Cyberoam
Unified Threat Management

Console Guide

Version 10

Document version 10.01.0286 - 1.0-17/11/2010

IMPORTANT NOTICE

Elitecore has supplied this Information believing it to be accurate and reliable at the time of printing, but is presented without warranty of any kind, expressed or implied. Users must take full responsibility for their application of any products. Elitecore assumes no responsibility for any errors that may appear in this document. Elitecore reserves the right, without notice to make changes in product design or specifications. Information is subject to change without notice.

USER'S LICENSE

The Appliance described in this document is furnished under the terms of Elitecore's End User license agreement. Please read these terms and conditions carefully before using the Appliance. By using this Appliance, you agree to be bound by the terms and conditions of this license. If you do not agree with the terms of this license, promptly return the unused Appliance and manual (with proof of payment) to the place of purchase for a full refund.

LIMITED WARRANTY

Software: Elitecore warrants for a period of ninety (90) days from the date of shipment from Elitecore: (1) the media on which the Software is furnished will be free of defects in materials and workmanship under normal use; and (2) the Software substantially conforms to its published specifications except for the foregoing, the software is provided AS IS. This limited warranty extends only to the customer as the original licenses. Customers exclusive remedy and the entire liability of Elitecore and its suppliers under this warranty will be, at Elitecore or its service center's option, repair, replacement, or refund of the software if reported (or, upon, request, returned) to the party supplying the software to the customer. In no event does Elitecore warrant that the Software is error free, or that the customer will be able to operate the software without problems or interruptions. Elitecore hereby declares that the anti virus and anti spam modules are powered by Kaspersky Labs and by Commtouch respectively and the performance thereof is under warranty provided by Kaspersky Labs and by Commtouch. It is specified that Kaspersky Lab does not warrant that the Software identifies all known viruses, nor that the Software will not occasionally erroneously report a virus in a title not infected by that virus.

Hardware: Elitecore warrants that the Hardware portion of the Elitecore Products excluding power supplies, fans and electrical components will be free from material defects in workmanship and materials for a period of One (1) year. Elitecore's sole obligation shall be to repair or replace the defective Hardware at no charge to the original owner. The replacement Hardware need not be new or of an identical make, model or part; Elitecore may, in its discretion, replace the defective Hardware (or any part thereof) with any reconditioned product that Elitecore reasonably determines is substantially equivalent (or superior) in all material respects to the defective Hardware.

DISCLAIMER OF WARRANTY

Except as specified in this warranty, all expressed or implied conditions, representations, and warranties including, without limitation, any implied warranty or merchantability, fitness for a particular purpose, non-infringement or arising from a course of dealing, usage, or trade practice, and hereby excluded to the extent allowed by applicable law.

In no event will Elitecore or its supplier be liable for any lost revenue, profit, or data, or for special, indirect, consequential, incidental, or punitive damages however caused and regardless of the theory of liability arising out of the use of or inability to use the product even if Elitecore or its suppliers have been advised of the possibility of such damages. In no event shall Elitecore's or its supplier's liability to the customer, whether in contract, tort (including negligence) or otherwise, exceed the price paid by the customer. The foregoing limitations shall apply even if the above stated warranty fails of its essential purpose.

In no event shall Elitecore or its supplier be liable for any indirect, special, consequential, or incidental damages, including, without limitation, lost profits or loss or damage to data arising out of the use or inability to use this manual, even if Elitecore or its suppliers have been advised of the possibility of such damages.

RESTRICTED RIGHTS

CORPORATE HEADQUARTERS

Elitecore Technologies Ltd.
904 Silicon Tower,
Off. C.G. Road,
Ahmedabad – 380015, INDIA
Phone: +91-79-66065606
Fax: +91-79-26407640
Web site: www.elitecore.com , www.cyberoam.com

Contents

Annexure I - Contents

Preface

Welcome to Cyberoam's – Console guide.

Cyberoam is an Identity-based UTM Appliance. Cyberoam's solution is purpose-built to meet the security needs of corporate, government organizations, and educational institutions.

Cyberoam's perfect blend of best-of-breed solutions includes user based Firewall, Content filtering, Anti Virus, Anti Spam, Intrusion Prevention System (IPS), and VPN – IPSec and SSL.

Cyberoam provides increased LAN security by providing separate port for connecting to the publicly accessible servers like Web server, Mail server, FTP server etc. hosted in DMZ which are visible the external world and still have firewall protection.

Cyberoam Console guide helps you administer, monitor and manage Cyberoam with the help of Console.

Note that by default, Cyberoam Console password is 'admin'. It is recommended to change the default password immediately after deployment.

Guide Audience

Cyberoam Console Guide provides functional and technical information of the Cyberoam Software. This Guide is written to serve as a technical reference and describes features that are specific to the Console.

Guide also provides the brief summary on using the Console commands.

This guide is intended for the Network Administrators and Support personnel who perform the following tasks:

- Configure System & Network
- Manage and maintain Network
- Manage various services
- Troubleshooting

This guide is intended for reference purpose and readers are expected to possess basic-to-advanced knowledge of systems networking.

Note

The Corporate and individual names, data and images in this guide are for demonstration purposes only and does not reflect the real data.

If you are new to Cyberoam, use this guide along with the 'Cyberoam User Guide'

Technical Support

You may direct all questions, comments, or requests concerning the software you purchased, your registration status, or similar issues to Customer care/service department at the following address:

Corporate Office
eLitecore Technologies Ltd.
904, Silicon Tower
Off C.G. Road
Ahmedabad 380015
Gujarat, India.
Phone: +91-79-66065606
Fax: +91-79-26407640
Web site: www.elitecore.com

Cyberoam contact:
Technical support (Corporate Office): +91-79- 26400707
Email: support@cyberoam.com
Web site: www.cyberoam.com

Visit www.cyberoam.com for the regional and latest contact information.

Typographic Conventions

Material in this manual is presented in text, screen displays, or command-line notation.

Item	Convention	Example
Server		Machine where Cyberoam Software - Server component is installed
Client		Machine where Cyberoam Software - Client component is installed
User		The end user
Username		Username uniquely identifies the user of the system
Topic titles	Shaded font typefaces	Introduction
Subtitles	Bold and Black typefaces	Notation conventions
Navigation link	Bold typeface	**Group Management → Groups → Create** it means, to open the required page click on Group management then on Groups and finally click Create tab
Notes & points to remember	Bold typeface between the black borders	**Note**

Introduction

Cyberoam CLI console provides a collection of tools to administer, monitor and control certain Cyberoam components.

Accessing Cyberoam CLI Console

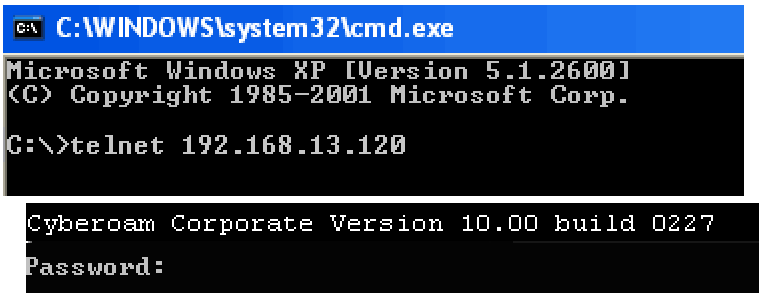
Two ways to access Cyberoam CLI console:

1. Direct Console connection - attaching a keyboard and monitor directly to the Cyberoam
2. Remote connection
   a) Using remote login utility – TELNET
   b) Using SSH client

Accessing CLI Console via remote login utility - TELNET

To use TELNET, IP Address of the Cyberoam is required.

Use command “telnet <Cyberoam IP address>” to start TELNET utility from command prompt and log on with default password “admin”



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\>telnet 192.168.13.120
```

```
Cyberoam Corporate Version 10.00 build 0227

Password:
```

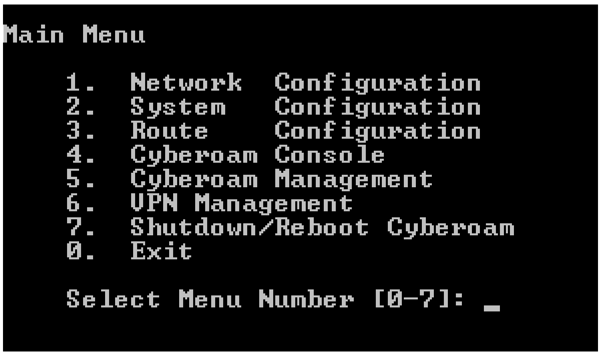
Screen - Console login screen

Accessing CLI Console using SSH client

Access Cyberoam CLI console using any of the SSH client. Cyberoam IP Address is required.

Start SSH client and create new Connection with the following parameters:
Hostname - <Cyberoam IP Address>
Username – admin
Password – admin

On successful login, following Main menu screen will be shown.



```
Main Menu

    1.  Network  Configuration
    2.  System   Configuration
    3.  Route    Configuration
    4.  Cyberoam Console
    5.  Cyberoam Management
    6.  VPN Management
    7.  Shutdown/Reboot Cyberoam
    0.  Exit

    Select Menu Number [0-7]: _
```

To access any of the menu items, type the number corresponding to the menu item against ‘Select Menu Number’ and press <Enter> key.

Example

To access	Type
System Configuration	2
VPN Management	6
Exit	0 or Ctrl -C

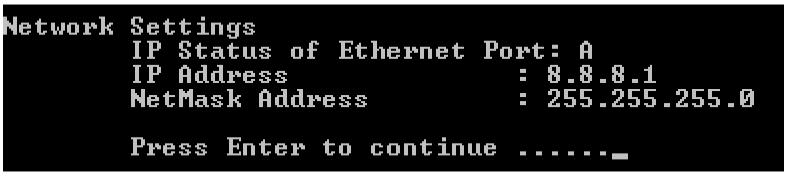
Network configuration

Use this menu to

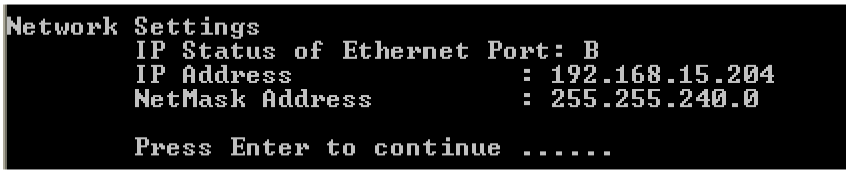
- View & change network setting
- Set IP address
- Set Alias (only when Cyberoam is deployed in transparent mode)
- Add VLAN ID (only when Cyberoam is deployed in transparent mode)

For Gateway mode

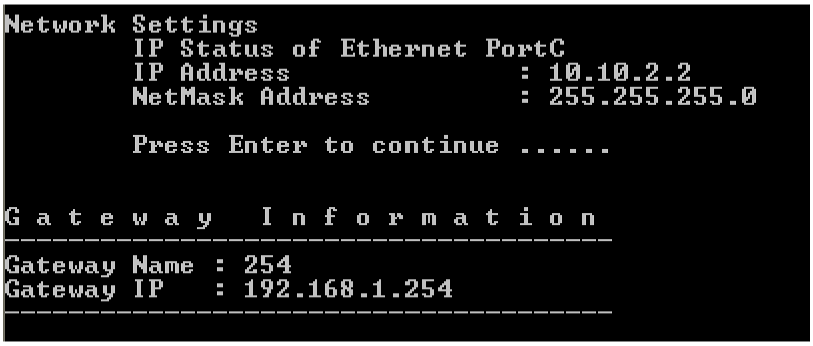
Following screen displays the current Network setting like IP address & Netmask for all the Ports. In addition, it also displays IP address and Netmask of Aliases if configured.



```
Network Settings
        IP Status of Ethernet Port: A
        IP Address                : 8.8.8.1
        NetMask Address           : 255.255.255.0

        Press Enter to continue ......
```



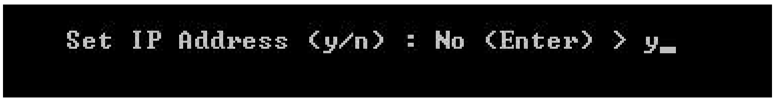
```
Network Settings
        IP Status of Ethernet Port: B
        IP Address                : 192.168.15.204
        NetMask Address           : 255.255.240.0

        Press Enter to continue ......
```



```
Network Settings
        IP Status of Ethernet PortC
        IP Address                : 10.10.2.2
        NetMask Address           : 255.255.255.0

        Press Enter to continue ......


G a t e w a y   I n f o r m a t i o n
--------------------------------------
Gateway Name : 254
Gateway IP   : 192.168.1.254
--------------------------------------
```

Set IP Address

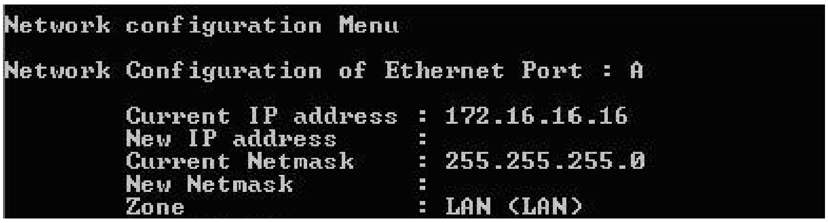
Following screen allows setting or modifying the IP address for any port. Type ‘y’ and press <Enter> to set IP address



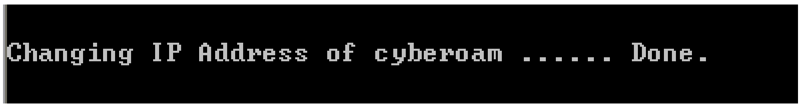
```
    Set IP Address (y/n) : No (Enter) > y
```

Displays the IP address, Netmask and Zone and prompts for the new IP address and Netmask for each Port.

Press <Enter> if you do not want to change any details.



```
Network configuration Menu

Network Configuration of Ethernet Port : A

        Current IP address  : 172.16.16.16
        New IP address      :
        Current Netmask     : 255.255.255.0
        New Netmask         :
        Zone                : LAN (LAN)
```



```
Changing IP Address of cyberoam ...... Done.
```

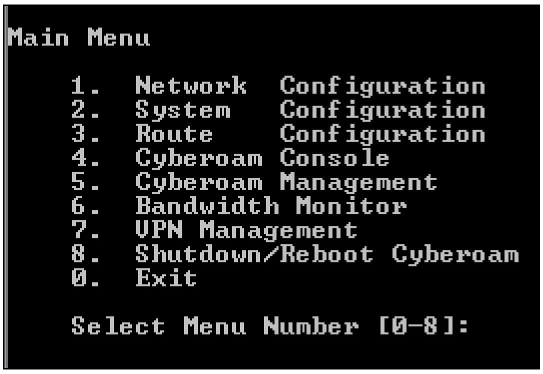
Note

One can assign or bind more than one IP address to the same Ethernet or the Network card. These are Aliases. It is possible to define Aliases for both Internal as well as External network. Maximum eight IP addresses (Aliases) can be bound to a single Network card.

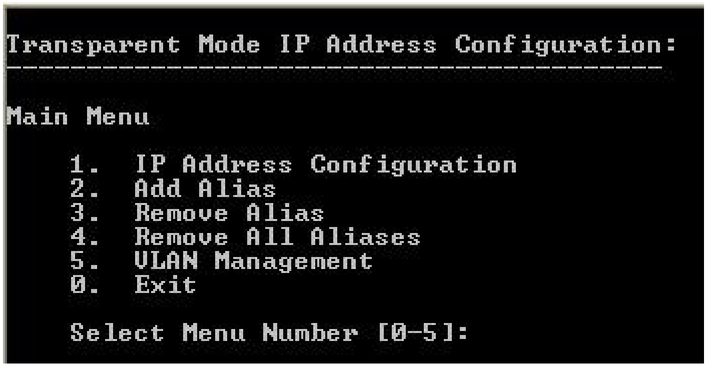
Press <Enter> to return to the Main menu.

For Transparent (bridge) mode

Use the menu to set or change the IP address, add and remove alias, add and remove VLAN ID



```
Main Menu

    1.   Network  Configuration
    2.   System   Configuration
    3.   Route    Configuration
    4.   Cyberoam Console
    5.   Cyberoam Management
    6.   Bandwidth Monitor
    7.   VPN Management
    8.   Shutdown/Reboot Cyberoam
    0.   Exit

    Select Menu Number [0-8]:
```



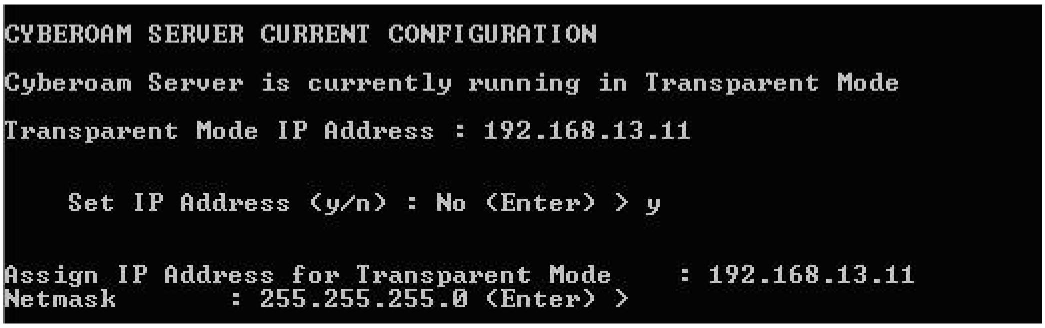
```
Transparent Mode IP Address Configuration:
-------------------------------------------

Main Menu

    1.   IP Address Configuration
    2.   Add Alias
    3.   Remove Alias
    4.   Remove All Aliases
    5.   VLAN Management
    0.   Exit

    Select Menu Number [0-5]:
```

1.1 IP address configuration

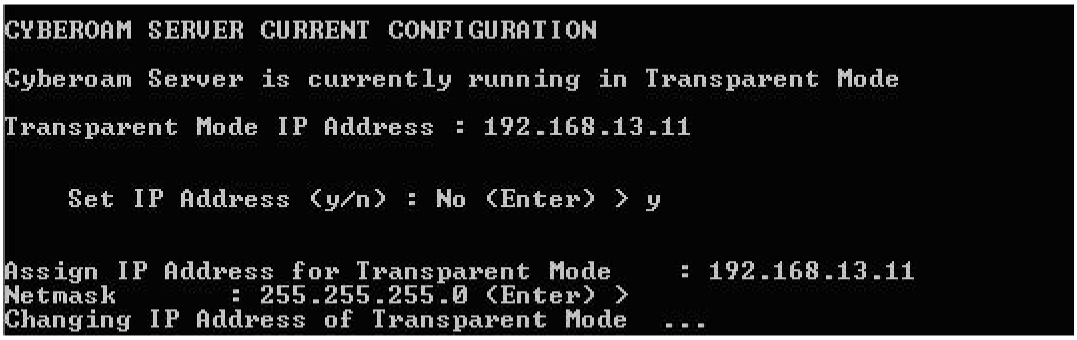
Screen displays the current IP address.

Type ‘y’ and press <Enter> to set IP address. It prompts for the new IP address and Net mask.

Specify IP address and press <Enter> if you do not want to change netmask. Cyberoam will take some time to restart as it automatically restarts management services once you change the IP address.



```
CYBEROAM SERVER CURRENT CONFIGURATION

Cyberoam Server is currently running in Transparent Mode

Transparent Mode IP Address : 192.168.13.11


    Set IP Address (y/n) : No (Enter) > y


Assign IP Address for Transparent Mode    : 192.168.13.11
Netmask       : 255.255.255.0 (Enter) >
```

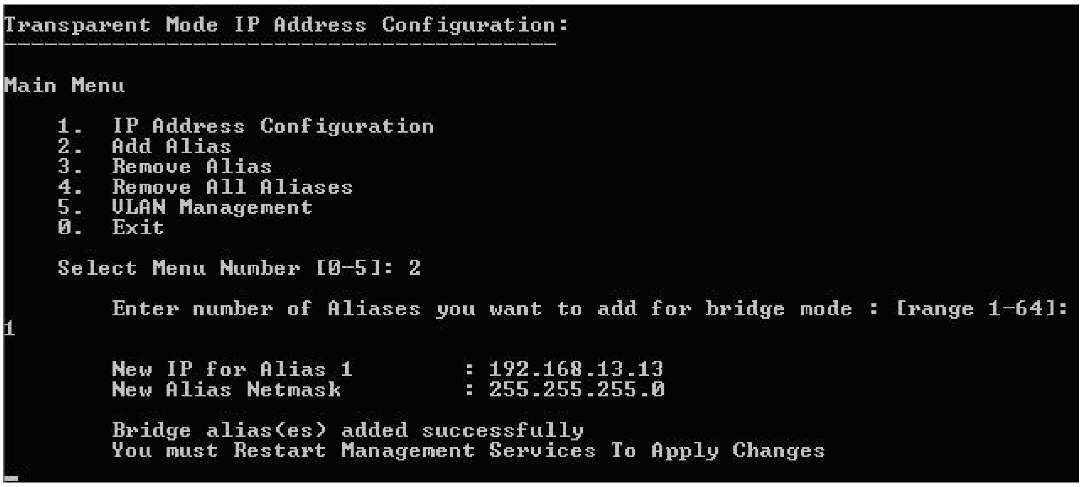


```
CYBEROAM SERVER CURRENT CONFIGURATION

Cyberoam Server is currently running in Transparent Mode

Transparent Mode IP Address : 192.168.13.11


    Set IP Address (y/n) : No (Enter) > y


Assign IP Address for Transparent Mode    : 192.168.13.11
Netmask       : 255.255.255.0 (Enter) >
Changing IP Address of Transparent Mode  ...
```

1.2 Add Alias

Use to add interface alias.

Specify number of aliases to be added. Specify IP address and netmask for Alias. You will be prompted to restart management services (RMS) after alias is added successfully. Unless you do RMS, you will not be able to use Alias.

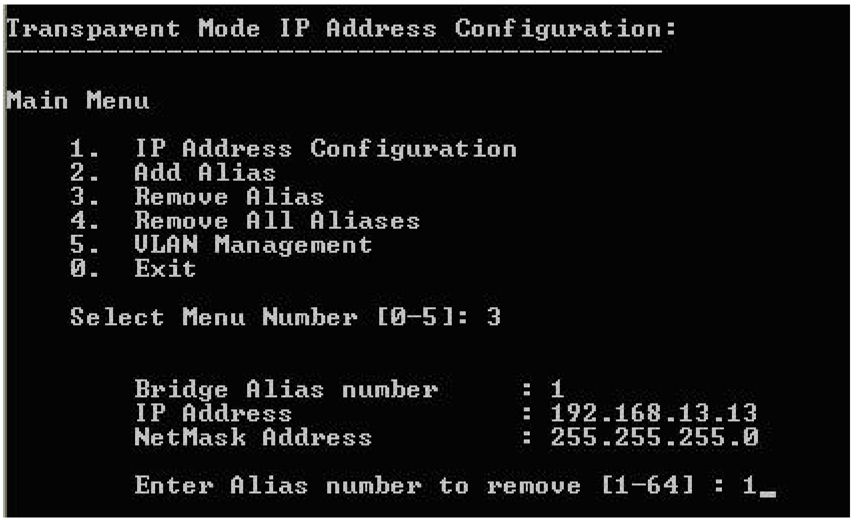


```
Transparent Mode IP Address Configuration:
-----------------------------------------

Main Menu

    1.  IP Address Configuration
    2.  Add Alias
    3.  Remove Alias
    4.  Remove All Aliases
    5.  VLAN Management
    0.  Exit

    Select Menu Number [0-5]: 2

        Enter number of Aliases you want to add for bridge mode : [range 1-64]:
1

        New IP for Alias 1          : 192.168.13.13
        New Alias Netmask           : 255.255.255.0

        Bridge alias(es) added successfully
        You must Restart Management Services To Apply Changes
_
```

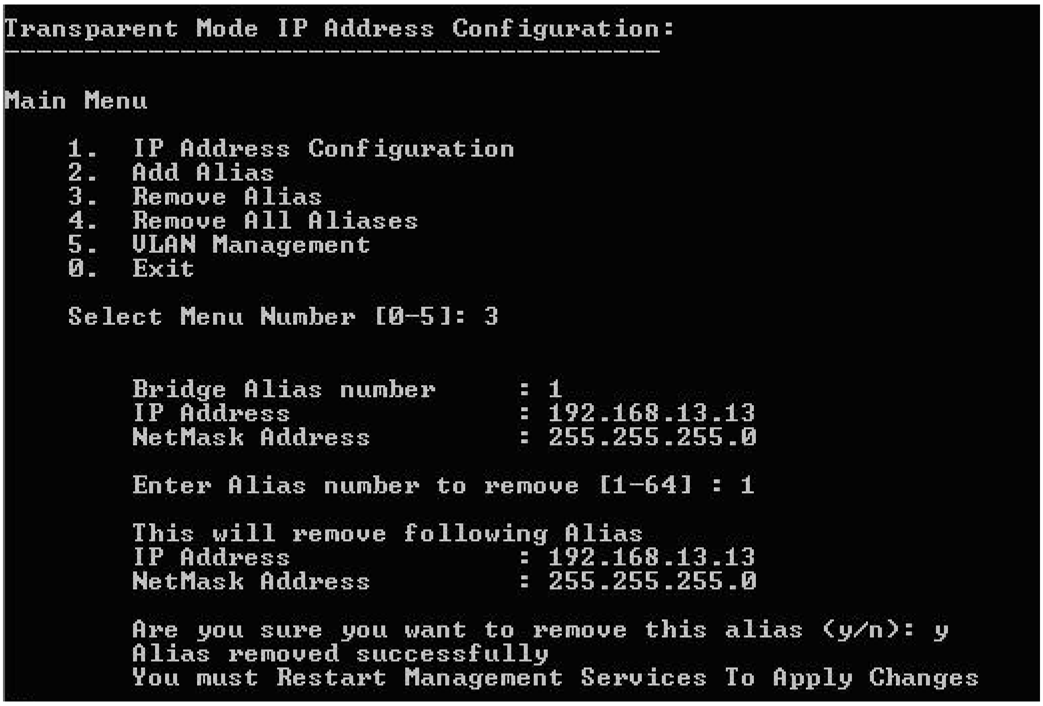
1.3 Remove Alias

Use to remove interface aliases.

All the configured aliases are displayed. Specify Alias number to be removed and follow the screen steps. You will be prompted to restart management services (RMS) after alias is removed successfully.



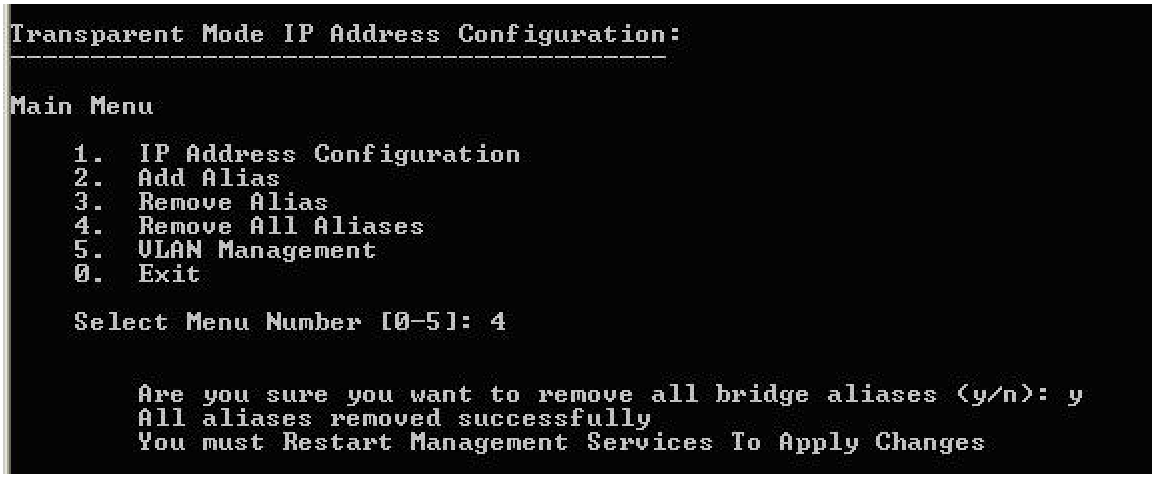
```
Transparent Mode IP Address Configuration:
-----------------------------------------

Main Menu

    1.  IP Address Configuration
    2.  Add Alias
    3.  Remove Alias
    4.  Remove All Aliases
    5.  VLAN Management
    0.  Exit

    Select Menu Number [0-5]: 3


        Bridge Alias number     : 1
        IP Address              : 192.168.13.13
        NetMask Address         : 255.255.255.0

        Enter Alias number to remove [1-64] : 1_
```



```
Transparent Mode IP Address Configuration:
-----------------------------------------

Main Menu

    1.  IP Address Configuration
    2.  Add Alias
    3.  Remove Alias
    4.  Remove All Aliases
    5.  VLAN Management
    0.  Exit

    Select Menu Number [0-5]: 3


        Bridge Alias number     : 1
        IP Address              : 192.168.13.13
        NetMask Address         : 255.255.255.0

        Enter Alias number to remove [1-64] : 1

        This will remove following Alias
        IP Address              : 192.168.13.13
        NetMask Address         : 255.255.255.0

        Are you sure you want to remove this alias (y/n): y
        Alias removed successfully
        You must Restart Management Services To Apply Changes
```

1.4 Remove All Alias

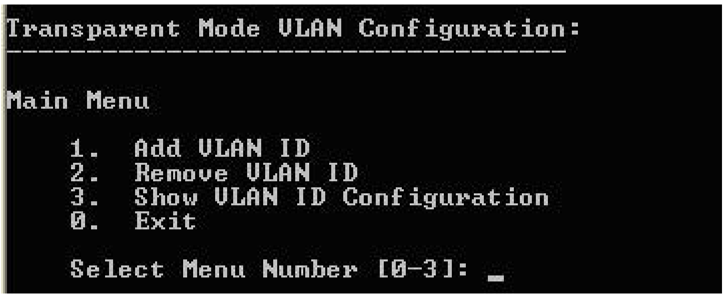
Use to remove all the configured aliases in one step. You will be prompted to restart management services (RMS) after aliases are removed successfully.



```
Transparent Mode IP Address Configuration:
------------------------------------------

Main Menu

    1.  IP Address Configuration
    2.  Add Alias
    3.  Remove Alias
    4.  Remove All Aliases
    5.  VLAN Management
    0.  Exit

    Select Menu Number [0-5]: 4


        Are you sure you want to remove all bridge aliases (y/n): y
        All aliases removed successfully
        You must Restart Management Services To Apply Changes
```

1.5 VLAN Management

Use to add, remove or view VLAN IDs.

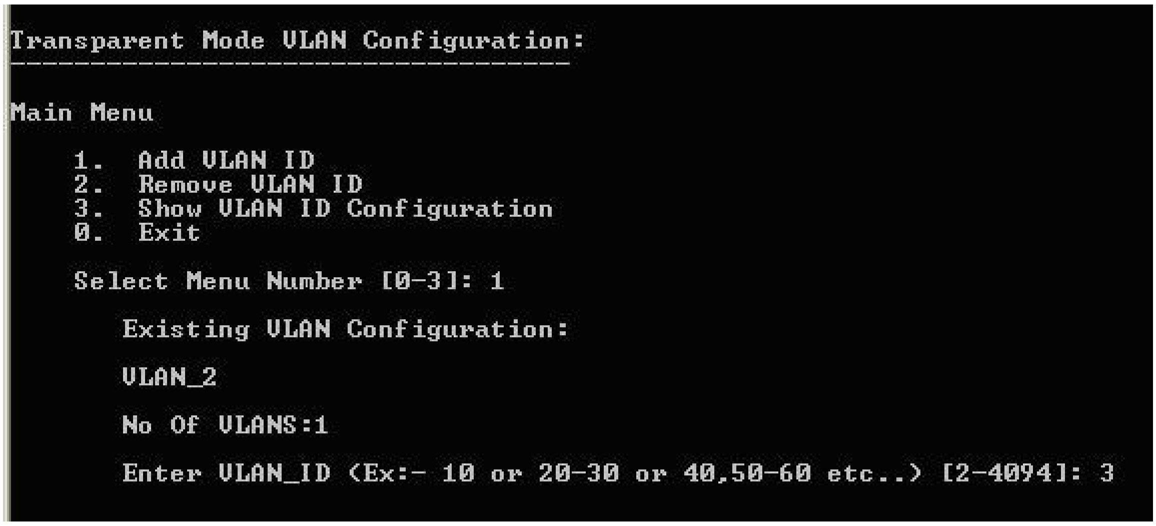


```
Transparent Mode VLAN Configuration:
-----------------------------------

Main Menu

    1.  Add VLAN ID
    2.  Remove VLAN ID
    3.  Show VLAN ID Configuration
    0.  Exit

    Select Menu Number [0-3]: _
```

1.5.1 Add VLAN ID

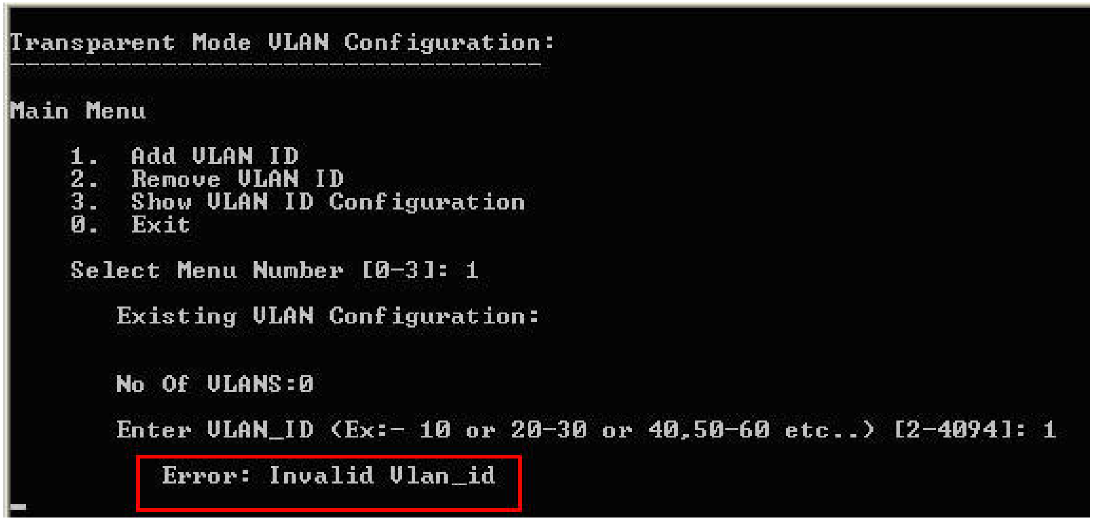
Screen displays list of VLAN IDs if configured for bridge interface and prompts to specify new VLAN ID.

VLAN ID can be any number between 2 and 4094.



```
Transparent Mode VLAN Configuration:
-----------------------------------

Main Menu

    1.  Add VLAN ID
    2.  Remove VLAN ID
    3.  Show VLAN ID Configuration
    0.  Exit

    Select Menu Number [0-3]: 1

       Existing VLAN Configuration:

       VLAN_2

       No Of VLANS:1

       Enter VLAN_ID (Ex:- 10 or 20-30 or 40,50-60 etc..) [2-4094]: 3
```

Error “Invalid VLAN_id” is displayed if VLAN ID is not between 2 and 4094

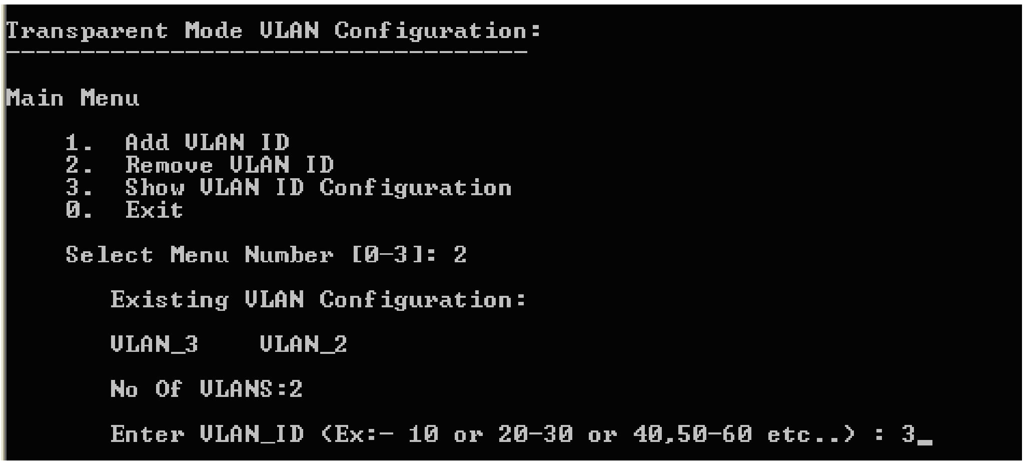


```
Transparent Mode VLAN Configuration:
------------------------------------

Main Menu

    1.  Add VLAN ID
    2.  Remove VLAN ID
    3.  Show VLAN ID Configuration
    0.  Exit

    Select Menu Number [0-3]: 1

       Existing VLAN Configuration:


       No Of VLANS:0

       Enter VLAN_ID (Ex:- 10 or 20-30 or 40,50-60 etc..) [2-4094]: 1

          Error: Invalid Vlan_id
_
```

1.5.2 Remove VLAN ID

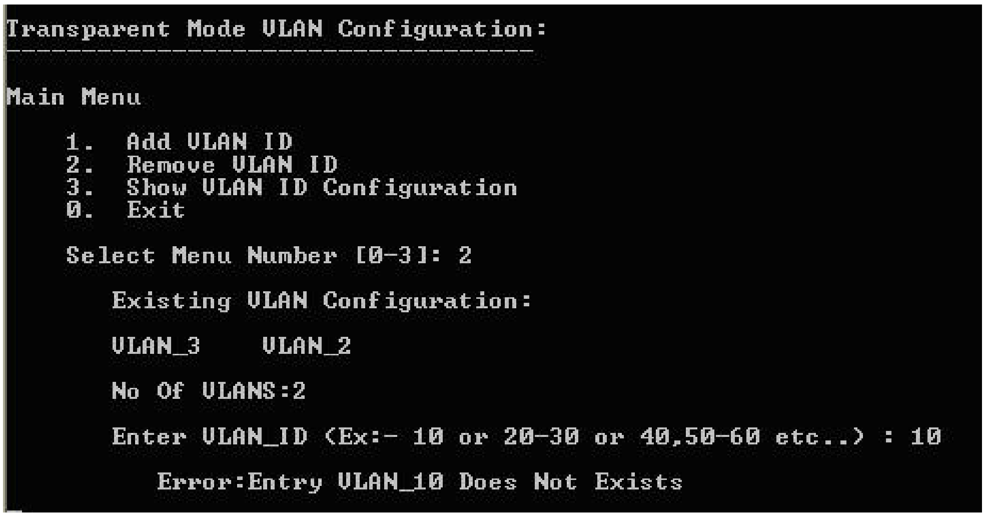
Use to remove configured VLAN IDs.

Screen displays list of all the configured VLAN IDs for the bridge interface and prompts to specify VLAN ID to be removed.



```
Transparent Mode VLAN Configuration:
------------------------------------

Main Menu

    1.  Add VLAN ID
    2.  Remove VLAN ID
    3.  Show VLAN ID Configuration
    0.  Exit

    Select Menu Number [0-3]: 2

       Existing VLAN Configuration:

       VLAN_3    VLAN_2

       No Of VLANS:2

       Enter VLAN_ID (Ex:- 10 or 20-30 or 40,50-60 etc..) : 3_
```

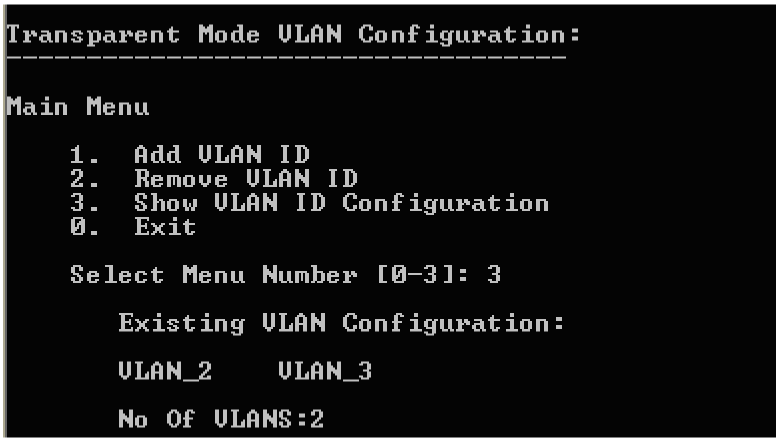
Error “Entry VLAN_xx Does Not Exists” if one specifies VLAN ID which is not added.



```
Transparent Mode VLAN Configuration:
------------------------------------

Main Menu

    1.  Add VLAN ID
    2.  Remove VLAN ID
    3.  Show VLAN ID Configuration
    0.  Exit

    Select Menu Number [0-3]: 2

       Existing VLAN Configuration:

       VLAN_3    VLAN_2

       No Of VLANS:2

       Enter VLAN_ID (Ex:- 10 or 20-30 or 40,50-60 etc..) : 10

          Error:Entry VLAN_10 Does Not Exists
_
```

1.5.3 Show VLAN ID Configuration

Use to view list of VLAN IDs added for the bridge interface.



```
Transparent Mode VLAN Configuration:
-----------------------------------

Main Menu

    1.  Add VLAN ID
    2.  Remove VLAN ID
    3.  Show VLAN ID Configuration
    0.  Exit

    Select Menu Number [0-3]: 3

       Existing VLAN Configuration:

       VLAN_2    VLAN_3

       No Of VLANS:2
```

1.5.0 Exit

Type ‘0’ to exit from VLAN configuration menu

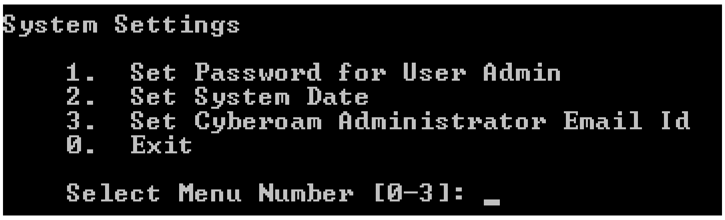
1.0 Exit

Type ‘0’ to exit from Transparent mode IP configuration menu

System Settings

Use this menu to

- View & change various system properties

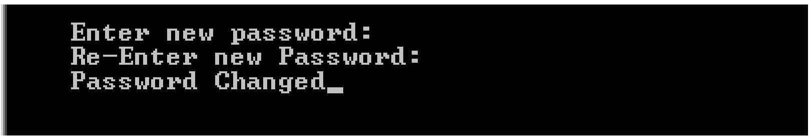


```
System Settings

    1.  Set Password for User Admin
    2.  Set System Date
    3.  Set Cyberoam Administrator Email Id
    0.  Exit

    Select Menu Number [0-3]: _
```

2.1 Set Password for User Admin

Use to change the password of the user “admin”

Type new password, retype for confirmation, and press <Enter>



```
    Enter new password:
    Re-Enter new Password:
    Password Changed_
```

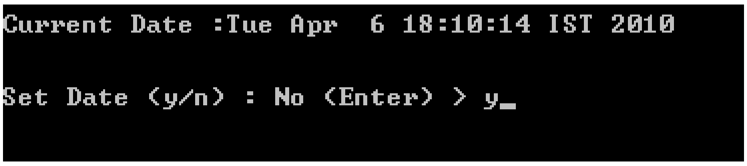
Displays successful completion message.

Press <Enter> to return to the System Setting Menu.

2.2 Set System Date

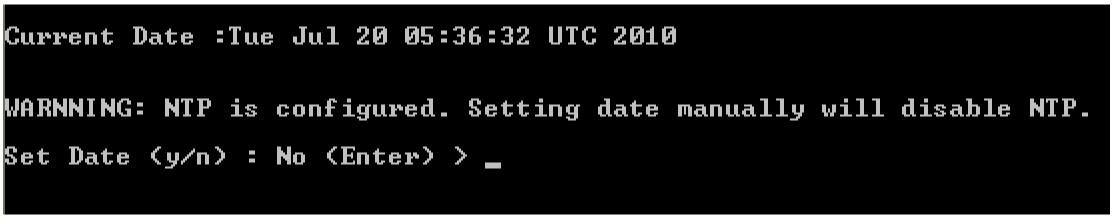
Use to change time zone and system date

Type ‘y’ to set new time and press <Enter>



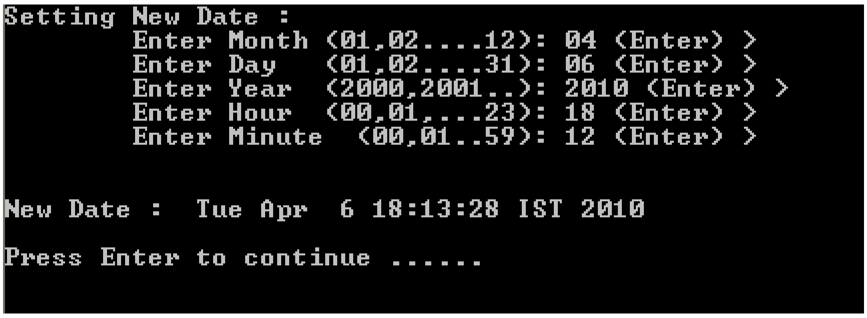
```
Current Date :Tue Apr  6 18:10:14 IST 2010

Set Date (y/n) : No (Enter) > y_
```

If NTP server is configured for synchronizing date and time, screen with the warning message as given below will be displayed. If you set date manually, NTP server will be disabled automatically.



```
Current Date :Tue Jul 20 05:36:32 UTC 2010

WARNNING: NTP is configured. Setting date manually will disable NTP.
Set Date (y/n) : No (Enter) > _
```

Type Month, Day, Year, Hour, Minutes



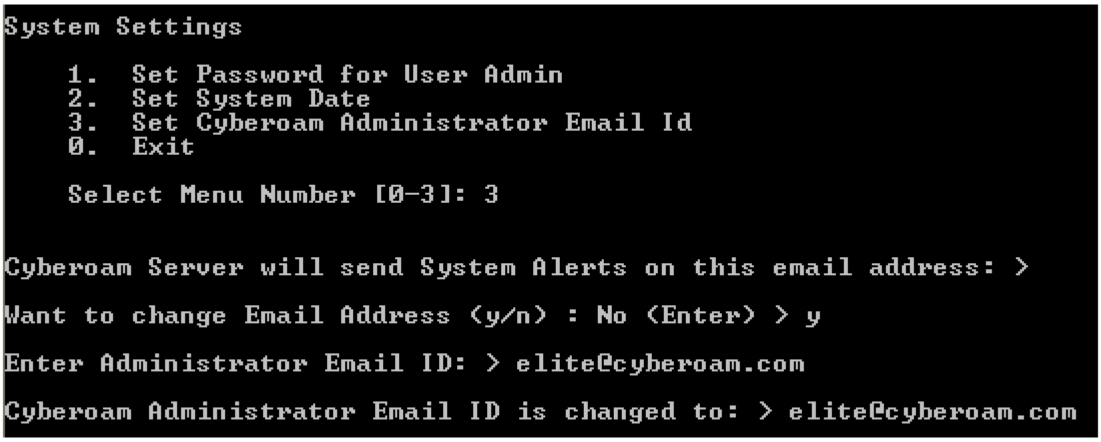
```
Setting New Date :
        Enter Month (01,02....12): 04 (Enter) >
        Enter Day   (01,02....31): 06 (Enter) >
        Enter Year  (2000,2001..): 2010 (Enter) >
        Enter Hour  (00,01,...23): 18 (Enter) >
        Enter Minute  (00,01..59): 12 (Enter) >


New Date :  Tue Apr  6 18:13:28 IST 2010

Press Enter to continue ......
```

Press <Enter> to return to the System Menu

2.3 Set Cyberoam Administrator Email ID

Use to change the Email ID of Administrator “cyber”. Cyberoam sends system alert mails on the specified Email ID.

Type Email ID and press <Enter>. It displays the new Email ID.



```
System Settings

    1.  Set Password for User Admin
    2.  Set System Date
    3.  Set Cyberoam Administrator Email Id
    0.  Exit

    Select Menu Number [0-3]: 3

Cyberoam Server will send System Alerts on this email address: >

Want to change Email Address (y/n) : No (Enter) > y

Enter Administrator Email ID: > elite@cyberoam.com

Cyberoam Administrator Email ID is changed to: > elite@cyberoam.com
```

Press <Enter> to return to the System Setting Menu

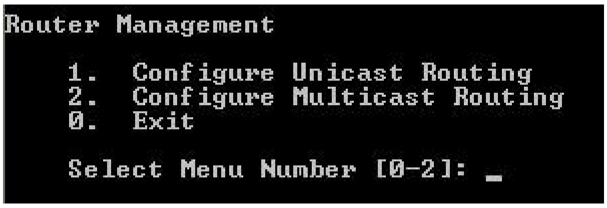
2.0 Exit

Type ‘0’ to exit from System Setting menu and return to the Main Menu.

Route Configuration

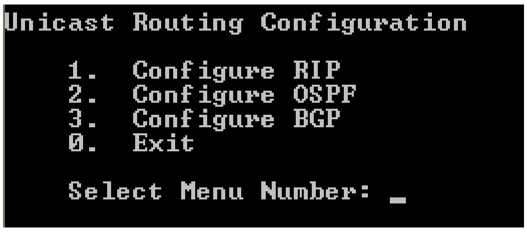
Use this menu to configure static routes, RIP, OSPF and enable or disable multicast forwarding. Cyberoam adheres to Cisco terminology for routing configuration and provides Cisco-compliant CLI to configure static routes and dynamic routing protocols.

Traditionally, IP packets are transmitted in one of either two ways – Unicast (1 sender – 1 receiver) or Broadcast (1 sender – everybody on the network). Multicast delivers IP packets simultaneously to a group of hosts on the network and not everybody and not just 1.



```
Router Management

    1.  Configure Unicast Routing
    2.  Configure Multicast Routing
    0.  Exit

    Select Menu Number [0-2]: _
```

3.1 Configure Unicast Routing



```
Unicast Routing Configuration

    1.  Configure RIP
    2.  Configure OSPF
    3.  Configure BGP
    0.  Exit

    Select Menu Number: _
```

Options Configure RIP, Configure OSPF and Configure BGP are not available when Cyberoam is deployed in transparent mode.

3.1.1 Configure RIP

This option is available only when Cyberoam is deployed in Gateway mode.

Routing Information Protocol (RIP) is a distance-vector routing protocol documented in RFC 1058. RIP uses broadcast User Datagram Protocol (UDP) data packets to exchange routing information.

The Cyberoam implementation of RIP supports

- RIP version 1 (as described in RFC 1058)
- RIP version 2 (as described in RFC 2453)
- Plain text and Message Digest 5 (MD5) authentication for RIP Version 2

RIP configuration Task List

Prerequisite
Interface IP addresses configured from Network Configuration Wizard

RIP must be enabled before carrying out any of the RIP commands. To configure RIP, use the following commands from CLI Console:

1. Go to Option 3 (Route Configuration)
2. Go to Option 1 (Configure Unicast Routing)
3. Go to Option 1(Configure RIP)
4. To configure RIP, perform the tasks described in the following table.

Steps	Command	Purpose
Enable RIP	rip> enable	Enables a RIP routing process and places you in Global Configuration mode.
Specify a list of networks for the Routing Information Protocol (RIP) routing process	rip# configure terminal	Enables the RIP configuration mode which places you in the Router Configuration mode and allows you to configure from the terminal.
	rip(config)# router rip	Allows to configure and start RIP routing process
	rip(config-router)# network *ip-address* Specify ip-address with the subnet information For example, if the network for 10.0.0.0/24 is RIP enabled, this would result in all the addresses from 10.0.0.0 to 10.0.0.255 being enabled for RIP.	Enables RIP interfaces between specified network address. RIP routing updates will be sent and received only through interfaces on this network. Also, if the network of an interface is not specified, the interface will not be advertised in any RIP update. The interfaces which have addresses matching with network are enabled.
	rip(config-router)#end	Exits from the Router Configuration mode and places you into the Enable mode.
Configure Authentication	rip# configure terminal	Enables the RIP configuration mode which places you in the Router Configuration mode and allows you to configure from the terminal.
	To set authentication mode as text and set the authentication string rip(config)# interface *ifname* rip(config-if)# ip rip authentication mode {text [*string*]} For example, rip(config)# interface *A* rip(config-if)# ip rip authentication mode text rip(config-if)# ip rip authentication string *teststring* To set authentication mode as MD5 and set the authentication string rip(config)# interface *ifname* rip(config-if)# ip rip authentication	Defines authentication mode for the each interface. By, default, authentication is on for all the interfaces. If authentication is not required for any of the interface, it is to be explicitly disabled. RIP Version 1 does not support authentication. RIP Version 2 supports Clear Text (simple password) or Keyed Message Digest 5 (MD5) authentication. To enable authentication for RIP Version 2 packets and to specify the

	mode {md5 [key-chain *name of key chain*]} For example, rip(config)# interface *A* rip(config-if)# ip rip authentication mode md5 key-chain *testkeychain* To disable authentication rip(config)# interface *ifname* rip(config-if)# no ip rip authentication mode For example, disable authentication for interface A rip(config)# interface *A* rip(config-if)# no ip rip authentication mode	set of keys that can be used on an interface, use the ip rip authentication key-chain command in interface configuration mode. If authentication is not required for any of the interface, use the no form of this command.
	rip(config-if)# end	Exits from the Router Configuration mode and places you into the Enable mode.
Exit to Router Management Menu	rip(config-if)# exit	Exits to the Router Management Menu

Removing routes

To remove route configuration, execute the 'no network' command from the command prompt as below:

```
rip(config-router)# no network <ip address>
```

Disabling RIP

To disable RIP routing configuration, execute the 'no router' command from the command prompt as below:

```
rip(config)# no router rip
```

Execute 'exit' command to return to the previous mode.

3.1.3 Configure OSPF

This option is available only when Cyberoam is deployed in Gateway mode.

OSPF is one of IGPs (Interior Gateway Protocols). Compared with RIP, OSPF can serve much more networks and period of convergence is very short. OSPF is widely used in large networks such as ISP backbone and enterprise networks.

The Cyberoam implementation of OSPF supports:

- OSPF version 2 (as described in RFC 2328)
- Plain text and Message Digest 5 (MD5) authentication

How OSPF works

OSPF keeps track of a complete topological database of all connections in the local network. It is typically divided into logical areas linked by area border routers. An area comprises a group of contiguous networks. An area border router links one or more areas to the OSPF network backbone.

Cyberoam participates in OSPF communications, when it has an interface to an OSPF area. Cyberoam uses the OSPF Hello protocol to acquire neighbors in an area. A neighbor is any router that has an interface to the same area as the Cyberoam. After initial contact, the Cyberoam exchanges Hello packets with its OSPF neighbors at regular intervals to confirm that the neighbors can be reached.

OSPF-enabled routers generate link-state advertisements and send them to their neighbors whenever the status of a neighbor changes or a new neighbor comes online. If OSPF network is stable, link-state advertisements between OSPF neighbors does not occur. A Link-State Advertisement (LSA) identifies the interfaces of all OSPF-enabled routers in an area, and provides information that enables OSPF-enabled routers to select the shortest path to a destination. All LSA exchanges between OSPF-enabled routers are authenticated. The Cyberoam maintains a database of link-state information based on the advertisements that it receives from OSPF-enabled routers. To calculate the shortest path to a destination, the Cyberoam applies the Shortest Path First (SPF) algorithm to the accumulated link-state information.

The Cyberoam updates its routing table dynamically based on the results of the SPF calculation to ensure that an OSPF packet will be routed using the shortest path to its destination.

OSFP configuration Task List

Prerequisite

Interface IP addresses configured from Network Configuration Wizard

OSPF must be enabled before carrying out any of the OSPF commands. To configure OSPF, use the following commands from CLI Console:

1. Go to Option 3 (Route Configuration)
2. Go to Option 1 (Configure Unicast Routing)
3. Go to Option 2 (Configure OSPF)
4. To configure OSPF, perform the tasks described in the following table:

Steps	Command	Purpose
Enable OSPF	ospf> enable	Enables OSPF routing process and places you in the Global Configuration mode.
Specify a list of networks for the Routing Information Protocol (OSPF) routing process	ospf# configure terminal	Enables the OSPF configuration mode which places you in the Router Configuration mode and allows you to configure from the terminal.
	ospf(config)# router ospf	Allows to configure and start OSPF routing process
	ospf(config-router)# network *ip-address* area *area-id* Specify ip-address with the subnet information	Assigns an interface to a area. The area-id is the area number we want the interface to be in. The area-id can be an integer between 0 and 4294967295 or can take a form similar to an IP address A.B.C.D.

		Interfaces that are part of the network are advertised in OSPF link-state advertisements.
	ospf(config-router)# show running-config	View configuration
	ospf(config-router)#end	Exits from the Router Configuration mode and places you into the Enable mode.
Exit to Router Management Menu	ospf(config-if)# exit	Exits to the Router Management Menu

Removing routes

To remove route configuration, execute the 'no network' command from the command prompt as below:

```
ospf(config-router)# no network <ip address> area <area-id>
```

Disabling OSPF

To disable OSPF routing configuration, execute the 'no router' command from the command prompt as below:

```
ospf(config)# no router ospf
```

3.1.3 Configure Border Gateway Protocol (BGP)

This option is available only when Cyberoam is deployed in Gateway mode.

BGP is a path vector protocol that is used to carry routing between routers that are in the different administrative domains (Autonomous Systems) e.g. BGP is typically used by ISPs to exchange routing information between different ISP networks.

The Cyberoam implementation of OSPF supports:

- Version 4 (RFC 1771)
- Communities Attribute (RFC 1997)
- Route Reflection (RFC 2796)
- Multiprotocol extensions (RFC 2858)
- Capabilities Advertisement (RFC 2842)

Additionally, a firewall rule is to be configured for the zone for which the BGP traffic is to be allowed i.e. LAN to LOCAL or WAN to LOCAL.

How BGP works

When BGP is enabled, the Cyberoam advertises routing table updates to neighboring autonomous systems whenever any part of the Cyberoam routing table changes. Each AS, including the local AS of which the Cyberoam unit is a member, is associated with an AS number. The AS number references a particular destination network.

BGP updates advertise the best path to a destination network. When the Cyberoam unit receives a BGP update, the Cyberoam examines potential routes to determine the best path to a destination network before recording the path in the Cyberoam routing table.

BGP configuration Task List

Prerequisite

Interface IP addresses configured from Network Configuration Wizard

BGP must be enabled before carrying out any of the BGP commands. To configure BGP, use the following commands from CLI Console:

1. Go to Option 3 (Route Configuration)
2. Go to Option 1 (Configure Unicast Routing)
3. Go to Option 3 (Configure BGP)
4. To configure BGP, perform the tasks described in the following table.

Steps	Command	Purpose
Enable BGP	bgp> enable	Enables BGP routing process and places you in the Global Configuration mode.
Specify a list of networks for the Routing Information	bgp# configure terminal	Enables the BGP configuration mode which places you in the Router Configuration mode and allows you to configure from the

Protocol (BGP) routing process		terminal.
	bgp(config)# router bgp *AS number*	Allows to configure and start BGP routing process AS number the number of the local AS that the Cyberoam unit is a member of.
	bgp(config-router)# network *ip-address* Specify ip-address with the subnet information of the network to be advertised	The IP addresses and network masks of networks to advertise to BGP peers. The Cyberoam may have a physical or VLAN interface connected to those networks.
	bgp(config-router)# show running-config	View configuration By default, router ID is Cyberoam IP address. Router ID is used to identify the Cyberoam to other BGP routers. You can change the router ID using the following command: bgp(config-router)#bgp router-id *IP address* The router-id can be an integer or can take a form similar to an IP address A.B.C.D
	bgp(config-router)#end	Exits from the Router Configuration mode.
Exit to Router Management Menu	bgp# exit	Exits to the Router Management Menu

Removing routes

To remove route configuration, execute the 'no network' command from the command prompt as below:

```
bgp(config-router)# no network <ip address>
```

Disabling BGP

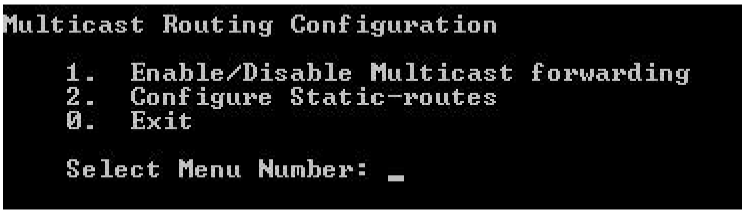
To disable BGP routing configuration, execute the 'no router' command from the command prompt as below:

```
bgp(config)# no router bgp AS number
```

3.1.0 Exit

Type '0' to exit from Unicast Routing configuration menu and return to Router Management.

3.2 Configure Multicast Routing



```
Multicast Routing Configuration

    1.  Enable/Disable Multicast forwarding
    2.  Configure Static-routes
    0.  Exit

    Select Menu Number: _
```

IP Multicast

Internet Protocol (IP) multicast is a bandwidth-conserving technology that reduces traffic by simultaneously delivering a single stream of information to thousands of recipients and homes. IP Multicast delivers source traffic to multiple receivers without adding any additional burden on the source or the receivers.

Applications like videoconferencing, corporate communications, distance learning, and distribution of software, stock quotes, and news use IP multicasting.

If IP multicast is not used, source is required to send more than one copy of a packet or individual copy to each receiver. In such case, high-bandwidth applications like Video or Stock where data is to be send more frequently and simultaneously, uses large portion of the available bandwidth. In these applications, the only efficient way of sending information to more than one receiver simultaneously is by using IP Multicast.

Multicast Group

Multicast is based on the concept of a group. An arbitrary group of receivers expresses an interest in receiving a particular data stream. This group does not have any physical or geographical boundaries—the hosts can be located anywhere on the Internet. Hosts that are interested in receiving data flowing to a particular group must join the group. Hosts must be a member of the group to receive the data stream.

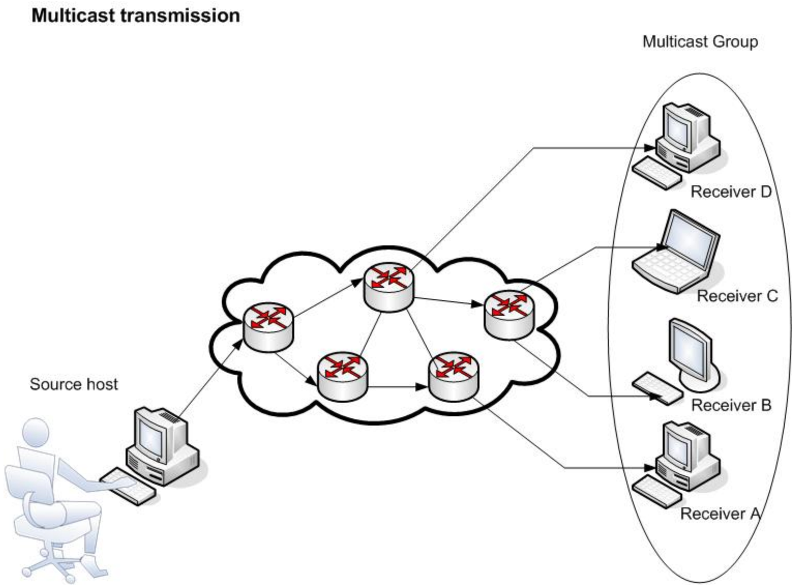
IP Multicast Addresses

Multicast addresses specify an arbitrary group of IP hosts that have joined the group and want to receive traffic sent to this group.

IP Class D Addresses

The Internet Assigned Numbers Authority (IANA) controls the assignment of IP multicast addresses. Multicast addresses fall in Class D address space ranging from 224.0.0.0 to 239.255.255.255.

This address range is only for the group address or destination address of IP multicast traffic. The source address for multicast datagrams is always the unicast source address.



Multicast forwarding

In multicast routing, the source is sending traffic to a group of hosts represented by a multicast group address. The multicast router must determine which direction is upstream (toward the source) and which direction (or directions) is downstream. If there are multiple downstream paths, the router replicates the packet and forwards the traffic down the appropriate downstream paths—which is not necessarily all paths.

3.2.1 Enable/Disable Multicast forwarding

With multicast forwarding, a router forwards multicast traffic to networks where other multicast devices are listening. Multicast forwarding prevents the forwarding of multicast traffic to networks where there are no nodes listening.

For multicast forwarding to work across inter-networks, nodes and routers must be multicast-capable.

A multicast-capable node must be able to:

- Send and receive multicast packets.
- Register the multicast addresses being listened to by the node with local routers, so that multicast packets can be forwarded to the network of the node.

IP multicasting applications that send multicast traffic must construct IP packets with the appropriate IP multicast address as the destination IP address. IP multicasting applications that receive multicast traffic must inform the TCP/IP protocol that they are listening for all traffic to a specified IP multicast address.

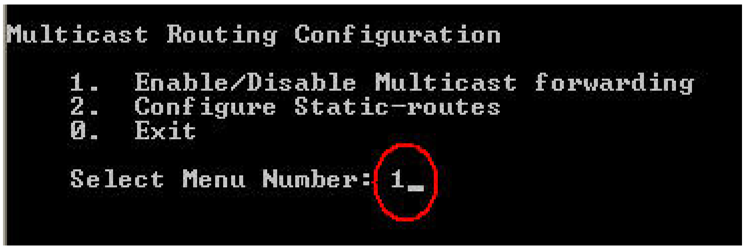
Setting up IP Multicast forwarding

Configuring multicast forwarding is two step process:

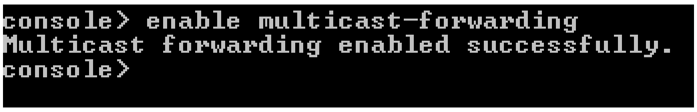
- Enable multicast forwarding (both the modes)
- Configure multicast routes (only in gateway mode)

To enable multicast forwarding, go to Option 3 (Route Configuration)> Option 2 (Configure Multicast Routing), Option 1 (Enable/Disable Multicast forwarding) and execute following command:

```
console>enable multicast-forwarding
```



```
Multicast Routing Configuration

    1.  Enable/Disable Multicast forwarding
    2.  Configure Static-routes
    0.  Exit

    Select Menu Number: 1_
```



```
console> enable multicast-forwarding
Multicast forwarding enabled successfully.
console>
```

3.2.2 Configure Static multicast routes

Go to Option 3 (Route Configuration)> Option 2 (Configure Multicast Routing), Option 2 (Configure Static-routes) and execute following command:

Multicast routes cannot be added before enabling multicast forwarding.

console> mroute add input-interface Port<port number> source-ip <ipaddress> dest-ip <ipaddress> output-interface Port<port number>

where,

input-interface - interface from which the multicast traffic is supposed to arrive (interface that leads to the source of multicast traffic).This is the port through which traffic arrives.

source-ip – unicast IP address of source transmitting multicast traffic

destination-ip – class D IP address (224.0.0.0 to 239.255.255.255)

output-interface – interface on which you want to forward the multicast traffic (interface that leads to destination of multicast traffic) This is the port through which traffic goes.

For example,

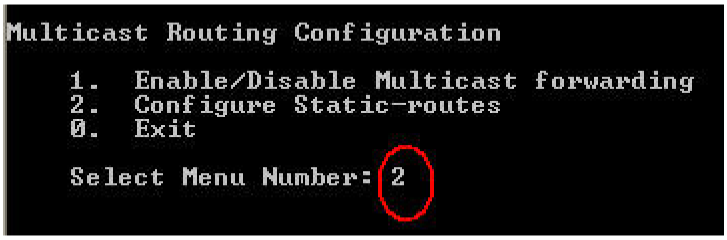
console> mroute add input-interface PortA source-ip 1.1.1.1 dest-ip 230.1.1.2 output-interface PortB

Cyberoam will forward multicast traffic received on interface PortA from IP address 1.1.1.1 to 230.1.1.2 through interface PortB

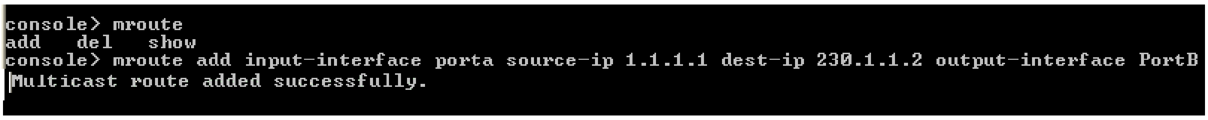
If you want to inject multicast traffic to more than one interface, you have to add routes for each destination interface. For example,

console> mroute add input-interface PortA source-ip 1.1.1.1 dest-ip 230.1.1.2 output-interface PortB

console> mroute add input-interface PortA source-ip 1.1.1.1 dest-ip 230.1.1.2 output-interface PortC



```
Multicast Routing Configuration

    1.  Enable/Disable Multicast forwarding
    2.  Configure Static-routes
    0.  Exit

    Select Menu Number: 2
```

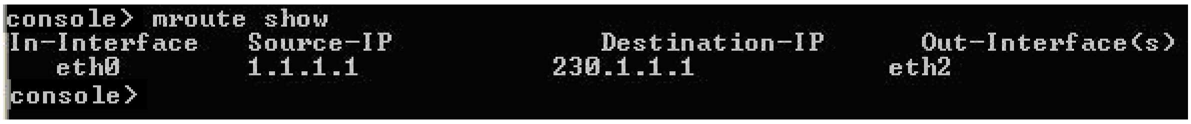


```
console> mroute
add   del   show
console> mroute add input-interface porta source-ip 1.1.1.1 dest-ip 230.1.1.2 output-interface PortB
Multicast route added successfully.
```

Viewing routes

Go to Option 3 (Route Configuration)> Option 2 (Configure Multicast Routing), Option 2 (Configure Static-routes) and execute following command:

console> mroute show

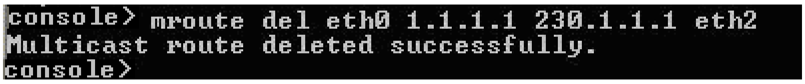


```
console> mroute show
In-Interface   Source-IP           Destination-IP      Out-Interface(s)
   eth0        1.1.1.1           230.1.1.1           eth2
console>
```

Removing route

Go to Option 3 (Route Configuration)> Option 2 (Configure Multicast Routing), Option 2 (Configure Static-routes) and execute following command:

console> mroute del input-interface PortA source-ip 1.1.1.1 dest-ip 230.1.1.2 output-interface PortC



```
console> mroute del eth0 1.1.1.1 230.1.1.1 eth2
Multicast route deleted successfully.
console>
```

Please note

- Source and destination interfaces cannot be same for multicast route
- Multiple destination interfaces cannot be defined. Route manipulation per interface is required to add/delete such routes.
- Non-Ethernet interfaces like - ipsec0, etc. are not supported

3.2.0 Exit

Type ‘0’ to exit from Multicast Routing Configuration menu and return to Router Management.

3.0 Exit

Type ‘0’ to exit from Routing tables menu and return to Main Menu.

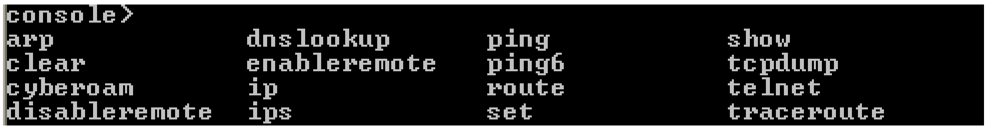
Cyberoam Console

Use to perform various checks and view logs for troubleshooting

Generally, when using command line help, one has to remember parameters/arguments of the command or has to go to the help and check for the parameters. Users using command line for the first time face difficulty in both the situation.

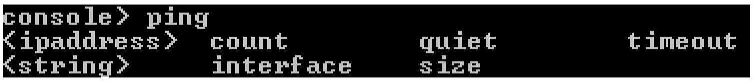
To remove the above difficulty, Cyberoam has inbuilt help at the command prompt itself.

Press ‘Tab’ to view the list of commands supported.



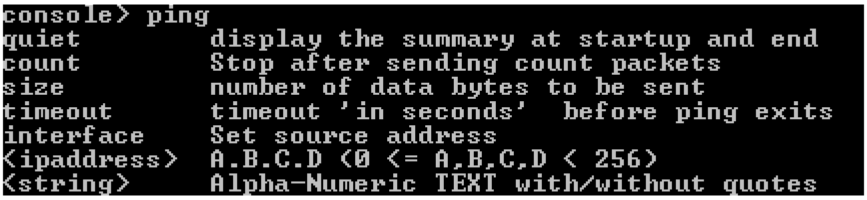
```
console>
arp             dnslookup       ping            show
clear           enableremote    ping6           tcpdump
cyberoam        ip              route           telnet
disableremote   ips             set             traceroute
```

Type command and then press tab to view the list of argument(s) supported or required. For example after typing ping press tab, it shows what all parameters are required or allowed



```
console> ping
<ipaddress>  count        quiet        timeout
<string>     interface    size
```

Type command and then press question mark to view the list of argument(s) supported with its description. For example after typing ping press question mark, it shows what all parameters are required or allowed with description



```
console> ping
quiet         display the summary at startup and end
count         Stop after sending count packets
size          number of data bytes to be sent
timeout       timeout 'in seconds'  before ping exits
interface     Set source address
<ipaddress>   A.B.C.D (0 <= A,B,C,D < 256)
<string>      Alpha-Numeric TEXT with/without quotes
```

Type Exit to return to the Main menu

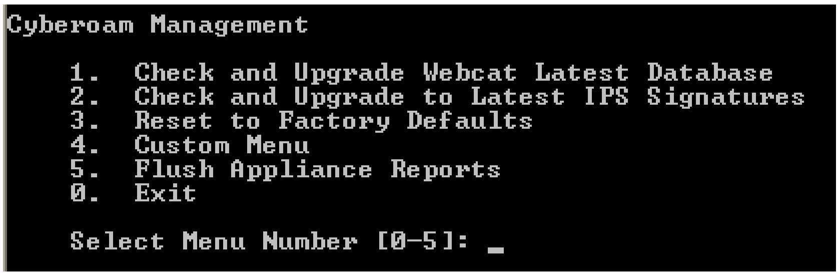
Note

Refer to Annexure A for the detailed help on various commands supported.

Cyberoam Management

Use this menu to

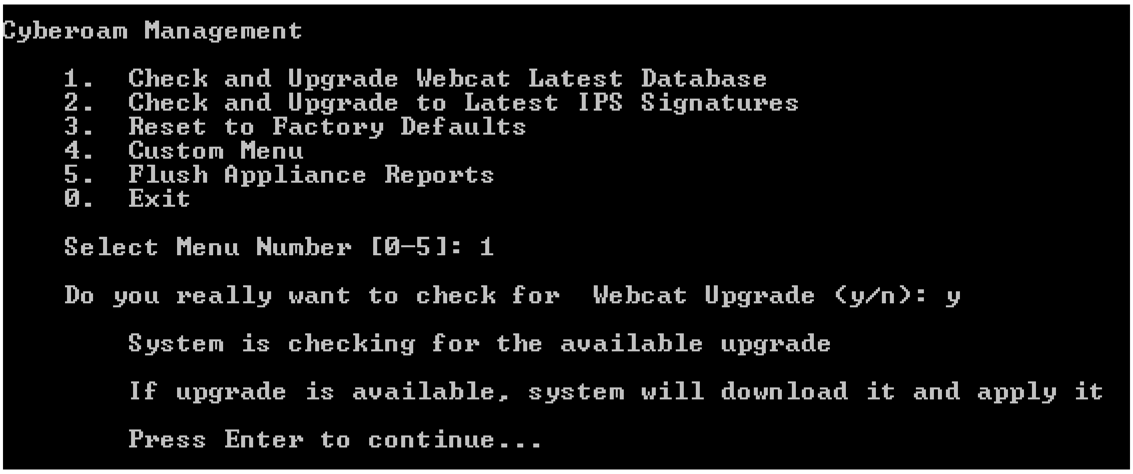
- Reset Web Admin Console password
- Remove Firewall rules
- Manage various Databases
- Reset to factory defaults



```
Cyberoam Management

    1.  Check and Upgrade Webcat Latest Database
    2.  Check and Upgrade to Latest IPS Signatures
    3.  Reset to Factory Defaults
    4.  Custom Menu
    5.  Flush Appliance Reports
    0.  Exit

    Select Menu Number [0-5]: _
```

5.1 Check and Upgrade Webcat Latest Database

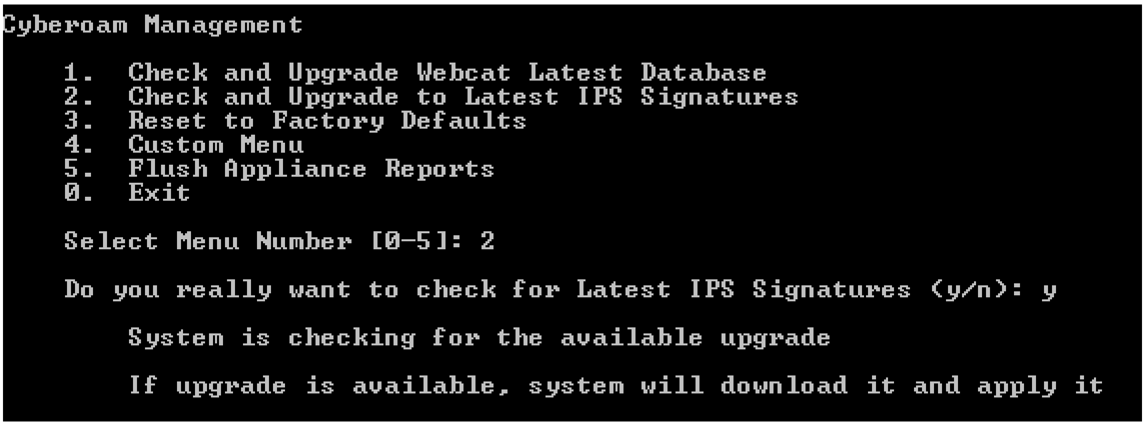
Use to check and upgrade latest webcat database



```
Cyberoam Management

    1.  Check and Upgrade Webcat Latest Database
    2.  Check and Upgrade to Latest IPS Signatures
    3.  Reset to Factory Defaults
    4.  Custom Menu
    5.  Flush Appliance Reports
    0.  Exit

    Select Menu Number [0-5]: 1

    Do you really want to check for  Webcat Upgrade (y/n): y

        System is checking for the available upgrade

        If upgrade is available, system will download it and apply it

        Press Enter to continue...
```

5.2 Check and Upgrade to Latest IPS Database

Use to check and upgrade latest IPS database



```
Cyberoam Management

    1.  Check and Upgrade Webcat Latest Database
    2.  Check and Upgrade to Latest IPS Signatures
    3.  Reset to Factory Defaults
    4.  Custom Menu
    5.  Flush Appliance Reports
    0.  Exit

    Select Menu Number [0-5]: 2

    Do you really want to check for Latest IPS Signatures (y/n): y

        System is checking for the available upgrade

        If upgrade is available, system will download it and apply it
```

5.3 Reset to Factory Defaults

This option resets all the customized configurations to their original state and un-registers Cyberoam. All customization done after the initial deployment will be deleted including network configuration, HTTP proxy cache, passwords, groups, users and policies.

5.5 Flush Appliance Reports

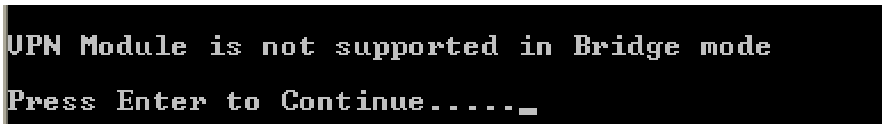
This option will flush all the Cyberoam-iView reports. This will make appliance inaccessible for some time as flushing reports takes time.

5.0 Exit

Type ‘0’ to exit from Cyberoam Management menu and return to Main menu

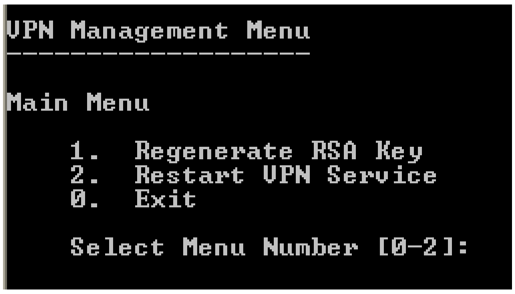
VPN Management

If Cyberoam is deployed in transparent mode, following screen will be displayed:



```
VPN Module is not supported in Bridge mode

Press Enter to Continue....._
```

Below given menu will be displayed only when Cyberoam is deployed in Gateway mode.



```
VPN Management Menu
-------------------

Main Menu

    1.  Regenerate RSA Key
    2.  Restart VPN Service
    0.  Exit

    Select Menu Number [0-2]:
```

7.1 Regenerate RSA Key

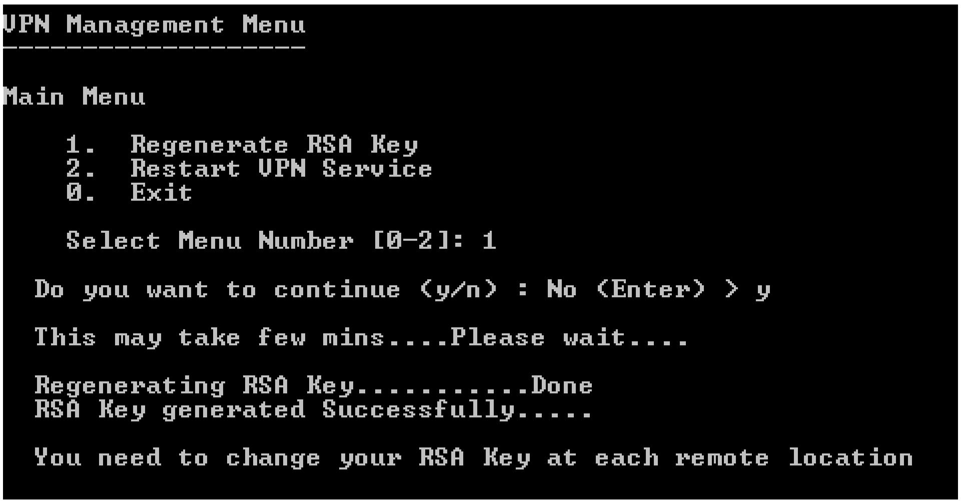
Use to regenerates the local public key used for authenticating users.

Public key authentication uses two keys – public key available to anyone and a private key held by only one individual. The sender encrypts the data with the recipient's public key. Only the recipient can decrypt the data, being the only one who possesses the corresponding private key.

RSA key is used for authenticating user, when authentication type is defined as 'Public key' for Net to Net connection. Connection type and Authentication type are defined from Web based Administration Console.

Public key available to all is termed as Local Public/RSA key while private key known to only one individual is termed as Remote Public key.

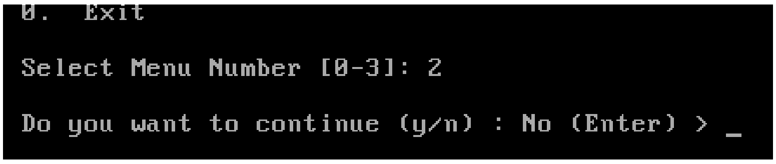
Longer the key life, larger the risk as it becomes easier to intercept the ciphered text, hence it is better to regenerate the RSA key after certain time interval.



```
VPN Management Menu
-------------------

Main Menu

    1.  Regenerate RSA Key
    2.  Restart VPN Service
    0.  Exit

    Select Menu Number [0-2]: 1

  Do you want to continue (y/n) : No (Enter) > y

  This may take few mins....Please wait....

  Regenerating RSA Key...........Done
  RSA Key generated Successfully.....

  You need to change your RSA Key at each remote location
```

7.2 Restart VPN service

Use to restart VPN Service



```
0.  Exit

Select Menu Number [0-3]: 2

Do you want to continue (y/n) : No (Enter) > _
```

7.0 Exit

Type '0' to exit from VPN menu and return to the Main menu

Shutdown/Reboot Cyberoam

Use to shutdown or reboot Cyberoam.

0. Exit

Type ‘0’ to exit from Cyberoam Console Management

Annexure A

clear

Clears the screen

Syntax

clear

cyberoam

Cyberoam Management

Syntax

cyberoam [appliance_access | application_classification | auth | dhcp | diagnostics | ha | ips_autoupgrade | ipsec_route | ipv6 | link_failover | restart | route_precedence | shutdown | system_modules | wwan]

Parameter list & description

Keywords & Variables	Description
appliance_access [disable | enable | show] (**for CR15wi, CR15i, CR25i models only)**)	To override or bypass the configured Appliance Access and allow access to all the Cyberoam services. Disable to reapply Appliance Access. By default, it is disabled. Enable and disable event will be logged in Admin Logs.
application_classification [off | on | show]	If enabled, traffic will be categorized on the basis of application and traffic discovery live connections on Web Admin Console will be displayed based on the application. If disabled, traffic will be categorized on port-based applications and traffic discovery based on applications will not display any signature-based application. By default, it is off.
auth [cta { collector (add (collector-ip <ipaddress>) | (delete (collector-ip <ipaddress>)) | disable | enable | show} | thin-client {add (citrix-ip <ipaddress>) | (delete (citrix-ip <ipaddress>) | show}]	Enable authentication: transparent authentication, thin client authentication for AD users cta - Add and remove CTA collector IP address for clientless single sign on configuration thin-client – add and remove citrix server ip address for thin-client support
dhcp [dhcp-options {binding ((add dhcpname <dhcp server name> | optionname <name of the option> | value <number>))| delete (dhcpname	Cyberoam supports configuration of DHCP options, as defined in RFC 2132. DHCP options allow users to specify additional DHCP parameters in the form of pre-defined, vendor-specific information that is stored in the

<dhcp server name> | optionname <name of the option> | value <number>) | show (dhcpname <dhcp server name>)) | list}]	options field of a DHCP message. When the DHCP message is sent to clients on the network, it provides vendor-specific configuration and service information. Appendix B provides a list of DHCP options by RFC-assigned option number.
diagnostics	Various tools to check appliance health
ha [disable | load-balancing | show {details | logs lines <number>}]	disable - Option to disable HA. One can enable HA from Web Admin Console – System > HA load-balancing – Option to disable traffic load balancing between the cluster appliances. By default, as soon as Active-Active is configured, traffic load balancing is enabled. show – Displays HA configuration details like HA status and state, current and peer appliance key, dedicated port and IP address, load balancing and Auxiliary Administrative port and IP address. It also displays HA logs if HA is configured.
ips_autoupgrade [off | on | show]	Enable or disable IPS auto-upgrade. One can enable /disable from Web Admin Console – System > Maintenance > Updates also.
ipsec_route [add {(host <ipaddress> | tunnelname) | (net <network> tunnelname)} | del { (host <ipaddress> tunnelname) | (net <network> tunnelname) } | show]	Configure IPSec routes and view route details like tunnel name, host/network and netmask
ipv6 [interface {Port<port name>(address (add <ipaddress6> | delete <ipaddress6> | show) | (prefix (add <ipaddress6> | delete <ipaddress6> | show) | (router-adv [default-life <number> | hop-limit <number> | link-mtu <number> | manage-flag <enable | disable> | max-interval <number> | min-interval <number> | other-flag <enable | disable>| reachable-time | retrans-time | send-adv | show]) } | neighbour {clear | show} | reset-router-adv | route {add | del | show} | tunnel {add | del | show}]	Configure ipv6 protocol address – add and remove v6 IP address prefix - add and remove v6 IP address prefix default-life – Router lifetime (0-9000 seconds) hop-limit – Current Hop Limit. (0-255) link-mtu – MTU Value manage-flag – Managed address configuration max-interval – Maximum time interval between sending unsolicited multicast router advertisements. (4-1800 seconds) min-interval – Minimum time interval between sending unsolicited multicast router advertisements. (4-1800 seconds) other-flag – Other stateful configuration reachable-time – Reachable Time (0-3600 milliseconds) retrans-time – Retransmission Time send-adv – Send periodic router advertisements and respond to router solicitations

	show - Show-Router-Advertisement-Configuration
link_failover [add {primarylink port <port name> backuplink <vpn tunnel name> monitor (ping host <ipaddress> | udp host port <port name> | tcp host port <port name>) }| del | show]	VPN can be configured as a Backup link. With this, whenever primary link fails, traffic will be tunneled through VPN connection and traffic will be routed again through the primary link once it is UP again.
restart [all]	Restart Cyberoam
route_precedence [set {static vpn}| show]	Set the route precedence
shutdown	Shutdown Cyberoam
system_modules [h23 {load | unload} | irc {load | unload} | pptp {load | unload} | show | sip {load | unload} | tftp {load | unload}]	Load or unload the system modules like h23, irc, sip, tftp By default, all the modules are loaded. Load/unload modules to enhance the network performance and reduce the potential security risk. Do not enable any modules that are not in use. Any enabled module could present a potential security risk. A hacker might find a way to misuse the enabled services to access your network. Usage of these services affects the network security and network performance due to the traffic it generates and consumes high bandwidth. H323 - The H.323 standard provides a foundation for audio, video, and data communications across IP-based networks, including the Internet. H.323 is an umbrella recommendation from the International Telecommunications Union (ITU) that sets standards for multimedia communications over Local Area Networks (LANs) that do not provide a guaranteed Quality of Service (QoS). It enables users to participate in the same conference even though they are using different videoconferencing applications. PPTP - PPTP (Point to Point Tunneling Protocol) is a network protocol that enables secure transfer of data from a remote client to a private server, creating a VPN tunnel using a TCP/IP based network IRC - IRC (Internet Relay Chat) is a multi-user, multi-channel chatting system based on a client-server model. Single Server links with many other servers to make up an IRC network, which transport messages from one user (client) to another. In this manner, people from all over the world can talk to each other live and simultaneously. DoS attacks are very common as it is an open network and with no control on file sharing, performance is affected. SIP – SIP (Session Initiation Protocol) is a signaling protocol which enables the controlling of media communications such as VOIP. The protocol is generally used for maintaining unicast and multicast sessions consisting of several media systems. SIP is a text based and TCP/IP supported Application layer protocol.

	TFTP - Trivial File Transfer Protocol (TFTP) is a simple form of the File Transfer Protocol (FTP). TFTP uses the User Datagram Protocol (UDP) and provides no security features.
wwan [enable | disable | set {disconnect-on-systemdown <on | off> |modem-convert-timeout <number> | modem-learn-timeout <number>}| show]	Enable or disable wireless WAN. Wireless WAN menu will be available on Web Admin Console only when wwan is enabled from CLI.

arp

Used for debugging purposes, to get a complete dump of the ARP cache

Syntax

arp [ping | show]

Parameter list & description

Keywords & Variables	Description
ping [count | duplicate | interface | silent | source | timeout]	Sends ICMP ECHO_REQUEST packets to network hosts. Refer to Ping command for details.
show	Show / manipulate arp cache.

diagnostics

Used for debugging purposes

Syntax

cyberoam diagnostics [ctr-log-lines | purge-all-logs | purge-old-logs | show | subsystems | utilities]

Parameter list & description

Keywords & Variables	Description
ctr-log-lines <250 - 10000>	Generate CTR report with specified number of lines Input range – 250 – 10000 lines Default – 100 lines
purge-all-logs	Purges all logs
purge-old-logs	Purges old logs
show {cpu | ctr-log-lines | disk | interrupts | memory | subsystem-info | syslog <number> | sysmsg | uptime | version-info}	cpu – displays CPU details ctr-log-lines – displays number of lines configured for CTR log disk – displays disk usage. It displays space utilized by configuration, signature and reports. interrupts – displays list of interrupts memory – displays memory used by various utilities subsystem-info – displays status of various subsystems

	syslog – displays raw log sysmsg – displays system uptime – displays system uptime and load average version-info – displays appliance model number, public key and Cyberoam version running on the appliance. Also displays loader version, Config, Signature and Report DB version, IPS signature version, Webcat signature version, Antivirus signature version, Proxy – web, SMTP, POP/IMAP/FTP and IM version, Logging Daemon version.
subsystems {Access-Server | Bwm | CSC | IM | IPSEngine | LoggingDaemon | Msyncd | POPIMAPFTPDeamon | Pktcapd | SMTPD | SSLVPN | SSLVPN-RPD | WebProxy | Wifiauthd} |	debug <on | off>- Enable subsystem for debugging purge-log – Flush logs purge-old-log – Flush old logs
utilities	arp - complete dump of the ARP cache bandwidth-monitor – displays bandwidth used by each port. connections [delete {conn_id <number> | dst_ip <destination ipaddress> | proto <string> | src_ip <source ipaddress>} | show {dst_ip <destination ipaddress> | dst_port <number> | proto <string> | src_ip <source ipaddress> | src_port <number>}] – view and delete connection details dnslookup drop-packet-capture [<text> | interface Port<port ID> | snaplen <number of bytes to capture>] - Packet capture displays dropped packets details on the specified interface. It will provide connection details and details on which module is dropping packets e.g. firewall, IDP along with information like firewall rule number, user, Internet Access policy number etc. This will help Cyberoam administrators to troubleshoot errant firewall rule. ip ping ping6 route traceroute

dnslookup

Query Internet domain name servers for hostname resolving

Syntax

dnslookup {host [<ipaddress> | <string>] | server <ipaddress> }

Parameter list & description

Keywords & Variables	Description
host [<ipaddress> | <string>]	Host to be searched
server [<ipaddress> [host]]	Internet name or address of the name server

ip

Utility from iproute2 package

Syntax

ip [addr | link | maddr | monitor | mroute | neigh | route | rule | tunnel]

Parameter list & description

Keywords & Parameters	Description
addr [show]	Display Protocol addresses deprecated - (IPv6 only) list deprecated addresses dev [Port<port number>] – Network device dynamic - List only those addresses configured in stateless address configuration label - List addresses with label matching the pattern permanent - List only permanent addresses primary - List only primary addresses scope [host | link | global] – displays the scope of the ip address secondary - List only secondary addresses tentative - List IP address which did not pass duplicate address detection to - <string> List IP address matching the string
link [show {Port<port ID>}]	View network device configuration for different ports
maddr [show [dev {Port<port ID}>]]	View Multicast Address Management for different ports
monitor [<string> | all]	State Monitoring. The following objects are monitored: link – network device address – protocol (ip or ipv6) address on the device neighbour – ARP or NDISC cache entry

	route - routing table entry. rule - rule in routing policy database. maddress - multicast address. mroute - multicast routing cache entry. tunnel - tunnel over IP
mroute [show [interface Port <Port ID> from <string> | to <string>]]	Multicast Routing Cache Management
neigh [show]	Neighbour/Arp Tables Management nud [noarp | permanent | reachable | stale] - Neighbour Unreachability Detection dev [Port <port number>] – Network device to - <string> List IP address matching the string
route [add {<string> | blackhole <string> | broadcast | local | multicast | nat | prohibit <string> | throw <string> | unicast <string> | unreachable <string>} | append {<string> | blackhole <string> | broadcast | local | multicast | nat | prohibit <string> | throw <string> | unicast <string> | unreachable <string>} | change {<string> | blackhole <string> | broadcast | local | multicast | nat | prohibit <string> | throw <string> | unicast <string> | unreachable <string>} del {<string> | blackhole <string> | broadcast | local | multicast | nat | prohibit <string> | throw <string> | unicast <string> | unreachable <string>} | flush {exact <string> | match <string> | proto | root | scope | table | type} | get <ipaddress> { { from <ipaddress> | input_iface Port <port ID> | output_iface Port <port number> tos <number> } | list {root | match | exact | table | proto | type | scope | table} | replace {<string>| blackhole | broadcast | local | multicast | nat | prohibit | throw | unicast | unreachable }]	Routing Table Management root - Only list routes with strings not shorter than <string> match - Only list routes matching the string exact - Only list routes exactly same as string proto - Only list routes of this protocol type - Only list routes of this type scope - Only list routes with this scope table – Show routes for the table
rule [list]	lists all the IP rules
tunnel [show]	(IP tunnel devices only.) Configure the physical source and destination address for IP tunnel interfaces

	csum <interface> - (only GRE tunnels) - generate/require checksums for tunneled packets dev [Port<port number>] - Network device icsum <interface> -Generate/require checksums for tunneled packets ikey [<ipaddress> | <number>] -Use keyed GRE with this Input key iseq - Flag enables sequencing of incoming packets key [<ipaddress> | <number>] -(only GRE tunnels) use keyed GRE with key local <ipaddress> - Set the fixed local address for tunneled packets mode [gre | ipip | sit] - Set the tunnel mode nopmtudisc - Disable Path MTU Discovery on this tunnel ocsum - Generate/require checksums for tunneled packets okey [<ipaddress> | <number>] -Use keyed GRE with this output key oseq - Flag enables sequencing of outgoing packets pmtudisc - Enable Path MTU Discovery on this tunnel remote <ipaddress> - Set the remote endpoint of the tunnel seq - Flag is equivalent to the combination `iseq oseq' tos <number> - Type of Service ttl <number> - Time to Live

ping

Sends ICMP ECHO_REQUEST packets to network hosts

Syntax

ping [<ipaddress> | <string> | count | interface | quiet | size | timeout]

Parameter list & description

Keywords & Variables	Description
ipaddress	IP address to be pinged
string	Domain to be pinged
count <number>	Stop sending packets after count
interface [Port <port ID>]	Set source address

quiet	Display the summary at startup and end
size <number>	Number of data bytes to be sent
timeout <number>	Stop sending packets and exit after specified time

ping6

Sends ICMP ECHO_REQUEST packets to ipv6 hosts

Syntax

Ping6 [<ipaddress6> **|** count **|** interface **|** quiet **|** size]

Parameter list & description

Keywords & Variables	Description
ipaddress	IPv6 address to be pinged
count <number>	Stop sending packets after count
interface [Port <port ID>]	Set source address
quiet	Display the summary at startup and end
size <number>	Number of data bytes to be sent

route

Use to view / manipulate the IP routing table. Route manipulates the kernel's IP routing tables. Its primary use is to set up temporary routes to specific hosts or networks via an interface. When the add or del options are used, route modifies the routing tables. Without these options, route displays the current contents of the routing tables

Syntax

route [show]

Parameter list & description

Keywords & Variables	Description
show	displays the routing table

Routing table

Destination The destination network or destination host

Gateway The gateway address or '*' if not set

Genmask The netmask for the destination net; '255.255.255.255' for a host destination and '0.0.0.0' for the default route

Flags Possible flags include

U (route is up)
H (target is a host)
G (use gateway)

R (reinstate route for dynamic routing)
D (dynamically installed by daemon or redirect)
M (modified from routing daemon or redirect)
A (installed by addrconf)
C (cache entry)
! (reject route)

Metric The ‘distance’ to the target (usually counted in hops). It is not used by recent kernels, but may be needed by routing daemons.

Ref Number of references to this route. (Not used in the Linux kernel.)

Use Count of lookups for the route. Depending on the use of -F and -C this will be either route cache misses (-F) or hits (-C).

Iface Interface to which packets for this route will be sent

traceroute

Use to trace the path taken by a packet from the source system to the destination system, over the Internet.

The Internet is a large and complex aggregation of network hardware, connected together by gateways. Tracking the route one's packets follow (or finding the miscreant gateway that is discarding your packets) can be difficult. Traceroute utilizes the IP protocol `time to live' field and attempts to elicit an ICMP TIME_EXCEEDED response from each gateway along the path to some host.

Syntax

traceroute [<ipaddress> | <string> | first-ttl | icmp | max-ttl | no-frag | probes | source | timeout | tos]

Keywords & Variables	Description
<ipaddress> [size <number>]	Set the IP address to be traced
<string> [size <number>]	Set the domain to be traced
first-ttl	Set the initial time-to-live used in the first outgoing probe packet
icmp	Use ICMP ECHO instead of UDP datagrams
max-ttl	Set the max time-to-live
no-frag	Set the 'don't fragment' bit
probes	Probes are sent at each ttl -default 3
source	Use given IP address as source address
timeout	Set the timeout -in seconds for a response to a probe -default 5
tos	Set the type-of-service

enableremote

Allows to connect to the Cyberoam remotely i.e. allows to establish remote (SSH) connection. By default remote connection is not allowed

Syntax

enableremote [port <number> | serverip <ipaddress>]

Parameter list & description

Keywords & Parameters	Description
port <number>	Port through which the remote SSH connection can be established
serverip <ipaddress>	IP address of the Cyberoam to which the remote connection can be established

disableremote

Disables the remote (SSH) connection, if enabled. By default, it is not allowed. Refer to enable remote to allow to establish the remote connection.

Syntax

disableremote

set

Set entities

Syntax

set [advanced-firewall | arp-flux | bandwidth | http_proxy | network | service-param]

Parameter list & description

Keywords & Variables	Description
advanced-firewall [bypass-stateful-firewall-config {add <dest_host <ipaddress> | dest_network <ipaddress> | source_host <ipaddress> | source_destination <ipaddress>> | del <dest_host <ipaddress> | dest_network <ipaddress>| source_host <ipaddress> | source_destination <ipaddress>>} | cr-traffic-nat {add (destination <ipaddress> | interface Port <port name> | snat <ipaddress>| netmask <netmask>) | delete (destination <ipaddress>| interface Port <port name> | snat	Configure advanced firewall setting bypass-stateful-firewall-config – Add host or network when the outbound and return traffic does not always traverse through Cyberoam fragmented-traffic - Allow or deny fragmented traffic ftpbounce-prevention - Prevent ftp-bounce attack on FTP control and data connection midstream-connection-pickup - Configure

<ipaddress>| netmask <netmask>) } | fragmented-traffic <allow | deny> | ftpbounce-prevention <control | data> | midstream-connection-pickup <on | off> | strict-policy <on | off> | tcp-est-idle-timeout <2700 - 432000> | tcp-seq-checking <on | off> | tcp-window-scaling <on | off>]	midstream connection pickup settings. Enabling midstream pickup of TCP connections will help while plugging in the Cyberoam appliance as a bridge in a live network without any loss of service. It can also be used for handling network behavior due to peculiar network design and configuration. E.g. atypical routing configurations leading to ICMP redirect messages. By default, Cyberoam is configured to drop all untracked (mid-stream session) TCP connections in both the deployment modes strict-policy on - Applies strict firewall policy. It drops UDP Dst Port 0, TCP Src Port 0 and/or Dst Port 0, Land Attack, Winnuke Attack, Data On TCP Sync, Zero IP Protocol, TTL Value 0 traffic strict-policy off - Disables strict firewall policy tcp-est-idle-timeout - Set Idle Timeout between 2700-432000 seconds for TCP connections in the established state tcp-seq-checking – Every TCP packet contains a Sequence Number (SYN) and an Acknowledgement Number (ACK). Cyberoam monitors SYN and ACK numbers within a certain window to ensure that the packet is indeed part of the session. However, certain application and third party vendors use non-RFC methods to verify a packet's validity or for some other reason a server may send packets in invalid sequence numbers and expect an acknowledgement. For this reason, Cyberoam offers the ability to disable this feature. By default, this option is ON.
arp-flux [on | off]	ARP flux occurs when multiple ethernet adaptors often on a single machine respond to an ARP query. Due to this, problem with the link layer address to IP address mapping can occur. Cyberoam may respond to ARP requests from both Ethernet interfaces. On the machine creating the ARP request, these multiple answers can cause confusion. ARP flux affects only when Cyberoam has multiple physical connections to the same medium or broadcast domain. on - Cyberoam may respond to ARP requests from both Ethernet interfaces when Cyberoam has multiple physical connections to the same medium or broadcast domain. off - Cyberoam responds to ARP requests from respective Ethernet interface when Cyberoam has multiple physical connections to the same

	medium or broadcast domain.
bandwidth [default-policy {guaranteed <number> burstable <number> priority <number> | graph} | guarantee {enforced | lenient} | max-limit <number>]	default-policy and guarantee allows to define the bandwidth restriction on the traffic on which the bandwidth policy is not applied while max-limit allows to define the link bandwidth. • To set the link bandwidth i.e. bandwidth provided by Service Provider and can be used as "**set bandwidth max-limit <number>"** and to view the configured limit, use the command "**show bandwidth max-limit**". Default=100mbps • To enforce bandwidth restriction on the traffic on which the bandwidth policy is not applied so that guaranteed bandwidth is available to the users to whom the guaranteed bandwidth policy is applied, configure "**set bandwidth guarantee enforced"**. • If guarantee is enforced, default bandwidth policy will be applicable to the traffic on which bandwidth policy is not applied. You can set the guaranteed and burstable bandwidth and priority on this traffic. This bandwidth is applicable on Internal (LAN and DMZ) to External zone (WAN and VPN) traffic and External to Internal zone traffic. Default Guaranteed bandwidth = 0 kbps, Burstable bandwidth = max-limit, priority = 7 (lowest). Guaranteed and burstable bandwidth can be defined as "**set bandwidth default-policy guaranteed <number> burstable <number> priority <number>"** • If you do not want to enforce the bandwidth restriction on the traffic on which the bandwidth policy is not applied, configure "**set bandwidth guarantee lenient**".
http_proxy [add_via_header <on | off > | dos (add {connection <number> | method (GET <number> | POST <number>) | delete { connection | method (GET | POST) } | host-entries (add {host-name <string> | delete {host-name<string>}) |	Set proxy parameters add via header - By default, it is ON dos – Configure number of HTTP requests per source IP or number of HTTP requests per TCP connection. Number of requests higher than the configured rate is considered as attack and the traffic from the said source is dropped. One can either configure allowed number of connections or for granular controls can configure allowed number of requests per Method – GET and PUT. Applicable only when Cyberoam is deployed transparent mode.
ips	Configure IPS settings
network [interface-speed [Port<port	Configure network interface parameters

name> <1000fd | 1000hd | 100fd | 100hd | 10fd | 10hd | auto >] | mtu-mss [port <port name > {mtu <number> | default | mss (<number> | default) }]	interface speed - Speed mismatch between Cyberoam and 3rd party routers and switches can result into errors or collisions on interface, no connection or traffic latency, slow performance. mss – Maximum Segment Size – It defines the amount of data that can be transmitted in a single TCP packet Range – 576 – 1460 bytes mtu - Maximum Transmission Unit - It specifies the largest physical packet size, in bytes, that a network can transmit. This parameter becomes an issue when networks are interconnected and the networks have different MTU sizes. Any packets larger than the MTU value are divided (fragmented) into smaller packets before being sent. Default – 1500 bytes MTU size is based on addressing mode of the interface. Range – 576 – 1500 bytes for static mode Range – 576 – 1500 bytes for DHCP mode Range – 576 – 1492 bytes for PPPoE mode
on-appliance-reports [on | off]	Generate on-appliance reports By default, it is ON
proxy-arp[add [interface Port<port name> | dst_ip <ipaddress> | dst_iprange (from_ip <ipaddress>] | to_ip <ipaddress>] | del | [interface Port<port number> | dst_ip <ipaddress> | dst_iprange (from_ip <ipaddress>] | to_ip <ipaddress>]]	Add and delete proxy ARP
service-param [FTP {add | delete} | HTTP {add | delete} | HTTPS {deny_unknown_proto <on | off> | invalid_certificate <allow | block> } | IMAP {add | delete} | IM_MSN {add | delete} | IM_YAHOO {add | delete} | POP | SMTP {add | delete}]	By default, Cyberoam inspects all inbound HTTP, HTTPS, FTP, SMTP, POP and IMAP traffic on the standard ports. “service-param” enables inspection of HTTP, HTTPS, FTP, SMTP, POP, IMAP, IM – MSN and Yahoo traffic on non-standard ports also. add Port<port name > – enable inspection for a specified port number. delete Port<port name> - disable inspection for a specified port number. deny_unknown_proto - Allow/deny traffic not following HTTPS protocol i.e. invalid traffic through HTTPS port By default, it is ON invalid_certificate - If you enable HTTPS

	scanning, you need to import Cyberoam SSL Proxy certificate in Internet Explorer, Firefox Mozilla or any other browsers for decryption on SSL Inspection otherwise browser will always give a warning page when you try to access any secure site. "**Invalid Certificate error"** warning appears when the site is using an invalid SSL certificate. Cyberoam blocks all such sites. Use this command, if you wan to allow access to such sites.
sslvpn[proxy-sslv3 <on | off> | web-access <on | off>]	Enable/disable SSL V3 and web access mode support
vpn [l2tp {authentication (ANY | CHAP | MS_CHAPv2 | PAP)} | pptp (ANY | CHAP | MS_CHAPv2 | PAP)]	Set authentication protocol for l2tp and pptp connections

ips

Configure IPS settings

Syntax

ips [lowmem-settings | maxsesbytes-settings | packet-streaming | show-all-settings]

Parameter list & description

Keywords & Parameters	Description
lowmem-settings [off | on | show]	Set whether low memory settings to be applied or not. Low memory settings are applied in case of system having memory issues. show - Displays current status of low memory settings. By default, it is off. on – enable low memory settings. off – disable low memory settings.
maxpkts [<number> | all | default]	Set number of packets to be sent for Application Classification number – any number above 8 all - pass all of the session packets for application classification default - pass first 8 packets of the session of each direction for application classification (total 16)
maxsesbytes-settings [update <number>]	maxsesbytes-settings allows you to set the maximum allowed size. Any file beyond the configured size is bypassed and not scanned. Update – set the value for maximum bytes allowed per session
packet-streaming [on | off]	Set whether packet streaming is to be allowed or not. packet-streaming is used to restrict streaming of

	packets in situations where system is experiencing memory issues. on - Enables packet streaming. off - disable packet streaming.

show

Displays various parameters configured

Syntax

show [advanced-firewall | arp-flux | bandwidth | date | http_proxy | ips-settings | network | on-appliance-reports | port-affinity | pppoe | proxy-arp | service-param | sslvp | vpn]

tcpdump

tcpdump prints out the headers of packets on a network interface that match the boolean expression. Only packets that match expression will be processed by tcpdump.

Syntax

tcpdump [<text> | count | filedump | hex | interface | llh | no_time | quite | verbose]

Parameter list & description

Keywords & Variables	Description
<text>	Packet filter expression. Based on the specified filter, packets are dumped. If no expression is given, all packets are dumped else only packets for which expression is `true' are dumped. The expression consists of one or more primitives. Primitives usually consist of an id (name or number) proceeded by one or more qualifiers. Refer to the below given table on writing filtering expressions.
count	Exit after receiving count packets
filedump	Tcpdump output can be generated based on criteria required. Save tcpdump output in a binary file and can be downloaded from http://<cyberooam_ip>/documents/tcpdump.out File contains the troubleshooting information useful to analyze the traffic with advanced tool like ethereal for Cyberoam Support team.
hex	Print each packet (minus its link level header) in hexadecimal notation
interface	Listen on <interface>
llh	View packet contents with Ethernet or other layer 2 header information
no_time	Do not print a timestamp on each dump line
quite	Print less protocol information so output lines are shorter.
verbose	Verbose output. For example, the time to live, identification, total length and options in an IP packet are printed. Also

	enables additional packet integrity checks such as verifying the IP and ICMP header checksum.

How to view traffic of the	tcpdump command	Example
specific host	tcpdump 'host <ipaddress>'	tcpdump 'host 10.10.10.1'
specific source host	tcpdump 'src host <ipaddress>'	tcpdump 'src host 10.10.10.1'
specific destination host	tcpdump 'dst host <ipaddress>'	tcpdump 'dst host 10.10.10.1'
specific network	tcpdump 'net <network address>'	tcpdump 'net 10.10.10.0'
specific source network	tcpdump 'src net <network address>'	tcpdump 'src net 10.10.10.0'
specific destination network	tcpdump 'dst net <network address>'	tcpdump 'dst net 10.10.10.0'
specific port	tcpdump 'port <port-number>'	tcpdump 'port 21'
specific source port	tcpdump 'src port <port-number>'	tcpdump 'src port 21'
specific destination port	tcpdump 'dst port <port-number>'	tcpdump 'dst port 21'
specific host for the particular port	tcpdump 'host <ipaddress> and port <port-number>'	tcpdump 'host 10.10.10.1 and port 21'
the specific host for all the ports except SSH	tcpdump 'host <ipaddress> and port not <port-number>'	tcpdump 'host 10.10.10.1 and port not 22'
specific protocol	tcpdump 'proto ICMP' tcpdump 'proto UDP' tcpdump 'proto TCP' tcpdump 'arp'	
paritcular interface	tcpdump interface <interface>	tcpdump interface eth1
specific port of a particular interface	tcpdump interface <interface> 'port <port-number>'	tcpdump interface eth1 'port 21'

Note: Expression can be combined using logical operators AND or OR and with NOT also. Make sure to use different combinations within single quotes.

telnet

Use telnet protocol to connect to another remote computer.

Syntax

telnet [<ipaddress>]

Parameter list & description

Keywords & Variables	Description
ipaddress { <port number> }	official name, an alias, or the Internet address of a remote host Port - indicates a port number (address of an application).

	If a number is not specified, the default telnet port is used.

Appendix B - DHCP options (RFC 2132)

A DHCP server can provide optional configurations to the client. Cyberoam provides support to configure following DHCP Options as defined in RFC 2132. To set the options, refer to DHCP Server Enhancements section.

Option Number	Name	Description	Data Type
2	Time Offset	Time offset in seconds from UTC	Four Byte Numeric Value
4	Time Ser vers	N/4 time server addresses	Array of IP-Address
5	Name Servers	N/4 IEN-116 server addresses	Array of IP-Address
7	Log Servers	N/4 logging server addresses	Array of IP-Address
8	Cookie Servers	N/4 quote server addresses	Array of IP-Address
9	LPR Servers	N/4 printer server addresses	Array of IP-Address
10	Impress Servers	N/4 impress server addresses	Array of IP-Address
11	RLP Servers	N/4 RLP server addresses	Array of IP-Address
12	Host Name	Hostname string	String
13	Boot File Size	Size of boot file in 512 byte chunks	Two Byte Numeric Value
14	Merit Dump File	Client to dump and name of file to dump to	String
16	Swap Ser ver	Swap ser ver addresses	IP-Address
17	Root Path	Path name for root disk	String
18	Extension File	Patch name for more BOOTP info	String
19	IP Layer Forwarding	Enable or disable IP forwarding	Boolean
20	Src route enabler	Enable or disable source routing	Boolean
22	Maximum DG Reassembly Size	Maximum datagram reassembly size	Two Byte Numeric Value
23	Default IP TTL	Default IP time-to-live	One Byte Numeric Value
24	Path MTU Aging Timeout	Path MTU aging timeout	Four Byte Numeric Value
25	MTU Plateau	Path MTU plateau table	Array of Two Byte Numeric Values
26	Interface MTU Size	Interface MTU size	Two Byte Numeric Value
27	All Subnets Are Local	All subnets are local	Boolean
28	Broadcast Address	Broadcast address	IP-Address
29	Perform Mask Discovery	Perform mask discovery	Boolean
30	Provide Mask to Others	Provide mask to others	Boolean
31	Perform Router Discovery	Perform router discovery	Boolean
32	Router Solicitation Address	Router solicitation address	IP-Address
34	Trailer Encapsulation	Trailer encapsulation	Boolean
35	ARP Cache Timeout	ARP cache timeout	Four Byte Numeric Value
36	Ethernet Encapsulation	Ethernet encapsulation	Boolean
37	Default TCP Time to Live	Default TCP time to live	One Byte Numeric Value

38	TCP Keepalive Interval	TCP keepalive inter val	Four Byte Numeric Value
39	TCP Keepalive Garbage	TCP keepalive garbage	Boolean
40	NIS Domain Name	NIS domain name	String
41	NIS Server Addresses	NIS server addresses	Array of IP-Address
42	NTP Ser vers Addresses	NTP ser vers addresses	Array of IP-Address
43	Vendor Specific Information	Vendor specific information	String
45	NetBIOS Datagram Distribution	NetBIOS datagram distribution	Array of IP-Address
46	NetBIOS Node Type	NetBIOS node type	One Byte Numeric Value
47	NetBIOS Scope	NetBIOS scope	String
48	X Window Font Ser ver	X window font ser ver	Array of IP-Address
49	X Window Display Manager	X window display manager	Array of IP-Address
50	Requested IP address	Requested IP address	IP-Address
51	IP Address Lease Time	IP address lease time	Four Byte Numeric Value
52	Option Overload	Overload “sname” or “file”	One Byte Numeric Value
53	DHCP Message Type	DHCP message type	One Byte Numeric Value
55	Parameter Request List	Parameter request list	Array of One Byte Numeric Values
56	Message	DHCP error message	String
57	DHCP Maximum Message Size	DHCP maximum message size	Two Byte Numeric Value
58	Renew Time Value	DHCP renewal (T1) time	Four Byte Numeric Value
59	Rebinding Time Value	DHCP rebinding (T2) time	Four Byte Numeric Value
60	Client Identifier	Client identifier	String
61	Client Identifier	Client identifier	String
62	Netware/IP Domain Name	Netware/IP domain name	String
64	NIS+ V3 Client Domain Name	NIS+ V3 client domain name	String
65	NIS+ V3 Server Address	NIS+ V3 server address	Array of IP-Address
66	TFTP Ser ver Name	TFTP ser ver name	String
67	Boot File Name	Boot file name	String
68	Home Agent Addresses	Home agent addresses	Array of IP-Address
69	Simple Mail Server Addresses	Simple mail ser ver addresses	Array of IP-Address
70	Post Office Server Addresses	Post office server addresses	Array of IP-Address
71	Network News Server Addresses	Network news server addresses	Array of IP-Address
72	WWW Server Addresses	WWW server addresses	Array of IP-Address
73	Finger Server Addresses	Finger server addresses	Array of IP-Address
74	Chat Server Addresses	Chat server addresses	Array of IP-Address
75	StreetTalk Ser ver Addresses	StreetTalk server addresses	Array of IP-Address
76	StreetTalk Directory Assistance Addresses	StreetTalk directory assistance addresses	Array of IP-Address