex. In case of the former, an alphanumeric value having a range of 8 to 63 characters can be entered, while in the latter case a hexadecimal value of 64 characters can be entered.
Temporal Key Integrity Protocol (TKIP)	TKIP is a security protocol used in Wi-Fi Protected Access (WPA). WPA is used for wireless networks to correct deficiencies in the older Wired Equivalent Privacy (WEP) standard. TKIP was designed to replace WEP without replacing legacy hardware.
Tertiary DNS	This refers to the second backup DNS server. If the secondary DNS server does not respond to a query within the Timeout Period, the system queries this server.
TR-069	TR-069 (short form for Technical Report 069) is a Broadband Forum technical specification entitled CPE WAN Management Protocol (CWMP). It defines an Internet protocol for remote management of home network devices and terminals. As a bi-directional SOAP/HTTP based protocol, it provides the communication between CPE and Auto Configuration Servers (ACS). It includes both a safe auto configuration and the control of other CPE management functions within an integrated framework.
Transmission Opportunity	Also known as TXOP is the interval of time period used by the Wi-Fi multimedia stations to transmit the packets on to the wireless network.
Turbo Mode	Turbo mode allows transmission on 2 channels, which improves data rate (up to 72 Mbps). This setting must be the same on the access point and clients or they will not be able to communicate with each other.
Universal Plug and Play (UPnP)	UPnP is a networking architecture for automatically configuring devices, discovering services and providing peer-to-peer data transfer over an IP network. UPnP works with wired or wireless networks and can be supported on any operating system. UPnP boasts device-driver independence and zero-configuration networking, which is automatic installation without manual configuration. UPnP devices can use many of the standard protocols in the TCP/IP stack including TCP, UDP, IGMP, ARP, and IP, as well as TCP/IP services such as DHCP and DNS.
Very High Speed Digital Subscriber Line (VDSL)	VDSL transmits data in the 13 Mbps - 55 Mbps range over short distances, usually between 1000 and 4500 feet (300 - 1500 meters), of twisted pair copper wire. The shorter the distance, the faster the connection rate. As the final length of cable into the home or office, VDSL connects to neighborhood Optical Network Units (ONUs), which connect to the central office's main fiber network backbone. This architecture will allow VDSL users to access the maximum bandwidth available through normal phone lines.
Wide Area Network (WAN)	WAN covers a broad geographical area and is used to connect various LAN. The most common WAN is the Internet.
Wi-Fi Protected Access (WPA)	WPA, a new security standard build upon WEP, is encryption method used to “encrypt” the traffic on your network and provides more advanced protection to your traffic than WEP. It works with PSK (Pre-Shared Key) to decrypt the transmitted data at the receiving end.
Wi-Fi Protected Access 2 (WPA2)	This security mode is advanced version of the WPA and aims at solving many security issues that WPA posed. It uses the AES encryption algorithm unlike WAP (that uses RC4 Encryption algorithm.
Wi-Fi Protected Access Pre-Shared Key (WpaPsk)	WpaPsk is based on the WEP and requires a key to be entered on both the access point and client. This key must be the same on both, only then you are allowed to connect to the network. WpaPsk uses a pass-phrase that is between 8 and 63 characters and 128-bit encryption to provide more secure wireless network.

Term	Description
Wi-Fi Protected Setup (WPS)	WPS is to simplify the process of configuring security on wireless networks by having an additional hardware integrated on the device. The WPS protocol consists of a series of EAP message exchanges that are triggered by a user action.
Wireless	Wireless is a node on a network that serves as an entrance to another network. In an office a Wireless can be a computer that routes the traffic from a workstation to the outside network that is serving the Web pages. In homes, the Wireless is the ISP that connects the user to the Internet. The Wireless is also associated with both a router, which use headers and forwarding tables to determine where packets are sent and a switch, which provides the actual path for the packet in and out of the Wireless.
Wireless Equivalent Privacy (WEP)	WEP is the oldest encryption method for your wireless network. It “encrypts” the traffic on your network so that a hacker cannot understand the transmitted data. A "key" or password is required to decrypt this data at the receiving end. This security mode encrypts the data using 40 bits of the secret WEP key and random 24 bits. The said data is decrypted using the same key and 24 bits.
Wireless Interface Mode	The wireless interface mode can be configured as Client and AP mode (called as the master), where the device controls association of the stations to the box. In the client mode or the managed mode, the box is able to connect to another AP.