BSR 2000 Command Reference Guide

MOTOROLA

526363-001-00 Rev. B
Release 1.0
MGBI

Notice

526363-001-00 Rev. B
Release 1.0
MGBI
Published: 2/06

Caring for the Environment by Recycling

When you see this symbol on a Motorola product, do not dispose of the product with residential or commercial waste.

Recycling your Motorola Equipment

Please do not dispose of this product with your residential or commercial waste. Some countries or regions, such as the European Union, have set up systems to collect and recycle electrical and electronic waste items. Contact your local authorities for information about practices established for your region. If collection systems are not available, call Motorola Customer Service for assistance.

Recyclage pour le respect de l'environnement

Lorsque vous voyez ce symbole sur un produit Motorola, ne le jetez pas avec vos ordures ménagères ou vos rebuts d'entreprise.

Recyclage de votre équipement Motorola

Veuillez ne pas jeter ce produit avec vos ordures ménagères ou vos rebuts d'entreprise. Certains pays ou certaines régions comme l'Union Européenne ont mis en place des systèmes de collecte et de recyclage des produits électriques et électroniques mis au rebut. Veuillez contacter vos autorités locales pour vous informer des pratiques instaurées dans votre region. Si aucun système de collecte n'est disponible, veuillez appeler le Service clientèle de Motorola qui vous apportera son assistance.

Umweltschutz durch Recycling

Wenn Sie dieses Zeichen auf einem Produkt von Motorola sehen, entsorgen Sie das Produkt bitte nicht als gewöhnlichen Haus- oder Büromüll.

Recycling bei Geräten von Motorola

Bitte entsorgen Sie dieses Produkt nicht als gewöhnlichen Haus- oder Büromüll. In einigen Ländern und Gebieten, z. B. in der Europäischen Union, wurden Systeme für die Rücknahme und Wiederverwertung von Elektroschrott eingeführt. Erkundigen Sie sich bitte bei Ihrer Stadt- oder Kreisverwaltung nach der geltenden Entsorgungspraxis. Falls bei Ihnen noch kein Abfuhr- oder Rücknahmesystem besteht, wenden Sie sich bitte an den Kundendienst von Motorola.

Cuidar el medio ambiente mediante el reciclaje

Cuando vea este símbolo en un producto Motorola, no lo deseche junto con residuos residenciales o comerciales.

Reciclaje de su equipo Motorola

No deseche este producto junto con sus residuos residenciales o comerciales. Algunos países o regiones, tales como la Unión Europea, han organizado sistemas para recoger y reciclar desechos eléctricos y electrónicos. Comuníquese con las autoridades locales para obtener información acerca de las prácticas vigentes en su región. Si no existen sistemas de recolección disponibles, solicite asistencia llamando el Servicio al Cliente de Motorola.

Cuidando do meio ambiente através da reciclagem

Quando você ver este símbolo em um produto Motorola, não descarte o produto junto com lixo residencial ou comercial.

Reciclagem do seu equipamento Motorola

Não descarte este produto junto com o lixo residencial ou comercial. Alguns países ou regiões, tais como a União Européia, criaram sistemas para colecionar e reciclar produtos eletro-eletrônicos. Para obter informações sobre as práticas estabelecidas para sua região, entre em contato com as autoridades locais. Se não houver sistemas de coleta disponíveis, entre em contato com o Serviço ao Cliente da Motorola para obter assistência.

Dbałość o środowisko – recycling

Produktów Motorola oznaczonych tym symbolem nie należy wyrzucać do komunalnych pojemników na śmieci.

Recykling posiadanego sprzętu Motorola

Produktu nie należy wyrzucać do komunalnych pojemników na śmieci. W niektórych krajach i regionach, np. w Unii Europejskiej, istnieją systemy zbierania i recyklingu sprzętu elektrycznego i elektronicznego. Informacje o utylizacji tego rodzaju odpadów należy uzyskać od władz lokalnych. Jeśli w danym regionie nie istnieją systemy zbierania odpadów elektrycznych i elektronicznych, informacje o utylizacji należy uzyskać od biura obsługi klienta firmy Motorola (Motorola Customer Service).

Beskyttelse af miljøet med genbrug

Når du ser dette symbol på et Motorola-produkt, må produktet ikke bortskaffes sammen med husholdningsaffald eller erhvervsaffald.

Genbrug af dit Motorola-udstyr

Dette produkt må ikke bortskaffes sammen med husholdningsaffald eller erhvervsaffald. Nogle lande eller områder, f.eks. EU, har oprettet systemer til indsamling og genbrug af elektriske og elektroniske affaldsprodukter. Kontakt de lokale myndigheder for oplysninger om gældende fremgangsmåder i dit område. Hvis der ikke findes tilgængelige indsamlingssystemer, kan du kontakte Motorola Kundeservice.

Milieubewust recycleren

Als u dit symbool op een Motorola-product ziet, gooi het dan niet bij het huishoudelijk afval of het bedrijfsafval.

Uw Motorola-materiaal recycleren.

Gooi dit product niet bij het huishoudelijk afval het of bedrijfsafval. In sommige landen of regio's zoals de Europese Unie, zijn er bepaalde systemen om elektrische of elektronische afvalproducten in te zamelen en te recycleren. Neem contact op met de plaatselijke overheid voor informatie over de geldende regels in uw regio. Indien er geen systemen bestaan, neemt u contact op met de klantendienst van Motorola.

Var rädd om miljön genom återvinning

När du ser den här symbolen på en av Motorolas produkter ska du inte kasta produkten tillsammans med det vanliga avfallet.

Återvinning av din Motorola-utrustning

Kasta inte denna produkt tillsammans med det vanliga avfallet. Vissa länder eller regioner, som t.ex. EU, har satt upp ett system för insamling och återvinning av el- och elektronikavfall. Kontakta dina lokala myndigheter för information om vilka regler som gäller i din region. Om det inte finns något insamlingssystem ska du kontakta Motorolas kundtjänst för hjälp.

Újrahasznosítással a környezet védelméért

Ha ezt a jelzést látja egy Motorola terméken, ne dobja ki azt lakossági vagy ipari hulladékba.

Motorola termékének újrahasznosítása

Kérjük ne dobja ki ezt a terméket lakossági vagy ipari hulladékba. Egyes országok ill. régiók, mint az Európai Unió is, már kialakították az elektronikai hulladékok begyûjtésének rendszerét. Lépjen kapcsolatba a helyi hatóságokkal a lakóhelyén alkalmazott gyakorlattal kapcsolatos információért. Amennyiben gyûjtõrendszer nem elérhetõ, hívja a Motorola Ügyfélszolgálatot segítségért.

Kujdesja per ambientin rrethues me ane te perdorimit te perseritur.

Neqoftese shikoni kete simbol ne produktin Motorola, mos e hidhni tej produktin, duke prishur keshtu ambientin e duke shkaktuar humbje komerciale.

Perdorimi i perseritur i pajisjeve Motorola.

Ju lutemi te mos e hidhni tej kete produkt, duke shkaktuar prishjen e ambientit dhe humbje komerciale. Disa vende e regjione, te tilla si Bashkimi Europjan, kane krijuar rrjetin e grumbullimit dhe perdorimit serish te detajeve elektrike dhe elektronike te panevojshme. Lidhuni me autoritetet tuaja lokale per te marr vesh, si veprohet ne regjionin tuaj. Neqoftese nje rrjet i tille nuk ekziston, drejtojuni per ndihme Sherbimit te Motorolas per lidhje me bleresit.

リサイクルによる環境保護

モトローラ製品にこの記号が表示されている場合、製品を家庭または商業廃棄物として処分しないでください。

モトローラ装置のリサイクル

本製品を家庭または商業廃棄物として処分しないでください。欧州連合などの国または地域によっては、電気的・電子的廃棄物を収集およびリサイクルするシステムがあります。お住まいの地域で決められている方法についての情報は、地方自治体にお問い合わせください。収集システムがない場合、モトローラ・カスタマーサービスまでお問い合わせください

重复利用，保护环境

如果 Motorola 产品上具有这个标识，请勿将产品丢弃到家庭或商业垃圾中。

Motorola 设备的重复利用

请勿将本产品丢弃到家庭或商业垃圾中。某些国家或地区，例如欧盟，已经建立起回收和重复利用电气与电子废弃物的体系。请与当地相关机构联系，获取有关所在地区相关规定的信息。如果当地尚未建立回收体系，请致电 Motorola 客户服务以寻求帮助。

注意環保問題

在你看到產品上有 Motorola 的標誌時，請勿以住家或商用的廢棄物方式處置。

Motorola 設備的回收

請勿以住家或商用的廢棄物方式處置。某些國家或地區，如歐盟，已對廢棄的電器和電子產品制訂回收以及再利用體制。請與您所在地的管理機構諮詢相關規定。
若您所在的地區並未設置回收機制，請電 Motorola 客服部諮詢相關事宜。

재활용으로 환경 보호하기

Motorola 제품에 이 표시가 있는 경우, 해당제품을 가정용 또는 상업용 폐기물과 함께 버리지 마십시오.

Motorola 기기의 재활용

이 제품을 가정용 또는 사업용 폐기물과 함께 버리지 마십시오.유럽연합과 같은 일부 국가 또는 지역에서는 전기 및 전자 폐기물 용품을 수집하여 재활용하는 시스템이 구축되어 있습니다.해당지역에 구축되어 있는 절차에 관한 정보는 지역 관할당국에 연락하십시오. 수집 시스템이 존재하지 않는 경우, 도움을 받기 위해 Motorola 고객서비스부로 연락하십시오.

Contents

6 Routing Policy Commands

Preface

Scope

This document describes how to install and configure the Motorola™ Broadband Services Router™ 2000 (BSR 2000™).

Audience

This document is for use by those persons who will install and configure the BSR 2000™ product. Only trained service personnel should install, maintain, or replace the BSR 2000.

Documentation Set

The following documents comprise the BSR 2000 documentation set:

- *BSR 2000 Command Reference Guide*

  This document contains the Command Line Interface (CLI) commands for managing, configuring, and maintaining the BSR 2000.

- *BSR 2000 Configuration and Management Guide*

  This document provides the instructions and procedures for configuring and managing the BSR 2000.

- *BSR 2000 Installation Guide*

  This document describes how to install the BSR 2000 HD product.

- *BSR 2000 Release Notes*

  These documents provide information about features not described or incorrectly documented in the main documentation set; known problems and anomalies; product limitations; and problem resolutions.

- *BSR 2000 SNMP MIB Reference Guide*

  This document describes the Simple Network Management Protocol (SNMP) MIBs; provides information that describes standard and proprietary MIB support; describes how to walk the MIBs and how to compile and load the SNMP MIBs. It also provides task examples.

Conventions

This document uses the conventions in the following table:

Convention	Example	Explanation
angle brackets < >	**ping** <*ip-address*> **ping 54.89.145.71**	Arguments in italic and enclosed by angle brackets must be replaced by the text the argument represents. In the example, **54.89.345.71** replaces <*ip-address*>. When entering the argument, do not type the angle brackets.
bar brackets [ ]	**disable** [*level*]	Bar brackets enclose optional arguments. The example indicates you can use the **disable** command with or without specifying a *level*. Some commands accept more than one optional argument. When entering the argument, do not type the bar brackets.
bold text	**cable relay-agent-option**	Boldface text must be typed exactly as it appears.
brace brackets {}	**page** {**on** | **off**}	Brace brackets enclose required text. The example indicates you must enter either **on** or **off** after **page**. The system accepts the command with only one of the parameters. When entering the text, do not type the brace brackets.
italic text	**boot system** <*filename*>	Italic type indicates variables for which you supply values in command syntax descriptions. It also indicates file names, directory names, document titles, or emphasized text.
`screen display`	`Wed May 6 17:01:03 2000`	This font indicates system output.
vertical bar |	**page** {**on** | **off**}	A vertical bar separates the choices when a parameter is required. The example indicates you can enter either command: **page on** or **page off** When entering the parameter, do not type the vertical bar or the brace brackets.

Notes, Cautions, Warnings

The following icons and associated text may appear in this document.

Note: A note contains tips, suggestions, and other helpful information, such as references to material not contained in the document, that can help you complete a task or understand the subject matter.

Caution: The exclamation point, within an equilateral triangle, is intended to alert the user to the presence of important installation, servicing, and operating instructions in the documents accompanying the equipment.

Warning: This symbol indicates that dangerous voltage levels are present within the equipment. These voltages are not insulated and may be of sufficient strength to cause serious bodily injury when touched. The symbol may also appear on schematics.

If You Need Help

If you need assistance while working with the BSR 2000, contact the Motorola Technical Response Center (TRC):

Inside the U.S.	1-888-944-HELP
	1-888-944-4357
Outside the U.S.	+1-215-323-0044
Motorola Online	*http://businessonline.motorola.com*

The TRC is on call 24 hours a day, 7 days a week. In addition, Motorola Online offers a searchable solutions database, technical documentation, and low-priority issue creation and tracking.

1

System Administration Commands

Introduction

This chapter describes the following types of commands for the BSR 2000™:

User management commands which establish authentication and to protect the network from unauthorized users.

Configuration file commands that handle the operating system and the system software for the BSR. The configuration file commands allow you to customize the operating system configuration at system startup, and to modify and store the configuration file for later use.

System services commands that globally configure IP system services used with the BSR, such as protocols, NVRAM, IP parameters, the operating system, and the system clock

Lightweight Directory Access Protocol (LDAP) commands that are used with the BSR to access online directory services over the TCP/IP network protocol. The BSR becomes an LDAP client and connects to an LDAP server to requests services and/or information.

Logger commands which provide a way to configure system event reporting intended for diagnostics. The information in the report contains actions such as system startup, status, and event classes.

System Administration Command Descriptions

This section contains an alphabetized list and descriptions of the system administration commands supported by the BSR.

aaa accounting commands default

The **aaa accounting commands default** command enables command use accounting on the BSR. Enabling command use accounting provides resource usage data for commands used at a specified privilege level by creating a default list of methods used for accounting services. The **no aaa accounting commands** command disables command use accounting.

Group Access

All

Command Mode

Global Configuration

Command Line Usage

aaa accounting commands {**exec** | **isp-ro** | **isp-rw** | **mso-ro** | **mso-rw** | **sysadmin**} **default** {**none** | **start-stop** | **stop-only** | **wait-start**} {**local** | **none** | **radius** | **tacacs**}

no aaa accounting commands [**exec** | **isp-ro** | **isp-rw** | **mso-ro** | **mso-rw** | **sysadmin**]

Command Syntax

exec	commands in the User EXEC privilege level
isp-ro	commands in the ISP Read/Only privilege level
isp-rw	commands in the ISP Read/Write privilege level
mso-ro	commands in the MSO Read/Only privilege level
mso-rw	commands in the MSO Read/Write privilege level
sysadmin	commands in the SYSADMIN privilege level
none	disables accounting services

start-stop	sends a "start" accounting notice at the beginning of a process and a "stop" accounting notice at the end of a process - the requested user process begins regardless of whether the "start" accounting notice was received by the accounting server
stop-only	sends a "stop" accounting notice at the end of the requested user process - does not send a "start" accounting request at the start of the process
wait-start	sends a "start" accounting notice at the beginning of a process and a "stop" accounting notice at the end of a process - the requested user process does not begin until the "start" accounting notice is received by the server
local	local database to be used as the accounting method
none	no method is specified as the accounting method
radius	RADIUS to be used as the accounting method.
tacacs	TACACS+ to be used as the accounting method.

aaa accounting exec default

The **aaa accounting exec default** command enables terminal session accounting on the BSR. Enabling terminal session accounting provides resource usage data for a specified terminal session and creates a default list of methods used for accounting services. The **no aaa accounting exec** command disables terminal session accounting.

Group Access

All

Command Mode

Global Configuration

Command Line Usage

aaa accounting exec {**none** | **start-stop** | **stop-only** | **wait-start**} **default** {**local** | **none** | **tacacs**}

no aaa accounting exec

Command Syntax

none	disables accounting services
start-stop	sends a "start" accounting notice at the beginning of a process and a "stop" accounting notice at the end of a process - the requested user process begins regardless of whether the "start" accounting notice was received by the accounting server
stop-only	sends a "stop" accounting notice at the end of the requested user process - does not send a "start" accounting request at the start of the process

wait-start	sends a "start" accounting notice at the beginning of a process and a "stop" accounting notice at the end of a process - the requested user process does not begin until the "start" accounting notice is received by the server
local	local database to be used as the authorization method.
none	no method is specified as the accounting method
radius	RADIUS to be used as the accounting method.
tacacs	TACACS+ to be used as the accounting method.

aaa authentication enable default

The **aaa authentication enable default** command enables AAA authentication to determine if a user can access the privilege level 15 (system administrator). The **no aaa authentication enable default** command disables AAA authentication.

Note: If multiple authentication methods are specified, the methods are invoked in the sequence they are configured.

Group Access

All

Command Mode

Global Configuration

Command Line Usage

aaa authentication enable default {**enable** | **local** | **none** | **radius** | **tacacs**}

no aaa authentication enable default

Command Syntax

enable	**enable password** command setup to be used as the authentication method
local	local database to be used as the authentication method
none	no method is specified as the authentication method
radius	RADIUS to be used as the authentication method
tacacs	TACACS+ to be used as the authentication method

aaa authentication fail-message

The **aaa authentication fail-message** command allows you to configure an error message to display when a TACACS login has failed. The **no aaa authentication login default** command disables the error message.

Group Access

System Administrator

Command Mode

Global Configuration

Command Line Usage

aaa authentication fail-message [<*LINE*>]

no aaa authentication fail-message

Command Syntax

LINE	the text message to display for the failed login/authentication

aaa authentication local-override

The **aaa authentication local-override** command enables local authentication. This command overrides any configured default authentication method. A configured default authentication method will be used only if local authentication fails. The **no aaa authentication local-override** disables local authentication.

Group Access

All

Command Mode

Global Configuration

Command Line Usage

aaa authentication local-override

no aaa authentication local-override

Command Default

Disabled

aaa authentication login default

The **aaa authentication login default** command enables AAA authentication to determine if a user can login to the BSR. The **no aaa authentication login default** command disables AAA login authentication.

Note: If multiple authentication methods are specified, the methods are invoked in the sequence they are configured.

Group Access

All

Command Mode

Global Configuration

Command Line Usage

aaa authentication login default {**enable** | **local** | **none** | **radius** | **tacacs**}

no aaa authentication login

Command Syntax

enable	**enable password** command setup to be used as the authentication method
local	local database to be used as the authentication method
none	no method is specified as the authentication method
radius	RADIUS to be used as the authentication method
tacacs	TACACS+ to be used as the authentication method

aaa authorization commands default

The **aaa authorization commands default** command enables command authorization on the BSR. Command authorization determines if a user is allowed to run commands at a specified privilege level by creating a default list of methods used for authorization services. The **no aaa authorization commands default** command disables command authorization.

Group Access

All

Command Mode

Global Configuration

Command Line Usage

aaa authorization commands {**exec** | **isp-ro** | **isp-rw** | **mso-ro** | **mso-rw** | **sysadmin**} **default** {**local** | **none** | **tacacs**}

no aaa authentication commands {**exec** | **isp-ro** | **isp-rw** | **mso-ro** | **mso-rw** | **sysadmin**}

Command Syntax

exec	commands in the User EXEC privilege level
isp-ro	commands in the ISP Read/Only privilege level
isp-rw	commands in the ISP Read/Write privilege level
mso-ro	commands in the MSO Read/Only privilege level
mso-rw	commands in the MSO Read/Write privilege level
sysadmin	commands in the SYSADMIN privilege level
local	local database to be used as the authorization method

none	no method is specified as the authorization method
tacacs	TACACS+ to be used as the authorization method

aaa authorization exec default

The **aaa authorization exec default** command enables privilege level authorization on the BSR. Privilege level authorization determines if a user is allowed to run an EXEC shell (user session) by creating a default list of methods used for authorization services. The **no aaa authorization exec default** command disables privilege level authorization.

Group Access

All

Command Mode

Global Configuration

Command Line Usage

aaa authorization exec default {**local** | **none** | **tacacs**}

no aaa authorization exec

Command Syntax

local	local database to be used as the authorization method
none	no method is specified as the authorization method
tacacs	TACACS+ to be used as the authorization method

aaa console authentication

The **aaa console authentication** command enables TACACS authentication for the console if AAA is configured. The **no aaa console authentication** command disables login authentication for the console.

Group Access

System Administrator

Command Mode

Global Configuration

Command Line Usage

aaa console authentication

no aaa console authentication

Command Default

Enabled

aaa console authorization commands default

The **aaa console authorization commands default** command enables command authorization for the console if AAA is configured. The **no aaa console authorization commands default** command disables command authorization for the console.

Group Access

System Administrator

Command Mode

Global Configuration

Command Line Usage

aaa console authorization commands default

no aaa console authorization commands default

Command Default

Disabled

aaa new-model

The **aaa new model** command enables the AAA network security model. The AAA network security model provides a software mechanism or framework for consistent authentication, authorization and accounting on the BSR. The **no aaa new model** disables the AAA network security model.

Group Access

All

Command Mode

Global Configuration

Command Line Usage

aaa new model

no aaa new model

Command Default

Disabled

alias

The **alias** command allows you to specify an alias for a CLI command in a specific command mode (User EXEC, Privileged EXEC, or Global Configuration). The **no alias** command deletes a specific alias defined within the command mode.

Group Access

All

Command Mode

Global Configuration

Command Line Usage

alias {**exec** | **priv** | **conf** | **all**} <*WORD*> <*WORD*>

no alias {**exec** | **priv** | **conf** | **all**} <*WORD*>

Command Syntax

exec	User EXEC mode alias command
priv	Privileged EXEC mode alias command
conf	Global Configuration mode alias command
all	Alias is visible in all modes.
WORD	name of alias
WORD	the command that is aliased

auto-negotiation

The **auto-negotiation** command sets the duplex/speed configuration mode for a particular Gigabit Ethernet interface.

Group Access

All

Command Mode

Interface Configuration

Command Line Usage

auto-negotiation

no auto-negotiation

banner motd

The **banner motd** command allows you to create a message-of the-day (motd) that displays *before* the login prompt. The **no banner motd** command deletes the message of the day.

Group Access

All

Command Mode

Global Configuration

Command Line Usage

banner motd [<*1-25*>] [...<*WORD*>]

no banner motd

Command Syntax

1-25	Message of the Day line number
WORD	Text of the Message of the Day

batch

The **batch** command executes a series of commands from a batch file stored in Flash memory or NVRAM.

Group Access

System Administrator

Command Mode

Privileged EXEC

Command Line Usage

batch {**flash**: | **nvram:**} [**acknowledge**]

Command Syntax

flash:	execute a batch file from Flash memory
nvram:	execute a batch file from NVRAM
acknowledge	acknowledge the execution of each command

boot system

The **boot system** command lets you boot the BSR using a boot image file stored in either Flash memory or NVRAM.

Group Access

System Administrator

Command Mode

Privileged EXEC

Command Line Usage

boot system {**flash:** | **nvram:**} {<*filename*>}

Command Syntax

flash:	specifies flash memory as the location of the boot image file
nvram:	specifies Non-volatile Random Access Memory (NVRAM) as the location of the boot image file
filename	filename of the boot image stored in Flash memory or NVRAM

boot-update

The **boot-update** command allows you upgrade the BSR boot ROM.

Group Access

System Administrator

Command Mode

Privileged EXEC

Command Line Usage

boot-update <*prefix*> <*string*>

Command Syntax

prefix	The server IP address.
string	The boot image name.

broadcast

The **broadcast** command is used to send a message to all connected users.

Group Access

System Administrator

Command Mode

Privileged EXEC

Command Line Usage

broadcast <*WORD*>

Command Syntax

WORD	The text message intended for broadcast

chkdsk

The **chkdsk** command checks for and corrects any file system errors found in files stored in Flash memory or NVRAM.

Group Access

System Administrator

Command Mode

Privileged EXEC

Command Line Usage

chkdsk {**flash**: | **nvram:** }

Command Syntax

flash:	check the Flash memory file system
nvram:	check the NVRAM filesystem

clear evt

The **clear evt** command resets the event count to "0" for all groups, a specified group, or specified events.

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

clear evt [<*NUM*> | <*WORD*>] [<*range*>]

Command Syntax

NUM	this is always 0 for the BSR 2000
WORD	the name of an EVT group - refer to Table 1-2
range	specific EVTs in the specified EVT group such as '1+5+8-13'. An asterisk "*" displays all EVTs (including EVTs with a count of "0") for a specific EVT group or individual EVT.

Table 1-1 EVT Event Subsystems

memchk	Memory Check	**drmr**	DOCSIS Redundancy Manager SRM	**accdhc**	ACC DHCP
net	Network	**swr**	Switched Reload	**reg**	REG
ipevt	IP Event System	**tacacs**	TACACS+	**range**	Range
tpt	Testpoint Facility	**vrfmgr**	VRF Manager	**dpm**	Data Path Mapping
arp	ARP	**ipsec**	IPSEC	**dra**	DOCSIS Redundancy Agent
rpt	SRM Repeater	**sys**	SYS UTIL	**ubsha**	Upstream Scheduler RTR
im	Interface Manager	**snmpa**	SNMP Agent	**ubsbst**	Upstream Scheduler Burst
icp	ICP	**dsgmib**	SNMP DSG	**ubsmac**	UBS CMTS MAC RTR
evtm	EVT Manager	**bufmgr**	Buffer Manager	**ubs**	Upstream Scheduler
evta	EVT Agent	**eth8**	Ethernet Switch	**ubsim**	UBS IM SYNC
rmbind	RM Bind	**fei**	FEI	**ubsmap**	UBS MAP
rm	Resource Manager	**srpcmt**	SRM Reporter CMTS	**macmr**	MAC MGR
crmbpi	CRM BPI	**maccfg**	MAC CFG	**docsif**	DOCS IF
crm	CRM	**cmtbuf**	CMTS Buffer	**macrtr**	MACRTR
crmsub	CRM SubMgt	**fpga**	CMTS FPGA	**brgtag**	BRG TAG
crmfft	CRM FFT	**bcm**	Broadcom Driver	**brg**	BRG
crmsnr	CRM SNR	**bcmpkt**	Broadcam Driver Per Packet	**brgrtr**	BRG RTR
crmutl	CRM Util	**frm**	FRM	**spafft**	Spectrum Agent FFT
crmdtm	CRM DOCSTEST	**ard**	ARD	**spasnr**	Spectrum Agent SNR
crmcli	CRM CLI	**ardpkt**	ARD PKT	**rssi**	Spectrum Agent RSSI
crmdsg	CRM DSG	**que**	QUE Manager	**spasc**	Spectrum Agent SC
dsgif	DSG Interface	**upc**	Upconverter	**ardrtr**	ARD RTR
csm	Certificate Storage Module	**res**	RES	**acctrt**	ACC RTR
brmtag	BRM VLAN Tagging	**resrtr**	RES RTR	**btp**	Boot Uptime
rsm	Redundancy SRM	**resaut**	RES AUTH	**mcns**	MCNS
rdb	Run Time Database	**ressf**	RES SF	**red**	CMTS Redundancy ICP
fpevt	FP EVT	**resmgr**	RES MGR	**ucc**	Upstream Channel Change
spcmgr	Spectrum Manager	**lbm**	Load Balancing	**dcc**	Dynamic Channel Change
dgm	DQM	**lbm2**	Load Balancing 2nd Table	**dsx**	Dynamic Service
dqos	PacketCable DQOS	**lbmsnr**	Load Balacing SNR	**svcflo**	Service Flow
pcmm	PacketCable Multimedia	**cms**	Cable Modem Selector	**cra**	CRA
em	PacketCable Event Message	**acc**	ACC	**cra2**	CRA SNR
lbgmgr	Load Balance Manage	**accpkt**	ACC Packet	**bcm1**	Broadcom 3138 Driver
drm	DOCSIS Redundancy Manager			**bcmmac**	Broadcom 3212 Driver
drme	DOCSIS Redundancy Manager Engine			**pream**	Preamble
				upcmot	Upconverter Motorola

clear log

The **clear log** command deletes buffered log data.

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

clear log

clock set

The **clock set** command sets the system clock.

Group Access

System Administrator

Command Mode

Privileged EXEC

Command Line Usage

clock set <*hh:mm:ss*> {<*1-31*> <*MONTH*> | <*MONTH*> <*1-31*>} <*2000-2035*>

Command Syntax

hh:mm:ss	current time in 24-hour format
1-31	numeric notation for the current day
MONTH	three letter abbreviated name of the current month
2000-2035	numeric notation for the current year

clock timezone

The **clock timezone** command allows you to set the time zone for the system. The **no clock timezone** command changes the system time to Universal Time Coordinated (UTC).

Group Access

System Administrator

Command Mode

Global Configuration

Command Line Usage

clock timezone <*WORD* > <*Hours_offset*> [<*Minute_offset*>] [**daylightsavings**] [**on** | **off**]

no clock timezone

Note: The **daylightsavings** option has no effect on the setting of time on the BSR. It is present only to satisfy a requirement for Packetcable. Packetcable has a field in a network bound event message that must be set to whether or not daylight savings time is in effect. To satisfy this, the user must manually configure this parameter when daylight savings time begins and also when it ends. For automatic setting of the time, the BSR can be configured to obtain its time via SNTP (Simple Network Time Protocol). Since SNTP has no way of indicating whether daylight savings time is in effect, the operator must use the **daylightsavings** option for compliance with Packetcable.

Command Syntax

WORD	time zone listed when standard time is in effect
Hours_offset	hours corrected from UTC, range -23 to 23
Minute_offset	non-negative difference in minutes corrected from UTC, range 0 to 59
daylightsavings	configure daylight savings
on | **off**	daylight savings on or off

Command Default

UTC

configure

The **configure** command lets you enter Global Configuration mode from Privileged EXEC mode.

Note: To return to Privileged EXEC mode, enter **exit**, **end**, or **Control-Z** at the Global Configuration Mode prompt.

Group Access

All

Command Mode

Privileged EXEC

Command Line Usage

configure

console authentication radius

The **console authentication radius** command enables RADIUS authentication for user console logins. The **no console authentication radius** command disables this feature.

Group Access

System Administrator

Command Mode

Global Configuration

Command Line Usage

console authentication radius [**local-password** | **username** <*WORD*>]

no console authentication radius [**local-password** | **username**]

Command Syntax

local-password	authenticate with a locally configured password if there is no response from the RADIUS server
username	configure a console username to use for authentication
WORD	the text of the console username - maximum of 64 characters

copy

The **copy** command copies a local or network file from one location to another, either locally or on the network.

Group Access

System Administrator

Command Mode

Privileged EXEC

Command Line Usage

copy {**flash:** | **ftp:** | **nvram:** | **running-config** | **startup-config** | **system:** | **tftp:**} | {**flash:** | **nvram:** | **running-config** | **startup-config** | **system:**}

Command Syntax

flash:	copy the configuration file from flash
ftp:	copy the configuration file from a File Transport Protocol (FTP) server
nvram:	copy the configuration file from NVRAM
running-config	copy from a currently running system configuration
startup-config	copy from the startup configuration in NVRAM
system:	copy from the system
tftp:	copy the configuration file from a Trivial File Transport Protocol (TFTP) server
flash:	copy the configuration file to flash
ftp:	copy the configuration file to a File Transport Protocol (FTP) server

nvram:	copy the configuration file to NVRAM
running-config	copy to the currently running system configuration
startup-config	copy to the startup configuration in NVRAM
system:	copy to the system
tftp:	copy the configuration file to a Trivial File Transport Protocol (TFTP) server

delete

The **delete** command deletes a file stored in Flash memory or NVRAM or deletes the startup configuration file.

Group Access

System Administrator

Command Mode

Privileged EXEC

Command Line Usage

delete {**flash**: | **nvram:** | **startup-config**}

Command Syntax

flash:	delete all files from Flash memory
nvram:	delete all files from NVRAM
startup-config	delete the startup-configuration file

description

The **description** command is used to specify descriptive information for any interface on the BSR. This information is limited to 79 characters. Use the characters: _ or - to separate words. For example, if a particular CMTS interface served a certain section of a city, the MSO could assign the following description:

```
MOT(config-if)#description charlestown_1
```

Note: The entered description can be seen in the running configuration, and in the command output of **show** commands such as the **show ip interface** and **show running-config** commands.

You can also use SNMP to view the descriptions. However, if you use SNMP to view the descriptions, be aware that SNMP has a display limit of 63 characters. Descriptions beyond this length will appear truncated when viewed via SNMP.

Command Mode

Interface Configuration (all interface types)

Command Line Usage

description <*LINE*>

Command Syntax

LINE	is the text that describes this interface.

dir

The **dir** command lists directories and files on a filesystem.

Group Access

All

Command Mode

Privileged EXEC

Command Line Usage

dir [**all** [**time**]] [**flash:** [**time**]] [**nvram:** [**time**]] [**time**]

Command Syntax

all	list all directories and files
flash:	list all directories and files in flash
nvram:	list all directories and files in NVRAM
time	sort by modification time

Command Default

NVRAM

disable

The **disable** command allows you to enter User EXEC mode from the Privileged EXEC mode.

Note: To return to Privileged EXEC mode, enter **enable** at the User EXEC prompt and, if required, a password.

Group Access

System Administrator

Command Mode

Privileged EXEC

Command Line Usage

disable

duplex

The **duplex** command configures an Ethernet interface for duplex mode (full or half) and enables/disables auto-negotiation

Group Access

ISP

Command Mode

Interface Configuration (Ethernet interface only)

Command Line Usage

duplex {**half** | **full** | **auto**}

no duplex {**half** | **full** | **auto**}

Command Syntax

half	configures the interface for half-duplex operation. Half-duplex operation allows the interface to send and receive signals, but not at the same time.
full	configures the interface for full-duplex operation. Full-duplex operation allows the interface to send and receive signals at the same time.
auto	configures the interface to auto negotiate its operational mode (either full-duplex or half-duplex) with the device to which it is physically connected.

Command Default

Auto negotiation enabled

enable

The **enable** command allows you to enter Privileged EXEC mode from User EXEC mode. If the system prompts you for a password, enter the password. After entering Privileged EXEC mode, the prompt changes from the User EXEC mode prompt (**hostname>**) to the privileged EXEC mode prompt (**hostname#)**.

Group Access

System Administrator

Command Mode

User EXEC

Command Line Usage

enable

enable authentication radius

The **enable authentication radius** command enables RADIUS authentication for user logins. The **no enable authentication radius** command disables this feature.

Group Access

ISP

Command Mode

Global Configuration

Command Line Usage

enable authentication radius [**local-password**]

no enable authentication radius [**local-password**]

Command Syntax

local-password	authenticate with a locally configured password if there is no response from the RADIUS server

enable password

The **enable password** command allows you to specify a password associated with the **enable** command. After specifying the password, entering the **enable** command at the User EXEC prompt causes the system to prompt you for the password. You must supply the password to enter the Privileged EXEC mode. The **no enable password** command deletes the password.

Group Access

System Administrator

Command Mode

Global Configuration

Command Line Usage

enable password <*LINE*>

enable password {**0** | **7** } <*WORD*>

no enable password

Command Syntax

LINE	the password (31 character maximum) - enclosed with double quotes if the password contains spaces). The "%" and "!" characters must not be used.
0	specifies an UNENCRYPTED password
7	specifies a HIDDEN password
WORD	the UNENCRYPTED or HIDDEN 'enable' password

enable rdn-process

This **enable rdn-process** command enables the process for collecting CPU utilization statistics.The **no enable rdn-process** command disables the collection of CPU utilization statistics.

Note: This feature is enabled by default, and must remain enabled if you intend to use it in conjunction with SNMP polling of the BSR.

Group Access

System Administrator

Command Mode

Global Configuration

Command Line Usage

enable rdn-process

no enable rdn-process

Command Default

enabled

enable secret

The **enable secret** command allows you to provide an encrypted password that supersedes the enabled password. The **no enable secret** command removes the secret.

Use the **enable secret** command to provide an encrypted password for entering Privileged EXEC mode in the running configuration file when then **no service password-encryption** command is in effect.

Group Access

System Administrator

Command Mode

Global Configuration

Command Line Usage

enable secret [**5**] <*WORD*>

no enable secret

Command Syntax

5	specifies an ENCRYPTED secret
WORD	the secret (31 character maximum) - enclosed with double quotes if the secret contains spaces). The "%" and "!" characters must not be used.

encapsulation snap

The **encapsulation snap** command specifies SNAP as the encapsulation method for Ethernet or Gigabit Ethernet interfaces. The SNAP encapsulation method, as specified in RFC 1042, allows Ethernet protocols to run on the IEEE 802.2 media. The **no encapsulation snap** command returns the interface encapsulation method to the default method which is ARPA.

Group Access

All

Command Mode

Interface Configuration (Ethernet and Gigabit Ethernet notifies only)

Command Line Usage

encapsulation snap

no encapsulation snap

erase

The **erase** command erases a file system stored in Flash memory or NVRAM or the contents of the startup-configuration file.

Group Access

System Administrator

Command Mode

Privileged EXEC

Command Line Usage

erase {**flash**: | **nvram:** | **startup-config**}

Command Syntax

flash:	erase all files in Flash memory
nvram:	erase all files in NVRAM
startup-config	erase the startup-configuration file

exit

The **exit** command (used from the Router Configuration, Interface Configuration, and Global Configuration modes) accesses the previous command mode in the command mode hierarchy. For example: using the **exit** command in Interface Configuration mode accesses Global Configuration mode.

Using the **exit** command in Privileged EXEC or User EXEC modes, ends the command line session.

Group Access

All

Command Mode

All modes

Command Line Usage

exit

format

The **format** command formats a filesystem in flash or NVRAM.

Group Access

System Administrator

Command Mode

Privileged EXEC

Command Line Usage

format {**flash:** | **nvram:**}

Command Syntax

flash:	format flash
nvram:	format NVRAM

help

The **help** command displays instructions for using the CLI help functionality. Refer to the *BSR 2000 Configuration and Management Guide* for additional instructions on using the CLI help functionality.

Group Access

All

Command Mode

All modes

Command Line Usage

help

history size

The **history size** command lets you specify the size of the history buffer by number of lines. The **no history** command deletes the history buffer.

Group Access

All

Command Mode

All modes

Command Line Usage

history size *<1-256>*

no history

Command Syntax

1-256	the number of lines in the history buffer

Command Default

10

hostname

The **hostname** command configures the name for the system host.

Group Access

System Administrator

Command Mode

Global Configuration

Command Line Usage

hostname <*WORD*>

Command Syntax

WORD	the system's alphanumeric network hostname

ip ftp password

The **ip ftp password** command displays the password to use to connect to the network using FTP. The **no ip ftp password** command deletes the password for an FTP connection.

Group Access

System Administrator

Command Mode

Global Configuration

Command Line Usage

ip ftp password 0 <*LINE*>

ip ftp password 7 <*LINE*>

ip ftp password <*LINE*>

no ip ftp <*LINE*>

Command Syntax

0	specifies an unencrypted password will follow
7	specifies a hidden password will follow
LINE	the password (31 character minimum, 78 character maximum for option 7) - enclosed with double quotes if the password contains spaces). The "%" and "!" characters must not be used.

ip ftp username

The **ip ftp username** command configures the connection to the network for using FTP. The **no ip ftp username** command configures the router anonymously for FTP.

Use the **ip ftp username** command that is related to an account on the server.

Group Access

System Administrator

Command Mode

Global Configuration

Command Line Usage

ip ftp username <*WORD*>

no ip ftp username

Command Syntax

WORD	username (31 character maximum)

ip netmask-format

The **ip netmask-format** command lets you specify the format in which netmask values appear in show command output. The **no ip netmask format** command sets the output format back to the default.

Group Access

ISP

Command Mode

Global Configuration

Command Line Usage

ip netmask-format {**bitcount** | **decimal** | **hexadecimal**}

no ip netmask-format {**bitcount** | **decimal** | **hexadecimal**}

Command Syntax

bitcount	displays netmask as number of significant bits
decimal	displays netmask in dotted decimal
hexadecimal	displays the netmask in hexadecimal

Command Default

bitcount

ip tacacs source-interface

The **ip tacacs source-interface** command allows an operator to control the source IP address of TACACS+ packets generated by the BSR by specifying an Ethernet or loopback interface as the source IP address for TACACS+ packets. The normal convention for generated TACACS+ packets is to set the source IP address equal to the IP address of the outgoing interface. The **ip tacacs source-interface** command overrides this convention and instead uses the IP address of a specified Ethernet or loopback interface. This command facilitates the use of one IP address entry associated with the TACACS+ client instead of maintaining a list of all IP addresses and is useful in cases where the a router has many interfaces and an operator wants to ensure that all TACACS+ packets from a particular router have the same IP address.

The **no ip tacacs source-interface** command removes the specified source interface.

Note: Before using the **ip tacacs source-interface** command, the interface must be configured, assigned an IP address, and up and running. Any configuration change with this command will not take effect until after the next BSR connection attempt.

Group Access

System Administrator

Command Mode

Global Configuration

Command Line Usage

ip tacacs source-interface {**ethernet** <*X*/*Y*> | **loopback** <*1-64*>}

no ip tacacs source-interface

Command Syntax

ethernet *X*/*Y*	*X* is 0; *Y* is the port number
loopback *1-64*	the loopback interface number

ip tftp source-interface loopback

The **ip tftp source-interface loopback** command allows an operator to control the source IP address of TFTP packets generated by the BSR by specifying a loopback interface as the source IP address for TFTP packets. The normal convention for generated TFTP packets is to set the source IP address equal to the IP address of the outgoing interface. The **ip tftp source-interface loopback** command overrides this convention and instead uses the IP address of the specified loopback interface. The **no ip tftp source-interface loopback** command removes the loopback source interface.

Note: Before using the **ip tftp source-interface loopback** command, the loopback interface must be configured and assigned an IP address.

Group Access

System Administrator

Command Mode

Global Configuration

Command Line Usage

ip tftp source-interface loopback <*1-64*>

no ip tftp source-interface loopback

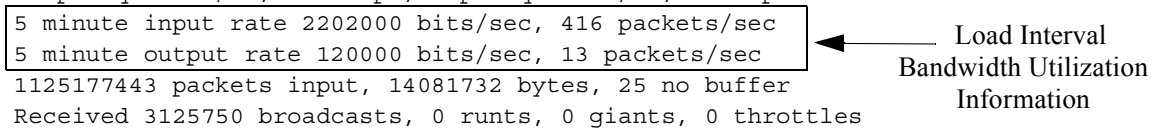
Command Syntax

1-64	the loopback interface number

load-interval

The **load-interval** command specifies the load interval timer value in minutes. The load interval timer captures bandwidth utilization information on a per-port basis for both received and transmitted data. Bandwidth utilization information can then be displayed with the **show interfaces** command. The following is typical load interval information as displayed with the **show interfaces** command:

```
Cable2/0 is up, line protocol is up
Hardware is BCM3210 ASIC, address is 0030.7b74.3238 (bia 0030.7b74.3238)
Internet address is 10.10.128.1/17
MTU 1500 bytes, BW 27000 Kbit, DLY 1000 usec,
reliability 255/255, txload 1/255, rxload 20/255
Encapsulation MCNS, loopback not set
Keepalive not set
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:00, output 00:00:00, output hang never
Last clearing of "show interface" counters never
Queueing strategy: fifo
Output queue 0/40, 69 drops; input queue 0/75, 7 drops
5 minute input rate 2202000 bits/sec, 416 packets/sec
5 minute output rate 120000 bits/sec, 13 packets/sec
1125177443 packets input, 14081732 bytes, 25 no buffer
Received 3125750 broadcasts, 0 runts, 0 giants, 0 throttles
1018 input errors, 87 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
25006326 packets output, 1183354279 bytes, 0 underruns
0 output errors, 0 collisions, 4 interface resets
0 output buffer failures, 0 output buffers swapped out
```



Group Access

All

Command Mode

Interface Configuration

Command Line Usage

load-interval <*1-300*>

Command Syntax

1-300	the load interval timer value in minutes

Command Default

5 minutes

logging

The **logging** command specifies the IP address of a remote SYSLOG server. The **no logging** command clears the IP address specification of a remote SYSLOG server.

Group Access

All

Command Mode

Global Configuration

Command Line Usage

logging <*A.B.C.D*>

no logging <*A.B.C.D*>

Command Syntax

A.B.C.D.	SYSLOG server IP address

logging admin-status

The **logging admin-status** command controls the transmission of traps and SYSLOG messages with respect to the threshold specified with the **logging rate-limit** command. The **logging admin-status** command is only relevant if DOCSIS logging control has been specified with the **logging control docsis** command.

In CLI logging control mode, the **logging admin-status** command will be ignored by the system and a warning message will display if it is used. In this mode, only the **logging rate-limit** command is relevant. In DOCSIS logging control mode, both the **logging admin-status** and **logging rate-limit** commands are needed to specify throttling.

Note: An event is always treated as a single event for threshold counting. For example: an event causing both a trap and a SYSLOG message is still treated as a one event.

Command Line Usage

logging admin-status {**inhibited** | **maintainBelowThreshold** | **stopAtThres** | **unconstrained**}

no logging admin-status {**inhibited** | **maintainBelowThreshold** | **stopAtThres** | **unconstrained**}

Command Syntax

inhibited	causes all trap transmission and SYSLOG messages to be suppressed - if a threshold has been specified with the **logging rate-limit** command, a warning message will be displayed
maintainBelowThreshold	causes trap transmission and SYSLOG messages to be suppressed if the number of traps/messages would exceed the threshold specified with the **logging rate-limit** command

stopAtThres	causes trap transmission SYSLOG messages to cease at the threshold specified with the **logging rate-limit** command - transmission will not resume until the **logging admin-status** command is reset to an option other than "stopAtThres" or the threshold is set to a higher value
unconstrained	causes all traps and SYSLOG messages to be transmitted - if a threshold has been specified with the **logging rate-limit** command, a warning message will be displayed

logging buffered

The **logging buffered** command sets the size of the logging buffer and the severity level. The **no logging buffered** command returns to the default buffer size (256 KB).

Note: Use the **show log** command, in Privileged EXEC mode, to display logged messages with the newest message displayed first.

Group Access

All

Command Mode

Global Configuration

Command Line Usage

logging buffered *<4096 -16777216>* [**alerts** | **critical** | **emergencies** | **errors** | **informational** | **notifications** | **warnings**]

no logging buffered *<4096 -16777216>* [**alerts** | **critical** | **emergencies** | **errors** | **informational** | **notifications** | **warnings**]

Command Syntax

4096 -16777216	logging buffer size in bytes

Severity Levels and Descriptions

emergencies	emergency conditions where the system is unusable - reserved for vendor-specific, fatal hardware or software errors that prevents normal system operation and causes reporting system to reboot (severity level = 0)
alert	conditions where immediate action is needed - a serious failure which causes the reporting system to reboot but is not caused by hardware or software malfunctioning (severity level = 1)

critical	critical conditions - a serious failure that requires immediate attention and prevents the device from transmitting data but the system could recover without rebooting (severity level = 2)
error	error conditions - a failure occurred that could interrupt the normal data flow (severity level = 3)
warnings	warning conditions - a failure occurred that could interrupt the normal data flow (severity level = 4)
notifications	normal but significant conditions - an event of importance occurred which is not a failure (severity level = 5)
information	informational descriptive system messages - an unimportant event, which could be helpful for tracing normal operations (severity level = 6)

Command Default

notifications, log file is 256 Kbytes

logging console

The **logging console** command enables the sending of system logging messages to the console. Additionally, the logging of messages displayed on the console terminal can be limited to a specified severity level. Use the **no logging console** command to disable console logging.

Group Access

All

Command Mode

Global Configuration

Command Line Usage

logging console [**alerts** | **critical** | **debugging** | **emergencies** | **errors** | **informational** | **notifications** | **warnings**]

no [**alerts** | **critical** | **debugging** | **emergencies** | **errors** | **informational** | **notifications** | **warnings**]

Command Syntax

Severity Levels and Descriptions

emergencies	emergency conditions where the system is unusable - reserved for vendor-specific, fatal hardware or software errors that prevents normal system operation and causes reporting system to reboot (severity level = 0)
alert	conditions where immediate action is needed - a serious failure which causes the reporting system to reboot but is not caused by hardware or software malfunctioning (severity level = 1)

critical	critical conditions - a serious failure that requires immediate attention and prevents the device from transmitting data but the system could recover without rebooting (severity level = 2)
error	error conditions - a failure occurred that could interrupt the normal data flow (severity level = 3)
warnings	warning conditions - a failure occurred that could interrupt the normal data flow (severity level = 4)
notifications	normal but significant conditions - an event of importance occurred which is not a failure (severity level = 5)
information	informational descriptive system messages - an unimportant event, which could be helpful for tracing normal operations (severity level = 6)

Command Default

notifications

logging control docsis

The **logging control docsis** command allows the DOCSIS *docsDevEvControlTable* to determine which severity logs go to which destinations.

Note: Any of the various **logging** <*destination*> <*severity*> commands in place are overridden with this command.

The **no logging control docsis** disables the *docsDevEvControlTable* and re-establishes CLI logging control. Any configurations previously set with the **logging** <*destination*> <*severity*> command will now control which severity logs go to which destinations.

Group Access

All

Command Mode

Global Configuration

Command Line Usage

logging control docsis

no logging control docsis

Command Default

no logging control docsis

logging default

The **logging default** command restores the default settings for all logging, including **logging** <*destination*> <*severity*>, **logging reporting**, and EVT configurations.

- The *docsDevEvControlTable* is restored to its DOCSIS-specified default values.
- CLI logging control is re-established.
- All **logging evt** configuration lines are removed from the running configuration file.
- Any **logging** <*A.B.C.D*> (for SYSLOG server) commands are unaffected.
- The **logging rate-limit** command is unaffected.
- The **logging buffered** <*size*> command is restored to its default size.
- The command restores the following entries to the running configuration file:

  no logging control docsis

  logging buffered notifications

  logging console error

  no logging trap

  no logging snmp-trap

  logging facility local7

Group Access

All

Command Mode

Global Configuration

Command Line Usage

logging default

logging disable bpi_auth_invalid_messages

The **logging disable bpi_auth_invalid_messages command** disables logging of the "BPI authorization invalid" DOCSIS error message. The **no logging disable bpi_auth_invalid_messages** enables the logging of this error message. This command is useful in situations where a high volume of this error message is being generated and logged.

Group Access

System Administrator

Command Mode

Global Configuration

Command Line Usage

logging disable bpi_auth_invalid_messages

no logging disable bpi_auth_invalid_message

Command Default

Logging of BPI authorization invalid messages is enabled by default.

logging disable bpi_auth_reject_messages

The **logging disable bpi_auth_reject_messages command** disables logging of the "BPI authorization reject" DOCSIS error message. The **no logging disable bpi_auth_reject_messages** enables the logging of this error message. This command is useful in situations where a high volume of this error message is being generated and logged.

Group Access

System Administrator

Command Mode

Global Configuration

Command Line Usage

logging disable bpi_auth_reject_messages

no logging disable bpi_auth_reject_messages

Command Default

Logging of BPI authorization reject messages is enabled by default.

logging disable bpi_map_reject_messages

The **logging disable bpi_map_reject_messages** command disables logging of the Map Reject DOCSIS error messages. The **no logging disable bpi_map_reject_messages** command enables the logging of Map Reject error messages. This command is useful in situations where large numbers of these error messages are being generated and logged.

Group Access

System Administrator

Command Mode

Global Configuration

Command Line Usage

logging disable bpi_map_reject_messages

no logging disable bpi_map_reject_messages

Command Default

Logging of Map Reject messages is enabled by default.

logging disable cm_ranging_fail_r103_0

The **logging disable cm_ranging_fail_r103_0** command disables logging of the "Unable to Successfully Range CM Retries Exhausted" DOCSIS error message. The **no logging disable cm_ranging_fail_r103_0** enables the logging of this error message. This command is useful in situations where a high volume of this error message is being generated and logged.

Group Access

System Administrator

Command Mode

Global Configuration

Command Line Usage

logging disable cm_ranging_fail_r103_0

no logging disable cm_ranging_fail_r103_0

Command Default

Logging of these error messages is enabled by default.

logging evt clear

The **logging evt clear** command disables logging of all EVTs or disables EVT logging for a specific logging destination (s). The **no logging evt clear** command restores the default EVT logging configuration.

Group Access

All

Command Mode

Global Configuration

Command Line Usage

logging evt clear {**l**|**t**|**s**|**c**} {<*slot*:*group*>} [<*range*>]

no logging evt clear {**l**|**t**|**s**|**c**} {<*slot*:*group*>} [<*range*>]

Command Syntax

l|**t**|**s**|**c**	the log message destination: l = local t = trap s = SYSLOG c = console
slot	this is always 0 for the BSR 2000
group	the name of an EVT group
range	specific EVTs in the specified EVT group such as '1+5+8-13'

logging evt set

The **logging evt set** command configures EVT logging to log messages to a different destination. The EVT messages logged can also be configured on a per-slot, per group, or single, per-event basis. The **no logging evt set** command with no specified EVT group name restores the original logging configuration changed with one or more **logging evt set** commands.

Command Line Usage

logging evt set {**l**|**t**|**s**|**c**} {<*slot*:*group*>} [<*range*>]

no logging evt set {**l**|**t**|**s**|**c**} {<*slot*:*group*>} [<*range*>]

Command Syntax

l|**t**|**s**|**c**	the log message destination: l = local t = trap s = SYSLOG c = console
slot	this is always 0 for the BSR 2000
group	the name of an EVT group
range	specific EVTs in the specified EVT group such as '1+5+8-13'

logging facility

The **logging facility** command specifies the SYSLOG facility to which error messages are sent. The **no logging facility** command reverts to the default of "local7".

Group Access

All

Command Mode

Global Configuration

Command Line Usage

logging facility {**local 0** | **local 1** | **local 2** | **local 3** | **local 4** | **local 5** | **local 6** | **local 7**}

no logging facility

Command Syntax

local 0-7	local facility 0 through 7

Command Default

local 7

logging on

The **logging on** command starts and stops the SYSLOG, and sends debug and error messages to a logging process. The **no logging on** command stops sending debug or error messages to a logging process.

Group Access

All

Command Mode

Global Configuration

Command Line Usage

logging on

no logging on

Command Default

Disabled

logging rate-limit

The **logging rate-limit** command limits the rate of system messages and SNMP traps logged per second. The **no logging rate-limit** command disables the rate limit.

Group Access

All

Command Mode

Global Configuration

Command Line Usage

logging rate-limit *<0-2147483647> <1-2147483647>*

no logging rate-limit

Command Syntax

0-2147483647	the number of logged messages
1-2147483647	the rate of messages logged per second

logging reporting

The **logging reporting** command specifies the recording mechanism for logging reports.

Group Access

All

Command Mode

Global Configuration

Command Line Usage

logging reporting {**alert | critical | debug | default | emergency | error | information | notice | warning**} {**all-clear | all-set | local | local-syslog | local-trap | local-trap-syslog**}

no logging reporting {**alert | critical | debug | default | emergency | error | information | notice | warning**} {**all-clear | all-set | local | local-syslog | local-trap | local-trap-syslog**}

Command Syntax

Severity Levels and Descriptions

emergency	emergency conditions where the system is unusable - reserved for vendor-specific, fatal hardware or software errors that prevents normal system operation and causes reporting system to reboot (severity level = 0)
alert	conditions where immediate action is needed - a serious failure which causes the reporting system to reboot but is not caused by hardware or software malfunctioning (severity level = 1)

critical	critical conditions - a serious failure that requires immediate attention and prevents the device from transmitting data but the system could recover without rebooting (severity level = 2)
error	error conditions - a failure occurred that could interrupt the normal data flow (severity level = 3)
warnings	warning conditions - a failure occurred that could interrupt the normal data flow (severity level = 4)
notice	normal but significant conditions - an event of importance occurred which is not a failure (severity level = 5)
information	informational descriptive system messages - an unimportant event, which could be helpful for tracing normal operations (severity level = 6)
debug	debugging messages (severity level = 7)
default	set all the severity levels to default

Logging Location Options

local	log messages to local-nonvolatile memory (NVRAM)
local-syslog	log messages to local NVRAM and the SYSLOG server
local-trap	log messages, excluding the specified trap level, to local NVRAM
local-trap-syslog	log messages, excluding the specified trap level, to local NVRAM and a SYSLOG server

all-clear	unsets all logging locations for the report.
all-set	sets all logging locations for the report.

Note: Debug messages will not be reported unless debugging has been turned on for a subsystem with the corresponding CLI **debug** command (e.g. **debug snmp**).

logging reporting default

The **logging reporting default** command is used to return to the default destination/ severity log reporting configuration.

Note: The default destination/severity log reporting configuration depends on which logging control mode is enabled.

Group Access

All

Command Mode

Global Configuration

Command Line Usage

logging reporting default

logging session

The **logging session** command enables the transmission of system logging messages to the current login session. The **no logging session** command disables the transmission of system logging messages to the current login session.

Group Access

All

Command Mode

Privileged EXEC

Command Line Usage

logging session

no logging session

logging snmp-trap

The **logging snmp-trap** command logs all SNMP traps or logs SNMP traps of a specified severity level and higher.

Note: The **logging snmp-trap** command limits SNMP trap logging to SNMP traps with a level up to and including the severity level specified with this command.

Group Access

All

Command Mode

Global Configuration

Command Line Usage

logging snmp-trap [**alerts** | **critical** | **emergencies** | **errors** | **informational** | **notifications** | **warnings**]

no logging snmp-trap [**alerts** | **critical** | **emergencies** | **errors** | **informational** | **notifications** | **warnings**]

Command Syntax

Severity Levels and Descriptions

emergencies	emergency conditions where the system is unusable - reserved for vendor-specific, fatal hardware or software errors that prevents normal system operation and causes reporting system to reboot (severity level = 0)
alert	conditions where immediate action is needed - a serious failure which causes the reporting system to reboot but is not caused by hardware or software malfunctioning (severity level = 1)

critical	critical conditions - a serious failure that requires immediate attention and prevents the device from transmitting data but the system could recover without rebooting (severity level = 2)
error	error conditions - a failure occurred that could interrupt the normal data flow (severity level = 3)
warnings	warning conditions - a failure occurred that could interrupt the normal data flow (severity level = 4)
notifications	normal but significant conditions - an event of importance occurred which is not a failure (severity level = 5)
information	informational descriptive system messages - an unimportant event, which could be helpful for tracing normal operations (severity level = 6)

logging source-interface loopback

The **logging source-interface loopback** command allows an operator to control the source IP address of SYSLOG packets generated by the BSR by specifying a loopback interface as the source IP address for SYSLOG packets. The normal convention for generated SYSLOG packets is to set the source IP address equal to the IP address of the outgoing interface. The **logging source-interface loopback** command overrides this convention and instead uses the IP address of the specified loopback interface. The **no logging source-interface loopback command removes the loopback source interface.**

Note: Before using the **logging source-interface loopback** command, the loopback interface must be configured and assigned an IP address.

Group Access

System Administrator

Command Mode

Global Configuration

Command Line Usage

logging source-interface loopback *<1-64>*

no logging source-interface loopback

Command Syntax

1-64	the loopback interface number

logging trap

The **logging trap** command filters messages logged to the SYSLOG servers based on severity. The command limits the log messages sent to a SYSLOG server to messages with a severity level up to and including the severity level specified with this command. The **no logging trap** command disables the logging of these messages to the SYSLOG servers.

Group Access

All

Command Mode

Global Configuration

Command Line Usage

logging trap {**alerts** | **critical** | **emergencies** | **errors** | **informational** | **notifications** | **warnings**}

no logging trap {**alerts** | **critical** | **emergencies** | **errors** | **informational** | **notifications** | **warnings**}

Command Syntax

Severity Levels and Descriptions

emergencies	emergency conditions where the system is unusable - reserved for vendor-specific, fatal hardware or software errors that prevents normal system operation and causes reporting system to reboot (severity level = 0)
alert	conditions where immediate action is needed - a serious failure which causes the reporting system to reboot but is not caused by hardware or software malfunctioning (severity level = 1)

critical	critical conditions - a serious failure that requires immediate attention and prevents the device from transmitting data but the system could recover without rebooting (severity level = 2)
error	error conditions - a failure occurred that could interrupt the normal data flow (severity level = 3)
warnings	warning conditions - a failure occurred that could interrupt the normal data flow (severity level = 4)
notifications	normal but significant conditions - an event of importance occurred which is not a failure (severity level = 5)
information	informational descriptive system messages - an unimportant event, which could be helpful for tracing normal operations (severity level = 6)

Command Default

notifications level (severity=5)

login

The **login** command logs a user on to the system.

Group Access

All

Command Mode

User EXEC

Command Line Usage

login [<*WORD*>]

Command Syntax

WORD	1 to 16 character username

logout

The **logout** command logs a user out of the system. Use the **logout** command to end the current session. The **logout** command is used the same way as the **exit** command.

In Privileged EXEC mode, use the **logout** command with a character argument to log a particular user out of the system. Only users with administrative privileges can log other users out.

Group Access

All

Command Mode

User EXEC and Privileged EXEC

Command Line Usage

logout [<*session-id*> | <*username*>] (Privileged EXEC mode only)

logout (User EXEC mode only)

Command Syntax

session-id	the session ID number of the user to log out
username	the name of the user to log out

macro

The **macro** command defines a group of existing CLI commands that can be executed by entering the macro name at the command line. The **no macro** command removes a macro from the macro list.

Group Access

All

Command Mode

All modes except User EXEC and Privileged EXEC

Command Line Usage

macro <*WORD*> {*Variable* | <*WORD*>} ... [*Variable* | <*WORD*>]}}

no macro <*WORD*>

Command Syntax

WORD	the macro name
Variable	macro variables
WORD	the CLI commands - CLI commands must be added one at a time

memory checkzero

The **memory checkzero** command enables memory checking on the BSR.

Note: Memory checking can use considerable BSR system resources.

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

memory checkzero <*0-1*>

Command Syntax

0-1	**1** = enable Memory Checking **0** = disable Memory Checking

message

The **message** command sends a message to a specified active user.

Group Access

System Administrator

Command Mode

Privileged EXEC

Command Line Usage

message <*WORD*> <*WORD*>

Command Syntax

WORD	session number or username
WORD	message to send

more

The **more** command displays the contents of a specified file.

Use the **more nvram:startup-config** command to view the startup configuration file in NVRAM. The *config_file* environmental table will be displayed if the startup configuration file is not displayed. The user can determine the status of the file which is either a complete or a distilled version of the configuration file.

Use the **more system:running-config** command to view the running configuration file. The **more system:running-config** command displays the version of the software and any changes that were previously made.

Note: You can use the **more** command to view files on remote systems.

Group Access

System Administrator

Command Mode

Privileged EXEC

Command Line Usage

more {**flash:** <*file*> | **ftp:** <*file*> | **nvram:** <*file*> | **nvram:startup-config** | **startup-config** | **system:startup-config** } [| {**begin** | **exclude** | **include**} {<*WORD*>}]

Command Syntax

file	file name
|	turns on output modifiers (filters)
begin	filter for output that begins with the specified string
exclude	filter for output that excludes the specified string

include	filter for output that includes the specified string
WORD	the specified string

network-clock-select bits e1

The **network-clock-select bits e1** command configures the BITS (network) clock. The **no network-clock-select bits** command deletes the network clock configuration and put the BITS clock in Free-run mode.

Group Access

ISP

Command Mode

Global Configuration

Command Line Usage

network-clock-select bits e1 {**pcm31-crc** | **pcm31-hdb3** | **pcm31-nocrc**}

no network-clock-select bits

Command Syntax

pcm31-crc	PCM-31 framing with AMI line coding, CRC Multiframe
pcm31-hdb3	PCM-31 framing with HDB3 line coding, CRC Multiframe
pcm31-nocrc	PCM-31 framing with AMI line coding, No CRC Multiframe

network-clock-select bits t1

The **network-clock-select bits t1** command configures the BITS (network) clock. The **no network-clock-select bits** command deletes the network clock configuration and put the BITS clock in Free-run mode.

Group Access

ISP

Command Mode

Global Configuration

Command Line Usage

network-clock-select bits t1 {**esf-b8zsc** | **sf-d4** | **slc96** | **t1dm**}

no network-clock-select bits

Command Syntax

esf-b8zs	ESF framing with B8ZS line coding
sf-d4	SF-D4 framing with AMI line coding
slc96	SLC96 framing with AMI line coding
t1dm	T1DM framing with AMI line coding

page

The **page** command controls the scrolling of system output displays.

Group Access

All

Command Mode

All modes

Command Line Usage

page {**off** | **on**}

Command Syntax

off	scrolling continues until the end of the display without stopping
on	controlled scrolling through the use of the Enter/Return key and spacebar

Command Default

on

password

The **password** command establishes a password that must be specified by users attempting to establish a console or telnet session with the BSR. A console or telnet session will not be established if the correct password is not specified by the user. The **no password** command removes the password.

Group Access

System Administrator

Command Mode

Global Configuration

Command Line Usage

password {**console** | **ssh-passphrase** | **telnet**}[**0** | **7**]<*WORD*>

no password {**console** | **ssh-passphrase** | **telnet**}

Command Syntax

console	password for console connections
ssh-passphrase	password for SSH connections
telnet	password for telnet connections
0	specifies an UNENCRYPTED password
7	specifies a HIDDEN password
WORD	the password (31 character maximum, 78 character maximum for option 7) - enclosed with double quotes if the key contains spaces). The "%" and "!" characters must not be used.

privilege restricted

The **privilege restricted** command designates a specific CLI command or group of commands as belonging to the "restricted" user group. Only users in the "restricted" user group have read-write access to commands designated as "restricted".

Note: By default, users in the "restricted" user group will not be able to execute any commands unless they have been specified as "restricted" with the **privilege restricted** command.

Group Access

All

Command Mode

Global Configuration

Command Line Usage

privilege restricted {<*WORD*> [<*...WORD*>] | **all**}

no privilege {<*WORD*> [<*...WORD*>] | **all**}

Command Syntax

WORD	the command whose privilege level is to be changed to "restricted" - multiple commands can be specified separated by spaces
all	changes the privilege level to "restricted" for all of the sub-options of a given command

radius-server

The **radius-server** command configures a RADIUS client to allow communication with a RADIUS server. Configuring a RADIUS client involves the following tasks:

- specifying the RADIUS server
- defining the shared encryption key for authentication between the RADIUS server and the RADIUS client
- specifying the number of retry attempts if there is no response from an active RADIUS server
- specifying the time interval between retry attempts if there is no response from from an active RADIUS server

Group Access

System Administrator

Command Mode

Global Configuration

Command Line Usage

radius-server host {<*A.B.C.D*>|<*Hostname*>} [**auth-port** <*0-65535*> [**primary**]]

radius-server key <*WORD*>

radius-server retransmit <*0-100*>

radius-server timeout <*1-1000*>

no radius-server host {<*A.B.C.D*>|<*Hostname*>} [**auth-port**]

no radius-server key

no radius-server retransmit

no radius-server timeout

Command Syntax

host	specifies a RADIUS server
A.B.C.D	the IP address of the RADIUS server

Hostname	the hostname of the RADIUS server
auth-port *0-65535*	specify a UDP port number for RADIUS authentication - default port number is 1812
primary	select this server as the primary RADIUS server
key *WORD*	text of the encryption key shared between the RADIUS client and the RADIUS servers - Motorola recommends a 22 character minimum
retransmit *0-100*	specify the number of retry attempts if there is no response from an active RADIUS server - default is 3 retries
timeout *1-1000*	specify the time interval in seconds between retry attempts if there is no response from from an active RADIUS server - default is 5 seconds

radius-server source-interface loopback

The **radius-server source-interface loopback** command allows an operator to control the source IP address of Radius authentication protocol packets generated by the BSR by specifying a loopback interface as the source IP address for Radius authentication protocol packets. The normal convention for generated Radius authentication protocol packets is to set the source IP address equal to the IP address of the outgoing interface. The **radius-server source-interface loopback** command overrides this convention and instead uses the IP address of the specified loopback interface. The **no radius-server source-interface loopback command removes the loopback source interface.**

Note: Before using the **radius-server source-interface loopback** command, the loopback interface must be configured and assigned an IP address.

Group Access

System Administrator

Command Mode

Global Configuration

Command Line Usage

radius-server source-interface loopback <*1-64*>

no radius-server source-interface loopback

Command Syntax

1-64	the loopback interface number

reload

The **reload** command reloads the operating system. The **reload** command is most often used to reload upgraded software.

Group Access

System Administrator

Command Mode

Privileged EXEC

Command Line Usage

reload [**at** <*hh:mm:*> <*LINE*> <*MONTH*> | **cancel** | **fast** | **in** {*countdown* [<*LINE*>]} | **reason** {<*LINE*>}]

Command Syntax

at	reloads at a specific time
hh:mm	specific hour and minute to reload
LINE	text of the reason to reload
MONTH	name of the month
cancel	cancels a pending reload
fast	reloads the system immediately
in	reloads after a time interval
countdown	time interval in *mm* or *hh:mm*
reason	specify a reason for reloading

repeat

The **repeat** command repeats a command or series of commands

Group Access

All

Command Mode

Privileged EXEC

Command Line Usage

repeat {<*NUM*>} {<*WORD*> [...<*WORD*>] | **delay** <*NUM*> {<*WORD*> [...<*WORD*>]}}

Command Syntax

NUM	the number of times to repeat the command or series of commands
WORD	the command or series of commands
delay *NUM*	the delay (in seconds) between the execution of each command

service password-encryption

The **service password-encryption** command enables password encryption. The **no service password-encryption** disables password encryption.

The **service password-encryption** command will also encrypt previously specified passwords in the running-config file that are currently unencrypted.

Note: Once passwords appearing in the running configuration file are encrypted, they cannot be unencrypted using the **no service password-encryption** command.

Group Access

System Administrator

Command Mode

Global Configuration

Command Line Usage

service password-encryption

no service password-encryption

Command Default

No encryption

session-timeout

The **session-timeout** command lets you specify the length of time (in minutes) before the BSR terminates any inactive session. An inactive session is a session has received no user input or system output during the specified time interval.

Group Access

System Administrator

Command Mode

Global Configuration

Command Line Usage

session-timeout {**console** | **telnet**} *<0-30>*

Command Syntax

console	specifies console sessions
telnet	specifies telnet sessions
0-30	length of time in minutes before the session is terminated automatically by the BSR

Command Default

5 minutes for telnet sessions

0 for console sessions (session maintained indefinitely)

session-window set

The **session-window set** command specifies the height and width parameters of the current CLI session window.

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

session-window set {**height** <*4-128*> | **width** <*16-384*>}

Command Syntax

height *4-128*	sets window height in number of lines
width *16-384*	sets window width in number of columns

show aliases

The **show aliases** command displays any one of the following:

- Aliases for commands in all modes
- Aliases for commands in a specific mode.
- Aliases for all commands that begin with, include, or exclude a specified string.
- Aliases for a specific mode that begin with, include, or exclude a specified string.

Group Access

All

Command Mode

All except User EXEC

Command Line Usage

show alias [**all** | **conf** | **exec** | **priv**] [| {**begin** | **exclude** | **include**} {<*WORD*>} | {**count** | **count-only**}]

show alias [**all** | **conf** | **exec** | **priv**] [| {**count** | **count-only**}]

Command Syntax

all	Alias visible in all modes
conf	specifies aliases for Global Configuration mode
exec	specifies aliases for User EXEC mode
priv	specifies aliases for Privileged EXEC mode
|	turns on output modifiers (filters)
begin	filter for output that begins with the specified string
exclude	filter for output that excludes the specified string

include	filter for output that includes the specified string
WORD	the specified string
count	count the number of outputted lines
count-only	count the number of lines while suppressing screen output

show boot

The **show boot** command lists the boot parameters. Use the **show boot** command to display the contents of the BOOT environment variables and the configuration register setting.

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show boot [| {**begin** | **exclude** | **include**} {<*WORD*>} | {**count** | **count-only**}]

show boot [| {**count** | **count-only**}]

Command Syntax

|	turns on output modifiers (filters)
begin	filter for output that begins with the specified string
exclude	filter for output that excludes the specified string
include	filter for output that includes the specified string
WORD	the specified string
count	count the number of outputted lines
count-only	count the number of lines while suppressing screen output

show clock

The **show clock** command shows the system clock.

Group Access

All

Command Mode

All modes

Command Line Usage

show clock [| {**begin** | **exclude** | **include**} {<*WORD*>} | {**count** | **count-only**}]

show clock [| {**count** | **count-only**}]

Command Syntax

|	turns on output modifiers (filters)
begin	filter for output that begins with the specified string
exclude	filter for output that excludes the specified string
include	filter for output that includes the specified string
WORD	the specified string
count	count the number of outputted lines
count-only	count the number of lines while suppressing screen output

show evt

The **show evt** command displays EVT counts for all EVT groups, a specific EVT group, EVT group counts that only occur on a specific BSR slot, or individual event. By default, only EVT groups with non-zero event counts are displayed. The following is an example of typical screen output from the **show evt** command:

```
Slot 0: CRA    - Cra event system                EVT Base : 4608
   Num   Title                                    Count      Sv Logging
   ---   ---------------------------------------  ---------- -- --------
   1     rcvd crm msg                                    144 D
   14    Received CA Certificate SET request               3 D
   18    Sent GET CA Cert. message to CRM                  1 D
   23    cmtsSendCrmCmAdd                                 12 D
   24    cmtsSendCrmCmDel                                  8 D
   25    cmtsSendCrmCmReg                                 12 D


Slot 0: MACCFG - macCfg event system             EVT Base : 9984
   Num   Title                                    Count      Sv Logging
   ---   ---------------------------------------  ---------- -- --------
   1     Flap tree add success                             3 D
   3     Flap tree delete success                          3 D
   8     FlapListAdd success                               3 D
   10    FlapListDel success                               3 D
   15    FlapListAgeout success                            2 D
   18    set cmh flap rowstatus to active                  3 D
   19    set cmh flap rowstatus to destroy                 3 D
   22    set cmh flap mac addr                             4 D
```

In addition to the BSR 2000 slot number, EVT group name, and EVT base number, the following information is displayed

Num	the EVT number - EVTs are numbered from 1 to 255 (maximum)
Title	the title of the individual event

Count	the number of times the EVT has occurred since the count was last reset
Sv	the severity level of the event - in order of increasing severity, the abbreviations are: D = Debug I = Informational N = Notice W = Warning E = Error C = Critical A = Alert E = Emergency
Logging	indicates to which logging subsystems EVT messages are forwarded: L = Local log file T = Trap to SNMP S = SYSLOG C = Console

Group Access

All

Command Mode

All modes

Command Line Usage

show evt [<*NUM*> | <*WORD*>] [<*range*>]

Command Syntax

NUM	this is always 0 for the BSR 2000
WORD	the name of an EVT group - refer to Table 1-2
range	specific EVTs in the specified EVT group such as '1+5+8-13'. An asterisk "*" displays all EVTs (including EVTs with a count of "0") for a specific EVT group or individual EVT.

Table 1-2 EVT Event Subsystems

memchk	Memory Check	**drmr**	DOCSIS Redundancy Manager SRM	**accdhc**	ACC DHCP
net	Network			**reg**	REG
ipevt	IP Event System	**swr**	Switched Reload	**range**	Range
tpt	Testpoint Facility	**tacacs**	TACACS+	**dpm**	Data Path Mapping
arp	ARP	**vrfmgr**	VRF Manager	**dra**	DOCSIS Redundancy Agent
rpt	SRM Repeater	**ipsec**	IPSEC		
im	Interface Manager	**sys**	SYS UTIL	**ubsha**	Upstream Scheduler RTR
icp	ICP	**snmpa**	SNMP Agent	**ubsbst**	Upstream Scheduler Burst
evtm	EVT Manager	**dsgmib**	SNMP DSG	**ubsmac**	UBS CMTS MAC RTR
evta	EVT Agent	**bufmgr**	Buffer Manager	**ubs**	Upstream Scheduler
rmbind	RM Bind	**eth8**	Ethernet Switch	**ubsim**	UBS IM SYNC
rm	Resource Manager	**fei**	FEI	**ubsmap**	UBS MAP
crmbpi	CRM BPI	**srpcmt**	SRM Reporter CMTS	**macmr**	MAC MGR
crm	CRM	**maccfg**	MAC CFG	**docsif**	DOCS IF
crmsub	CRM SubMgt	**cmtbuf**	CMTS Buffer	**macrtr**	MACRTR
crmfft	CRM FFT	**fpga**	CMTS FPGA	**brgtag**	BRG TAG
crmsnr	CRM SNR	**bcm**	Broadcom Driver	**brg**	BRG
crmutl	CRM Util	**bcmpkt**	Broadcam Driver Per Packet	**brgrtr**	BRG RTR
crmdtm	CRM DOCSTEST			**spafft**	Spectrum Agent FFT
crmcli	CRM CLI	**frm**	FRM	**spasnr**	Spectrum Agent SNR
crmdsg	CRM DSG	**ard**	ARD	**rssi**	Spectrum Agent RSSI
dsgif	DSG Interface	**ardpkt**	ARD PKT	**spasc**	Spectrum Agent SC
csm	Certificate Storage Module	**que**	QUE Manager	**ardrtr**	ARD RTR
		upc	Upconverter	**acctrt**	ACC RTR
brmtag	BRM VLAN Tagging	**res**	RES	**btp**	Boot Uptime
rsm	Redundancy SRM	**resrtr**	RES RTR	**mcns**	MCNS
rdb	Run Time Database	**resaut**	RES AUTH	**red**	CMTS Redundancy ICP
fpevt	FP EVT	**ressf**	RES SF	**ucc**	Upstream Channel Change
spcmgr	Spectrum Manager	**resmgr**	RES MGR	**dcc**	Dynamic Channel Change
dgm	DQM	**lbm**	Load Balancing	**dsx**	Dynamic Service
dqos	PacketCable DQOS	**lbm2**	Load Balancing 2nd Table	**svcflo**	Service Flow
pcmm	PacketCable Multimedia			**cra**	CRA
em	PacketCable Event Message	**lbmsnr**	Load Balacing SNR	**cra2**	CRA SNR
		cms	Cable Modem Selector	**bcm1**	Broadcom 3138 Driver
lbgmgr	Load Balance Manage			**bcmmac**	Broadcom 3212 Driver
drm	DOCSIS Redundancy Manager	**acc**	ACC	**pream**	Preamble
		accpkt	ACC Packet	**upcmot**	Upconverter Motorola
drme	DOCSIS Redundancy Manager Engine				

show history

The **show history** command displays a list of commands executed during a session. The list size is determined by the setting of the **history size** command.

Group Access

All

Command Mode

All modes

Command Line Usage

show history [| {**begin** | **exclude** | **include**} {<*WORD*>} | {**count** | **count-only**}]

show history [| {**count** | **count-only**}]

Command Syntax

|	turns on output modifiers (filters)
begin	filter for output that begins with the specified string
exclude	filter for output that excludes the specified string
include	filter for output that includes the specified string
WORD	the specified string
count	count the number of outputted lines
count-only	count the number of lines while suppressing screen output

show log

The **show log** command displays message logging in the log file the newest message first.The **show log** command displays log file contents and information about users who have logged into the BSR. The following is an example of typical screen output from the **show log** command:

```
Preparing log file for reading ...
[02/11-10:39:08- 07:telnet01]-N-user enabled-user authenticated
[02/11-10:39:04- 07:telnet01]-N-connection made from 10.14.11.218 on session 01
[02/10-18:41:11- 07:RMs]-N-Module state RUNNING CMTS slot 1
[02/10-18:41:11- 07:RMs]-I-Slot 1 booted with version 2.1.0T00P39.KRBU
[02/10-18:41:09- 07:SPECMGR]-N-No shut down succeed for channel ifIndex = 98561
.
[02/10-18:41:09- 07:CRMTASK]-N-link up notification, ifIndex = 98561.
[02/10-18:41:08- 07:CRMTASK]-N-link up notification, ifIndex = 98305.
[02/10-18:41:08- 07:IM]-N-IP Interface cable 1/0 on 150.31.41.1 is up
[02/10-18:41:08- 07:IM]-N-Interface cable 1/0 is up
[02/10-18:41:07- 07:RMsc]-N-configuration change by [hotswapper]: cable downstre
am schedule priority-wfq
[02/10-18:41:07- 07:RMsc]-I-restoring:  cable downstream schedule priority-wfq
[02/10-18:41:07- 07:RMsc]-E-bad return value 0 from parse() in loadInterfaceConf
iguration(), for config line:' cable dynamic-service authorization-mode disable'
[02/10-18:41:07- 07:RMsc]-I-restoring:  cable dynamic-service authorization-mode
 disable
[02/10-18:41:07- 07:RMsc]-N-configuration change by [hotswapper]: cable upstream
 3 shutdown
[02/10-18:41:07- 07:RMsc]-I-restoring:  cable upstream 3 shutdown
[02/10-18:41:07- 07:RMsc]-N-configuration change by [hotswapper]: cable upstream
 2 shutdown
[02/10-18:41:07- 07:RMsc]-I-restoring:  cable upstream 2 shutdown
[02/10-18:41:07- 07:RMsc]-N-configuration change by [hotswapper]: cable upstream
 1 shutdown
[02/10-18:41:07- 07:RMsc]-I-restoring:  cable upstream 1 shutdown
[02/10-18:41:07- 07:RMsc]-N-configuration change by [hotswapper]: no cable upstr
eam 0 shutdown
[02/10-18:41:07- 07:RMsc]-I-restoring:  no cable upstream 0 shutdown
[02/10-18:41:07- 07:RMsc]-N-configuration change by [hotswapper]: cable upstream
```

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show log [| {**begin** | **exclude** | **include**} {<*WORD*>} [| {**count** | **count-only**}]]

show log [| {**count** | **count-only**}]

Command Syntax

|	turns on output modifiers (filters)
begin	filter for output that begins with the specified string
exclude	filter for output that excludes the specified string
include	filter for output that includes the specified string
WORD	the specified string
count	count the number of outputted lines
count-only	count the number of lines while suppressing screen output

show logging evt

The **show logging evt** command displays the EVT configuration entries in the running configuration file. The following is an example of typical screen output from the **show logging evt** command:

```
EVT RUNNING CONFIG:
logging evt set c drme 82
logging evt set c rdb 197
logging evt set c dra 121
```

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show logging evt

show logging reporting

The **show logging reporting** command displays the recording mechanism for logging messages based on their severity level. The display output is in the format: **logging reporting** <*severity*> <*logging location*> e.g. logging reporting alert local. The following is an example of typical screen output from the **show logging reporting** command:

```
no logging control docsis
logging reporting emergency local
logging reporting alert local
logging reporting critical local-trap-syslog
logging reporting error local-trap-syslog
logging reporting warning local-trap-syslog
logging reporting notice local-trap-syslog
logging reporting information all-clear
logging reporting debug all-clear
```

The following information is displayed:

Severity Levels and Descriptions

emergency	emergency conditions where the system is unusable - reserved for vendor-specific, fatal hardware or software errors that prevents normal system operation and causes reporting system to reboot (severity level = 0)
alert	conditions where immediate action is needed - a serious failure which causes the reporting system to reboot but is not caused by hardware or software malfunctioning (severity level = 1)
critical	critical conditions - a serious failure that requires immediate attention and prevents the device from transmitting data but the system could recover without rebooting (severity level = 2)

error	error conditions - a failure occurred that could interrupt the normal data flow (severity level = 3)
warnings	warning conditions - a failure occurred that could interrupt the normal data flow (severity level = 4)
notice	normal but significant conditions - an event of importance occurred which is not a failure (severity level = 5)
information	informational descriptive system messages - an unimportant event, which could be helpful for tracing normal operations (severity level = 6)
debug	debugging messages (severity level = 7)
default	set all the severity level to default

Logging Location Options

local	log messages for the report go to local-nonvolatile memory (NVRAM)
local-syslog	log messages for the report go to local NVRAM and the SYSLOG server
local-trap	log messages for the report go to local NVRAM. SNMP traps are also sent to an SNMP manager
local-trap-syslog	log messages for the report go to local NVRAM and a SYSLOG server - SNMP traps are also sent to an SNMP manager
all-clear	unsets all logging locations for the report
all-set	sets all logging locations for the report

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show logging reporting

show logging syslog

The **show logging syslog** command displays a counter of the total number of log messages sent to the SYSLOG server and the number of messages dropped if a logging threshold has been exceeded.

The following is an example of typical screen output from the **show logging syslog** command:

```
Syslog Messages Sent:                       654
Syslog Messages Dropped due to throttling: 0
```

The following information is displayed:

Syslog Messages Sent:	the number of log messages logged to the SYSLOG server
Syslog Messages Dropped due to throttling:	the number of log messages that were to be logged to the SYSLOG server but were discarded because the threshold set with the **logging rate-limit** command was exceeded

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show logging syslog

show macro

The **show macro** command lists all configured macros on the BSR.

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show macro [| {**begin** | **exclude** | **include**} {<*WORD*>} [| {**count** | **count-only**}]]

show macro [| {**count** | **count-only**}}]

Command Syntax

|	turns on output modifiers (filters)
begin	filter for output that begins with the specified string
exclude	filter for output that excludes the specified string
include	filter for output that includes the specified string
WORD	the specified string
count	count the number of outputted lines
count-only	count the number of lines while suppressing screen output

show memory

The **show memory** command displays the memory content of the starting address. Use the **show memory** command to view information about memory available after the system image decompresses and loads.

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show memory [<*address*> <*1-4294967295*> | **byte** | **end** <*address*> | **long** | **short**] [**information** [**brief**]] [| {**begin** | **exclude** | **include**} {<*WORD*>} [| {**count** | **count-only**}]]

show memory [<*address*> <*1-4294967295*> | **byte** | **end** <*address*> | **long** | **short**] [**information** [**brief**]] [| {**count** | **count-only**}]]

Command Syntax

address	the starting memory address expressed in hexadecimal notation
1-4294967295	the number of bytes to dump
byte	display in byte format
end	the ending memory address expressed in hexadecimal notation
long	display in long format
short	display in short format
brief	display only the summary
information	displays free memory statistics and a summary of memory usage
|	turns on output modifiers (filters)

begin	filter for output that begins with the specified string
exclude	filter for output that excludes the specified string
include	filter for output that includes the specified string
WORD	the specified string
count	count the number of outputted lines
count-only	count the number of lines while suppressing screen output

Command Default

32 bit

show network-clocks

The **show network-clocks** command displays the current BITS clock state and alarms.

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show network-clocks

show pool

The **show pool** command displays information on data buffering including all memory buffer pools, application-specific pools, the network pool, system physical structures, and all mBuf pool names.

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show pool [<*WORD*> | **all** | **application** | **names** | **network** | **system**] [| {**begin** | **exclude** | **include**} {<*WORD*>} [| {**count** | **count-only**}]]

show pool [<*WORD*> | **all** | **application** | **names** | **network** | **system**] [| {**count** | **count-only**}]

Command Syntax

WORD	the name of the buffer pool
all	view all memory buffer pools
application	view all application-specific pools
names	view the network pool where network data transfer information for the stack is located
network	view the network pool where network data transfer information for the stack is located
system	view system pool physical structures such as the number of sockets, routes, interface addresses, PCB, and multicast addresses
|	turns on output modifiers (filters)
begin	filter for output that begins with the specified string

exclude	filter for output that excludes the specified string
include	filter for output that includes the specified string
WORD	the specified string
count	count the number of outputted lines
count-only	count the number of lines while suppressing screen output

show process

The **show process** command displays information about software processes that are running on the router.

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show process [**cpu** | **memory** | **msg-q-info** | **semaphores** | **stack**] [| {**begin** | **exclude** | **include**} {<*WORD*>} [| {**count** | **count-only**}]]

show process [**cpu** | **memory** | **msg-q-info** | **semaphores** | **stack**] [| {**count** | **count-only**}]

Command Syntax

cpu	cpu utilization by each process
memory	memory information per process
msg-q-info	information about current message queues
semaphores	display state of semaphore(s)
stack	process stack usage and interrupt routines, including the reason for the last system reboot
|	turns on output modifiers (filters)
begin	filter for output that begins with the specified string
exclude	filter for output that excludes the specified string
include	filter for output that includes the specified string
WORD	the specified string

count	count the number of outputted lines
count-only	count the number of lines while suppressing screen output

show process cpu

The **show process cpu** command displays detailed CPU usage statistics for the BSR 2000. The module type (for example: `1x4 CMTS slot <NUM>`) is displayed along with the CPU usage statistics for that module. For HSIM modules, the module sub type (for example: `Sub Type: SMGE`) is displayed.

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show process cpu [**frequency** *<30-200>* | **restart | stop**] [| {**begin** | **exclude** | **include**} {*<WORD>*} [| {**count** | **count-only**}]]

show process cpu [**frequency** *<30-200>* | **restart | stop**] [| {**count** | **count-only**}]

Command Syntax

frequency *30-200*	how many times per second a CPU statistic measurement is taken in 30-200 Hz
restart	restart the utilization measurement process on the BSR 2000
stop	stops the utilization measurement process
|	turns on output modifiers (filters)
begin	filter for output that begins with the specified string
exclude	filter for output that excludes the specified string
include	filter for output that includes the specified string
WORD	the specified string

count	count the number of outputted lines
count-only	count the number of lines while suppressing screen output

Command Default

frequency = 60 Hz

show process memory

The **show process memory** command displays per process memory usage information about software processes that are running on the BSR. The following screen output is displayed:

```
NAME                 TID STATUS      Memory Requested  Overhead   HW mark
--------------- --------- -------- --------- --------- --------- ---------
tRootTask         bfffdf8          61713912  61706523      7389  61713936
tShell            aeea888 PEND         3248      2981       267      3248
ctrlMon           aeb20e8 PEND          152       128        24       152
tCmdHdlQ          ae92450 READY        3712      3548       164     14016
tLogTask          aeb7308 PEND+T        136       108        28       136
DiagTask          ac2fd28 PEND         1928      1856        72      1928
redMonitorTask    ac2d2a0 DELAY      379008    378976        32    379008
redSyncMsgTask    ac2c018 DELAY      380664    380584        80    380664
redIcpTask        ac2ad90 PEND       380696    380600        96    380696
redSTSIHTask      ac28a70 PEND           48        32        16        48
IcpTask           ac42d78 READY       65832     65772        60     74528
tEVTA             ac3d3f0 PEND         2952      2920        32      4440
StatsMgrTask      ac32dd8 PEND+T        528       464        64       528
tUpc              aafe4d0 PEND         1680      1616        64     12520
fpgaDsTask        908f280 READY          48        32        16        48
tDftTask          908a570 DELAY          48        32        16        48
tArdTim           8583fb8 DELAY          48        32        16        48
dpsDsTask         8582b00 PEND          104        60        44     16144
resMgrTask        853e440 PEND        22240     22072       168     22768
tSftTask          853c088 PEND           48        32        16        48
tUbs              8446a40 READY       563368    562880       488    563896
tMcns2            8436000 PEND           48        32        16        48
tMacTask          842a5c0 READY     34793632  34792500      1132  34795744
rdnBpiMain        843e7b8 PEND+T     4048960   4048228       732   4048960
tMcnsLogTask      8434de0 PEND          6344      6284        60      6344
tRcyc             84223a0 READY          352       288        64       352
tCmacStats        8420180 PEND        262440    262368        72    262440
tSrmReporter      841df60 PEND+T         112        80        32       112
tRLimit           841bd40 DELAY          352       288        64       352
tMacRtr           8419b20 PEND        409352    408640       712    409880
tAccDhcp          8293c48 DELAY          48        32        16        48
tSPA              8292a28 PEND        148232    148188        44    148232
tDra              8286e18 PEND+T      184224    183832       392    185280
tCRA              5c26998 PEND        395976    395784       192    396632
tDownloadTask     5bbc540 PEND         15528     15480        48     15528
tRdb005           5bb1eb0 PEND+T       16352     16216       136     16880
tMcnsTask         842c7e0 READY           56        28        28        56

 37 tasks used                    103802408 103789516     12892
```

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show process memory {<*process-id*> [**bytes** | **kilobytes** | **megabytes**]} | {<*process-name***>** [**bytes** | **kilobytes** | **megabytes**]} {**sorted** [**bytes** | **high-water-mark** [**bytes** | **kilobytes** | **megabytes**] | **kilobytes** | **megabytes** | **name** [**bytes** | **kilobytes** | **megabytes**] | **no-sort** [**bytes** | **kilobytes** | **megabytes**] | **use** [**bytes** | **kilobytes** | **megabytes**]} [| {**begin** | **exclude** | **include**} {<*WORD*>} [| {**count** | **count-only**}]]

show process memory {<*process-id*> [**bytes** | **kilobytes** | **megabytes**]} | {<*process-name***>** [**bytes** | **kilobytes** | **megabytes**]} {**sorted** [**bytes** | **high-water-mark** [**bytes** | **kilobytes** | **megabytes**] | **kilobytes** | **megabytes** | **name** [**bytes** | **kilobytes** | **megabytes**] | **no-sort** [**bytes** | **kilobytes** | **megabytes**] | **use** [**bytes** | **kilobytes** | **megabytes**]} [| {**count** | **count-only**}]

Command Syntax

process-id	A process identifier in hexadecimal format
bytes	Display total sizes in bytes
kilobytes	Display total sizes in kilobytes
megabytes	Display total sizes in megabytes
process-name	The alphanumeric process name up to 15 characters
sorted	Display sorted memory information for all processes
high-water-mark	Sort by maximum memory used
name	Sort by name
no-sort	Display the first memory request order

use	Sort by memory used now
|	turns on output modifiers (filters)
begin	filter for output that begins with the specified string
exclude	filter for output that excludes the specified string
include	filter for output that includes the specified string
WORD	the specified string
count	count the number of outputted lines
count-only	count the number of lines while suppressing screen output

Command Defaults

All display output is shown in bytes

Sorting is disabled

show process msg-q-info

The **show process msg-q-info** command displays information about current message queues.

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show process msg-q-info [| {**begin** | **exclude** | **include**} {<*WORD*>} [| {**count** | **count-only**}]]

show process msg-q-info [| {**count** | **count-only**}]

Command Syntax

|	turns on output modifiers (filters)
begin	filter for output that begins with the specified string
exclude	filter for output that excludes the specified string
include	filter for output that includes the specified string
WORD	the specified string
count	count the number of outputted lines
count-only	count the number of lines while suppressing screen output

show process semaphores

The **show process semaphores** command creates a message when an attempt to unlock a semaphore when it is already unlocked.

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show process semaphores [| {**begin** | **exclude** | **include**} {<*WORD*>} [| {**count** | **count-only**}]]

show process semaphores [| {**count** | **count-only**}]

Command Syntax

|	turns on output modifiers (filters)
begin	filter for output that begins with the specified string
exclude	filter for output that excludes the specified string
include	filter for output that includes the specified string
WORD	the specified string
count	count the number of outputted lines
count-only	count the number of lines while suppressing screen output

show process stack

The **show process stack** command monitors the stack utilization of processes and interrupt routines.

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show process stack [**procID** | **procName**] [| {**begin** | **exclude** | **include**} {<*WORD*>} [| {**count** | **count-only**}]]

show process stack [**procID** | **procName**] [| {**count** | **count-only**}]

Command Syntax

procID	process identifier in decimal or hexadecimal format (0x is required)
procName	the name of the process
|	turns on output modifiers (filters)
begin	filter for output that begins with the specified string
exclude	filter for output that excludes the specified string
include	filter for output that includes the specified string
WORD	the specified string
count	count the number of outputted lines
count-only	count the number of lines while suppressing screen output

show reload

The **show reload** command displays the status of a Hitless Upgrade in progress after a software reload of all modules in the BSR chassis has been initiated with the **reload switched** command.

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show reload

show running-config

The **show running-config** command displays configuration information currently running on the BSR.

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show running-config [**interface** [**cable** <*X*/*Y*> **ethernet** <*X*/*Y*> | **gigaether** <*X*/*Y*> | **loopback** <*1-64*>]] [| {**begin** | **exclude** | **include**} {<*WORD*>} [| {**count** | **count-only**}]]

show running-config [**interface** [**cable** <*X*/*Y*> **ethernet** <*X*/*Y*> | **gigaether** <*X*/*Y*> | **loopback** <*1-64*>]] [| {**count** | **count-only**}]

show running-config [**bgp** | **verbose**] [| {**begin** | **exclude** | **include**} {<*WORD*>} [| {**count** | **count-only**}]]

show running-config [**bgp** | **verbose**] [| {**count** | **count-only**}]

Command Syntax

interface	display running configuration information on all interfaces or a specific interface card
cable *X*/*Y*	*X* is 0. *Y* is the cable port number on the BSR.
ethernet *X*/*Y*	*X* is 0. *Y* is the Ethernet/Fast Ethernet IEEE 802.3 port number on the BSR.
gigaether *X*/*Y*	*X* is 0. *Y* is the Gigabit Ethernet port number on the BSR.
loopback *1-64*	the loopback interface number
bgp	Border Gateway Protocol parameters
verbose	runs the show running-config command in verbose mode

|	turns on output modifiers (filters)
begin	filter for output that begins with the specified string
exclude	filter for output that excludes the specified string
include	filter for output that includes the specified string
WORD	the specified string
count	count the number of outputted lines
count-only	count the number of lines while suppressing screen output

show startup-config

The **show startup-config** command displays the contents of the system startup configuration file.

Group Access

All

Command Mode

Privileged EXEC

Command Line Usage

show startup-config [| {**begin** | **exclude** | **include**} {<*WORD*>} [| {**count** | **count-only**}]]

show startup-config [| {**count** | **count-only**}]

Command Syntax

|	turns on output modifiers (filters)
begin	filter for output that begins with the specified string
exclude	filter for output that excludes the specified string
include	filter for output that includes the specified string
WORD	the specified string
count	count the number of outputted lines
count-only	count the number of lines while suppressing screen output

show stats summary error

The **show stats summary error** command displays FEC error counts and ratios. The following is an example of typical screen output from the **show stats summary error** command:

```
MAC Address       I/F     SID    CorrFec    CorrFec      UnCorrFec   UnCorrFec
                                 Count      Ratio        Count       Ratio
0008.0e16.e6e2   0/0/U1   2      0          0.00000000   0           0.00000000
0008.0e16.f954   0/0/U1   1      0          0.00000000   0           0.00000000
00e0.0c60.02b4   0/0/U1   3      0          0.00000000   0           0.00000000
```

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show stats summary error [**sid** <*1-2049*>]

Command Syntax

sid *1-2049*	display cable modem service flow identifier (SID) Forward Error Correction (FEC) error counts and ratios

show tacacs

The **show tacacs** command displays statistics for all TACACS+ servers on the network including the IP address of the servers, connections, failed connection attempts, and packets sent and received. If there is more than one TACACS+ server configured, the command output displays statistics for all servers in the order in which they were configured. The following is an example of typical screen output from the **show tacacs** command:

```
Tacacs+ Server : 11.14.162.80/49
Number of Sessions: 1
Socket opens: 3
Socket closes: 3
Socket aborts: 0
Socket errors: 0
Socket Timeouts: 0
Failed Connect Attempts: 0
No current connection
Session 1 Statistics
    Total Packets Sent: 7
    Total Packets Recv: 7
    Expected Replies: 0
```

Note: TACACS+ statistics can also be displayed with the **show ip traffic** command.

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show tacacs

show tacacs statistics

The **show tacacs statistics** command displays overall TACACS+ statistics including the total number of access (AAA) requests, the number of denied requests, and the number of allowed requests. The following is an example of typical screen output from the **show tacacs statistics** command:

```
TACACS+ Overall Statistics
    Number of access requests       : 7
    Number of access deny responses : 1
    Number of access allow responses: 6
```

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show tacacs statistics

show tech

The **show tech** command displays statistics and log information from the output of the following technical support related **show** commands:

- **show version**
- **show running-config**
- **show interfaces**
- **show ip traffic**
- **show log**
- **show stats cmts**
- **show controllers cable**
- **show process memory**
- **show memory information**
- **show pool**
- **show process cpu**
- **show process msg-q-info**
- **show process semaphores**
- **show process stack**
- **show ip route summary**
- **show evt**
- **show cable modem summary**

The screen output of the **show tech** command is a compilation of the above **show** commands and can take several minutes to display on the screen. The output can also be saved to a file for later viewing. For a sample display of the output of the **show tech** command, see the individual **show** commands listed above.

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show tech [**flash:** | **nvram:**]

Command Syntax

flash:	output to a file on the Flash memory file system
nvram:	output to a file on the NVRAM file system

show user-group

The **show user-group** command displays the group access level for a specific CLI command. The group access levels are as follows:

SYSADMIN	access for users with System Administrator privileges
ISP	access for users with Internet Service Provider privileges
MSO	access for users with Multiple Service Operator privileges
RESTRICTED	access for users with "restricted" privileges
ALL	access for all users

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show user-group <*WORD*>

For example, entering the following:

show user-group password telnet 0 test

would return the following:

The command "password telnet 0 test" is set to SYSADMIN access

Command Syntax

WORD	the command name - the complete command syntax must be entered otherwise the system will return an "is not a valid command" error message

show users

The **show users** command displays information about active Telnet sessions including the username, user group and privilege level, the IP address of the originating host, and the session ID.

Group Access

All

Command Mode

Privileged EXEC and Global Configuration

Command Line Usage

show users [| {**begin** | **exclude** | **include**} {<*WORD*>} [| {**count** | **count-only**}]]

show users [| {**count** | **count-only**}]

Command Syntax

|	turns on output modifiers (filters)
begin	filter for output that begins with the specified string
exclude	filter for output that excludes the specified string
include	filter for output that includes the specified string
WORD	the specified string
count	count the number of outputted lines
count-only	count the number of lines while suppressing screen output

show version

The **show version** command displays the configuration of the system hardware, the software version, the names and sources of configuration files, and the boot images.

Boot ROM:	the boot version
Image:	the current software version running on the module
Date Built:	the date the above version was built
CPU:	the processor type name
Memory Size:	the processor memory size

Depending on the module type, the remaining output in each show version display shows the format version, assembly type, hardware revision, serial, part, and product numbers, FPGA Version number, and buffer management information.

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show version [| {**begin** | **exclude** | **include**} {<*WORD*>} [| {**count** | **count-only**}]]

show version [| {**count** | **count-only**}]

Command Syntax

|	turns on output modifiers (filters)
begin	filter for output that begins with the specified string
exclude	filter for output that excludes the specified string
include	filter for output that includes the specified string
WORD	the specified string
count	count the number of outputted lines
count-only	count the number of lines while suppressing screen output

speed

The **speed** command specifies the speed at which the Ethernet interface operates. The default speed is auto-negotiated but the speed can be manually set to either 10 Mbps or 100 Mbps.

Group Access

ISP

Command Mode

Interface Configuration (Ethernet interface only)

Command Line Usage

speed {**100** | **10** | **auto**}

no speed {**100** | **10** | **auto**}

Command Syntax

100	100 Mbps
10	10 Mbps
auto	autonegotiate the connection speed (100 Mbps or 10 Mbps) with the device at the other end of the physical connection.

Command Default

Auto negotiation enabled

tacacs-server host

The **tacacs-server host** command is used to specify and configure individual TACACS+ servers. The command can also be used to configure multiple TACACS+ servers. The TACACS+ client will contact the servers in the order in which they are specified.The **no tacacs-server host** command removes a TACACS+ server from the list.

Note: Since the key, port, retry, and timeout parameters specified with the **tacacs-server host** command override any global settings made by the **tacacs-server key**, **tacacs-server port**, **tacacs-server retry**, and **tacacs-server timeout** commands, the tacacs-server host command can be used to enhance network security by uniquely configuring individual TACACS+ servers.

Group Access

All

Command Mode

Global Configuration

Command Line Usage

tacacs-server host {<*hostname*> | <*A.B.C.D*>} [**key** <*WORD*> | **port** <*0-65535*>| **retry** <*0-100*> | **single-connection** | **timeout** <*1-1000*>]

no tacacs-server host [<*hostname*> | <*A.B.C.D*>]

Command Syntax

key *WORD*	specifies an authentication and encryption key - specifying a key with this command overrides the global key specified by the **tacacs-server key** command for this TACACS+ server only
port *0-65535*	specifies a server port number - this value overrides the global port number value set with the **tacacs-server port** command for this TACACS+ server only

retry *0-100*	specifies a retry value - this value overrides the global retry value set with the **tacacs-server retry** command for this TACACS+ server only
single-connection	opens a new TCP connection for every TACACS session established
timeout *1-1000*	specifies a timeout value in seconds - this value overrides the global timeout value set with the **tacacs-server timeout** command for this TACACS+ server only

tacacs-server key

The **tacacs-server key** command is used to specify a global authentication encryption key used for all TACACS+ communications between the TACACS+ client and the TACACS+ server. A global encryption key is used if no encryption key is specifically configured for this TACACS+ server. The **no tacacs-server key** disables authentication encryption.

Note: The key entered must match the key used on the TACACS+ server. All leading spaces are ignored; spaces within and at the end of the key are not. If spaces are used within the key, the key should not be enclosed in quotation marks unless the quotation marks themselves are part of the key.

Group Access

All

Command Mode

Global Configuration

Command Line Usage

tacacs-server key <*WORD*>

no tacacs-server key

Command Syntax

WORD	specifies an authentication and encryption key - this key must match the key used by the TACACS+ server

tacacs-server port

The **tacacs-server port** command to specify a global port number for all communication between the TACACS+ server and the TACACS client. A global port number is used if no port number is specifically configured for this TACACS+ server. The **no tacacs-server port** command restores the default port number value of 49.

Group Access

All

Command Mode

Global Configuration

Command Line Usage

tacacs-server port <*0-65536*>

no tacacs-server port

Command Syntax

0-65536	specifies the global port number used for all communication between the TACACS+ server and the TACACS client.

Command Default

49

tacacs reset-connections

The **tacacs reset-connections** command is used to reset all the TACACS+ server connections and associated sessions. After reset, all connections will be re-established. The **tacacs reset-connections** command is useful to initiate a reset and re-establish the existing connections after making any connection-specific configuration changes.

Group Access

All

Command Mode

Global Configuration

Command Line Usage

tacacs reset-connections

tacacs-server retry

The **tacacs-server retry** command is used to globally specify a retry count for all TACACS+ servers. A global retry count is used if no retry count is specifically configured for this TACACS+ server. The **no tacacs-server retry** command restores the global default value of 3 retries.

Group Access

All

Command Mode

Global Configuration

Command Line Usage

tacacs-server retry <*0-100*>

no tacacs-server retry

Command Syntax

0-100	the retry count

Command Default

3 retries

tacacs-server timeout

The **tacacs-server timeout** command is used to specify a global timeout interval for all TACACS+ servers. A global timeout value is used if no timeout value is specifically configured for this TACACS+ server. The **no tacacs-server timeout** command restores the global default timeout value or specifies another value.

Group Access

All

Command Mode

Global Configuration

Command Line Usage

tacacs-server timeout <*1-1000*>

no tacacs-server timeout [<*1-1000*>]

Command Syntax

1-1000	timeout value in seconds.

Command Default

10 seconds

telnet

The **telnet** command establishes a telnet connection between the BSR and a remote system.

Group Access

All

Command Mode

Privileged EXEC

Command Line Usage

telnet {<*A.B.C.D*> | <*WORD*>}

Command Syntax

A.B.C.D	the IP address of a remote system
WORD	the hostname of a remote system

telnet authentication radius

The **telnet authentication radius** command enables RADIUS authentication for telnet access. The **no telnet authentication radius** command disables this feature.

Group Access

ISP

Command Mode

Global Configuration

Command Line Usage

telnet authentication radius [**fail-message** <*LINE*> | **local-password**]

no telnet authentication radius [**fail-message** | **local-password**]

Command Syntax

fail-message *LINE*	specify message to display for a failed login/ authentication
local-password	authenticate with a locally configured password if there is no response from the RADIUS server

telnet session-limit

The **telnet session-limit** command specifies a limit on the number of concurrent telnet sessions allowed to the BSR. Setting the session-limit to "0" will disallow any telnet sessions from being accepted. Setting a session-limit value will not affect any currently open telnet sessions.

The **no telnet session-limit** command restores the default session limit of 64 concurrent telnet sessions.

Group Access

ISP

Command Mode

Global Configuration

Command Line Usage

telnet session-limit <*0-8*>

no telnet session-limit [<*0-8*>]

Command Syntax

0-8	the telnet session limit number

Command Default

8

update-fpga

The **update-fpga** command allows you upgrade the BSR FPGA.

Group Access

System Administrator

Command Mode

Privileged EXEC

Command Line Usage

update-fpga <*prefix*> <*string*>

Command Syntax

prefix	The server IP address.
string	The FPGA image name.

username

The **username** command establishes a login authentication system based on a username.

Group Access

System Administrator

Command Mode

Global Configuration

Command Line Usage

username <*WORD*> **password** [**0** | **7**]<*WORD*>

username <*WORD*> **nopassword**

Command Syntax

WORD	the username, up to 16 characters
nopassword	no password is required for the user to log in
password	specify a password for the user (31 character maximum) - enclosed with double quotes if the key contains spaces). The "%" and "!" characters must not be used.
0	specifies an UNENCRYPTED password
7	specifies a HIDDEN password will follow
WORD	the UNENCRYPTED (cleartext) user password (31 character maximum) - enclosed with double quotes if the key contains spaces). The "%" and "!" characters must not be used.

Note: Refer to Defining a User Name with an Encrypted Password in the *BSR 2000 Configuration and Management Guide for Release 3.1* for details on encrypting passwords.

username privilege

The **username privilege** command sets a privilege level for a user.

Group Access

System Administrator

Command Mode

Global Configuration

Command Line Usage

username <*WORD*> **privilege** {**ro** | **rw**}

Command Syntax

WORD	the username, up to 16 characters
privilege	the user privilege level
ro	read-only privilege
rw	read and write privilege

username user-group

The **username user-group** command assigns a user to a user group. The **no username user-group** command removes a user from a user group.

Group Access

System Administrator

Command Mode

Global Configuration

Command Line Usage

username <*WORD*> **user-group** {**isp** <*1-1*> | **mso** | **restricted** | **sysadmin**}

no username <*WORD*> **user-group** {**isp** <*1-1*> | **mso** | **restricted** | **sysadmin**}

Command Syntax

WORD	the username, up to 16 characters
user-group	assigns the user group name
isp	provides this user access to most CLI commands including routing commands but excluding cable commands
1-1	the number of the virtual ISP
mso	provides this user access to most CLI commands including cable commands but excluding routing commands
restricted	only provides this user access to CLI commands with a designated privilege level of "restricted" as defined with the **privilege restricted** CLI command.
sysadmin	provides this user access to all CLI commands

2

IP Commands

Introduction

This chapter describes the following types of commands for the BSR:

Interface commands not associated with a specific protocol can be used to configure interface features with any device on the network.

Transmission Control Protocol/Internet Protocol (TCP/IP) commands handle network communications between network nodes. This includes network addressing information, control information that enables packets to be routed, and reliable transmission of data.

Address Resolution Protocol (ARP) commands dynamically maps IP addresses to physical hardware addresses. An ARP cache is used to maintain a correlation between each MAC address and its corresponding IP address.

Domain Name System (DNS) commands are used to map hostnames to IP addresses, and to control Internet routing information. Lists of domain names and IP addresses are distributed throughout the Internet with DNS servers.

Simple Network Time Protocol (SNTP) commands are used to synchronize computer clocks in the global internet. SNTP operates in unicast, broadcast, and IP multicast modes.

Tunneling commands provide a way to encapsulate packets inside of a transport protocol. IP in IP Encapsulation for tunnel interfaces is supported by the BSR.

IP Command Descriptions

This section contains an alphabetized list and descriptions of the IP commands supported by the BSR.

arp

The **arp** command adds a permanent entry in the ARP cache. The **no arp** command removes the entry in the ARP cache. The **arp** command can also specify the type of ARP packet that is used, whether to use an alias if proxy arp is enabled, and to specify a cable bundle interface if cable bundling is being used.

Note: Proxy ARP is not enabled by default. ARP cache entries translate 32-bit addresses into 48-bit hardware addresses. If the host supports dynamic resolution, static entries are usually not needed. Use the **clear arp-cache** command to remove all dynamically learned entries.

Group Access

ISP

Command Mode

Global Configuration

Command Line Usage

arp <*A.B.C.D*> <*H.H.H*> {**arpa** | **snap**}

no arp <*A.B.C.D*> <*H.H.H*> {**arpa** | **snap**}

Command Syntax

A.B.C.D	four-part dotted-decimal format matching the local data link
H.H.H	48-bit local data link address
arpa	standard Ethernet-style ARP, RFC 826
snap	IEEE 802.3 usage of ARP packets conforming to RFC 1042

Command Default

no entries in table

arpa (ethernet ARP)

arp timeout

The ARP timeout feature is used to prevent unnecessary flooding of traffic over the cable network. ARP resolution requests are terminated after a defined interval when attempts to resolve addressing information, for a device entry in the ARP cache table.

The ARP cache table expiration value is disabled by default. The **arp timeout** command configures the amount of time an entry stays in the ARP cache. The **no arp timeout** command restores the default ARP timeout condition. The **show interfaces** command displays the current ARP timeout value.

Note: When the arp timeout value is changed, the change affects all the existing entries in addition to the entries subsequently created.

Group Access

ISP

Command Mode

Interface Configuration

Command Line Usage

arp timeout <*4-6000*>

no arp timeout <*4-6000*>

Command Syntax

4-6000	The expiration value in minutes for the amount of time an entry is allowed to stay in the ARP cache

Command Default

60 minutes

cable helper-address

The cable helper address function disassembles a DHCP broadcast packet, and reassembles it into a unicast packet so that the packet can traverse the router and communicate with the DHCP server. The **cable helper-address** command enables broadcast forwarding for User Datagram Protocol (UDP) packets.

The **cable helper-address** command is also used to bind a cable helper address to a secondary IP subnet of a CM which is connected to CPEs belonging to a particular ISP. This allows CPEs to have their IP address assigned from the DHCP server belonging to the corresponding ISP.

Note: The **isp-bind** option is only available after selecting the **host** or **mta** options. It is not available for the **cable modem** option.

Group Access

ISP

Command Mode

Interface Configuration (cable and loopback interfaces only)

Command Line Usage

cable helper-address <*A.B.C.D*> {**cable-modem** | **host** | **mta**} [**isp-bind** <*A.B.C.D*>]

no cable helper-address <*A.B.C.D*> {**cable-modem** | **host** | **mta**} [**isp-bind** <*A.B.C.D*>]

Command Syntax

A.B.C.D	the IP address of the destination DHCP server.
cable-modem	specifies that only CM UDP broadcasts are forwarded.
host	specifies that only CPE UDP broadcasts are forwarded.

mta	specifies that only CPE MTA broadcasts are forwarded.
isp-bind *A.B.C.D*	specifies the secondary IP subnet to which the cable-helper is bound.

clear arp-cache

The **clear arp-cache** command clears dynamic entries from ARP cache.

Group Access

ISP

Command Mode

Privileged EXEC

Command Line Usage

clear arp-cache [<*A.B.C.D*>]

Command Syntax

A.B.C.D	the IP address for ARP table entry to be cleared

clear counters

The **clear counters** command is used to clear a specific counter or all interface counters.

Group Access

ISP

Command Mode

Privileged EXEC

Command Line Usage

clear counters [**ethernet** <*X*/*Y*>| **cable** <*X*/*Y*> **gigaether** <*X*/*Y*> | **ipsec** | **loopback** <*1-64*>]

Command Syntax

cable *X/Y*	clears the cable counters for the specified slot and port
ethernet *X/Y*	clears the Ethernet counters for the specified port (*X* is always 0, *Y* is the port number)
gigaether *X/Y*	clears the Gigabit Ethernet counters for the specified port (*X* is always 0, *Y* is the port number)
ipsec	clears the IPSEC counters
loopback *1-64*	clears the loopback for the specified loopback interface number

clear host

The **clear host** command deletes DNS host entries from the host-name-and-address cache.

Group Access

ISP

Command Mode

Privileged EXEC

Command Line Usage

clear host {<*WORD*> | *****}

Command Syntax

WORD	deletes a specific DNS host entry
*	deletes all DNS host entries

clear ip route

The **clear ip route** command deletes route table entries.

Group Access

ISP

Command Mode

Privileged EXEC

Command Line Usage

clear ip route {***** | <*A.B.C.D*> [<*A.B.C.D*>]}

Command Syntax

*****	Deletes all routes.
A.B.C.D	Destination network IP address.
A.B.C.D	Destination network subnet mask.

clear ip traffic

The **clear ip traffic** command resets the IP traffic statistic counters to zero.

Group Access

ISP

Command Mode

Privileged EXEC

Command Line Usage

clear ip traffic

host authorization

The host authorization feature is used for security purposes on the cable network. When enabled, host authorization denies access to any hacker who tries to take or "spoof" an IP address from any legitimate user on the same cable network. A hacker takes the IP address from this user to steal their data service. The hacker accomplishes this by changing the IP address on their PC to the IP address that the DHCP server assigned to a legitimate user's CPE. Cable operators can create static entries to deny hackers from stealing service from users. Through static entries, cable operators can manually bind the CPE MAC (hardware) and IP address to a particular cable modem. This command may be used in circumstances when DHCP is not used to assign the CPE IP addresses

The **host authorization** command is used to enforce the bind of the CM and CPE MAC addresses to the IP address assigned to them (statically or through DHCP). The **no host authorization** command disables host authorization on the cable interface.

Group Access

ISP

Command Mode

Interface Configuration mode (cable interface only)

Command Line Usage

host authorization {<*mac*> {**cpe** <*mac*> <*prefix*> | **cpr** <*mac*> <*prefix*>}} | **on**}

no host authorization on {<*mac*> {**cpe** <*mac*> <*prefix*> | **cpr** <*mac*> <*prefix*>}} | **on**}

Command Syntax

mac	the cable modem mac address in the form of xxxx.xxxx.xxxx
cpe	specify customer premise equipment
mac	the MAC address of the customer premises equipment (CPE) or customer premises router (CPR)
prefix	the CPE or CPR's IP address

cpr	specify a customer premise router
on	enable host authorization

Command Default

Disabled

interface

The **interface** command specifies an interface for further configuration. Once the interface is selected you enter Interface configuration mode.

Group Access

ISP

Command Mode

Global Configuration

Command Line Usage

interface {**cable** <*X*/*Y*> | **ethernet** <*X*/*Y*> | **gigaether** <*X*/*Y*> | **loopback** <*1-64*>}

Command Syntax

cable *X/Y*	CMTS that provides 1 downstream channel and 4 upstream channels. Commonly referred to as the cable interface.
ethernet *X/Y*	On the BSR 2000, Ethernet interface 0 is a 10 Mbps management interface that does not support the negotiation feature. Ethernet ports 1 and 2 are typically used to support an external T1/E1 BITS clock. (*X* is always 0, *Y* is the port number)
gigaether *X/Y*	Provides two 1000 Mbps optical Ethernet interfaces (*X* is always 0, *Y* is the port number)
loopback *1-64*	Loopback interfaces are used to act as inbound logical interfaces when physical interfaces go down.

ip access-group

The **ip access-group** command configures an interface to use an access list. The **no ip access-group** command does not allow incoming or outgoing packets.

Group Access

ISP

Command Mode

Interface Configuration

Command Line Usage

ip access-group {*<1-199> <1300-2699>* {**in** | **out**}

no ip access-group {*<1-199> <1300-2699>* {**in** | **out**}

Command Syntax

1-199	Standard number range from 1 to 199.
1300-2699	Extended number range from 1300 to 2699.
in	Incoming packet is processed only if the source-address is in the access-list.
out	Same as **in**, outgoing packet is processed only if access-list permits the packet.

Command Default

No access groups defined.

ip address

The **ip address** command configures a primary or secondary IP address for an interface or defines the Gateway IP address (giaddr) for Customer Premises Equipment (CPE), Multimedia Telephone Adapter (MTA), or cable modem DHCP requests. The **no ip address** command is used to remove an IP address from the interface. When configuring the cable interface IP address two additional options are supported; the **host** and **mta** options.

The additional options are only available from cable interface configuration mode when selecting an IP address. During the DHCP process, the relay agent requests an IP address in a particular subnet by inserting the IP address of the interface into the DHCP requests from CMs, hosts, and MTAs. The primary address is always inserted in cable modem DHCP requests. If a secondary address or a secondary host address is defined, then the first secondary or secondary host IP address in the list is inserted into DHCP requests from hosts. If one or multiple secondary mta IP address are defined, then the first secondary mta IP address defined is inserted into DHCP requests from secondary MTA devices. The **ip dhcp relay information option** command must be enabled to allow the BSR to determine what type of device originated the DHCP request. By default, the primary address will be inserted into DHCP requests.

The **ip address** command is also used to bind a secondary IP address to a secondary IP subnet of a CM which is connected to CPEs belonging to a particular ISP. This allows the BSR to set the giaddr of the CPE's DHCP packets to the secondary address of the CM to which the secondary addresses of the CPE are bound.

Note: You must configure a primary IP address before configuring a secondary IP address.

Note: The BSR supports 128 secondary IP subnets per cable bundle. The maximum number of IP subnets that can be configured on the BSR chassis is 1024.

Group Access

System Administrator

Command Mode

Interface Configuration (cable or loopback interfaces only)

Command Line Usage

ip address <*A.B.C.D*> <*A.B.C.D*> [**secondary** [**host** | **mta**][**isp-bind** <*A.B.C.D*>]]]

no ip address <*A.B.C.D*> <*A.B.C.D*> [**secondary** [**host** | **mta**][**isp-bind** <*A.B.C.D*>]]]

Command Syntax

A.B.C.D	the IP address
A.B.C.D	the subnetwork mask for the IP address - the BSR supports up to a 30-bit subnetwork IP address mask
secondary	designates the specified IP address as a secondary IP address - on a cable interface, defines this IP address as the IP address to be inserted into host DHCP requests
host	defines the IP address for the cable interface as the giaddr for host DHCP requests - on the cable interface, defines this IP address as the IP address to be inserted into host DHCP requests (this option is only available on the cable interface)
mta	defines the IP address for the cable interface as the giaddr for all MTA DHCP requests - on the cable interface, defines this IP address as the IP address to be inserted into MTA DHCP requests (this option is only available on the cable interface)
isp-bind *A.B.C.D*	specifies the secondary IP subnet to which this secondary address is bound.

ip broadcast-address

The **ip broadcast-address** command creates a broadcast address for an interface. The **no ip broadcast-address** command deletes the broadcast address for an interface.

Group Access

ISP

Command Mode

Interface Configuration

Command Line Usage

ip broadcast-address <*A.B.C.D*>

no ip broadcast-address <*A.B.C.D*>

Command Syntax

A.B.C.D	broadcast IP address assigned to the interface

ip dhcp relay information

The **ip dhcp relay information** command enables the BSR to insert DHCP relay information option (option-82) into received DHCP client messages being forwarded to a DHCP server (configured using the **cable helper** command). Support for DHCP Option-82, sub-option 2 (Agent Remote ID), which is enabled by the **ip dhcp relay information option** command, allows the relay agent in the BSR to insert the MAC address of the modem that the DHCP client is behind into outbound DHCP client requests (i.e., DHCP Discovers and DHCP Requests as they traverse the BSR). This enables the receiving DHCP server to identify the user sending the request and to treat that client appropriately.

Support for DHCP Option-82, sub-option 1 (Agent Circuit ID), which is enabled by the **ip dhcp relay information spectrum-group-name** command, allows the relay agent in the BSR to insert, when available, the Spectrum Group name associated with the upstream channel that the DHCP client is using into outbound DHCP client requests (i.e., DHCP Discovers and DHCP Requests as they traverse the BSR).

Note: f you are configuring two MAC domains on the 2x8 CMTS module, the **ip dhcp relay information option** command must be entered for each MAC domain. If this command is not entered in for each domain, CMs cannot register in that domain.

Note: If a DHCP client on a particular subnet is using an upstream frequency that is not configured as a member of a Spectrum Group, the Spectrum Group name is not inserted by the DHCP relay agent into the DHCP discover packet.

Group Access

ISP

Command Mode

Interface Configuration (cable interface only)

Command Line Usage

ip dhcp relay information {**option | spectrum-group-name**}

no ip dhcp relay information {**option | spectrum-group-name**}

Command Syntax

option	insert a MAC address (Agent Remote ID) only into a client's DHCP discover packets
spectrum-group-name	insert the Spectrum Group name into all DHCP outbound requests

ip domain-list

The **ip domain-list** command provides up to six domain names to resolve unqualified host names when the primary domain, specified by the **ip domain-name** command, fails to resolve.

Use the **ip domain-list c**ommand to define a list of secondary domain names. Secondary domain names are used if the primary domain name fails to resolve.

Group Access

ISP

Command Mode

Global Configuration

Command Line Usage

ip domain-list <*WORD*> [<*WORD*>] [<*WORD*>] [<*WORD*>] [<*WORD*>] [<*WORD*>]

no ip domain-list <*WORD...***>**

Command Syntax

WORD	Domain name.

ip domain-lookup

The **ip domain-lookup** command enables the IP Domain Name System (DNS) based host name-to-address translation. The **no ip domain-lookup** command disables the IP DNS-based name-to-address translation.

Group Access

ISP

Command Mode

Global Configuration

Command Line Usage

ip domain-lookup

no ip domain-lookup

Command Default

Enabled

ip domain-name

For each BSR, you should configure the name of the domain in which the BSR is located. This is the default domain name that is appended to host names that are not fully qualified. The **ip domain-name** command is used to configure a domain name. The **no ip domain-name** command removes the domain name.

Group Access

ISP

Command Mode

Global Configuration

Command Line Usage

ip domain-name <*WORD*>

no ip domain-name <*WORD*>

Command Syntax

WORD	name of domain being established

Command Default

No domain is configured.

ip forward-protocol udp

The **ip forward-protocol udp** command controls what type of UDP packet to forward when broadcasting packets or allows all types of UDP packets to be forwarded. The **no ip forward-protocol udp** command disables IP forwarding.

Group Access

ISP

Command Mode

Global Configuration

Command Line Usage

ip forward-protocol udp [*<0-65535>* | **bootpc** | **bootps** | **domain** | **netbios-dgm** | **netbios-ns** | **tacacs** | **tftp** | **time**]

no ip forward-protocol udp [*<0-65535>* | **bootpc** | **bootps** | **domain** | **netbios-dgm** | **netbios-ns** | **tacacs** | **tftp** | **time**]

Command Syntax

0-65535	Specific UDP port number.
bootpc	Bootstrap Protocol (BOOTP) client (68)
bootps	Bootstrap Protocol (BOOTP) server (67)
domain	Domain Name Service (DNS, 53)
netbios-dgm	NetBios datagram service (138)
netbios-ns	NetBios name service (137)
tacacs	TAC Access Control System (49)
tftp	Trivial File Transfer Protocol (69)
time	Time (37)

ip helper-address

The **ip helper-address** command determines the destination IP address of the DHCP server for where broadcast packets are forwarded. The **no ip helper-address** command removes the IP address where broadcast packets are forwarded.

Use the **ip-helper address** command to forward broadcast packets received on an interface.

Group Access

ISP

Command Mode

Interface Configuration

Command Line Usage

ip helper-address <*A.B.C.D*>

no ip helper-address <*A.B.C.D*>

Command Syntax

A.B.C.D	Destination broadcast/host address to be used.

ip host

The **ip host** command is used to add a static, classless DNS host entry to the ip hostname table by matching the host IP address to its DNS host name mapping. The **no ip host** command deletes the host address-to-name mapping in the host cache.

Note: The initial character of the name must be a letter.

Group Access

ISP

Command Mode

Global Configuration

Command Line Usage

ip host <*WORD*> <*A.B.C.D*>

no ip host <*WORD*> <*A.B.C.D*>

Command Syntax

WORD	name of host
A.B.C.D	IP address

Command Default

No hosts configured

ip irdp

The **ip irdp** command enables the ICMP Router Discovery Protocol (IRDP) on an interface. The **no ip irdp** command disables the ICMP IRDP on an interface.

Group Access

ISP

Command Mode

Interface Configuration (Ethernet and Gigabit Ethernet interfaces only)

Command Line Usage

ip irdp [**address** <*A.B.C.D*> | **holdtime** <*1-9000*> | **maxadvertinterval** <*4-1800*> | **minadvertinterval** <*3-1800*> | **multicast** | **preference** <*-2147483648-2147483647*>]

no ip irdp [**address** <*A.B.C.D*> | **holdtime** <*1-9000*> | **maxadvertinterval** <*4-1800*> | **minadvertinterval** <*3-1800*> | **multicast** | **preference** <*-2147483648-2147483647*>]

Command Syntax

address	IP addresses to proxy-advertise, preference value.
A.B.C.D	IP address to advertise.
holdtime	amount of time, in seconds, advertisements hold valid
1-9000	value in seconds
maxadvertinterval	maximum time between advertisements
4-1800	value in seconds
minadvertinterval	minimal time between advertisement in seconds
multicast	advertisements are sent with multicast

preference	preference value for this interface, -2^{31} to 2^{31}, higher value increases performance, preferred router
-2147483648-2147483647	preference for this address (higher values preferred)

Command Default

holdtime	=	1800 seconds
maxadvertinterval	=	600 seconds
minadvertinterval	=	450 seconds
preference	=	*-2147483648-2147483647*

ip mask-reply

The **ip mask-reply** command enables Internet Control Message Protocol (ICMP) netmask reply messages. The **no ip mask-reply** command disables ICMP netmask reply messages.

Group Access

ISP

Command Mode

Interface Configuration

Command Mode

ip mask-reply

no ip mask-reply

Command Default

Enabled

ip mtu

The **ip mtu** command configures the Maximum Transmission Unit (MTU) packet size allowed on the interface. The **no ip mtu** command resets the default.

Group Access

ISP

Command Mode

Interface Configuration

Command Line Usage

ip mtu <*68-4000*>

no ip mtu

Command Syntax

68-4000	MTU size in bytes

Command Default

1496 bytes

ip name-server

The **ip name-server** command is used to enter the IP address of one or more Domain Name Servers (DNS). Up to six DNS can be configured on the BSR. The **no ip name-server** command deletes a DNS entry.

Group Access

ISP

Command Mode

Global Configuration

Command Line Usage

ip name-server <*A.B.C.D*> [<...*A.B.C.D*>]

no ip name-server <*A.B.C.D*> [<...*A.B.C.D*>]

Command Syntax

A.B.C.D	IP addresses of your DNS.

ip proxy-arp

The **ip proxy-arp** command enables proxy ARP on the interface. The **no ip proxy-arp** command disables proxy ARP on an interface.

Note: If a host in the local network is incapable of responding to an ARP request for some reason, the router will respond on behalf of the host when proxy arp is enabled and the IP-to-MAC address mapping of the host is stored in the router with a static arp command, with the alias option specified.

To verify ARP status, use the **show running-config** command.

The BSR will also respond to an ARP request for a network on a different interface when proxy ARP is turned on.

Group Access

ISP

Command Mode

Interface Configuration

Command Line Usage

ip proxy-arp

no ip proxy-arp

Command Default

Disabled

ip rarp-server

The **ip rarp-server** command is used to enable the router to act as a RARP server. The **no ip rarp-server** command disables the router to act as a RARP server.

The RARP server can be configured on each interface to ensure that the router does not affect RARP traffic on other subnetworks that do not need RARP assistance. The following conditions must be satisfied before receiving RARP support:

- The **ip rarp-server** command must be configured on the requesting interface
- A static entry, must exist in the IP ARP table, mapping the MAC address in the RARP request to an IP address

The IP address should be set to whatever address the user configures as the primary address for the interface.

Group Access

ISP

Command Mode

Interface Configuration

Command Line Usage

ip rarp-server <*A.B.C.D*>

no ip rarp-server <*A.B.C.D*>

Command Syntax

A.B.C.D	The IP address that is provided as the source protocol address field of the RARP response packet.

Command Default

Disabled

ip redirects

The **ip redirects** command enables messages to be redirected if a packet needs to be resent through the interface that received the packet. The **no ip redirects** command disables messages that are redirected if a packet needs to be resent through the interface that received the packet.

Group Access

ISP

Command Mode

Interface Configuration (not supported for Cable interfaces)

Command Line Usage

ip redirects

no ip redirects

ip route

The **ip route** command is used to configure a static route when the router cannot dynamically build a route to the specific destination or if the route must be in place permanently. The **no ip route** command remove a static route.

Group Access

ISP

Command Mode

Global Configuration

Command Line Usage

ip route <*A.B.C.D*> <*A.B.C.D*> {<*A.B.C.D*> | **null** <*0-0*>} [<*1-255*> | [**tag** <*1-4294967295*>]

no ip route <*A.B.C.D*> <*A.B.C.D*> {<*A.B.C.D*> | **null** <*0-0*>} [<*1-255*> | [**tag** <*1-4294967295*>]

Command Syntax

A.B.C.D	static route destination prefix
A.B.C.D	static route destination prefix mask
A.B.C.D	the forwarding router's IP address
null *0-0*	null slot and port, valid values 0 and 0
1-255	administrative distance, default value 1
tag *1-4294967295*	match value to control route-map redistribution, valid values 1 to 4294967295

Command Default

Administrative distance = 1

ip routing

The **ip routing** command enables IP routing. The **no ip routing** command disables IP routing.

Group Access

ISP

Command Mode

Global Configuration

Command Line Usage

ip routing

no ip routing

Command Default

Enabled

ip source-route

The **ip source-route** command allows the BSR to handle IP datagrams with source routing header options. The **no ip source-route** command discards any IP datagram containing a source-route option.

Group Access

ISP

Command Mode

Global Configuration

Command Line Usage

ip source-route

no ip source-route

ip unreachables

The **ip unreachables** command enables processing of an ICMP unreachable message when the BSR cannot deliver a received packet. The **no ip unreachables** command disables ICMP unreachable message processing when the router cannot deliver a received a packet.

Group Access

ISP

Command Mode

Interface Configuration and Global Configuration

Command Line Usage

ip unreachables

no ip unreachables

Command Default

Enabled

passive-interface

The **passive-interface** command suppresses routing updates from being transmitted over a specific ethernet or cable routing interface. The **no passive-interface** re-enables route updates to be transmitted over the routing interface.

Note: Updates from routers that are directly connected to the passive interface continue to be received and processed.

Group Access

ISP

Command Mode

Router Configuration

Command Line Usage

passive-interface {**cable** <*X/Y*> | **ethernet** <*X/Y*> | **gigaether** <*X/Y*>| **loopback** <*1-64*> **| default**}

no passive-interface {**cable** <*X/Y*> | **ethernet** <*X/Y*> | **gigaether** <*X/Y*>| **loopback** <*1-64*> **| default**}

Command Syntax

cable *X*/*Y*	*X* is 0. *Y* is the cable interface port number.
ethernet *X*/*Y*	*X* is 0. *Y* is the Ethernet interface port number.
gigaether *X*/*Y*	*X* is 0. *Y* is the Gigabit Ethernet interface port number.
loopback <*1-64*>	<*1-64*> is the Loopback interface number.
default	Suppress routing updates on all interfaces.

Command Default

Routing updates are transmitted over the router.

ping

The Packet Internet Groper (PING) **ping** command sends an Internet Control Message Protocol (ICMP) echo request to a remote host that reports errors and provides information relevant to IP packet addressing.

Use the **ping** command to check host reach ability and network connectivity, or to confirm basic network connectivity.

Note: The address of the source in an echo message will be the destination of the echo reply message. To form an echo reply message, the source and destination addresses are simply reversed, the type code changed to 0, and the checksum recomputed.

ICMP is used to report problems with delivery of IP datagrams within an IP network. It can also show when a particular node is not responding, when an IP network is not reachable, when a node is overloaded, when an error occurs in the IP header information, etc. The protocol is also frequently used by Internet managers to verify correct operations of nodes and to check that routers are correctly routing packets to the specified destination address.

Group Access

All

Command Mode

User EXEC and Privileged EXEC

Command Line Usage

ping {<*A.B.C.D*> | **Hostname**}[**size** <*40-65515*] [<*1-65535*>] [**timeout** <*1-1024*>] [**source** <*A.B.C.D*>] [**tos** <*0-255*>] [**ttl** <*0-255*>] [**df**]

ping docsis {<*mac*> | <*prefix*>} **<***1-100***>**

Command Syntax

A.B.C.D	IP address of the remote system to ping
Hostname	name of the remote system to ping
size *1-165535*	size of the echo message in bytes,

1-65535	number of ping requests to send
timeout *1-1024*	timeout in seconds
source *A.B.C.D*	source IP address to use to send the ping request
tos *0-255*	the type of service of the ping packets
ttl *0-255*	Time to live value in seconds
df	sets the "don't fragment" IP flag in the outgoing ping IP header
docsis	DOCSIS-complaint cable modem
mac	The cable modem mac address in the form of xxxx.xxxx.xxxx
prefix	Cable modem IP address
1-100	Number of ping messages to be sent to the cable modem

show arp

The **show arp** command displays static and dynamic entries in the ARP table. The following is typical screen output from the **show arp** command:

```
Protocol          Address   Age(min)   Hardware Address   Type    Interface
Internet       10.10.10.10       -      0030.b801.c5f4    ARPA     ethernet 0/0
Internet        10.255.4.1       -      0000.0000.0004    ARPA
Internet        10.255.5.1       -      0000.0000.0005    ARPA
Internet        10.255.6.1       -      0000.0000.0006    ARPA
Internet        10.255.7.1       -      0000.0000.0007    ARPA
Internet       150.31.60.1      41      00e0.6367.99b1    ARPA     ethernet 0/0
Internet      150.31.60.10       -      0030.b801.c570    ARPA     ethernet 0/0
Internet      150.31.60.99       -      0000.0000.9999    ARPA     ethernet 0/0
Internet      150.31.61.23      21      0008.0ee4.84e8    ARPA     cable 0/0
Internet      150.31.61.27      31      0008.0ee4.d550    ARPA     cable 0/0
Internet      150.31.61.28       3      0020.4026.77c0    ARPA     cable 0/0
Internet      150.31.61.29       3      0020.4027.a028    ARPA     cable 0/0
Internet      150.31.61.34       3      0020.4026.d5dc    ARPA     cable 0/0
Internet      150.31.61.37       3      0020.4026.77bc    ARPA     cable 0/0
Internet      150.31.61.80       3      0020.4029.19dc    ARPA     cable 0/0
Internet      150.31.61.81       3      0020.4027.a038    ARPA     cable 0/0
```

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show arp [| {**begin** | **exclude** | **include**} {<*WORD*>} [| {**count** | **count-only**}]]
show arp [| {**count** | **count-only**}]

Command Syntax

|	turns on output modifiers (filters)
begin	filter for output that begins with the specified string

exclude	filter for output that excludes the specified string
include	filter for output that includes the specified string
WORD	the specified string
count	count the number of outputted lines
count-only	count the number of lines while suppressing screen output

show controllers

The **show controllers** command displays detailed hardware and configuration information for each module on installed in the BSR chassis.

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show controllers cable <*X*/*Y*> [**upstream** <*0-3*> | **downstream** <*0-0*>| **mac**] [| {**begin** | **exclude** | **include**} {<*WORD*>} [| {**count** | **count-only**}]]

show controllers cable <*X*/*Y*> [**upstream** <*0-3*> | **downstream** | **mac**] [| {**count** | **count-only**}]

show controllers ethernet [<*X*/*Y*>]

show controllers gigaether [<*X*/*Y*>]

Command Syntax

cable *X/Y*	display cable interface controller information for the specified BSR port number including RF signal information, the type of hardware installed, FEC information for both corrected and uncorrected packets, the spectrum group and the status of the cable interface (*X* is 0. *Y* is the port number)
downstream *0-0*	**display information for the downstream port** including downstream modulation type, frequency (label), and symbol rate

mac	display MAC layer (layer 2) information for all cable modems on this specific CMTS module
upstream *0-3*	display information for an upstream port including the upstream modulation type, channel width, frequency, and modulation profile information (i.e minislots, interleave, preamble, etc.)
|	turns on output modifiers (filters)
begin	filter for output that begins with the specified string
exclude	filter for output that excludes the specified string
include	filter for output that includes the specified string
WORD	the specified string
count	count the number of outputted lines
count-only	count the number of lines while suppressing screen output
ethernet *X/Y*	display Ethernet interface controller information for the entire BSR chassis or the optional, specified port number (*X* is 0. *Y* is the port number.)
gigaether *X/Y*	display Gigabit Ethernet interface controller information for the entire BSR chassis or the optional, specified port number (*X* is 0. *Y* is the port number.)

show host authorization

The **show host authorization** command displays the host authorization enabled state and displays all cable host entries in the ARP authorization table. The following screen output is displayed:

```
Device Type State     Seconds   Modem MAC Addr  Host IP Addr    Host MAC Addr
Host   Dyn  Ack       90000     0008.0e72.bf70  150.31.43.3     0008.0e72.bf72
Modem  Dyn  Ack-TD-TF 90000     0008.0e72.bf70  150.31.42.2     0008.0e72.bf70
Host   Dyn  Ack       90000     0008.0e73.1dba  150.31.43.2     0008.0e73.1dbc
Modem  Dyn  Ack-TD-TF 90000     0008.0e73.1dba  150.31.42.3     0008.0e73.1dba
```

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show host authorization

show host authorization cpe

The **show host authorization cpe** command is used to display the dynamic or static ARP entries for CPEs only. The following screen output is displayed:

```
Type       Host IP Address      Host MAC Address
Dynamic    150.31.43.3          0008.0e72.bf72
Dynamic    150.31.43.2          0008.0e73.1dbc
```

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show host authorization cpe {**leased** | **static**} [| {**begin** | **exclude** | **include**} {<*WORD*>} [| {**count** | **count-only**}]]

show host authorization cpe {**leased** | **static**} [| {**count** | **count-only**}]

Command Syntax

leased	display dynamically configured host authorization entries
static	display statically configured host authorization entries
|	turns on output modifiers (filters)
begin	filter for output that begins with the specified string
exclude	filter for output that excludes the specified string
include	filter for output that includes the specified string

WORD	the specified string
count	count the number of outputted lines
count-only	count the number of lines while suppressing screen output

show host authorization summary

The **show host authorization summary** command is used to display the dynamic or static ARP entries for CPEs only. The following screen output is displayed:

```
Interface      Total     Total    Total      Dynamic    Static     Total
               Modems    Hosts    Routers    Entries    Entries    Entries
Cable  4/0     2         2        0          4          0          4
```

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show host authorization summary [| {**begin** | **exclude** | **include**} {<*WORD*>} [| {**count** | **count-only**}]]

show host authorization summary [| {**count** | **count-only**}]

Command Syntax

|	turns on output modifiers (filters)
begin	filter for output that begins with the specified string
exclude	filter for output that excludes the specified string
include	filter for output that includes the specified string
WORD	the specified string

count	count the number of outputted lines
count-only	count the number of lines while suppressing screen output

show host unauthorized cpe

The **show host unauthorized cpe** command displays the list of hosts/CPEs that are unauthorized due to a failed DHCP lease query response.

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show host unauthorized cpe

show hosts

The **show hosts** command displays the cache list of host names and addresses, and the lookup service type.

Group Access

ISP

Command Mode

Privileged EXEC

Command Line Usage

show hosts

show interfaces

Use the **show interfaces** command to display the status and statistics for the network interfaces. Use the **show interfaces** command without the slot and interface argument to display all interfaces.

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show interfaces [**ethernet** <*X/Y*> | **gigaether** <*X/Y*> | **cable** <*X/Y*> | **loopback** <*1-64*>] [**accounting**] [| {**begin** | **exclude** | **include**} {<*WORD*>} [| {**count** | **count-only**}]]

show interfaces [**ethernet** <*X/Y*> | **gigaether** <*X/Y*> | **cable** <*X/Y*> | **loopback** <*1-64*>] [**accounting**] [| {**count** | **count-only**}]

Command Syntax

ethernet *X/Y*	*X* is 0. *Y* is the Ethernet interface port number.
gigaether *X/Y*	*X* is 0. *Y* is the Gigabit Ethernet interface port number.
cable *X/Y*	*X* is 0. *Y* is the cable interface port number.
loopback *1-64*	Loopback interface number
accounting	Displays the number of packets for each protocol type that has been sent through an interface
|	turns on output modifiers (filters)
begin	filter for output that begins with the specified string
exclude	filter for output that excludes the specified string

include	filter for output that includes the specified string
WORD	the specified string
count	count the number of outputted lines
count-only	count the number of lines while suppressing screen output

show ip arp

The **show ip arp** command displays the Internet Protocol (IP) Address Resolution Protocol (ARP) cache table entries for individual interfaces or all interfaces on the BSR. Each ARP entry describes the protocol type, IP address to MAC address binding, age time, ARP type, and interface location and type. Use the additional command arguments to filter the output information you want to receive.

Group Access

All

Command Mode

All modes except for User EXEC

Command Line Usage

show ip arp [<*A.B.C.D*> | <*H.H.H*> | **Hostname** | **cable** <*X*/*Y*> | **ethernet** <*X*/*Y*> | **gigaether** <*X*/*Y*>] [| {**begin** | **exclude** | **include**} {<*WORD*>} [| {**count** | **count-only**}]]

show ip arp [<*A.B.C.D*> | <*H.H.H*> | **Hostname** | **cable** <*X*/*Y*> | **ethernet** <*X*/*Y*> | **gigaether** <*X*/*Y*>] [| {**count** | **count-only**}]

Command Syntax

A.B.C.D	Displays entries matching IP address
H.H.H	Displays entries showing a 48 bit MAC address.
Hostname	Displays entries matching a hostname
cable *X*/*Y*	Cable interface ARP entries for a specified BSR slot and port number.
ethernet *X*/*Y*	Ethernet interface ARP entries for a specified BSR port number. *X* is 0. *Y* is the port number.
gigaether *X*/*Y*	Gigabit Ethernet interface ARP entries for a specified BSR port number. *X* is 0. *Y* is the port number.
|	turns on output modifiers (filters)

begin	filter for output that begins with the specified string
exclude	filter for output that excludes the specified string
include	filter for output that includes the specified string
WORD	the specified string
count	count the number of outputted lines
count-only	count the number of lines while suppressing screen output

show ip dhcp stats

The **show ip dhcp stats** command displays DHCP server statistical information. including memory usage, counters, and DHCP messages sent and received for a specified slot or all slots on the BSR.

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show ip dhcp stats [<*NUM*>]

Command Syntax

NUM	This is always 0 for the BSR 2000.

show ip interface

The **show ip interface** command displays the status, statistical information, and configuration for the network interfaces. The **show ip interface** command without any command arguments displays status, statistical information, and configuration for all interfaces.

Group Access

All

Command Mode

Privileged EXEC

Command Line Usage

show ip interface [**brief** | **cable** <*X*/*Y*> | **ethernet** <*X*/*Y*> | **gigaether** <*X*/*Y*> | **loopback** <*1-64*>] [| {**begin** | **exclude** | **include**} {<*WORD*>} [| {**count** | **count-only**}]]

show ip interface [**brief** | **cable** <*X*/*Y*> | **ethernet** <*X*/*Y*> | **gigaether** <*X*/*Y*> | **loopback** <*1-64*>] [| {**count** | **count-only**}]

Command Syntax

brief	Provides a brief summary of IP status and configuration information for a specific interface or all interfaces.
cable *X*/*Y*	*X* is 0. *Y* is the Cable interface port number.
ethernet *X*/*Y*	*X* is 0. *Y* is the Ethernet interface port number.
gigaether *X*/*Y*	*X* is 0. *Y* is the Gigabit Ethernet interface port number.
loopback *1-64*	Loopback interface number.
|	turns on output modifiers (filters)
begin	filter for output that begins with the specified string

exclude	filter for output that excludes the specified string
include	filter for output that includes the specified string
WORD	the specified string
count	count the number of outputted lines
count-only	count the number of lines while suppressing screen output

show ip irdp

The **show ip irdp** command displays ICMP Router Discovery Protocol information including interface holdtime values, configured preface values, and advertisement values for specified Ethernet or Gigabit Ethernet interfaces or all Ethernet or Gigabit Ethernet interfaces on the BSR.

Group Access

All

Command Mode

Privileged EXEC

Command Line Usage

show ip irdp [**cable** <*X*/*Y*> | **ethernet** <*X*/*Y*> | **gigaether** <*X*/*Y*>] [| {**begin** | **exclude** | **include**} {<*WORD*>} [| {**count** | **count-only**}]]

show ip irdp [**cable** <*X*/*Y*> | **ethernet** <*X*/*Y*> | **gigaether** <*X*/*Y*>] [| {**count** | **count-only**}]

Command Syntax

cable <*X*/*Y*>	*X* is 0. *Y* is the Cable interface port number
ethernet <*X*/*Y*>	*X* is 0. *Y* is the Ethernet interface port number.
gigaether <*X*/*Y*>	*X* is 0. *Y* is the Gigabit Ethernet interface port number.
|	turns on output modifiers (filters)
begin	filter for output that begins with the specified string
exclude	filter for output that excludes the specified string
include	filter for output that includes the specified string
WORD	the specified string

count	count the number of outputted lines
count-only	count the number of lines while suppressing screen output

show ip protocols

The **show ip protocols** command is used for debugging routing activity and processes by displaying the status of routing protocol processes currently on the system.

Group Access

All

Command Mode

Privileged EXEC

Command Line Usage

show ip protocols [**bgp** | **summary**] [| {**begin** | **exclude** | **include**} {<*WORD*>} [| {**count** | **count-only**}]]

show ip protocols [**bgp** | **summary**] [| {**count** | **count-only**}]

Command Syntax

bgp	display the status of Border Gateway Protocol processes
summary	display a summary of system routing protocol processes
|	turns on output modifiers (filters)
begin	filter for output that begins with the specified string
exclude	filter for output that excludes the specified string
include	filter for output that includes the specified string
WORD	the specified string
count	count the number of outputted lines
count-only	count the number of lines while suppressing screen output

show ip route

The **show ip route** command displays the active entries in the routing table.

Note: The information displayed reflects the routes that the routing table has exported in the routing protocol that were filtered by that protocol's export routing policy statements.

Group Access

All

Command Mode

Privileged EXEC and Global Configuration

Command Line Usage

show ip route [<*A.B.C.D*> [<*A.B.C.D*> | **longer-prefixes**]] [**bgp** | **connected** | **hostname** | **ospf** | **rip** | **static** | **summary**] [| {**begin** | **exclude** | **include**} {<*WORD*>} [| {**count** | **count-only**}]]

show ip route [<*A.B.C.D*> [<*A.B.C.D*> | **longer-prefixes**]] [**bgp** | **connected** | **hostname** | **ospf** | **rip** | **static** | **summary**] [| {**count** | **count-only**}]

Command Syntax

A.B.C.D	Displays route for an IP address.
A.B.C.D	Enter the subnet mask for the specified IP address to filter routes from a specific subnetwork.
longer-prefixes	Display routes matching the specified Network/Mask pair only.
bgp	Displays Border Gateway Protocol routes.
connected	Displays connected routes.
hostname	Displays routes for the internet hostname.
ospf	Displays OSPF routes.

rip	Displays RIP routes.
static	Displays static routes.
summary	Displays a summary of routes in the BSR routing table.
|	turns on output modifiers (filters)
begin	filter for output that begins with the specified string
exclude	filter for output that excludes the specified string
include	filter for output that includes the specified string
WORD	the specified string
count	count the number of outputted lines
count-only	count the number of lines while suppressing screen output

show ip traffic

The **show ip traffic** command displays IP, ICMP, UDP, TCP, ARP, OSPF, IGMP, PIM, and RADIUS protocol packet statistics, depending on what protocols are in use on the BSR.

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show ip traffic [| {**begin** | **exclude** | **include**} {<*WORD*>} [| {**count** | **count-only**}]]

show ip traffic [| {**count** | **count-only**}]

Command Syntax

|	turns on output modifiers (filters)
begin	filter for output that begins with the specified string
exclude	filter for output that excludes the specified string
include	filter for output that includes the specified string
WORD	the specified string
count	count the number of outputted lines
count-only	count the number of lines while suppressing screen output

show sntp

The Simple Network Time Protocol (SNTP) provides system time with high accuracy. The **show sntp** command output displays the following SNTP information for the BSR:

SNTP server	Configured SNRP to request NTP packets or broadcast NTP server address
stratum	Number of NTP hops a machine is from an authoritative time source
version	NTP server version
last receive	When the last update was received
trusted server	"Yes" - if an authentication was attempted and succeeded; "No" - otherwise

Group Access

System Administrator

Command Mode

Privileged EXEC

Command Line Usage

show sntp

show tcp brief

The **show tcp brief** command displays a brief summary of TCP status and configuration.

Group Access

All

Command Mode

Privileged EXEC

Command Line Usage

show tcp brief

show tcp statistics

The **show tcp statistics** command displays the Transmission Control Protocol (TCP) statistics. The **show tcp statistics** command displays the following information:

rcvd	Statistics in this section refer to packets received by the router.
total	Packets received.
no port	Number of packets received with no port.
checksum error	number of packets received with checksum error
bad offset	number of packets received with bad offset to data
too short	number of packets received that were too short
packets in sequence	number of data packets received in sequence
dup packets	number of duplicate packets received
partially dup packets	number of packets received with partially duplicated data
out-of-order packets	number of packets received out of order
packets with data after window	number of packets received with data that exceeds the receiver window size
packets after close	number of packets received after the connection has been closed
window probe packets	number of window probe packets received
window update	number of window update packets received
dup ack packets	number of duplicate acknowledgment packets received
ack packets with unsent data	number of acknowledgment packets with unsent data received

ack packets	number of acknowledgment packets received
sent	statistics for packets sent by the router
total	total number of packets sent
urgent packets	number of urgent packets sent
control packets	number of control packets (SYN, FIN, or RST) sent
data packets	number of data packets sent
data packets retransmitted	number of data packets retransmitted
ack only packets	number of packets sent that are acknowledgments only
window probe packets	number of window probe packets sent
window update packets	number of window update packets sent
connections initiated	number of connections initiated
connections accepted	number of connections accepted
connections established	number of connections established
connections closed	number of connections closed
total rxmt timeout	number of times the router tried to retransmit, but timed out
connections dropped in rxmit timeout	number of connections dropped in retransmit timeout
keepalive timeout	number of keepalive packets in timeout
keepalive probe	number of keepalive probes
connections dropped in keepalive	number of connections dropped in keepalive

Group Access

All

Command Mode

Privileged EXEC

Command Line Usage

show tcp statistics

shutdown

The **shutdown** command disables an interface. An interface is in a shutdown state when some configuration tasks must be performed on the interface.

All interfaces on the BSR are shutdown by default. The **no shutdown** command is used to enable a disabled interface.

Note: Use the **show interfaces** command to display which interfaces are enabled or disabled.

Group Access

System Administrator

Command Mode

Interface Configuration

Command Line Usage

shutdown

no shutdown

sntp authenticate

The **sntp authenticate** command enables authentication for SNTP. The **no sntp authenticate** command disables authentication for SNTP.

Group Access

System Administrator

Command Mode

Global Configuration

Command Line Usage

sntp authenticate

no sntp authenticate

sntp authentication-key

The **sntp authentication-key** command enables authentication for SNTP. The **no sntp authentication-key** command disables authentication for SNTP.

Use the **sntp authentication-key** command to authenticate SNTP sources for additional security.

Group Access

System Administrator

Command Mode

Global Configuration

Command Line Usage

sntp authentication-key <*1-4294967295*> [**md5** <*WORD*>]

no sntp authentication-key <*1-4294967295*>

Command Syntax

1-4294967295	Key number.
md5	Use the md5 algorithm (presently this is the only algorithm supported).
WORD	Key value, up to 8 characters.

sntp broadcastdelay

The **sntp broadcastdelay** command establishes the length of a round trip between the system and a broadcast server. The **no sntp broadcastdelay** command removes the length of a round trip between the system and a broadcast server and returns it to the default.

Use the **sntp broadcastdelay** command to set the exact time between the router as a broadcast client and the network.

Group Access

System Administrator

Command Mode

Global Configuration

Command Line Usage

sntp broadcastdelay <*1-999999*>

no sntp broadcastdelay <*1-999999*>

Command Syntax

1-999999	Microseconds calculated on round-trip time for SNTP transactor.

Command Default

3000 microseconds

sntp broadcast client

The **sntp broadcast client** command configures a router to listen for SNTP broadcasts. The **no sntp broadcast client** command blocks the router from receiving SNTP broadcast traffic.

Use the **sntp broadcast client** command to receive NTP traffic from a broadcast server.

Group Access

System Administrator

Command Mode

Global Configuration

Command Line Usage

sntp broadcast client

no sntp broadcast client

sntp disable

The **sntp disable** command disables SNTP on an interface. The **no sntp disable** command enables the interface to accept NTP traffic from other servers.

Group Access

System Administrator

Command Mode

Global Configuration

Command Line Usage

sntp disable

no sntp disable

Command Default

Enabled

sntp server

The **sntp server** command configures a router for SNTP to accept NTP traffic. The **no sntp server** command disables the router receiving NTP traffic.

Note: When the server address is set to 224.0.1.1, the assigned multicast address for NTP, the BSR operates in unicast mode. It transmits a request to this multicast address and waits for replies. It then "binds" to the first server who replies. All subsequent transactions happen in a unicast mode. This way, the server address need not be known beforehand.

If you configure the BSR to operate in authenticated mode, you must also configure an authentication key (**sntp authentication-key** command) and a trusted key (trusted-key command).

Caution: If the sntp server configuration command is specified, the clock timezone command must also be specified. Otherwise, the timezone may not be initialized properly and wildly fluctuating time changes may be recorded.

Group Access

System Administrator

Command Mode

Global Configuration

Command Line Usage

sntp server {**224.0.1.1** | <*A.B.C.D*> | **Hostname**} [**key** <*1-4294967295*>]

no sntp server

Command Syntax

224.0.1.1	NTP Multicast group
A.B.C.D	Server IP address.

Hostname	Host server name.
key *1-4294967295*	Key number for authentication purpose.

Command Default

SNTP traffic not accepted from a time server

sntp timer

The **sntp timer** command specifies the time interval between queries to the SNTP server. The **no sntp timer** command remove the time interval.

Group Access

System Administrator

Command Mode

Global Configuration

Command Line Usage

sntp timer <*1-86400*>

no sntp timer

Command Syntax

1-86400	the time interval in seconds

sntp trusted-key

The **sntp trusted-key** command authorizes synchronization and authenticates system identity. The **no ntp trusted-key** command disables synchronization and removes system identity.

Use the **sntp trusted-key** command to establish a key or keys following the **sntp authentication-key** command to synchronize the system. The **sntp trusted-key** command synchronizes with only those systems that are trusted delivering additional security.

Group Access

System Administrator

Command Mode

Global Configuration

Command Line Usage

sntp trusted-key <*1-4294967295*>

no sntp trusted-key <*1-4294967295*>

Command Syntax

1-4294967295	Trusted authentication key-number for trusted time source.

Command Default

No trusted keys defined

traceroute

The **traceroute** command is used to trace the route that packets take through the network from their source to their destination. The BSR sends out a sequence of User Datagram Protocol (UDP) datagrams to an invalid port address at the remote host to trace the route through the network, as follows:

- First, three UDP datagrams are sent, each with a TTL field value set to 1. The TTL value of 1 causes the datagram to "timeout" as soon as it reaches the first router in the path. The router responds with an ICMP "time exceeded" message indicating that the datagram has expired.
- Next, three more UDP datagrams are sent, each with the TTL value set to 2. This causes the second router in the path to the destination to return an ICMP "time exceeded" message.

This process continues until the UDP datagrams reach the destination and the system originating the traceroute has received an ICMP "time exceeded" message from every router in the path to the destination. Since the UDP datagrams are trying to access an invalid port at the destination host, the host responds with an ICMP "port unreachable" message which signals the traceroute program to finish. The following is typical screen output from the **traceroute** command:

```
traceroute to 150.31.40.10 : 1-64 hops, 38 byte packets
 1  172.17.103.65   0.000 ms  0.000 ms  0.000 ms
 2  172.17.1.1   0.000 ms  0.000 ms  0.000 ms
 3  150.31.1.21   0.000 ms  16.7 ms  0.000 ms
 4  150.31.40.10   0.000 ms  0.000 ms  0.000 ms

Trace complete
```

Group Access

All

Command Mode

User EXEC and Privileged EXEC

Command Line Usage

traceroute {<*A.B.C.D*> | **Hostname**} [**Source** <*A.B.C.D*>] [**timeout** <*1-1024*>] [**nprobes** <*1-1024*>] [**minhops** <*1-64*>] [**maxhops** <*2-1024*>] [**port** <*0-65535*>] [**tos** <*0-255*>] [**df**]

Command Syntax

A.B.C.D	the source IP address.
Hostname	the Domain Name Server (DNS) hostname.
Source *A.B.C.D*	the IP address of the source interface
timeout *1-1024*	the number of seconds to wait for a response to a probe packet
nprobes *1-1024*	the number of probes to send
minhops *1-64*	the TTL value for the first probe - the default value is 1 but can be set to a higher value to suppress the display of known hops
maxhops *2-1024*	the largest TTL value that can be used - the **traceroute** command terminates when the destination or this value is reached
port *0-65535*	the destination port used by the UDP probe messages
tos *0-255*	the type of service value
df	set the "Don't Fragment" flag in the IP header

Command Defaults

timeout = 3 seconds

nprobes = 3

minhops = 1

maxhops = 64

port = 32868

tos = 0

df = disabled

trap-enable-if

The **trap-enable-if** command enables the *ifLinkUpDownTrapEnable* trap. The *ifLinkUpDownTrapEnable* trap indicates whether a link up or link down trap should be generated for an interface. The **no trap-enable-if** command disables the *ifLinkUpDownTrapEnable* trap.

Group Access

All

Command Mode

Interface Configuration

Command Syntax

trap-enable-if

no trap-enable-if

Command Default

Disabled

trap-enable-rdn

The **trap-enable-rdn** command enables the *rdnCardIfLinkUpDownEnable* trap. The *rdnCardIfLinkUpDownEnable* trap indicates whether a link up or link down trap should be generated for a BSR module. The **no trap-enable-rdn** command disables the *rdnCardIfLinkUpDownEnable* trap.

Group Access

All

Command Mode

Interface Configuration

Command Syntax

trap-enable-rdn

no trap-enable-rdn

Command Default

Disabled

3

SNMP Commands

Introduction

This chapter describes the Simple Network Management Protocol (SNMP) commands used to manage the BSR 2000.

Since it was developed in 1988, SNMP has become the de facto standard for internetwork management. SNMP is an application layer protocol and is based on the manager/agent model. SNMP is referred to as simple because the agent requires minimal software. Most of the processing power and the data storage resides on the management system, with a subset of those functions residing in the managed system.

A typical agent usually implements the SNMP protocol, stores and retrieves management data (as defined by the MIB); can asynchronously signal an event to the manager; and can be a proxy for some non-SNMP network node.

A typical manager implemented as a Network Management Station (NMS) Network-management stations implements the SNMP protocol; learns of problems by receiving event notifications, called traps, from network devices implementing SNMP; is able to query agents; gets responses from agents; sets variables in agents; and acknowledges synchronous events from agents.

The primary protocols that SNMP runs on are the User Datagram Protocol (UDP) and IP. SNMP also requires Data Link Layer protocols such as Ethernet to implement the communication channel from the management to the managed agent.

SNMP Command Descriptions

This section contains an alphabetized list and descriptions of the SNMP commands supported by the BSR.

show snmp

The **show snmp** command displays SNMP statistics, determine the running status, and display configuration information such as chassis ID, system description, and system location, chassis ID, and counter information for the SNMP process. The **show snmp** command, without arguments, displays the following information:

SNMP In Packets	total number of SNMP packets received by the SNMP agent
Bad SNMP version errors	number of bad SNMP packets received with bad SNMP version errors
Unknown community names	number of SNMP packets received with unknown community names
Illegal operations for community names supplied	number not allowed
ASN parse errors	number incorrectly encoded
Requested variables	variables requested by SNMP managers
Changed variables	variables altered by SNMP managers
Get requests	numberof get-request PDUs received
Get-next requests	number of get-next PDUs received
Set requests	number of set request PDUs received
SNMP Out Packets	number of SNMP packets sent by the agent
Packets too big	larger than maximum packet size sent by the agent
No such name errors	name errors nonexistent number, undefinable Management Information Base (MIB)
Bad values	number of set requests that detail an invalid value for a MIB object

General errors	number of requests failed due to some other error, excluding a *noSuchName* error, *badValue* error, or any of the other specific errors
Responses	number of responses
Traps	number of traps sent
Traps Dropped due to throttling	number of traps dropped due to exceeding a throttling rate limit
Informs	number of inform requests sent
Notification Errors	number of notification errors sent
Probes	number of probes sent
Inform Retries	number of inform retries sent
Probe Retries	number of probe retries sent

Group Access

All

Command Mode

show snmp without arguments - all modes

show snmp with arguments - all modes except User EXEC

Command Line Usage

show snmp [**access** | **chassis-id** | **community** | **contact** | **context** | **description** | **engineID** | **group** | **host** | **location** | **packetsize** | **port** | **sysname** | **traps** | **users** | **view**]

Command Syntax

access	Displays SNMPv3 access rights for SNMP groups and users with security models and levels. It also displays the associations between SNMP views and these security parameters.
chassis-id	Displays SNMP chassis-id information
community	Displays information about configured SNMP communities.
contact	Displays SNMP system contact information from the MIB object *sysContact*.
context	Displays SNMPv3 context information from the MIB object *sysContext*.
description	Display SNMP system description from MIB object *sysDescr*.
engineID	Displays the local and remote SNMPv3 engines that were configured on the BSR.
group	Displays SNMPv3 groups.
host	Displays the hosts configured to receive SNMP notifications - both SNMP Traps and Informs.
location	Displays SNMP system location information from the *sysLocation* MIB object.
packetsize	Displays the maximum SNMP packet size that the SNMP agent can send and receive. The maximum packet size is 484-17940 bytes.
port	Displays the UDP port number on which the SNMP agent is configured.
sysname	Displays the system information from the *sysName* MIB object.

traps	Displays a list of SNMP traps.
users	Displays a list of configured SNMPv3 users stored in the SNMP group username table and their associated access privileges, such as engineID and security level.
view	Displays the SNMPv3 view-name and the object-identifier subtrees associated with it

snmp-server access

The **snmp-server access** command defines access policy information. The **no snmp-server access** command clears the SNMP access policies..

Note: Community Name Access Method is used predominantly with SNMP v1 and v2c.

Group Access

System Administrator

Command Mode

Global Configuration

Command Line Usage

snmp-server access <*WORD*> {**v1** | **v2c** | **v3** {**noauth** | **auth** | **priv** }} [**notify** <*WORD*>] [**match** {**exact** | **prefix**} | **prefix** <*WORD*>] [**read** <*WORD*> [**notify** | **write**]] [**write** <*WORD*> [**notify**]]

no snmp-server access <*WORD*> {**v1** | **v2c** | **v3** {**noauth** | **auth** | **priv** }} [**prefix** <*WORD*>]

Command Syntax

WORD	SNMP group name
v1	access group using v1 security model
v2c	access group using v2c security model
v3	access group using v3 security model (USM)
noauth	no authentication
auth	authentication
priv	privacy

notify *WORD*	specify a notify view name from 0 to 32 bits in length
prefix *WORD*	specify a prefix name from 0 to 32 bits in length
match	specify match parameters
exact	match exact
prefix	match prefix
read *WORD*	specify a read view name from 0 to 32 bits in length
notify	specify a notify view for this access group
write	specify a write view for this access group
write *WORD*	specify a write view name from 0 to 32 bits in length

snmp-server chassis-id

The **snmp-server chassis-id** command specifies a new chassis ID to uniquely identify the SNMP server's chassis. The **no snmp-server chassis-id** command returns the chassis ID to the default value which is the serial number of the chassis.

Group Access

System Administrator

Command Mode

Global Configuration

Command Line Usage

snmp-server chassis-id <*string*>

no snmp-server chassis-id <*string*>

Command Syntax

string	a unique ID string which overwrites the MIB object *chassisId*

Command Default

Defaults to chassis serial number

snmp-server community

The **snmp-server community** command enables SNMP and sets community strings and access privileges. The **no snmp-server community** command removes community strings and access privileges to a particular SNMP community.

Group Access

System Administrator

Command Mode

Global Configuration

Command Line Usage

snmp-server community <*WORD*> [<*1-199*> | **ro** | **rw** | **view** <*WORD*>]

no snmp-server community <*WORD*>

Command Syntax

1-199	IP access list allowed access with this community string
ro	set read-only access with this community string
rw	sets read-write access; authorized management stations can retrieve and modify MIB objects
view *WORD*	MIB view to restrict community

snmp-server community-table

The **snmp-server community-table** command configures the *snmpCommunityTable* which is part of the *snmpCommunityMIB* (RFC 2576). The *snmpCommunityMIB* defines objects to help support coexistence between SNMPv1, SNMPv2c, and SNMPv3.

The *snmpCommunityTable* contains a database of community strings and provides mappings between community strings and the parameters required for View-based Access Control.

Group Access

System Administrator

Command Mode

Global Configuration

Command Line Usage

snmp-server community-table <*octet-string*> <*octet-string*> [**access-list** <*num*> | **active** | **context-name** | **eng-id** | **index** | **nonvolatile** | **not-in-service** | **transport-tag** | **volatile**]

no snmp-server community-table <*octet-string*>

Command Syntax

octet-string	the community string (*snmpCommunityName*) whose configuration is represented by a row in this community-table
octet-string	a string representing the corresponding value of *snmpCommunityName* in a Security Model independent format
access-list *num*	the number (1-199) of the IP access-list allowed access with this community string
active	set the *snmpCommunityStatus* object to "active"

context-name	the context in which management information is accessed when using the community string specified by the *snmpCommunityName*
eng-id	specifies the context EngineID (*snmpCommunityContextEngineID*) indicating the location of the context in which management information is accessed when using the community string specified by the corresponding value of the *snmpCommunityName* object
index	the unique index value of a row in the *snmpCommunityTable*
nonvolatile	specifies the storage type (*snmpCommunityStorageType)* as nonvolatile which is defined as having persistent memory so that the storage content remains after the device is turned off and on again
not-in-service	sets the *snmpCommunityStatus* object to "notInService"
transport-tag	specifies the transport tag (*snmpCommunityTransportTag*) which is a set of transport endpoints from which a SNMP command responder application will accept management requests - if a management request containing this community is received on a transport endpoint other than the transport endpoints identified by this object, the request is deemed unauthentic
volatile	specifies the storage type (*snmpCommunityStorageType)* as volatile which is the defined as having temporary memory and so that the storage content is deleted if the device is turned off

Command Default

snmpCommunityStatus = active

snmpCommunityStorageType = nonvolatile

snmp-server contact

The **snmp-server contact** command specifies the contact information in the *sysContact* MIB object

Group Access

System Administrator

Command Mode

Global Configuration

Command Line Usage

snmp-server contact <*string*>

Command Syntax

string	name of system contact person- provides text for the MIB object *sysContact*

Command Default

no contact set

snmp-server context

The **snmp-server context** defines or updates a context record. The **no snmp-server context** command clears a context record.

Note: By defining a context record, an access policy can be specified that includes the context. The context record identifies object resources that are accessible.

Group Access

System Administrator

Command Mode

Global Configuration

Command Line Usage

snmp-server context <*WORD*>

no snmp-server context <*WORD*>

Command Syntax

WORD	the name of context record - provides text for the MIB object *sysContext*

snmp-server convert

The **snmp-server convert** command converts a key or password to a localized authentication key.

Group Access

System Administrator

Command Mode

Global Configuration

Command Line Usage

snmp-server convert {**key** <*WORD*> | **password** <*WORD*> } {**md5** | **sha**} [**eng-id** <*HEX*>]

Command Syntax

key *WORD*	specify the key to convert to a localized authentication key
password *WORD*	specify the password to convert to a localized authentication key
md5	use MD5 Authentication
sha	use SHA Authentication
eng-id *HEX*	specify the engine-id- if not specified the local engine ID is used

snmp-server docs-trap-control

The **snmp-server docs-trap-control** command enables various CMTS traps. The **no snmp-server docs-trap-control** disables the CMTS trap.

Group Access

System Administrator

Command Mode

Global Configuration

Command Line Usage

snmp-server docs-trap-control {**cmtsBPKMTrap** | **cmtsBpiInitTrap** | **cmtsDCCAckFailTrap** | **cmtsDCCReqFailTrap** | **cmtsDCCRspFailTrap** | **cmtsDynServAckFailTrap** | **cmtsDynServReqFailTrap** | **cmtsDynServRspFailTrap** | **cmtsDynamicSATrap** | **cmtsInitRegAckFailTrap** | **cmtsInitRegReqFailTrap** | **cmtsInitRegRspFailTrap**}

no snmp-server docs-trap-control {**cmtsBPKMTrap** | **cmtsBpiInitTrap** | **cmtsDCCAckFailTrap** | **cmtsDCCReqFailTrap** | **cmtsDCCRspFailTrap** | **cmtsDynServAckFailTrap** | **cmtsDynServReqFailTrap** | **cmtsDynServRspFailTrap** | **cmtsDynamicSATrap** | **cmtsInitRegAckFailTrap** | **cmtsInitRegReqFailTrap** | **cmtsInitRegRspFailTrap**}

Command Syntax

cmtsBPKMTrap	the failure of a BPKM operation detected on the CMTS side
cmtsBpiInitTrap	the failure of a BPI initialization attempt happened during the CM registration process and detected on the CMTS side
cmtsDCCAckFailTrap	the failure of a dynamic channel change acknowledgement that happened during the dynamic channel change process on the CMTS side

cmtsDCCReqFailTrap	the failure of a dynamic channel change request that happened during the dynamic channel change process on the CM side and detected on the CMTS side
cmtsDCCRspFailTrap	the failure of a dynamic channel change response that happened during the dynamic channel change process on the CMTS side
cmtsDynServAckFailTrap	the failure of a dynamic service acknowledgement that happened during the dynamic services process and detected on the CMTS side
cmtsDynServReqFailTrap	the failure of a dynamic service request that happened during the dynamic services process and detected on the CMTS side
cmtsDynServRspFailTrap	the failure of a dynamic service response that happened during the dynamic services process and detected on the CMTS side
cmtsDynamicSATrap	the failure of a dynamic security association operation detected on the CMTS side
cmtsInitRegAckFailTrap	the failure of a registration acknowledgement from the CM that happened during the CM initialization process and was detected on the CMTS side
cmtsInitRegReqFailTrap	the failure of a registration request from the CM happened during the CM initialization process and was detected on the CMTS side
cmtsInitRegRspFailTra	the failure of a registration response happened during the CM initialization process and was detected on the CMTS side

snmp-server enable informs

The **snmp-server enable informs** command enables SNMP informs and allows this SNMP management station to send SNMP informs to hosts also configured to accept informs using this command.

The **snmp-server host** command configures a host or hosts to accept SNMP informs. At least one SNMP-server host must be configured. For a host to receive an inform, an **snmp-server host informs** command must be configured for that host, and the inform must then be enabled globally through the use of the **snmp-server enable informs** command.

The **no snmp-server enable informs** command disables sending inform notification messages from this SNMP management station.

Group Access

System Administrator

Command Mode

Global Configuration

Command Line Usage

snmp-server enable informs

no snmp-server enable informs

Command Default

Disabled

snmp-server enable traps

The **snmp-server enable traps** command enables SNMP traps and allows the SNMP agent to send an unsolicited notification to one or more pre-configured management stations. The **no snmp-server enable traps** command disables all SNMP traps or a specific trap type.The **snmp-server enable traps** command enables all SNMP traps or specific types of traps and allows this SNMP management station to send SNMP traps to hosts identified to receive traps with the **snmp-server host** command. At least one SNMP-server host must be configured.

Note: The **snmp-server enable traps** command without arguments enables BGP, OSPF, and SNMP state change traps.

Group Access

System Administrator

Command Mode

Global Configuration

Command Line Usage

snmp-server enable traps [**bgp** | **docsdevcmts** | **entity** | **flap** | **ospf** | **pim** | **registration** | **snmp** | **snr**]

no snmp-server enable traps [**bgp** | **docsdevcmts** | **entity** | **flap** | **ospf** | **pim** | **registration** | **snmp** | **snr**]

Command Syntax

bgp	enable BGP state change traps
docsdevcmts	enable docs device cmts traps
entity	enable entity state change traps
flap	enable flap state change traps
ospf	enable OSPF state change traps
pim	enable PIM state change traps

registration	enable CM (de)registration traps
snmp	enable SNMP state change traps
snr	enable signal-to-noise ratio measurement traps

Command Default

Disabled

snmp-server engineID

The **snmp-server engineID** command specifies an identification name (ID) for a local or remote SNMPv3 engine. The **no snmp-server engineID** command returns the local agent engineID to the default, or deletes a remote engineID from the agent.

Note: A local SNMP Engine ID must be configured to use SNMPv3.The SNMP agent is configured with a default Engine ID equal to the MAC address of the chassis.

Group Access

System Administrator

Command Mode

Global Configuration

Command Line Usage

snmp-server engineID {**local** <*HEX*>} {**remote** <*A.B.C.D*> [**udp-port** <*0-65535*>] <*HEX*>}

no snmp-server engineID {**local** <*HEX*>} {**remote** <*A.B.C.D*> [**udp-port** <*0-65535*>] <*HEX*>}

Command Syntax

local	sets local engine identification
HEX	engine ID octet string
remote	change or add remote engine id parameters
A.B.C.D	IP address of remote SNMP notification host
udp-port	configures a remote engine-ID
0-65535	UDP port number

snmp-server group

The **snmp-server group** command associates (or maps) SNMP groups to SNMP users. Use the **no snmp-server group** command to delete the group or a table to match SNMP users with SNMP groups.

The **snmp-server group** command is used to create an SNMP group, associate it with an SNMP user, and define a security level (SNMPv1, v2c, v3) for use with the group.

Group Access

System Administrator

Command Mode

Global Configuration

Command Line Usage

snmp-server group <*WORD*> <*WORD*> [**v1** | **v2c** | **v3**]

no snmp-server group <*WORD*> <*WORD*> [**v1** | **v2c** | **v3**]]

Command Syntax

WORD	security name belonging to this group
WORD	name of user creating group - user (security name) belonging to this group
v1	provides the least security
v2c	provides the next level of security
v3	provides the most security

snmp-server host

The **snmp-server host** command configures the SNMP agent to send notifications to a remote host. You configure an SNMP inform or trap host with the **snmp-server host** command by specifying the receiver of specific inform or trap types. All informs or raps are sent if one is not specified. Each time the **snmp-server host** command is used, one host acting as a inform or trap recipient is configured. The **no snmp-server host** clears the host recipient from receiving SNMP notification activity.

Note: A maximum of 40 remote hosts can be specified with the **snmp-server host** command.

Note: If the *community-string* is not defined using **snmp-server community** command prior to using the **snmp-server host** command, the default form of the **snmp-server community** command is automatically inserted into the configuration. The password (*community-string*) used for this default configuration is the same as that specified in the **snmp-server host** command.

When removing an SNMP trap host from the trap host list with the **no snmp-server host** command, the community name that is specified in the command must exist. If the community name does not exist, the command will fail.

Group Access

System Administrator

Command Mode

Global Configuration

Command Line Usage

snmp-server host <*A.B.C.D*> {<*WORD*>} {**informs** {<*WORD*> | **version** {**1** | **2c** | **3** {**auth** | **noauth** | **priv**}}} {**traps** {<*WORD*> | **version** {**1** | **2c** | **3** {**auth** | **noauth** | **priv**}}} {**version** {**1** | **2c** | **3** {**auth** | **noauth** | **priv**} {<*WORD*>}}} [**bgp** | **docsdevcmts** | **entity** | **environ** | **flap** | **ospf** | **pim** | **snmp** | **snr** | **udp-port**<*0-65535*>]

no snmp-server host <*A.B.C.D*> {<*WORD*>} {**informs** {<*WORD*> | **version** {**1** | **2c** | **3** {**auth** | **noauth** | **priv**}}} {**traps** {<*WORD*> | **version** {**1** | **2c** | **3** {**auth** | **noauth** | **priv**}}} {**version** {**1** | **2c** | **3** {**auth** | **noauth** | **priv**} {<*WORD*>}}} [**bgp** | **docsdevcmts** | **entity** | **environ** | **flap** | **ospf** | **pim** | **snmp** | **snr** | **udp-port**<*0-65535*>]

ommand Syntax

A.B.C.D	IP address of SNMP notification host
WORD	1 to 32 alphabetic characters specifying an SNMP community
informs	enable SNMP informs
version	version to use for notification messages
1	lowest security level
2c	second level, more than security level 1
auth	most secure level, authenticates without encryption
no auth	no authentication, unscrambled packet
priv	privileged level, authenticates and scrambles packet
traps	enable SNMP traps
bgp	send BGP state change informs or traps
docsdevcmts	send *docsdevicecmts* change informs or traps
entity	send entity state change informs or traps
environ	send SNMP environment change informs or traps
flap	send flap state change informs or traps
ospf	send OSPF state change informs or traps
pim	send PIM state change informs or traps
snmp	send SNMP state change informs or traps

snr	enable signal-to-noise ratio meaurement traps
udp-port *0-65535*	the UDP port number for the host to use

Command Default

No hosts configured

snmp-server location

The **snmp-server location** command specifies the system location information in the *sysLocation* MIB object.

Group Access

System Administrator

Command Mode

Global Configuration

Command Line Usage

snmp-server location <*string*>

Command Syntax

string	text for MIB object *sysLocation*; identifies the physical location of the SNMP server, using 1 to 255 alphanumeric characters including spaces

snmp-server notify

The **snmp-server notify** command specifies the target addresses for notifications by setting the *snmpNotifyName* object in the *snmpNotifyTable* and the *snmpNotifyTag* object in the *snmpTargetAddrTable*.

The *snmpNotifyTable* contains entries which are used to select which entries in the *snmpTargetAddrTable* should be used for generating notifications and the type of notifications to be generated.

Group Access

System Administrator

Command Mode

Global Configuration

Command Line Usage

snmp-server notify <*octet-string*> <*octet-string*> {**inform** | **trap**} {**nonvolatile** | **volatile**} [**active** | **not-in-service**]

no snmp-server notify <*octet-string*>

Command Syntax

octet-string	specifies the *snmpNotifyName* (index into the *snmpNotifyTable*) which is a unique identifier associated with this *snmpNotifyEntry*
octet-string	specifies the *snmpNotifyTag* object which is used to select entries in the *snmpTargetAddrTable*
inform	send Inform notification messages to the host identified in the *snmpTargetAddrTable* through the corresponding *snmpNotifyTag*
trap	send Trap notification messages to the host identified in the *snmpTargetAddrTable* through the corresponding *snmpNotifyTag*

nonvolatile	specifies the storage type (*snmpNotifyStorageType*) as nonvolatile which is defined as having persistent memory so that the storage content remains after the device is turned off and on again
volatile	specifies the storage type (*snmpNotifyStorageType*) as volatile which is the defined as having temporary memory and so that the storage content is deleted if the device is turned off
active	sets the *snmpNotifyRowStatus* object to "active"
not-in-service	sets the *snmpNotifyRowStatus* object to "notInService"

Command Default

snmpNotifyRowStatus = active

snmpNotifyStorageType = nonvolatile

snmp-server notify-filter

The **snmp-server notify-filter** configures the *snmpNotifyFilterTable*.The *snmpNotifyFilterTable* is a table containing filter profiles. Filter profiles are used to determine whether a particular management target should receive particular notifications. When a notification is generated, it must be compared to the filters associated with each management target that is configured to receive notifications in order to determine whether the notification can be sent to that management target.

Entries in the *snmpNotifyFilterTable* are created and deleted using the *snmpNotifyFilterRowStatus* object.

Group Access

System Administrator

Command Mode

Global Configuration

Command Line Usage

snmp-server notify-filter <*octet-string*> <*OID*> <*octet-string*> {**excluded** | **included**} {**nonvolatile** | **volatile**} [**active** | **not-in-service**]

no snmp-server notify-filter <*octet-string*> <*OID*>

Command Syntax

octet-string	the name of the filter profile (*snmpNotifyFilterProfileName*) to be used when generating notifications using the corresponding entry in the *snmpTargetAddrTable*
OID	the MIB subtree (*snmpNotifyFilterSubtree*) which, when combined with the corresponding value of the *snmpNotifyFilterMask* object, defines a family of subtrees which are included in or excluded from the filter profile

octet-string	the bit mask (*snmpNotifyFilterMask*) which, in combination with the corresponding OID value of the *snmpNotifyFilterSubtree* object, defines a family of subtrees which are included in or excluded from the filter profile
excluded	indicates whether the family of filter subtrees defined by the *snmpNotifyFilterSubtree* and *snmpNotifyFilterMask* objects are excluded from a filter
included	indicates whether the family of filter subtrees defined by the *snmpNotifyFilterSubtree* and *snmpNotifyFilterMask* objects are included in a filter
nonvolatile	specifies the storage type (*snmpNotifyFilterStorageType)* as nonvolatile which is defined as having persistent memory so that the storage content remains after the device is turned off and on again
volatile	specifies the storage type (*snmpNotifyFilterStorageType)* as volatile which is the defined as having temporary memory and so that the storage content is deleted if the device is turned off
active	sets the *snmpNotifyFilterRowStatus* object to "active"
not-in-service	sets the *snmpNotifyFilterRowStatus* object to "notInService"

Command Default

snmpNotifyFilterMask = empty

snmpNotifyFilterRowStatus = active

snmpNotifyFilterStorageType = nonvolatile

snmp-server notify-filter-profile

The **snmp-server notify-filter-profile** command configures the *snmpNotifyFilterProfileTable*. The *snmpNotifyFilterProfileTable* is used to associate a notification filter profile with a particular set of target parameters. An entry in this table indicates the name of the filter profile to be used when generating notifications using the corresponding entry in the *snmpTargetParamsTable*.

Entries in the *snmpNotifyFilterProfileTable* are created or deleted using the *snmpNotifyFilterProfileRowStatus* object.

Group Access

System Administrator

Command Mode

Global Configuration

Command Line Usage

snmp-server notify-filter-profile <*octet-string*> <*octet-string*> {**nonvolatile** | **volatile**} [**active** | **not-in-service**]

no snmp-server notify-filter-profile <*octet-string*>

Command Syntax

octet-string	specifies the *snmpTargetParamsName* (index into the *snmpTargetParamsTable*) which is a unique identifier associated with this *snmpTargetParamsEntry*
octet-string	specifies the *snmpNotifyFilterProfileName* which is the name of the filter profile to be used when generating notifications using the corresponding entry in the *snmpTargetAddrTable*

nonvolatile	specifies the storage type (*snmpNotifyFilterProfileStorType*) as nonvolatile which is defined as having persistent memory so that the storage content remains after the device is turned off and on again
volatile	specifies the storage type (*snmpNotifyFilterProfileStorType*) as volatile which is the defined as having temporary memory and so that the storage content is deleted if the device is turned off
active	set the *snmpNotifyFilterProfileRowStatus* object to "active"
not-in-service	set the *snmpNotifyFilterProfileRowStatus* object to "notInService"

Command Default

snmpNotifyFilterProfileRowStatus = active

snmpNotifyFilterProfileStorType = nonvolatile

snmp-server packetsize

The **snmp-server packetsize** command sets the maximum SNMP packet size that the server sends or receives. The **no snmp-server packetsize** command sets SNMP packet size back to the default.

Group Access

System Administrator

Command Mode

Global Configuration

Command Line Usage

snmp-server packetsize <*484-17940*>

no snmp-server packetsize

Command Syntax

484-17940	maximum packet size in bytes

Command Default

1400 bytes

snmp-server port number

The **snmp-server port number** sets the UDP port number the SNMP agent is to use. The **no snmp-server port number** sets the UDP port number the SNMP agent is to use back to the default.

Group Access

System Administrator

Command Mode

Global Configuration

Command Line Usage

snmp-server port number <*0-65535*>

no snmp-server port number <*0-65535*>

Command Syntax

0-65535	port number for the SNMP agent to listen

Command Default

161

snmp-server shutdown

The **snmp-server shutdown** command shuts down the SNMP Agent, preventing it from further processing SNMP packets, while retaining all SNMP configuration data in the event the agent is restarted. The **snmp-server shutdown delete** command shuts down the SNMP Agent and deletes all SNMP configuration data (all SNMP configuration data is lost).

Note: The **snmp-server shutdown** command is identical to the **no snmp-server** command.

Group Access

System Administrator

Command Mode

Global Configuration

Command Line Usage

snmp-server shutdown {**delete**}

Command Syntax

delete	deletes all SNMP configuration data upon shutting down (without this option all SNMP configuration data is retained and the agent is suspended).

Command Default

Disabled

snmp-server sysname

The **snmp-server sysname** command specifies the system name information in the *sysLocation* MIB object.

Note: The *sysName* MIB variable is the name of the node. The **show snmp sysname** command gets the *sysName* MIB variable.

Group Access

System Administrator

Command Mode

Global Configuration

Command Line Usage

snmp-server sysname <*string*>

Command Syntax

string	text for the MIB object *sysName*

snmp-server target-addr

The **snmp-server target-addr** command configures the SNMP target address entries in the *snmpTargetAddressTable*. The *snmpTargetAddrTable* contains information about transport domains and addresses to be used in the generation of SNMP operations. It also contains the *snmpTargetAddrTagList* object which provides a mechanism for grouping table entries.

Entries in the *snmpTargetAddrTable* are created or deleted using the *snmpTargetAddrRowStatus* object.

Group Access

System Administrator

Command Mode

Global Configuration

Command Line Usage

snmp-server target-addr <*octet-string*> <*A.B.C.D*> **udp-port** <*0-65535*> <*0-2147483647*> <*0-255*> <*octet-string*> <*octet-string*> <*octet-string*> {0 | <*484-2147483647*>} {**nonvolatile** | **volatile**} [**active** | **not-in-service**]

no snmp-server target-addr <*octet-string*>

Command Syntax

octet-string	specifies the *snmpTargetAddrName* (index into the *snmpTargetAddrTable*) which is a unique identifier associated with this *snmpTargetAddrEntry*
A.B.C.D	the IP address of the SNMP notification host
udp-port *0-65535*	specifies the SNMP notification host's UDP port number
0-2147483647	the expected maximum round trip time (*snmpTargetAddrTimeout*) for communicating with the transport address defined by this row

0-255	specifies a default number of retries (*snmpTargetAddrRetryCount*) to be attempted when a response is not received for a generated message - if an application provides its own retry count, the value of this object is ignored
octet-string	sets the *snmpTargetAddrTagList* object which is a list of tag values which are used to select target addresses for a particular operation - if there is more than one tag, use quotation marks to separate each tag
octet-string	sets the *snmpTargetAddrParams* object which identifies an entry in the *snmpTargetParamsTable* - the identified entry contains SNMP parameters to be used when generating messages to be sent to this transport address
octet-string	sets the *snmpTargetAddrTMask* object which is the mask associated with *snmpTargetParamsTable*
0 | *484-2147483647*	the maximum message size in bytes specified by the *snmpTargetAddrMMS* object - "0" = an empty message
nonvolatile	specifies the storage type (*snmpTargetAddrStorageType)* as nonvolatile which is defined as having persistent memory so that the storage content remains after the device is turned off and on again
volatile	specifies the storage type (*snmpTargetAddrStorageType)* as volatile which is the defined as having temporary memory so that the storage content is deleted if the device is turned off

active	sets the *snmpTargetAddrRowStatus* object to "active"
not-in-service	sets the *snmpTargetAddrRowStatus* object to "notInService"

Command Default

snmpTargetAddrMMS = 484

snmpTargetAddrRowStatus = active

snmpTargetAddrStorageType = nonvolatile

snmp-server target-params

The **snmp-server target-params** configures the *snmpTargetParamsTable*. The *snmpTargetParamsTable* contains information about SNMP version and security information to be used when sending messages to particular transport domains and addresses.

Entries in the *snmpTargetParamsTable* are created or deleted using the *snmpTargetParamsRowStatus* object.

Group Access

System Administrator

Command Mode

Global Configuration

Command Line Usage

snmp-server target-params <*octet-string*> <*0-3*> <*0-3*> <*octet-string*> {**authNoPriv** | **authPriv** | **noAuthNoPriv**} {**nonvolatile** | **volatile**} [**active** | **not-in-service**]

no snmp-server target-params <*octet-string*>

Command Syntax

Command Default

snmpTargetParamsRowStatus = active

snmpTargetParamsStorageType = nonvolatile

octet-string	specifies the *snmpTargetParamsName* (index into the *snmpTargetParamsTable*) which is a unique identifier associated with this *snmpTargetParamsEntry*
0-3	the message processing model (*snmpTargetParamsMPModel*) to be used when generating SNMP messages using this entry 0 = SNMPv1, 1 = SNMPv2c 2 = SNMPv2u and SNMPv2 3 = SNMPv3
0-3	the security model (*snmpTargetParamsSecurityModel*) to be used when generating SNMP messages using this entry - an implementation may choose to return an "inconsistentValue" error if an attempt is made to set this variable to a value for a security model which the implementation does not support 0 = any 1 = SNMPv1 2 = SNMPv2c 3 = USM (User-Based Security)
octet-string	the security name (*snmpTargetParamsSecurityName*) for generating notifications which identifies the principal on whose behalf SNMP messages will be generated using this entry
authNoPriv	set the *snmpTargetParamsSecurityLevel* object to "authorization/no privilege"

authPriv	set the *snmpTargetParamsSecurityLevel* object to "authorization/privilege"
noAuthNoPriv	set the *snmpTargetParamsSecurityLevel* object to "no authorization/no privilege"
nonvolatile	specifies the storage type (*snmpTargetParamsStorageType*) as nonvolatile which is defined as having persistent memory so that the storage content remains after the device is turned off and on again
volatile	specifies the storage type (*snmpTargetParamsStorageType*) as volatile which is the defined as having temporary memory and so that the storage content is deleted if the device is turned off
active	set *snmpTargetParamsRowStatus* to "active"
not-in-service	set *snmpTargetParamsRowStatus* to "notInService"

snmp-server trap rate-limit

The **snmp-server trap rate-limit** command constricts the rate of SNMP messages and log messages sent to a remote host and used by the agent to send an unsolicited notification to one or more pre-configured management stations. The **no snmp-server trap rate-limit** clears the SNMP agent and increases the number of traps sent to a remote host.

Group Access

System Administrator

Command Mode

Global Configuration

Command Line Usage

snmp-server trap rate-limit *<0-2147483647> <0-2147483647>*

no snmp-server trap rate-limit *<0-2147483647> <0-2147483647>*

Command Syntax

0-2147483647	number of SNMP traps; affects both trap and SYSLOG
0-2147483647	per unit time in seconds

snmp-server trap-source loopback

The **snmp-server trap-source loopback** command allows an operator to control the source IP address of SNMP traps generated by the BSR by specifying a loopback interface as the source IP address for SNMP traps. The normal convention for generated SNMP traps is to set the source IP address equal to the IP address of the outgoing interface. The **snmp-server trap-source loopback** command overrides this convention and instead uses the IP address of the specified loopback interface. The **no snmp-server trap-source loopback command removes the loopback source interface.**

Note: Before using the **snmp-server trap-source loopback** command, the loopback interface must be configured and assigned an IP address.

Group Access

System Administrator

Command Mode

Global Configuration

Command Line Usage

snmp-server trap-source loopback *<1-64>*

no snmp-server trap-source loopback *<1-64>*

Command Syntax

<1-64>	the loopback interface number

snmp-server user

The **snmp-server user** command adds a new user to an SNMP group. The **no snmp-server user** command removes a user from an SNMP group.

Group Access

System Administrator

Command Mode

Global Configuration

Command Line Usage

snmp-server user <*WORD*> [**auth** {**sha** | **md5**} {**key** <*string*> [**eng-id** <*HEX*>| **priv des56** <*string*> | **public** <*octet-string*>] | **local** <*string*> [**eng-id** <*HEX*>| **priv des56** <*string*> | **public** <*octet-string*>] | **password** <*string*> [**eng-id** <*HEX*>| **priv des56** <*string*> | **public** <*octet-string*>] | <*string*> [**eng-id** <*HEX*>| **priv des56** <*string*>]}]

no snmp-server user <*WORD*> [**eng-id** <*HEX*>]

Command Syntax

WORD	username
auth	authentication parameters for user
md5	uses HMAC/MD5 algorithm for authentication
sha	uses HMAC/SHA algorithm for authentication
key *string*	specifies a non-localized authentication key (SHA = 20 octets, MD5 = 16 octets)
local *string*	specifies a localized authentication key (SHA = 20 octets, MD5 = 16 octets)
password *string*	specifies a password string (must be at least 8 characters)
string	specifies an authentication password string for this user

eng *HEX*	specifies engine-id with this user; local value of engine ID
priv des56	provides DES-56 bit encryption with authentication based on the CBC-DES (DES-56) standard
public *octet-string*	sets the *usmUserPublic* MIB object

snmp-server view

The **snmp-server view** command defines an SNMPv2 MIB view. The **no snmp-server view** command removes the defined view. You can assign MIB views to SNMP Groups or community strings to limit the MIB objects that an SNMP manager can access. You can use a predefined view or create your own view. Other SNMP commands, such as **snmp-server community**, can use the view to create records associated with a view.

Group Access

System Administrator

Command Mode

Global Configuration

Command Line Usage

snmp-server view <*WORD*> [<*OID*> **| at | bgp | directory | docsif** | **dod** | **dot3** | **egp** | **experimental** | **icmp** | **ifmib** | **igmp** | **interfaces** | **internet** | **ip** | **iso** | **mgmt** | **mib-2** | **org** | **ospf** | **ppp** | **private** | **rip2** | **riverdelta** | **security** | **snmp** | **snmpv2** | **system** | **tcp** | **transmission** | **udp**] {**included** | **excluded**}

no snmp-server view <*WORD*> [<*OID*> **| at | bgp | directory | docsif** | **dod** | **dot3** | **egp** | **experimental** | **icmp** | **ifmib** | **igmp** | **interfaces** | **internet** | **ip** | **iso** | **mgmt** | **mib-2** | **org** | **ospf** | **ppp** | **private** | **rip2** | **riverdelta** | **security** | **snmp** | **snmpv2** | **system** | **tcp** | **transmission** | **udp**] {**included** | **excluded**}

Command Syntax

WORD	used for reference identification to view record being generated or removed reference identification
OID	subtree of MIB view family name (ex: 1.3.6.1.= internet, 1.3.6.1.2.1.1 = system)
at	AT MIB group
bgp	BGP MIB group
directory	directory MIB group

docsif	docsisIf MIB group
dod	DOD MIB group
dot3	ether-like MIB group
egp	EGP MIB group
experimental	experimental MIB group
icmp	ICMP MIB group
ifmib	ifMib MIB group
igmp	IGMP MIB group
interfaces	interfaces MIB group
internet	internet MIB group
ip	IP MIB group
iso	ISO MIB group
mgmt	mgmt MIB group
mib-2	MIB-2 MIB group
org	org MIB group
ospf	OSPF MIB group
ppp	PPP MIB group
private	private MIB group
rip2	RIP2 MIB group
riverdelta	RiverDelta Networks proprietary MIB groups
security	security MIB group
snmp	SNMP MIB group
snmpv2	SNMPv2 MIB group
system	System MIB group
tcp	TCP MIB group

transmission	transmission MIB group
udp	UDP MIB group
included	specifies MIB group is included from view
excluded	specifies MIB group is excluded from view

4

Debug Commands

Introduction

This chapter describes the debug commands supported by the BSR 2000. Debug commands help to isolate the source of a system failure. The output provides diagnostic information, protocol status, and network activity which can be used to diagnose and resolve networking problems.

Debug Command Descriptions

This section contains an alphabetized list and descriptions of the debug commands supported by the BSR.

debug arp

The **debug arp** command displays Address Resolution Protocol (ARP) information exchanges between the BSR and other devices on the network. The **no debug arp** command turns off ARP debugging.

Group Access

ISP

Command Mode

All modes except User EXEC

Command Line Usage

debug arp

no debug arp

debug cable cra

The **debug cable cra** command turns on cra debugging which displays internal CMTS resource agent activity. The **no debug cable cra** command turns off cra debugging.

Group Access

MSO

Command Mode

Privileged EXEC

Command Line Usage

debug cable cra

no debug cable cra

debug cable err

The **debug cable err** command displays miscellaneous error conditions.

Group Access

MSO

Command Mode

Privileged EXEC

Command Line Usage

debug cable err

no debug cable err

debug cable keyman

The **debug cable keyman** command activates debugging of TEK and KEK baseline privacy key activity. The **no debug cable keyman** turns off this debugging operation.

Group Access

MSO

Command Mode

Privileged EXEC

Command Line Usage

debug cable keyman

no debug cable keyman

debug cable mac

The **debug cable mac** command displays dynamic service messages and/or MAC layer management information MAC-layer information. The **no debug cable mac** command turns off MAC-layer debugging.

Group Access

MSO

Command Mode

Privileged EXEC

Command Line Usage

debug cable mac {**dynsrv** | **information**}

no debug cable mac {**dynsrv** | **information**}

debug cable map

The **debug cable map** command displays map debugging messages. The **no debug cable map** command turns off this debugging operation.

Group Access

MSO

Command Mode

Privileged EXEC

Command Line Usage

debug cable map

no debug cable map

debug cable modem-select

The **debug cable modem-select** command lets you select a specific cable modem for debug tracing. The **no debug cable modem-select** command turns off this debugging operation.

Group Access

MSO

Command Mode

Privileged EXEC

Command Line Usage

debug cable modem-select <*mac***>**

no debug cable modem-select <*mac***>**

Command Syntax

mac	MAC address of a specific cable modem

debug cable privacy

The **debug cable privacy** command activates debugging of baseline privacy. The **no debug cable privacy command turns off this debugging operation.**

Group Access

MSO

Command Mode

Privileged EXEC

Command Line Usage

debug cable privacy

no debug cable privacy

debug cable qos

The **debug cable qos** command activates debugging of Quality of Service (QoS). The **no debug cable qos command turns off this debugging operation.**

Group Access

MSO

Command Mode

Privileged EXEC

Command Line Usage

debug cable qos

no debug cable qos

debug cable range

The **debug cable range** command displays ranging messages exchanged between cable modems and the CMTS. The **no debug cable range** command turns off this debugging operation.

Group Access

MSO

Command Mode

Privileged EXEC

Command Line Usage

debug cable range

no debug cable range

debug cable reg

The **debug cable reg** command displays registration messages exchanged between cable modems and the CMTS. The **no debug cable reg** command turns off this debugging operation.

Group Access

MSO

Command Mode

Privileged EXEC

Command Line Usage

debug cable reg

no debug cable reg

debug cable ucc

The **debug cable ucc** command displays upstream channel change (UCC) messages generated when cable modems request or are assigned a new channel. The **no debug cable ucc** command turns of this debugging operation.

Group Access

MSO

Command Mode

Privileged EXEC

Command Line Usage

debug cable ucc

no debug cable ucc

debug ip access-list

The **debug ip access-list** command enables IP access-list debugging. The **no debug ip access-list** command turns IP access-list debugging off.

Group Access

ISP

Command Mode

All modes except User EXEC

Command Line Usage

debug ip access-list [{**in** | **out** }]

no debug ip access-list [{**in** | **out** }]

Command Syntax

in	debug inbound packets
out	debug outbound packets

Command Default

Disabled

debug ip bgp

The **debug ip bgp** command displays Border Gateway Protocol (BGP) transactions. The **no debug ip bgp** command turns off this debugging operation. Use the **debug ip bgp** command to:

- Show events that change the state of the BGP session with any peer
- Show open messages sent and received between peers
- Show keepalive messages sent and received between peers
- Show update messages sent and received between peers including advertised routes and withdrawn routes
- Show notification messages sent and received between peers
- Troubleshoot BGP peer sessions and route exchanges

Group Access

ISP

Command Mode

All modes except User EXEC

Command Line Usage

debug ip bgp [*<A.B.C.D>* | **dampening** | **events** | **inbound-connection [access-list** [*<1-199>* | *<1300-2699>*]] | **keepalives** [**in** | **out**] | **message-dump** [**in** | **keepalive** | **notify** | **open** | **others** | **out** | **refresh** | **update**] | **notifies** [**in** | **out**] | **rules** [**in** | **out**] | **soft-reconfiguration-inbound** | **updates** [**in** | **out**]]

no debug ip bgp [*<A.B.C.D>* | **dampening** | **events** | **inbound-connection [access-list** [*<1-199>* | *<1300-2699>*]] | **keepalives** [**in** | **out**] | **message-dump** [**in** | **keepalive** | **notify** | **open** | **others** | **out** | **refresh** | **update**] | **notifies** [**in** | **out**] | **rules** [**in** | **out**] | **soft-reconfiguration-inbound** | **updates** [**in** | **out**]]

Command Syntax

A.B.C.D	neighbor IP address to debug
dampening	BGP dampening
events	enables logging of BGP state transitions

inbound-connection	information about peers trying to make a connection
access-list	select the peer from which inbound to display inbound connections
1-199	access list number
1300-2699	access list number (expanded range)
keepalives	BGP keepalives
in	incoming information
out	outgoing information
message dump	displays contents of messages
keepalive	display contents of KEEPALIVE messages
notify	display contents of NOTIFY messages
open	display contents of OPEN messages
others	display contents of any other messagesd
refresh	display contents of ROUTE-REFRESH messages
update	display contents of UPDATE messages
notifies	BGP notification messages
rules	display an explanation of the treatment of update messages
soft-reconfiguration-inbound	process **clear ip bgp soft in** updates
updates	generates per update messages

debug ip icmp

The **debug ip icmp** command displays Internet Control Message Protocol (ICMP) information exchanges between the BSR and other devices on the network. The **no debug ip icmp** turns off ICMP debugging.

Use the **debug ip icmp** command to determine whether the BSR is sending or receiving ICMP messages.

Group Access

ISP

Command Mode

All modes except User EXEC

Command Line Usage

debug ip icmp

no debug ip icmp

Command Default

Disabled

debug ip igmp

The **debug ip igmp** command displays all Internet Group Management Protocol (IGMP) packets, and all IGMP host-related actions. The **no debug ip igmp** command turns off the IGMP debugging.

Use the **debug ip igmp** command to target IGMP protocol messages and mtrace messages.

Group Access

ISP

Command Mode

All modes except User EXEC

Command Line Usage

debug ip igmp

no debug ip igmp

Command Default

Disabled

debug ip mfm

The **debug ip mfm** command displays Multicast Forwarding Manager (MFM) control packet activity. The **no debug ip mfm** command turns off MFM debugging.

Group Access

ISP

Command Mode

All modes except User EXEC

Command Line Usage

debug ip mfm {**all | general**}

no debug ip mfm {**all | general**}

Command Syntax

all	all MFM processing information
general	general, non-specific MFM application information

Command Default

Disabled

debug ip mrtm

The **debug ip mrtm** command displays changes made to the IP multicast routing table made by the Multicast Routing Table Manager. The **no debug ip mrtm** command turns off MRTM debugging.

Group Access

ISP

Command Mode

All modes except User EXEC

Command Line Usage

debug ip mrtm {**all** | **general**}

no debug ip mrtm {**all** | **general**}

Command Syntax

all	all MRTM processing information
general	general, non-specific MRTM application information

Command Default

Disabled

debug ip ospf

The **debug ip ospf** command displays Open Shortest Path First (OSPF)-related activity. The **no debug ip ospf** command turns off OSPF-related debugging. Use the **debug ip ospf** command to turn on debugging for IP OSPF.

The **debug ip ospf** command can be used to do the following:

- Confirm that the routers match the same IP mask
- Verify same hello interval
- Verify same dead interval
- Verify neighbors are part of the same area

Group Access

ISP

Command Mode

All modes except User EXEC

Command Line Usage

debug ip ospf {**adj** | **dr** | **events** | **lsa** | **packet** | **retransmission** | **spf** [**detail**] }

no debug ip ospf {**adj** | **dr** | **events** | **lsa** | **packet** | **retransmission** | **spf** [**detail**] }

Command Syntax

adj	debug OSPF adjacency events
dr	debug OSPF DR election events
events	debug all OSPFevents
lsa	debug OSPF LSA rx/tx events
packet	debug OSPF packets reception events
retransmission	debug OSPF retransmission events
spf	debug OSPF SPF calculation events
detail	display detailed SPF calculation events debug information

Command Default

Disabled

debug ip packet

The **debug ip packet** command displays general IP debugging information including packets received, generated, and forwarded. The **no debug ip packet** command turns IP debugging operations.

Note: The **debug ip packet** command uses considerable bandwidth to output debugging information. This may interrupt router activities.

Group Access

ISP

Command Mode

All modes except User EXEC

Command Line Usage

debug ip packet [<*1-199*> | <*1300-2699*> | **detail**]

no debug ip packet

Command Syntax

1-199	access list number
1300-2699	extended access list number
detail	display more detailed IP packet; debugging information

Command Default

Disabled

debug ip pim

The **debug ip pim** command enables PIM debugging. The **no debug ip pim** command turns PIM debugging off.

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

debug ip pim {**all** | **assert** | **bsr** | **cache** | **general** | **hello** | **join-prune** | **register** | **rp** | **rp-db** | **rt-change** }

no debug ip pim

Command Syntax

all	debug all pim processing information
assert	debug assert processing information
bsr	debug BSR-RP processing information
cache	debug internal cache maintenance information
general	debug non-specific PIM application information
hello	debug hello processing information
join-prune	debug Join/Prune processing information
register	debug register processing information
rp	debug RP processing information
rp-db	debug RPSet Database processing information
rt-change	debug route change processing information

Command Default

Disabled

debug ip policy

The **debug ip policy** command displays IP policy routing packet activity. The **debug ip policy** command displays information about whether a packet matches the routing policy criteria and the resulting routing information for the packet.The **no debug ip policy** command turns off IP policy debugging.

Note: The **debug ip policy** command uses considerable bandwidth to output debugging information. This may interrupt router activities.

Group Access

ISP

Command Mode

All modes except User EXEC

Command Line Usage

debug ip policy

no debug ip policy

Command Default

Disabled

debug ip redistribute to

The **debug ip redistribute to** command displays route redistribution information from one routing domain to another routing domain. The **no debug ip redistribute** command turns off IP redistribute debugging.

Group Access

ISP

Command Mode

All modes except User EXEC

Command Line Usage

debug ip redistribute to {**all** | **bgp** | **ospf** | **rip**} **from** {**all** | **bgp** | **connected** | **ospf** | **rip** | **static**}

no debug ip redistribute to {**all** | **bgp** | **ospf** | **rip**} **from** {**all** | **bgp** | **connected** | **ospf** | **rip** | **static**}

Command Syntax

to	to protocols
all	all supported protocols
bgp	routes redistributed into BGP
ospf	routes redistributed into OSPF
rip	routes redistributed into RIP
from	from protocols
all	all supported protocols
bgp	routes redistributed from BGP
connected	routes redistributed connected
ospf	routes redistributed from OSPF

rip	routes redistributed from RIP
static	routes redistributed static

Command Default

Disabled

debug ip rip

The **debug ip rip** command displays Routing Information Protocol (RIP) send and receive information. The **no debug ip rip** command turns off RIP debugging.

Group Access

ISP

Command Mode

All modes except User EXEC

Command Line Usage

debug ip rip [**database** | **events** | **trigger**]

no debug ip rip [**database** | **events** | **trigger**]

Command Syntax

database	RIP database events
events	RIP protocol events
trigger	RIP triggered events

Command Default

Disabled

debug ip rip database

The **debug ip rip database** command displays information on RIP route entry events; additions, deletions, and changes. The **no debug ip rip database** command turns off RIP database debugging.

Group Access

ISP

Command Mode

All modes except User EXEC

Command Line Usage

debug ip rip database

no debug ip rip database

debug ip rip events

The **debug ip rip events** command displays information on RIP-related events. The **no debug ip rip events** command turns off RIP-related event debugging.

Group Access

ISP

Command Mode

All modes except User EXEC

Command Line Usage

debug ip rip events

no debug ip rip events

Command Default

Disabled

debug ip rip trigger

The **debug ip rip trigger** command displays RIP routing events that occur as a result of RIP trigger extensions. The **no debug ip rip trigger** command turns off RIP triggered events debugging.

Group Access

ISP

Command Mode

All modes except User EXEC

Command Line Usage

debug ip rip trigger

no debug ip rip trigger

Command Default

Disabled

debug ip tcp transactions

The **debug ip tcp transactions** command displays information on significant TCP activity such as state changes, retransmissions, and duplicate packets. The **no debug tcp transactions** command turns off TCP debugging.

Note: The **debug ip tcp transactions** command reports output for packets the BSR 2000 transmits and receives, but does not display output for packets it forwards.

Group Access

ISP

Command Mode

All modes except User EXEC

Command Line Usage

debug ip tcp transactions

no debug ip tcp transactions

Command Default

Disabled

debug ip udp

The **debug ip udp** command displays UDP-based transactions.The debug output shows whether packets are being received from the host. The **no debug ip udp** command turns off UDP debugging.

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

debug ip udp [**dhcp** [<*mac*>]]

no debug ip udp [**dhcp** [<*mac*>]]

Command Syntax

dhcp	display Dynamic Host Configuration Protocol (DHCP) packet information
mac	client hardware/MAC address in the form of xxxx.xxxx.xxxx

Command Default

Disabled

debug ipsec ike

The **debug ipsec ike** command turns on IKE debugging and prints IKE debug messages to the console. The **debug ipsec ike command,** without additional arguments, turns on all IKE debugging. The **no debug ipsec ike** command turns IKE debugging off. IKE debugging must be re-enabled after a power-cycle or reload.

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

debug ipsec ike [{**chan-agent** | **del-msg** | **info-msg** | **key-exg** | **main** | **quick**}]

no debug ipsec ike [{**chan-agent** | **del-msg** | **info-msg** | **key-exg** | **main** | **quick**}]

Command Syntax

chan-agent	print channel agent debugging
del-msg	print del message debugging
info-msg	print informational debugging
key-exg	print key exchange debugging
main	print main mode debugging
quick	print quick modem debugging

Command Default

Disabled

debug ipsec ipsec

The **debug ipsec ipsec** command turns on IPSec debugging and prints IPSec debug messages to the console. The **debug ipsec ipsec command,** without additional arguments, turns on all IPSec debugging.The **no debug ipsec ipsec** command turns IPSec debugging off. IPSec debugging must be re-enabled after a power-cycle or reload.

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

debug ipsec ipsec

no debug ipsec ipsec

Command Default

Disabled

debug ipsec sadb

The **debug ipsec sadb** command turns on Security Association Database (SADB) debugging and prints SADB debug messages to the console. The **no debug ipsec sadb** command turns SADB debugging off. SADB debugging must be re-enabled after a power-cycle or reload.

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

debug ipsec sadb

no debug ipsec sadb

Command Default

Disabled

debug ipsec spd

The **debug ipsec spd** command urns on SPD debugging and prints SPD debug messages to the console. The **no debug ipsec spd** command turns SPD debugging off. SPD debugging must be re-enabled after a power-cycle or reload.

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

debug ipsec spd

no debug ipsec spd

Command Default

Disabled

debug packet-cable

The **debug packet-cable** command enables Packet Cable debugging. The **no debug packet-cable** command disables debugging output.

Group Access

ISP

Command Mode

Privileged EXEC

Command Line Usage

debug packet-cable [**gate** | **trace** [**cops** | **em**]]

no debug packet-cable [**gate** | **trace** [**cops** | **em**]]

Command Syntax

gate	enable gate debugging
trace	enable packet trace
trace cops	enable COPS packet trace
trace em	enable Event Message packet trace

Command Default

Disabled

debug radius

The **debug radius** command displays RADIUS client authentication transactions. The **no debug radius** command turns off RADIUS debugging.

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

debug radius

no debug radius

debug snmp

The **debug snmp** command display detailed information about every SNMP packet transmitted or received by the BSR 2000. The **no debug snmp** command turns off SNMP debugging.

Group Access

All

Command Mode

All modes

Command Line Usage

debug snmp {**headers** | **packets**}

no debug snmp {**headers** | **packets**}

Command Syntax

headers	display SNMP packet headers
packets	display SNMP packets

Command Default

Disabled

debug sntp

The **debug sntp** command displays information on Simple Network Time Protocol (SNTP) activity. The **no debug sntp** command turns off SNTP debugging.

Group Access

System Administrator

Command Mode

All modes except User EXEC

Command Line Usage

debug sntp

no debug sntp

debug specmgr

The **debug specmgr** command enables the display of spectrum management debugging messages. The command output displays a time stamp, the error rate, the number of word errors, total word count, and the upstream noise power level in one-tenth of a dBmV. The **no debug specmgr** stops displaying spectrum management debugging messages.

Group Access

MSO

Command Mode

Privileged EXEC

Command Line Usage

debug specmgr [**cable** <*NUM*> | **upstream** | <*NUM*>]

no debug specmgr [**cable** <*NUM*> | **upstream** | <*NUM*>]

Command Syntax

cable	display cable information
NUM	This number is always 0 for the BSR 2000.
upstream	display upstream information
NUM	upstream port number

debug ssh

The **debug ssh** command enables debugging for SSH. The **no debug ssh** command turns SSH debugging off.

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

debug ssh [**verbose** {*1-8*}]

no debug ssh [**verbose** {*1-8*}]

Command Syntax

verbose	display detailed SSH debug information
1-8	verbose debug level number

debug tacacs

The **debug tacacs** command displays debug information associated with TACACS+ Client operations.

Group Access

All

Command Mode

Privileged EXEC

Command Line Usage

debug tacacs

debug tacacs events

The **debug tacacs events** command displays debug information related to TACACS+ server events generated as a result of interaction with a client. This command can produce substantial amount of output on the console. The **debug tacacs events** command is generally used as a tool to collect data to analyze a problem reported by users.

Group Access

All

Command Mode

Privileged EXEC

Command Line Usage

debug tacacs events

show debugging

The **show debugging** command displays enabled debugging operations and other types of debugging functions on the system.

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show debugging [| {**begin** | **exclude** | **include**} {<*WORD*>} [| {**count** | **count-only**}]]

show debugging [| {**count** | **count-only**}]

Command Syntax

|	turns on output modifiers (filters)
begin	filter for output that begins with the specified string
exclude	filter for output that excludes the specified string
include	filter for output that includes the specified string
WORD	the specified string
count	count the number of outputted lines
count-only	count the number of lines while suppressing screen output

undebug all

The **undebug all** command disables all debugging functions on the system.

Group Access

System Administrator

Command Mode

All modes except User EXEC

Command Line Usage

undebug all

5

Access List Commands

Introduction

This chapter describes the access list commands used with the BSR 2000™.

Access lists are used on the BSR to control entry or exit access to or from the BSR. Access lists are also used within a route-map statement that is part of the routing configuration. Access lists can be configured for all routed network protocols to filter packets as the packets pass through the BSR. The access list criteria can be defined by the source or the destination address, upper-layer protocol, or other routing information.

There are many reasons to configure access lists including to restrict contents of routing updates or to provide traffic flow control. One of the most important reasons to configure access lists is to provide a basic level of security on the network. All packets passing through the BSR can be allowed onto all parts of the network if an access list is not part of the router configuration.

Access List Command Descriptions

This section contains an alphabetized list and descriptions of the access list commands supported by the BSR.

access-class in

The **access-class in** command filters incoming connections based on an IP access list.

Group Access

System Administrator

Command Mode

Global Configuration

Command Line Usage

access-class {*<1-99>* | *<1300-1999>*} **in**

Command Syntax

1-99	the IP access-list number
1300-1999	the IP access-list number (expanded range)

access-list (standard)

The standard **access-list** command defines a standard access list to configure and control the flow of routing information and traffic by matching a packet with a permit or deny result. The **no access-list** command deletes the access-list.

Use the **access-list** command to restrict routing update information; control the transmission of packets on an interface, or control virtual terminal line access.

Group Access

ISP

Command Mode

Global Configuration

Command Line Usage

access-list <*1-99*> <*1300-1999*> {**deny** | **permit**} {<*A.B.C.D*> [<*A.B.C.D*>] | **any** | **host** <*A.B.C.D*>}

no access-list <*1-99*> <*1300-1999*>

Command Syntax

1-99	standard access list
1300-1999	standard IP access list (expanded range)
deny	deny access if conditions are matched
permit	permit access if conditions are matched
A.B.C.D	address to match
A.B.C.D	wildcard bits
any	any source host
host *A.B.C.D*	a single source host

access-list (extended)

The extended **access-list** command defines an extended access list to configure and control the flow of routing information and traffic by matching a packet with a permit or deny result. The **no access-list** command deletes the access-list.

Use the **access-list** command to restrict routing update information; control the transmission of packets on an interface, or control virtual terminal line access.

Group Access

ISP

Command Mode

Global Configuration

Command Line Usage

To configure an extended access list for AHP, ESP, GRE, IP, IPINIP, OSPF, PCP, and PIM, use the following command:

access-list *<100-199> <2000-2699>* {**deny** | **permit**} {*<0-255>* | **ahp** | **esp** | **gre** | **ip** | **ipinip** | **ospf** | **pcp** | **pim**} {*<A.B.C.D> <A.B.C.D>* | **any** | **host** *<A.B.C.D>*} (*<A.B.C.D> <A.B.C.D>* | **any** | **host** *<A.B.C.D>*} [**diff-serv** *<0-63>*]

To configure an extended access list for ICMP, use the following command:

access-list *<100-199> <2000-2699>* {**deny** | **permit**} **icmp** {*<A.B.C.D> <A.B.C.D>* | **any** | **host** *<A.B.C.D>*} (*<A.B.C.D> <A.B.C.D>* | **any** | **host** *<A.B.C.D>*} [*<0-255>* | **administratively-prohibited** | **alternate-address** | **dod-host-prohibited** | **dod-net-prohibited** | **echo** | **echo-reply** | **general-parameter-problem** | **host-isolated** | **host-precedence-unreachable** | **host-redirect** | **host-tos-redirect** | **host-tos-unreachable** | **host-unknown** | **host-unreachable** | **information-reply** | **information-request** | **mask-reply** | **mask-request** | **net-redirect** | **net-tos-redirect** | **net-tos-unreachable** | **net-unreachable** | **network-unknown** | **no-room-for-option** | **option-missing** | **packet-too-big** | **parameter-problem** | **port-unreachable** | **precedence-unreachable** | **protocol-unreachable** | **reassembly-timeout** | **redirect** | **router-advertisement** | **router-solicitation** | **source-quench** | **source-route-failed** | **time-exceeded** | **timestamp-reply** | **timestamp-request** | **ttl-exceeded** | **unreachable**]

To configure an extended access list for IGMP, use the following command:

access-list *<100-199> <2000-2699>* {**deny** | **permit**} **igmp** {*<A.B.C.D> <A.B.C.D>* | **any** | **host** *<A.B.C.D>*} (*<A.B.C.D> <A.B.C.D>* | **any** | **host** *<A.B.C.D>*} [*<0-255>* | **diff-serv** | **host-query** | **host-report** | **pim**]

To configure an extended access list for TCP, use the following command:

access-list *<100-199> <2000-2699>* {**deny** | **permit**} **tcp** {*<A.B.C.D> <A.B.C.D>* | **any** | **host** *<A.B.C.D>*} (*<A.B.C.D> <A.B.C.D>* | **any** | **host** *<A.B.C.D>*} [**diff-serv** *<0-63>* | **eq** [*<0-65535>* | **bgp** | **chargen** | **cmd** | **daytime** | **discard** | **domain** | **echo** | **exec** | **finger** | **ftp** | **ftp-data** | **gopher** | **gt** | **hostname** | **ident** | **irc** | **klogin** | **kshell** | **login** | **lpd** | **lt** | **neq** | **nntp** | **pim-auto-rp** | **pop2** | **pop3** | **smtp** | **sunrpc** | **talk** | **telnet** | **time** | **uucp** | **whois** | **www**]]

To configure an extended access list for UDP, use the following command:

access-list *<100-199> <2000-2699>* {**deny** | **permit**} **udp** {*<A.B.C.D> <A.B.C.D>* | **any** | **host** *<A.B.C.D>*} (*<A.B.C.D> <A.B.C.D>* | **any** | **host** *<A.B.C.D>*} [**diff-serv** *<0-63>* |**eq** [*<0-65535>* | **biff** | **bootpc** | **discard** | **domain** | **echo** | **gt** | **lt** | **mobile-ip** | **neq** | **netbios-dgm** | **netbios-ns** | **netbios-ss** | **ntp** | **pim-auto-rp** | **rip** | **snmp** | **snmptrap** | **sunrpc** | **syslog** | **talk** | **tftp** | **time** | **who** | **xdmcp**]]

To remove an access list, use the following command:

no access-list *<100-199> <2000-2699>*

Command Syntax

100-199	extended access list
2000-2699	extended IP access list (expanded range)
deny	deny access if conditions are matched
permit	permit access if conditions are matched

0-255	name or number of an IP protocol
ahp	
esp	
gre	
icmp	
igmp	
ip	
ipinip	
ospf	
pcp	
pim	
tcp	
udp	
A.B.C.D	source address
A.B.C.D	source wildcard bits
any	any source host
host *A.B.C.D*	a single source host
A.B.C.D	destination address
A.B.C.D	destination wildcard bits
any	any destination host
host *A.B.C.D*	a single destination host
diff-serv <*0-63*>	Value of IP Diff-Serv

0-255 **administratively-prohibited** **alternate-address** **diff-serv** **dod-host-prohibited** **dod-net-prohibited** **echo** **echo-reply** **general-parameter-problem** **host-isolated** **host-precedence-unreachable** **host-redirect** **host-tos-redirect** **host-tos-unreachable** **host-unknown** **host-unreachable** **information-reply** **information-request** **mask-reply** **mask-request** **net-redirect** **net-tos-redirect** **net-tos-unreachable** **net-unreachable** **network-unknown** **no-room-for-option** **option-missing** **packet-too-big** **parameter-problem** **port-unreachable** **precedence-unreachable** **protocol-unreachable** **reassembly-timeout** **redirect** **router-advertisement** **router-solicitation** **source-quench** **source-route-failed** **time-exceeded**	filter ICMP packets by message type (*0-255*) or message type name

timestamp-reply **timestamp-request** **ttl-exceeded** **unreachable**	
0-255 **diff-serv** **host-query** **host-report** **pim**	filter IGMP packets by message type (0-255) or message type name
diff-serv **eq**	only match packets on a given TCP or UDP port number or name

0-65535	the number or name of a TCP port
bgp	
chargen	
cmd	
daytime	
discard	
domain	
echo	
exec	
finger	
ftp	
ftp-data	
gopher	
gt	
hostname	
ident	
irc	
klogin	
kshell	
login	
lpd	
lt	
neq	
nntp	
pim-auto-rp	
pop2	
pop3	

range
smtp
sunrpc
talk
telnet
time
uucp
whois
www

0-65535	the number or name of a UDP port
biff	
bootpc	
bootps	
diff-serv	
discard	
domain	
echo	
gt	
lt	
mobile-ip	
neq	
netbios-dgm	
netbios-ns	
netbios-ss	
ntp	
pim-auto-rp	
range	
rip	
snmp	
snmptrap	
sunrpc	
syslog	
talk	
tftp	
time	
who	
xdmcp	

ip access-group

Use the **ip access-group** command to assign an access list to an interface and determine if the interface accepts inbound or outbound packets, or both from this access list. The **no ip access-group** command removes the access list or disables inbound or outbound packets.

Group Access

ISP

Command Mode

Interface Configuration

Command Line Usage

ip access-group *<1-199> <1300-2699>* {**in** | **out**}

no ip access-group *<1-199> <1300-2699>* {**in** | **out**}

Command Syntax

1-199	access list number
1300-2699	access list number (expanded range)
in	inbound packets
out	outbound packets

ip access-list

The **ip access-list** command adds a standard or extended access-list entry. The **no ip access-list command removes the entry.**

Group Access

ISP

Command Mode

Global Configuration

Command Line Usage

ip access-list {**standard** <*1-99*> | **extended** <*100-199*>}

no ip access-list {**standard** <*1-99*> | **extended** <*100-199*>}

Command Syntax

standard *1-99*	standard access list number
extended *100-199*	extended access list number

show access-lists

The **show access-lists** command displays an access list, or all access lists, without displaying the entire configuration file.

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show access-lists [*<1-199> <1300-2699>*] [| {**begin** | **exclude** | **include**} {*<WORD>*} [| {**count** | **count-only**}]]

show access-lists [*<1-199> <1300-2699>*] [| {**count** | **count-only**}]

Command Syntax

1-199	access list number
1300-2699	access list number (expanded range)
|	turns on output modifiers (filters)
begin	filter for output that begins with the specified string
exclude	filter for output that excludes the specified string
include	filter for output that includes the specified string
WORD	the specified string
count	count the number of outputted lines
count-only	count the number of lines while suppressing screen output

Command Default

All access lists are displayed.

6

Routing Policy Commands

Introduction

This chapter contains the Routing Policy and Policy-Based Routing commands used with the BSR 2000™.

Routing Policy allows the control of information that is imported from or exported into different routing domains or Autonomous Systems (AS).

BSR Routing Policy allows the filtering and altering of routing information so that some of them can be advertised to other routers. The BSR Routing Policy is quite versatile and flexible.

The BSR also supports Policy-based routing. The BSR also supports Policy-based routing is a set of rules that define the criteria for obtaining specific routing paths for different users to give some users better-routed Internet connections than others. Policy-based routing is established by the source information of the packets, rather than the destination information that traditional routing protocols use. The network administrator determines and implements routing policies to allow or deny router paths.

Routing Policy Command Descriptions

This section contains an alphabetized list and descriptions of the routing policy commands supported by the BSR.

default-information originate

The **default-information originate** command injects the default network in a routing domain such as Border Gateway Protocol (BGP).The **no default-information originate** command disables the default network redistribution in the routing domain.

The **network 0.0.0.0** command in Router Configuration mode performs the same function as the **default-information originate** command. In the Routing Information Protocol (RIP) the metric is always set to 1. In BGP, the default route needs to exist in the BGP routing database. BGP uses the metric associated with the default entry in its database.

Group Access

ISP

Command Mode

Router Configuration

Command Line Usage

default-information originate [**always**] [**metric** <*0-16777214*>] [**metric-type** <*1-2*>]

no default-default-information originate [**always**] [**metric** <*0-16777214*>] [**metric-type** <*1-2*>]

Command Syntax

originate	software generates a default external route into an Open Shortest Path First (OSPF) domain to propagate another route if a default route exists
always	advertises the default route even when the default route does not exist (OSPF only)
metric *0-16777214*	metric for generating the default route, default is 1 if no *metric-value* value specified (OSPF only)
metric-type *1-2*	1- external type 1 (OSPF only) 2- external type 2 (OSPF only)

Command Default

Disabled

default-metric

The **default-metric** command sets the default metric value for redistribution of routes from one domain into another. The **no default-metric** command removes the set default value for metric.

Use the **default-metric** command with the **redistribute** command to enforce the same metric value for all redistributed routes.

Group Access

ISP

Command Mode

Router Configuration

Command Line Usage

default-metric {*<1-4294967295>* | *<1-16777214>* | *<1-16>*}

no default-metric [*<1-4294967295>* | *<1-16777214>* | *<1-16>*]

Command Syntax

1-4294967295 *1-16777214* *1-16*	default metric value; the range of values depends on the routing protocol for which this is configured; for RIP the range is *1-16*, for OSPF the range is *1 - 16777214* and for BGP the range is *1 - 4294967295*.

Command Default

A built-in automatic metric translation for each routing protocol

ip local policy route-map

The **ip local policy route-map** command enables local policy routing for a specified route map. The **no ip local policy route-map** command disables local policy routing for a specified route map.

Group Access

ISP

Command Mode

Global Configuration

Command Line Usage

ip local policy route-map <*WORD*>

no ip local policy route-map <*WORD*>

Command Syntax

WORD	the route map name

ip policy route-map

The **ip policy route-map** command identifies the route-map used on an interface to perform policy-based routing. The **no ip policy route-map** command removes the route-map on an interface, and disables policy-based routing on that interface.

Use the **ip policy route-map** command for paths other than the shortest path. This command has associated match and set commands: **match** commands specify policy routing rules, **set** commands perform tasks

Group Access

ISP

Command Mode

Interface Configuration

Command Line Usage

ip policy route-map <*WORD*>

no ip policy route-map <*WORD*>

Command Syntax

WORD	route-map name that must match a specified map tag

Command Default

No policy routing

match as-path

The **match as-path** command matches a BGP autonomous system path access list to a match entry or appends new list numbers to the existing match entry. The **no match as-path** command removes the list numbers from the match entry used in the command.

Use the **match as-path** command to match a BGP autonomous system path to advertise on the route-map. Values can be set using the **match as-path** command.

Use the **match as-path** command to match at least one BGP autonomous system path to ensure advertisement on the route-map.

Use the **match as-path** command to globally replace values matched and set with the **match as-path c**ommand and the **set weight** command to supersede weights established with the **neighbor weight** and the **neighbor filter-list** commands.

The values set by the **match** and **set** commands override global values. For example, the weights assigned with the **match as-path** and **set weight** route-map commands override the weights assigned using the **neighbor weight** and **neighbor filter-list** commands. The implemented weight is established by the initial autonomous system match.

Group Access

ISP

Command Mode

Route-map Configuration

Command Line Usage

match as-path [<*1-199*>]

no match as-path [<*1-199*>]

Command Syntax

1-199	as-path list number - you can specify a single number or multiple numbers separated by a space

match community

The **match community** command creates a BGP autonomous system community access list match entry or appends new list numbers to the existing match entry. The **no match community** command removes the match entry completely. The **no match community** command removes the list numbers or the **exact-match** attribute from the match entry.

Use the **match community-list** command to ensure that the route is advertised for outbound and inbound route-maps. If a change to some of the information is to match is needed, configure a second route-map with specifics.

Group Access

ISP

Command Mode

Route-map Configuration

Command Line Usage

match community [*<1-99> <100-199>*] **exact-match**]

no match community [*<1-99> <100-199>*] **exact-match**]

Command Syntax

1-99	standard community list number
100-199	extended community list number
exact-match	exact match required; all of the communities and only those communities in the community list must be present

match ip address

The **match ip address** command matches the destination and source IP address or other fields of the IP header on packets with a standard or extended access list allocated. The **no match ip address** command disables policy routing on packets. This command can also be used for filtering routes based on the destination network of the route.

Use the **match ip address** command to match any routes that have a source network number and a destination network number address that a standard or extended access list permits. To match both source and destination numbers, use an extended access list. The **match ip address** command can also be used to filter routing information.

Group Access

ISP

Command Mode

Route Map Configuration

Command Line Usage

match ip address [*<1-199>* | *<1300-2699>*]

no match ip address [*<1-199>* | *<1300-2699>*]

Command Syntax

1-199	standard access list number
1300-2699	extended access list number

match ip next-hop

The **match ip next-hop** command establishes the condition for the next hop IP address of a route to match against the specified access lists. The **no match ip next-hop** command removes the access-list from the match condition.

Use the match **ip next-hop** command to match any routes that have a next-hop router address permitted one of the specified access lists.

Group Access

ISP

Command Mode

Route Map Configuration

Command Line Usage

match ip next-hop [*<1-199>* | *<1300-2699>*]

no match ip next-hop [*<1-199>* | *<1300-2699>*]

Command Syntax

1-199	standard access list number
1300-2699	extended access list number

match ip route-source

The **match ip route-source** command specifies match conditions for the source IP address of a route to match against the specified address list(s). The **no match ip route-source** command removes access lists from such a match statement.

The **match ip route-source** command is used to match routes where source IP addresses are permitted by specified access lists.

Group Access

ISP

Command Mode

Route-map Configuration

Command Line Usage

match ip route-source [*<1-199>* | *<1300-2699>*]

no match ip route-source [*<1-199>* | *<1300-2699>*]

Command Syntax

1-199	standard access list number
1300-2699	extended access list number

match metric

The **match metric** command matches routes imported or otherwise with specified metric value. The **no match metric** command disables matching imported routes with specified metric values.

Use the **match metric** command to match a route for the specified metric value(s).

Group Access

ISP

Command Mode

Route-map Configuration

Command Line Usage

match metric [<*0-4294967295*>]

no match metric [<*0-4294967295*>]

Command Syntax

0-4294967295	metric value

match route-type external

The **match route-type external** command is used to match the type of OSPF routes. The **no match route-type external** clears the match condition.

Group Access

ISP

Command Mode

Route-map Configuration

Command Line Usage

match route-type external [**level-1** | **level-2** | **type-1** | **type-2**]

no match route-type external [**level-1** | **level-2** | **type-1** | **type-2**]

Command Syntax

type 1	matches only type 1 external route (OSPF)
type 2	matches only type 2 external route (OSPF)
level-1	IS-IS level-1 route
level-2	IS-IS level-2 route

match route-type internal

The **match route-type internal** command matches and redistributes OSPF routes of an internal type. The **no match route-type internal** command clears the condition.

Group Access

ISP

Command Mode

Route-map Configuration

Command Line Usage

match route-type internal [**level-1** | **level-2**]

no match route-type internal [**level-1** | **level-2**]

Command Syntax

level-1	IS-IS level-1 route
level-2	IS-IS level-2 route

match tag

The **match tag** command redistributes routes in the routing table that match a specified tag value. Use the **no match tag** command to disable redistributing routes in the routing table that match a specified tag.

Group Access

ISP

Command Mode

Route Map Configuration

Command Line Usage

match tag [<*0-4294967295*>]

no match tag

Command Syntax

0-4294967295	tag value

route-map

The **route-map** command defines the conditions for redistributing routes from one protocol to another, or to configure routing policies. The **no route-map** command removes some or all of the instances of the route map.

Use the **route-map** command and the **match** and **set** commands, to define the conditions for redistributing routes from one routing protocol into another, or for accepting routes from a neighboring router. Each **route-map** command has an associated list of **match** and **set** commands. The **match** commands specify the conditions under which redistribution is allowed for the current **route-map** command.

The **set** commands specify the particular redistribution actions to perform if the criteria enforced by the **match** commands are met. The **no route-map** command deletes the route-map, or an instance.

The **set** commands specify the redistribution *set actions* when all of a route-map's match criteria are met. When all match criteria are met, all set actions are performed.

Group Access

ISP

Command Mode

Global Configuration

Command Line Usage

route-map <*WORD*> [**permit** | **deny**] [*0-65535*]

no route-map <*WORD*> [**permit** | **deny**] [*0-65535*]

Command Syntax

WORD	tag name, more than one instance of the route-map can share name
permit	distributes route as controlled by set actions when permit is specified and the match criteria are met, the route is specified by the specific actions
deny	distributes route as controlled by set actions, if criteria not met, route not distributed
0-65535	position a new instance will have in the list of route-map instances already established with the same map name.

set as-path prepend

The **set as-path prepend** command modifies AS system path attributes for the matched BGP routes. The **no set as-path prepend** command ends modification of a system path for BGP routes.

Use the **set as-path prepend** command to guide the path information to control the BGP decision process.

Group Access

ISP

Command Mode

Route Map Configuration

Command Line Usage

set as-path prepend [*<1-65535>*]

no set as-path prepend [*<1-65535>*]

Command Syntax

1-65535	prepend string - you can specify a single number or multiple numbers separated by a space

set automatic-tag

The **set automatic-tag** command enables the automatic computing of tag values. The **no set automatic-tag** command disables the automatic computing of tag values.

Group Access

ISP

Command Mode

Route Map Configuration

Command Line Usage

set automatic-tag

no set automatic-tag

set comm-list

The **set comm-list** command deletes communities from the community attribute of an inbound or outbound update. The **no set comm-list** command deletes the entry.

Use the **set comm-list** command to delete communities from the community attribute of inbound or outbound updates using a route map to filter and determine the communities to be deleted.

If the standard list is referred in the **set comm-list delete** command, only the elements with the single community number or no community number in them will be used. All others will be quietly ignored. Any element specified with the 'internet' keyword is equivalent to element without community number.

If the **set community comm** and **set comm-list list-num delete** commands are configured in the same sequence of a route-map attribute, the deletion operation (set comm-list list-num delete) is performed before the set operation (set community comm).

Note: If the **set community** and **set comm-list delete** commands are configured in the same sequence of a route-map attribute, the deletion operation (**set comm-list delete**) is performed before the set operation (**set community**).

Group Access

ISP

Command Mode

Route-map Configuration

Command Line Usage

set comm-list {*<1-99>* | *<100-199>*} **delete**

no set comm-list {*<1-99>* | *<100-199>*} **delete**

Command Syntax

1-99	standard community list number

100-199	extended community list number
delete	delete inbound or outbound communities from the community attribute

set community

The **set community** command add or replace communities from the community attribute of an inbound or outbound update. Use the **no set community** command removes the specified communities from the set.

Use the **route-map** command, and the match and set commands to configure the rules for redistributing routes from one routing protocol to another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the match criteria, which are the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the set actions, the particular redistribution actions to perform if the criteria enforced by the **match** commands are met. The **no route-map** command deletes the route map.

Note: The communities could be specified as numbers; the result will be the same; none removes community attribute from the update unless additive is specified for the set entry. In this case it doesn't modify update community attributes.

In other words, the **no set community** command, if the entry had some community numbers in it before removal, and as the result of the removal no numbers are left, then the entry itself is deleted.

The command **set community none** removes all community numbers from set entry, if any, but leaves the value of the additive attribute intact.

Group Access

ISP

Command Mode

Route-map Configuration

Command Line Usage

set community {*<1-4294967295>* | **local-AS** | **no-advertise** | **no-export** | **additive** | **none**}

no set community {*<1-4294967295>* | **local-AS** | **no-advertise** | **no-export** | **additive** | **none**}

Command Syntax

1-4294967295	community number
additive	add to the existing community
local-AS	do not advertise this route to peers outside of the local autonomous system
no-advertise	do not advertise this route to any peer internal or external
no-export	routes with this community are sent to peers in other sub-autonomous systems within a confederation
none	no community attribute

set default interface null0

The **set default interface null0** command adds “null0” as the last entry in the interface list to force packets to be dropped and not routed with the default destination-based routing process. The **no set default interface null0** command disables this function.

Group Access

ISP

Command Mode

Route Map Configuration

Command Line Usage

set default interface null0

no set default interface null0

Command Default

Disabled

set interface null0

The **set interface null0** command adds “null0” as the last entry in the interface list to force packets to be dropped and not routed with the default destination-based routing process. The **no set interface null0** command disables this function.

Group Access

ISP

Command Mode

Route Map Configuration

Command Line Usage

set interface null0

no set interface null0

Command Default

Disabled

set ip default next-hop

The **set ip default next-hop** command specifies a default next hop IP address that indicates where the BSR sends packets that pass a match clause in a route map for policy routing but have no route to the destination. The **no set ip default next-hop** removes the default next hop IP address.

Note: The presence of a default route in the routing table will ensure that destination-based forwarding will always be applied and policy will be ignored.

Group Access

ISP

Command Mode

Route Map Configuration

Command Line Usage

set ip default next-hop <*A.B.C.D*>

no set ip default next-hop <*A.B.C.D*>

Command Syntax

A.B.C.D	the IP address of the next hop

set ip diff-serv

T**he set ip diff-serv command** assigns a differentiated service value which is placed in the IP packet header that determines which packets are given transmission priority. When these packets are received by another router, they are transmitted based on the precedence value. A higher precedence value indicates a higher priority. The **no set ip diff-serv command disables** assigning a differentiated service value.

Group Access

ISP

Command Mode

Route Map Configuration

Command Line Usage

set ip diff-serv <*0-63*>

no set ip diff-serv [<*0-63*>]

Command Syntax

0-63	IP packet precedence value.

The following table describes the number and name values for IP Precedence:

Number	Name
0	routine
1	priority
2	immediate
3	flash
4	flash-override
5	critical
6	internet
7	network

Command Default

0

set ip next-hop

The **set ip next-hop** command establishes a next-hop value for the AS path. The **no ip next-hop** command deletes the entry.

Use the **ip policy route-map** interface configuration command, the **route-map** global configuration command, and the **match** and **set** route-map configuration commands, to define the conditions for policy routing packets. The **ip policy route-map** command identifies a route map by name. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the *match criteria*---the conditions under which policy routing occurs. The **set** commands specify the *set actions*---the particular routing actions to perform if the criteria enforced by the **match** commands are met.

If the interface associated with the first next hop specified with the **set ip next-hop** command is down, the optionally specified IP addresses are tried in turn.

Group Access

ISP

Command Mode

Route-map Configuration

Command Line Usage

set ip next-hop <*A.B.C.D*>

no set ip next-hop

Command Syntax

A.B.C.D	IP address of the next hop to which packets are output; address of the adjacent router

Command Default

Disabled

set ip qos queue

The **set ip qos queue** command specifies Quality Of Service (QoS) queue number.

Group Access

All

Command Mode

Route Map Configuration

Command Line Usage

set ip qos queue <*0-3*>

Command Syntax

0-3	the QoS queue number

set local-preference

The **set-local preference** command establishes a preference value for the AS system path. Use the **set local-preference** command to send the local-preference to all routers in the local autonomous system.

Use the **no set-local preference** form of this command to delete the entry.

Note: In the **no set-local preference** command, the optional *<0-4294967295>* argument has no effect.

Group Access

ISP

Command Mode

Route-map Configuration

Command Line Usage

set local-preference *<0-4294967295>*

no set local-preference *<0-4294967295>*

Command Syntax

0-4294967295	local preference value

set metric

The **set metric** command sets the metric value for a routing protocol. The **no set metric** command changes the metric value for a routing protocol to the default value.

Group Access

ISP

Command Mode

Route Map Configuration

Command Line Usage

set metric *<0-4294967295>*

no set metric *<0-4294967295>*

Command Syntax

0-4294967295	metric value or bandwidth in Kbytes per second

Command Default

Metric value dynamically learned or a default value

set metric-type

The **set metric-type** command sets the metric type for the destination routing protocol. The **no set metric-type** command disables the metric type set for the destination routing protocol.

Use the **route-map** command to set the type of metric for the route imported by OSPF into its domain.

Group Access

ISP

Command Mode

Route Map Configuration

Command Line Usage

set metric-type {**external** | **internal** | **type-1** | **type-2**}

no set metric-type {**external** | **internal** | **type-1** | **type-2**}

Command Syntax

external	IS-IS external metric
internal	use IGP metric as the MED for BGP
type-1	OSPF external type 1 metric
type-2	OSPF external type 2 metric

Command Default

Disabled

set origin

The **set origin** command configures the conditions for redistributing routes from any protocol to any protocol. The **no set origin** command deletes the BGP origin code.

When the **set origin** command configures redistributing routes from any protocol to any protocol, any match clause is necessary which includes pointing to a “permit everything” to set tags.

Group Access

ISP

Command Mode

Route-map Configuration

Command Line Usage

set origin {**egp | igp** | **incomplete**}

no set origin {**egp | igp** | **incomplete**}

Command Syntax

egp	EGP
igp	remote IGP
incomplete	unknown history

set tag

The **set tag** command sets the value of the destination routing protocol. The **no set tag** command removes the value.

The **route-map** global configuration command and the **match** and **set** route-map configuration commands are used together to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the conditions for redistribution for the current **route-map** command. The **set** commands specify the particular redistribution actions to perform if the criteria enforced by the **match** commands are met. The **no route-map** command deletes the route map.

Group Access

ISP

Command Mode

Route-map Configuration

Command Line Usage

set tag <*0-4294967295*>

no set tag <*0-4294967295*>

Command Syntax

0-4294967295	tag value

Command Default

if not specified, tag is forwarded to the new destination protocol

set weight

The **set-weight** command to set the route weight on the network. The first autonomous system match determines the weight to be set.

Use the **set weight** command to set the route weight on the network. The first AS match determines the weight to be set. The route with the highest weight is chosen as the choice route when multiple routes are available on the network. Weights spoken when an as path is matched, override any weight set by the **neighbor** command. Any match clause is necessary which includes pointing to a “permit everything” to set tags

Group Access

ISP

Command Mode

Route-map Configuration

Command Line Usage

set weight <*0-65535*>

no set weight

Command Syntax

0-65535	weight value

show ip redistribute

The **show redistribute** command displays the routing protocols that are being redistributed to other routing domains.

Group Access

All

Command Mode

All except User EXEC

Command Line Usage

show ip redistribute [**bgp** | **ospf** | **rip**] [| {**begin** | **exclude** | **include**} {<*WORD*>} [| {**count** | **count-only**}]]

show ip redistribute [**bgp** | **ospf** | **rip**] [| {**count** | **count-only**}]

Command Syntax

bgp	displays routing domains redistributed into BGP
ospf	displays routing domains redistributed into OSPF
rip	displays routing domains redistributed into RIP
|	turns on output modifiers (filters)
begin	filter for output that begins with the specified string
exclude	filter for output that excludes the specified string
include	filter for output that includes the specified string
WORD	the specified string

count	count the number of outputted lines
count-only	count the number of lines while suppressing screen output

show ip traffic

The **show ip traffic** command displays the number of routing policy forwards and routing policy drops.

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show ip traffic [| {**begin** | **exclude** | **include**} {<*WORD*>} [| {**count** | **count-only**}]]

show ip traffic [| {**count** | **count-only**}]

Command Syntax

|	turns on output modifiers (filters)
begin	filter for output that begins with the specified string
exclude	filter for output that excludes the specified string
include	filter for output that includes the specified string
WORD	the specified string
count	count the number of outputted lines
count-only	count the number of lines while suppressing screen output

show route-map

The **show route-map** command displays route maps.

Group Access

All

Command Mode

All except User EXEC

Command Line Usage

show route-map [<*WORD*>] [| {**begin** | **exclude** | **include**} {<*WORD*>} [| {**count** | **count-only**}]]

show route-map [<*WORD*>] [| {**count** | **count-only**}]

Command Syntax

WORD	specified route-map
|	turns on output modifiers (filters)
begin	filter for output that begins with the specified string
exclude	filter for output that excludes the specified string
include	filter for output that includes the specified string
WORD	the specified string
count	count the number of outputted lines
count-only	count the number of lines while suppressing screen output

7

RIP Commands

Introduction

This chapter contains the Routing Information Protocol (RIP) commands used with the BSR 2000™.

RIP exchanges routing information to resolve routing errors. RIP coordinates routers on the network to broadcast their routing database periodically and determine the route with the least number of hops relative to the active routing table. Each hop determination message lists each destination with a *distance* in number of hops to the destination.

RIP Command Descriptions

This section contains an alphabetized list and descriptions of the RIP commands supported by the BSR.

auto-summary

The **auto-summary** command restores automatic summarization of subnet routes into network-level routes. The **no auto summary** command disables automatic summarization.

Note: RIP Version 1 always uses automatic summarization. RIP Version 2 when routing between disconnected subnets, requires automatic summarization to be off which is the default state.

Group Access

ISP

Command Mode

Router Configuration

Command Line Usage

auto summary

no auto summary

Command Default

Disabled

clear ip rip statistics

The **clear ip rip statistics** command clears all routes from the RIP routing table. This is the same route information displayed with the show ip rip database command.

Group Access

ISP

Command Mode

All modes except User EXEC

Command Line Usage

clear ip rip statistics

default-information originate

The **default-information originate** command generates a default route into the RIP database. The **no default-information originate** command disables default route generation.

Group Access

ISP

Command Mode

Router Configuration

Command Line Usage

default-information originate

no default-information originate

Command Default

Disabled

default-metric

The **default-metric** command specifies a new RIP default metric value. The **no metric** command returns the metric value to the default.

Use the **default-metric** command to set the current protocol to the same metric value for all distributed routes. The **default-metric** command is used with the **redistribute** command to obtain the same metric value for all distributed protocol-specific routes.

Note: This command assures that metrics are compatible during route redistribution. The default metric delivers an alternate for successful distribution if the network metrics are not converted.

Group Access

ISP

Command Mode

Router Configuration

Command Line Usage

default metric <*1-16*>

no default metric <*1-16*>

Command Syntax

1-16	the metric value

Command Default

Automatic metric translations given for each routing protocol

distance

The **distance** command sets the administrative distances for routes. The **no distance** command disables the administrative distance for routes.

Group Access

ISP

Command Mode

Router Configuration

Command Line Usage

distance <*1-255*>

no distance <*1-255*>

Command Syntax

1-255	administrative distance for setting routes

Command Default

120

distribute-list in

The **distribute-list in** command filters networks received in routing updates. The **no distribute-list in** command changes or cancels the filters received in updates.

Group Access

ISP

Command Mode

Router Configuration

Command Line Usage

distribute-list *<1-199> <1300-2699>* **in**

no distribute-list *<1-199> <1300-2699>* **in**

Command Syntax

1-199	access list number
1300-2699	extended access list number
in	applies access list to incoming route updates

Command Default

Disabled

distribute-list out

The **distribute-list out** command prevents networks from being advertised in updates. The **no distribute-list out** command enables update advertisements.

Use the **distribute-list out** command to apply the access list to outgoing route updates.

Group Access

ISP

Command Mode

Router Configuration

Command Line Usage

distribute-list *<1-199> <1300-2699>* **out**

no distribute-list *<1-199> <1300-2699>* **out**

Command Syntax

1-199 *1300-2699*	pre-defined access list number
out	applies access list to outgoing route updates

Command Default

Disabled

graceful-restart-period

The **graceful-restart-period** command enables RIP graceful restart. Graceful restart allows a RIP router to stay on the forwarding path even as its RIP software is being restarted. As the graceful restart procedure executes, the RIP routing table is updated with recalculated route entries that replace older entries in the routng table which are marked with a “replicated” flag. RIP graceful restart has a configurable time period (in seconds) that must elapse before routing table updates are completed and entries with the “replicated” flag are flushed from the routing table and the Fast Path database. The **no graceful-restart-period** command disables RIP graceful restart.

Group Access

ISP

Command Mode

Routing Configuration

Command Line Usage

graceful-restart-period <*0-360*>

no graceful-restart-period <*0-360*>

Command Syntax

0-360	the time period, in seconds, for completion of RIP graceful restart following an SRM switchover

Command Default

180 seconds

ip rip authentication key

The **ip rip authentication key** command enables RIP authentication on an interface by specifying a password or group of passwords that can be used on that interface. The **no rip authentication key** command deletes the associated password(s).

Note: Only RIP version 2 supports authentication.

Group Access

ISP

Command Mode

Interface Configuration

Command Line Usage

ip rip authentication key { **7** <*WORD*> | <*Password*>}

no ip rip authentication key <*Password*>

Command Syntax

7	specifies a that HIDDEN password will follow
WORD	the ENCRYPTED password: 18-50 hex digits (even number of digits)
Password	a plain text password with a 16 character maximum

ip rip host-routes

The **ip rip host-routes** command enables sending or receiving host routes with RIP version 1 for an interface. The **no ip rip host-routes** command disables sending or receiving host routes with RIP version 1 for an interface.

Group Access

ISP

Command Mode

Interface Configuration

Command Line Usage

ip rip host-routes

no ip rip host-routes

Command Default

Disabled

ip rip message-digest-key

The **ip rip message-digest-key** command enables RIP MD5 authentication. The **no ip rip message-digest-key** command disables RIP MD5 authentication.

Use the **ip rip message-digest-key** command to generate authentication information when sending packets and to authenticate incoming packets. Neighbor routers must have the same key identifier.

Group Access

ISP

Command Mode

Interface Configuration

Command Line Usage

ip rip message-digest-key <*1-255***> md5 <***password***>**

no ip rip message-digest-key <*1-255***>**

Command Syntax

1-255	key identifier
password	RIP password, string between 1 and 16 alphanumeric characters

Command Default

Disabled

ip rip receive version

The **ip rip receive version** command configures an interface to only receive packets from a specific version of the RIP protocol. Use the **ip rip receive version** command to configure the interface to receive one or both RIP versions. The **no ip rip receive version** command resets the RIP protocol version to RIP version 1 and 2.

Group Access

ISP

Command Mode

Interface Configuration

Command Line Usage

ip rip receive version {**0, 1, 2**}

no ip rip receive version {**0, 1, 2**}

Command Syntax

0	RIP version 1 and 2
1	RIP version 1 only
2	RIP version 2 only

Command Default

0

ip rip send version

The **ip rip receive version** command configures an interface to only transmit packets from a specific version of the RIP protocol. Use the **ip rip receive version** command to configure the interface to transmit one or both RIP versions. The **no ip rip receive version** command resets the RIP protocol version to RIP version 2.

Group Access

ISP

Command Mode

Interface Configuration

Command Line Usage

ip rip send version {**0, 1, 2, 3**}

no ip rip send version {**0, 1, 2, 3**}

Command Syntax

0	RIP 2 compatible
1	RIP version 1 only
2	RIP version 2 only
3	none

Command Default

2

ip split-horizon

The **ip split-horizon** command blocks route information from being advertised by a router out any interface from which that information originated. Enabling split-horizon optimizes communications among multiple routers, particularly when links are broken. The **no ip split-horizon** disables split-horizon.

Group Access

ISP

Command Mode

Interface Configuration

Command Line Usage

ip split-horizon

no ip split-horizon

Command Default

Enabled

maximum-paths

The **maximum-paths** command specifies the maximum number of parallel routes an IP routing protocol can support. The **no maximum-paths** command changes or cancels the number of maximum paths.

Group Access

RESTRICTED

Command Mode

Router Configuration

Command Line Usage

maximum-paths <*1-2*>

no maximum-paths

Command Syntax

1-2	the maximum number of parallel routes

network

The RIP version of the **network** command enables networks for the routing process. The **no network** command disables networks for the RIP routing process.

Note: If a network with RIP is not specified, the system does not advertise the network in any RIP routes.

Group Access

ISP

Command Mode

Router Configuration

Command Line Usage

network <*A.B.C.D*> [<*A.B.C.D*>]

no network <*A.B.C.D* [<*A.B.C.D*>]

Command Syntax

A.B.C.D	IP address of directly connected networks
A.B.C.D	associated IP address of the removed routes, subnet mask

offset-list

The **offset-list** command adds an offset to incoming and outgoing metrics to routes learned via RIP. The offset value is added to the routing metric. An offset-list with an interface slot/port is considered extended and takes precedence over an offset-list that is not extended. The **no offset-list** command removes the offset for incoming and outgoing metrics to routes learned via RIP.

Group Access

ISP

Command Mode

Router Configuration

Command Line Usage

offset-list {*1-99*} [**any**] {**in** | **out**} **<***0-16***>** [**cable** <*X*/*Y*> | **ethernet** <*X*/*Y* >| **gigaether** <*X*/*Y*>]

no offset-list {*1-99*} [**any**] {**in** | **out**} **<***0-16***>** [**cable** <*X*/*Y*> | **ethernet** <*X*/*Y* >| **gigaether** <*X*/*Y*>]

Command Syntax

1-99	standard access-list-number, if 0, no action is taken
any	apply offset to all networks
in	apply the offset to incoming metrics
out	apply the offset list to outgoing metrics
0-16	positive offset to be applied to metrics for networks matching the access list, if set to 0, no action is taken
cable *X/Y*	*X* is 0. *Y* is the cable interface port number to which the offset-list is applied.

ethernet *X/Y*	*X* is 0. *Y* is the Ethernet interface port number to which the offset-list is applied.
gigaether *X/Y*	*X* is 0. *Y* is the Gigabit Ethernet interface port number to which the offset-list is applied.

Command Default

Disabled

output-delay

The **output-delay** command changes the inter-packet delay for RIP updates to ensure that transmitted information is received by lower-speed routers. The **no output delay** command removes the inter-packet delay for RIP updates.

Note: This command helps prevent the loss of routing table information.

Group Access

ISP

Command Mode

Router Configuration

Command Line Usage

output-delay <*8-50*>

no output delay <*8-50*>

Command Syntax

8-50	time, in milliseconds, of multiple-packet RIP update

Command Default

0

passive-interface

The **passive-interface** command disables an interface from sending route updates by prohibiting packets from being transmitted from a specified port. When disabled, the subnet continues advertising to other interfaces. The **no passive-interface** command enables the interface to send route updates.

Group Access

ISP

Command Mode

Router Configuration

Command Line Usage

passive-interface {**cable** <*X/Y*> | **default** | **ethernet** <*X/Y*> | **gigaether** <*X/Y*> | **loopback** <*1-64*>}

no passive-interface {**cable** <*X/Y*> | **default** | **ethernet** <*X/Y*> | **gigaether** <*X/Y*> | **loopback** <*1-64*>}

Command Syntax

cable *X/Y*	*X* is 0. *Y* is the Cable interface port number.
default	suppresses routing updates on all interfaces
ethernet *X/Y*	*X* is 0. *Y* is the Ethernet interface port number.
gigaether *X/Y*	*X* is 0. *Y* is the Gigabit Ethernet interface port number.
loopback *1-64*	Loopback interface number

redistribute

The **redistribute** command redistributes routes from one protocol domain to another routing domain. The **no redistribute** command disables route distribution from one protocol domain to another routing domain.

Group Access

ISP

Command Mode

Router Configuration

Command Line Usage

redistribute {**bgp** | **connected** | **ospf** [**match** {**internal** | **external** | **external 1** | **external 2**}] | **static**} [**metric** <*1-16*>] [**route-map** <*WORD*>]

no redistribute {**bgp** | **connected** | **ospf** [**match** {**internal** | **external** | **external 1** | **external 2**}] | **static**} [**metric** <*1-16*>] [**route-map** <*WORD*>]

Command Syntax

bgp	BGP source protocol
connected	established routes as result of IP enabled on an interface
ospf	OSPF source protocol
match	the criteria by which OSPF routes are redistributed into RIP.
internal	routes that are internal to an autonomous system
external	routes external to an autonomous system, but are imported into OSPF as either Type 1 or Type 2 external route
external 1	routes that are external to an autonomous system, but are imported into OSPF as Type 1 external route

external 2	routes that are external to an autonomous system, but are imported into OSPF as Type 2 external route
static	IP or RIP static routes
metric	metric used for the redistributed route.
1-16	the RIP default metric
route-map	route-map used to conditionally control the route redistribution
WORD	the name of the route-map

Command Default

Disabled

router rip

The **router rip** command enables the routing process for RIP. The **no router rip** command disable the RIP routing process.

Group Access

ISP

Command Mode

Global Configuration

Command Line Usage

router rip

no router rip

show ip rip database

The **show ip rip database** command displays RIP database routing table information.The following is an example of typical screen output from the **show ip rip database** command:

```
172.19.13.0     255.255.255.0   redistributed      172.17.1.1      m:1  t:0
10.10.0.0       255.255.255.0   redistributed      58.58.58.2      m:1  t:0
172.22.251.0    255.255.255.0   redistributed      58.58.58.2      m:1  t:0
172.22.244.0    255.255.252.0   redistributed      58.58.58.2      m:1  t:0
10.10.10.0      255.255.255.0   via                58.58.58.2      m:2  t:12
12.12.12.0      255.255.255.0   redistributed      172.17.1.1      m:1  t:0
50.0.0.0        255.0.0.0       auto summary       50.50.50.4      m:1  t:0
21.21.21.0      255.255.255.0   directly connected 21.21.21.1      m:1  t:0
58.0.0.0        255.0.0.0       auto summary       58.58.58.1      m:1  t:0
80.0.0.0        255.0.0.0       auto summary       80.80.80.4      m:1  t:0
4.4.4.0         255.255.255.0   directly connected 4.4.4.4         m:1  t:0
80.80.80.0      255.255.255.0   directly connected 80.80.80.4      m:1  t:0
172.22.0.0      255.255.0.0     redistributed      58.58.58.2      m:1  t:0
10.0.0.0        255.0.0.0       via                58.58.58.2      m:1  t:0
4.0.0.0         255.0.0.0       auto summary       4.4.4.4         m:1  t:0
58.58.58.0      255.255.255.0   directly connected 58.58.58.1      m:1  t:0
12.0.0.0        255.0.0.0       redistributed      172.17.1.1      m:1  t:0
172.19.0.0      255.255.0.0     redistributed      172.17.1.1      m:1  t:0
172.168.0.0     255.255.0.0     redistributed      58.58.58.2      m:1  t:0
21.0.0.0        255.0.0.0       auto summary       21.21.21.1      m:1  t:0
50.50.50.0      255.255.255.0   directly connected 50.50.50.4      m:1  t:0
```

Note: The show ip route rip command can be used to display RIP routes in the routing table.

Group Access

ISP

Command Mode

All modes except User EXEC

Command Line Usage

show ip rip database [| {**begin** | **exclude** | **include**} {<*WORD*>} [| {**count** | **count-only**}]]

show ip rip database [| {**count** | **count-only**}]

Command Syntax

|	turns on output modifiers (filters)
begin	filter for output that begins with the specified string
exclude	filter for output that excludes the specified string
include	filter for output that includes the specified string
WORD	the specified string
count	count the number of outputted lines
count-only	count the number of lines while suppressing screen output

source-port 520

The **source-port 520** command enables UDP port 520 to be used by the RIP routing process. The **no source-port 520** command disables UDP port 520.

Group Access

ISP

Command Mode

Router Configuration

Command Line Usage

source port 520

no source port 520

Command Default

Disabled

timers basic

The **timers basic** command configures RIP network timers. The **no timers basic** command resets the network timer default.

Group Access

ISP

Command Mode

Router Configuration

Command Line Usage

timers basic <*update*> <*invalid*> <*flush*>

no timers basic <*update*> <*invalid*> <*flush*>

Command Syntax

update	clocks the interval between periodic routing updates, generally set to 30 seconds - small number of seconds added every time the timer is sent, to prevent collisions. 1-4294967295 rate (in seconds) at which updates are sent. This is the fundamental timing parameter of the routing protocol.

invalid	interval in seconds, routing updates 1-4294967295 Interval of time (in seconds) after which a route is declared invalid; it should be at least three times the value of the *update* argument. A route becomes invalid when there is an absence of updates that refresh the route. The route then enters into a *holddown* state. The route is marked inaccessible and advertised as unreachable. However, the route is still used for forwarding packets.
flush	number of seconds used before route removed from routing 1-4294967295 Amount of time (in seconds) that must pass before the route is removed from the routing table; the interval specified should be greater than the value of the *invalid* argument. If it is less than this sum, the proper *holddown* interval cannot elapse, which results in a new route being accepted before the *holddown* interval expires.

Command Default

update = 30 seconds

invalid = 180 seconds

flush = 300 seconds

version

The **version** command specifies the routing RIP version. The **no version** command disables the routing RIP version and resets the default.

Use the **ip rip receive version** and the **ip rip send version** commands to specify versions per interface.

Note: The basic timers for RIP are adjustable, but must be the same for all routers and servers on the network to execute a distributed, asynchronous routing algorithm. When the route-timeout timer expires, the route is marked invalid but is retained in the table until the route-flush timer expires.

Group Access

ISP

Command Mode

Router Configuration

Command Line Usage

version {**1** | **2**}

no version

Command Syntax

1	RIP version 1
2	RIP version 2

Command Default

RIP receives version 1 and 2, but sends only version 1

8

OSPF Commands

Introduction

This chapter describes the Open Shortest Path First (OSPF) commands used with the BSR 2000™.

OSPF is a link-state routing protocol that runs internally to a single Autonomous System, such as an enterprise network. At the core of the OSPF protocol is a distributed, replicated link-state database.

OSPF specifies a Link-state Advertisements (LSAs) that allow OSPF routers to update each other about the LAN and WAN links to which they connected. OSPF ensures that each OSPF router has an identical link-state database, except during period of convergence. Using the link-state database, each OSPF router calculates its IP routing table with the best routes through the network.

OSPF Command Descriptions

This section contains an alphabetized list and descriptions of the OSPF commands supported by the BSR.

area authentication

Use the **area authentication** command to enable authentication for an OSPF area to Type 1, Type 2, simple password, as specified in RFC 1247, while specification of Type 0 is assumed. Authentication type must match all routers and access servers in a particular area. The **no authentication** command disables authentication for the specified OSPF area.

Note: Ensure that the **ip ospf authentication-key** command is used to specify a password, which must be the same for all OSPF routers on a network, for communication to take place before the area authentication command is issued. If area authentication is enabled with MD5 authentication message-digest keyword, which is a type of password that must be configured using the **ip ospf message-digest-key** command.

Group Access

ISP

Command Mode

Router Configuration

Command Line Usage

area {*<0-4294967295>* | *<A.B.C.D>*} **authentication** [**message-digest**]

no area {*<0-4294967295>* | *<A.B.C.D>*} **authentication** [**message-digest**]

no area {*<0-4294967295>* | *<A.B.C.D>*}

Command Syntax

0-4294967295	OSPF area ID number in decimal format.
A.B.C.D	OSPF area ID in IP address format
message-digest	Enables MD5 authentication only on the area specified by the area ID or IP address.

Command Default

No authentication

area default-cost

Use the **area default-cost** command to specify a cost metric for the default summary route sent into the stub area by an area border router (ABR) only. The **no area default-cost** command removes the specified cost for the default summary route sent into a stub area.

Note: The **area stub** command is used in conjunction with the **area default-cost** command to define a specified area as a stub area for all routers and access servers attached to the area.

Group Access

ISP

Command Mode

Router Configuration

Command Line Usage

area {*<0-4294967295>* | *<A.B.C.D>*} **default-cost** *<0-65535>*

no area {*<0-4294967295>* | *<A.B.C.D>*} **default-cost** *<0-65535>*

Command Syntax

0-4294967295	OSPF area ID number in decimal format.
A.B.C.D	OSPF area ID in IP address format
0-65535	Outgoing OSPF cost metric for packets sent from an interface, which is an unsigned 16-bit integer from 0 to 65535.

area nssa

Use the **area nssa** command to configure an area as a Not So Stubby Area (NSSA). The **no nssa** command removes the NSSA configuration of an area.

Group Access

ISP

Command Mode

Router Configuration

Command Line Usage

area {*<0-4294967295>* | *<A.B.C.D>*} **nssa** [**default-information-originate**] [**no-redistribution**] [**no-summary**]

no area {*<0-4294967295>* | *<A.B.C.D>*} **nssa** [**default-information-originate**] [**no-redistribution**] [**no-summary**]

no area {*<0-4294967295>* | *<A.B.C.D>*}

Command Syntax

0-4294967295	OSPF area ID number in decimal format.
A.B.C.D	OSPF area ID in IP address format
default-information-originate	Originates a Type 7 default into the NSSA area on an NSSA Area Border Router (ABR) only.
no-redistribution	When router is NSSA ABR, the **redistribute** command imports routes into normal areas, but not into the NSSA area.
no-summary	Does not send summary LSAs into NSSA.

Command Default

No NSSA area is defined.

area range

Use the **area range** command to consolidate routes for an Area Border Router (ABR) only by advertising a single summary route that is advertised for each address range that is external to the area. The **no area range** command removes summarized routes for the ABR.

Group Access

ISP

Command Mode

Router Configuration

Command Line Usage

area {*<0-4294967295>* | *<A.B.C.D>*} **range** *<A.B.C.D>* *<A.B.C.D>* [**advertise** | **not-advertise** | *<cr>*]

no area {*<0-4294967295>* | *<A.B.C.D>*} **range** *<A.B.C.D>* *<A.B.C.D>* [**advertise** | **not-advertise**]

no area {*<0-4294967295>* | *<A.B.C.D>*}

Command Syntax

0-4294967295	OSPF area ID number in decimal format.
A.B.C.D	OSPF area ID in IP address format
A.B.C.D	IP address to match.
A.B.C.D	Subnet mask.
advertise	Sets address range status to advertise, generates a Type 3 summary LSA.
not-advertise	Sets address range status to DoNotAdvertise, Type 3 summary LSA is suppressed, and the component networks remain hidden from other networks.

area stub

Use the **area stub** command to configure an OSPF area as a stub area. A stub area allows a default route, intra-area routes, and inter-area routes, but disallows autonomous system (AS) external routes, virtual links, and Autonomous System Boundary Router (ASBR) routes.

Note: If there is more than one router within a stub area, ensure that the area that you are creating as a stub area is defined as a stub area on each of these routers.

The optional **area stub no-summary** command argument is used to prevent an area border router (ABR) from sending further Type 3 link-state advertisements (Lases) into the stub area. Use the **no area stub** command to return the area that you defined as a stub area to a non-stub OSPF area.

Group Access

ISP

Command Mode

Router configuration

Command Line Usage

area {*<0-4294967295>* | *<A.B.C.D>*} **stub** [**no-summary**]

no area {*<0-4294967295>* | *<A.B.C.D>*} **stub**

no area {*<0-4294967295>* | *<A.B.C.D>*}

Command Syntax

0-4294967295	OSPF area ID number in decimal format.
A.B.C.D	OSPF area ID in IP address format
no-summary	Prevents ABR from sending summary link advertisements into the stub area.

area virtual-link

Use the **area virtual link** command to create a virtual link that connects an OSPF area to the backbone area (area 0.0.0.0) without being physically connected to the OSPF backbone area. Use the **no area virtual-link** command to delete the defined OSPF virtual link.

Group Access

ISP

Command Mode

Router Configuration

Command Line Usage

area {*<0-4294967295>* | *<A.B.C.D>*} **virtual-link** *<A.B.C.D>* [**authentication-key** *<WORD>* | **dead-interval** *<1-65535>* | **hello-interval** *<1-65535>* | **message-digest-key** *<1-255>* {**md5** *<WORD>*}| **retransmit-interval** *<1-65535>* | **transmit-delay <***1-8192>*]

no area {*<0-4294967295>* | *<A.B.C.D>*} **virtual-link** *<A.B.C.D>* [**authentication-key** *<WORD>* | **dead-interval** *<1-65535>* | **hello-interval** *<1-65535>* | **message-digest-key** *<1-255>* {**md5** *<WORD>*}| **retransmit-interval** *<1-65535>* | **transmit-delay <***1-8192>*]

Command Syntax

0-4294967295	OSPF area ID number in decimal format.
A.B.C.D	OSPF area ID in IP address format
A.B.C.D	Router ID IP address that associated with the virtual link neighbor, 32-bit address.
authentication-key *WORD*	Unencrypted cleartext password that is 1 to 8 characters in length.
dead-interval *1-65535*	Number of seconds that the router does not receive hello packets from its neighbor before declaring the neighbor is down.

hello-interval *1-65535*	Time in seconds between hello packets on an interface, value must be the same for all routers and access servers attached to a common network.
message-migest-key *1-255*	OSPF MD5 authentication key.
md5 *WORD*	Encrypted md5 password (1-16 characters)
retransmit-interval *1-65535*	Expected round-trip delay between two routers on the attached network, value must be more than expected delay.
transmit-delay *1-8192*	Approximate time to transmit an LSA packet.

Command Defaults

hello-interval	=	10 seconds
retransmit-interval	=	5 seconds
transmit-delay	=	1 second
dead-interval	=	40 seconds

auto-cost reference-bandwidth

The BSR OSPF routing process calculates the OSPF cost metric for an interface according to the bandwidth of this interface. The cost of an interface depends on the type of interface. OSPF uses a reference bandwidth of 100 Mbps for cost calculation. The formula to calculate the cost is the reference bandwidth divided by interface bandwidth.

Use the **auto-cost reference-bandwidth** command to set the automatic cost metric that the OSPF routing process uses to differentiate the cost of multiple high-bandwidth links.

Use the **no auto-cost reference-bandwidth** command to remove the OSPF cost metric for a link.

Group Access

ISP

Command Mode

Router Configuration

Command Line Usage

auto-cost reference-bandwidth *<1-4294967>*

no auto-cost reference-bandwidth *<1-4294967>*

Command Syntax

1-4294967	The reference bandwidth in Mbps.

Command Default

10 Mbps

auto-virtual-link

Use the **auto-virtual-link** command to automatically detect and create OSPF virtual links. The **no auto-virtual-link** command disables automatic detection and creation of OSPF virtual links.

Group Access

ISP

Command Mode

Router Configuration

Command Line Usage

auto-virtual-link

no auto-virtual-link

Command Default

Disabled

clear ip ospf

The **clear ip ospf** command resets an OSPF connection using a soft reconfiguration.

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

clear ip ospf

default-information originate

The **default-information originate** command generates a default route into an OSPF routing domain by configuring the metric for redistributed routes and is used with the **redistribute** command to redistribute routes into an OSPF routing domain so they are included in an automatic Autonomous System Border Router (ASBR) summary.

The **no default-information originate** command removes default routes from the OSPF routing domain.

Group Access

ISP

Command Mode

Router Configuration

Command Line Usage

default-information originate [**always** | **metric** <*0-16777214*> | **metric-type** <*1-2*>]

no default-information originate [**always**] [**metric** <*0-16777214*>] [**metric-type** <*1-2*>]

Command Syntax

always	Always advertises the default route into the OSPF domain regardless of whether the routing table has a default route.
metric *0-16777214*	OSPF default metric to generate a default route.
metric type *1-2*	External link type associated with the default route advertised into the OSPF routing domain, values are 1 and 2, 1 being comparable to the link state metric and 2 larger than the cost of intra-AS path.

Command Default

Disabled

default-metric

The default metric feature is used to eliminate the need for separate metric definitions for each routing protocol redistribution.The **default-metric** command forces the OSPF routing protocol to use the same metric value for all distributed routes from other routing protocols. The **no default-metric** command removes or changes the default metric value for the OSPF routing protocol.

Group Access

ISP

Command Mode

Router Configuration

Command Line Usage

default-metric <*1-16777214*>

no default-metric

Command Syntax

1-16777214	Default metric value.

distance

The **distance** command sets all 3 OSPF distances for routes to the same administrative value. The **no distance** command disables the administrative distance for routes.

Group Access

ISP

Command Mode

Router Configuration

Command Line Usage

distance <*1-255*>

no distance <*1-255*>

Command Syntax

1-255	administrative distance for setting routes

Command Default

120

distance ospf

The **distance ospf** command defines OSPF route administrative distances based on route type. The **no distance ospf** command deletes OSPF route administrative distances based on route type.

Use the **distance ospf** command to set a distance for a group of routers, as opposed to any specific route passing an access list. The **distance ospf** command serves the same function as the **distance** command used with an access list.

Use the **distance ospf** command when OSPF processes have mutual redistribution, to choose internal routes from one external route to another.

Group Access

ISP

Command Mode

Router Configuration

Command Line Usage

distance ospf intra-area <*1-255*> **inter-area** <*1-255*> **external**

<*1-255*>

no distance ospf intra-area <*1-255*> **inter-area** <*1-255*> **external**

<*1-255*>

Command Syntax

intra-area *1-255*	sets distance for all routes within an area, default value 110
inter-area *1-255*	sets distance for all routes from one area to another area, default value 110
external *1-255*	sets distance for routes learned by redistribution from other routing domains

Command Default

intra-area distance = 110

inter-area distance = 110

external distance = 110

distribute-list

Use the **distribute-list** command to filter networks received and sent in routing updates and networks suppressed in routing updates by using access lists. The networks that are permitted or denied are defined in access lists. The **no distribute-list** command removes access list from an incoming or outgoing routing update.

Group Access

ISP

Command Mode

Router Configuration

Command Line Usage

distribute-list {*<1-199>* | *<1300-2699>*} {**in** | **out**}

no distribute-list {*<1-199>* | *<1300-2699>*} {**in** | **out**}

Command Syntax

1-199	Access list number that is used to filter incoming and outgoing routing updates.
1300-2699	Expanded range access list number that is used to filter incoming and outgoing routing updates.
in	Filters incoming routing updates.
out	Filters outgoing routing updates.

Command Default

Disabled

ip ospf authentication-key

The **ip ospf authentication-key** command assigns a password for use by neighboring OSPF routers that are using OSPF simple password authentication. The **no ip ospf authentication-key** command deletes the password assigned for use by neighboring OSPF routers that are using OSPF simple password authentication.

Note: All neighbor routers on the same network need the same password to exchange OSPF information.

Group Access

ISP

Command Mode

Interface Configuration

Command Line Usage

ip ospf authentication-key <*WORD*>

no ip ospf authentication-key <*WORD*>

Command Syntax

WORD	character string from 1 to 8 characters in length

ip ospf cost

The **ip ospf cost** command establishes a precise cost metric value for sending a packet on an OSPF interface. The **no ip ospf cost** command disables a precise cost metric value for sending the path cost to the default.

Use the **ip ospf cost** command to assign a cost metric value for a particular interface. The user can set the metric manually if the default needs to be changed.

Group Access

ISP

Command Mode

Interface Configuration

Command Line Usage

ip ospf cost *<1-65535>*

no ip ospf cost

Command Syntax

1-65535	the link state metric

ip ospf database-filter all out

The **ip ospf database-filter all out** command filters OSPF LSAs during synchronization and flooding on the specified interface. The **no ip ospf database-filter all out** command disables filtering OSPF LSAs during synchronization and flooding on the specified interface.

Group Access

ISP

Command Mode

Interface Configuration

Command Line Usage

ip ospf database-filter all out

no ip ospf database-filter all out

Command Default

Disabled

ip ospf dead-interval

The **ip ospf dead-interval** command sets the number of seconds during which the router hello packets are not seen before the neighboring routers consider the router to be down. The **no ip ospf dead-internal** removes the number of seconds set during which the router hello packets are not seen before the neighboring routers consider the router to be down.

Group Access

ISP

Command Mode

Interface Configuration

Command Line Usage

ip ospf dead-internal <*1-65535*>

no ip ospf dead-internal

Command Syntax

1-65535	integer that specifies the interval - the value must be the same for all routers on the network

Command Default

40

ip ospf hello-interval

The **ip ospf hello-interval** command sets the number of seconds between hello packets send by a router on the interface. The **no ip ospf hello-interval** command resets the number of seconds between hello packets sent by a router on an interface to the default value.

Use the **ip ospf hello-interval** command as a form of keepalive used by routers in order to acknowledge their existence on a segment.

Group Access

ISP

Command Mode

Interface Configuration

Command Line Usage

ip ospf hello-interval <*1-65535*>

no ip ospf hello-interval

Command Syntax

1-65535	integer that specifies the interval, value must be the same for all nodes on the network

Command Default

10

ip ospf message-digest-key

The **ip ospf message-digest-key** command enables OSPF MD5 authentication. The **no ip ospf message-digest-key** command disables OSPF MD5 authentication.

Use the **ip ospf message-digest-key md5** command to generate authentication information when sending packets and to authenticate incoming packets. Neighbor routers must have the same key identifier.

Group Access

ISP

Command Mode

Interface Configuration

Command Line Usage

ip ospf message-digest-key <*1-255***> md5** <*WORD*>

no ip ospf message-digest-key <*1-255***>**

Command Syntax

1-255	key identifier
WORD	OSPF password, string between 1 and 16 alphanumeric characters

Command Default

Disabled

ip ospf network

The **ip ospf network command** configures the OSPF network type to a type other than the default for a given media. The **no ip ospf network** command returns to the default network type.

Group Access

All

Command Mode

Interface Configuration

Command Line Usage

ip ospf network [**broadcast** | **point-to-point**]

no ip ospf network

Command Syntax

broadcast	specifies an OSPF broadcast multi-access network
point-to-point	specifies an OSPF point-to-point network - OSPF point-to-point networks reduces the time it takes for designated router election and peering

Command Default

Dependant upon the network type.

ip ospf priority

The **ip ospf priority** command sets router priority to aid in determining the OSPF designated router for a network. The **no ip ospf priority** command changes priority to aid in determining the OSPF designated router for a network to the default value.

Use the **ip ospf priority** command value to configure OSPF broadcast networks. The router with a higher priority takes precedence when attempting to become the designated router. If the routers share the same priority, router ID takes precedence.

Group Access

ISP

Command Mode

Interface Configuration

Command Line Usage

ip ospf priority <*0-255*>

no ip ospf priority <*0-255*>

Command Syntax

0-255	the priority value

Command Default

1

ip ospf retransmit-interval

The **ip ospf retransmit-interval** command establishes the number of seconds between LSAs retransmissions for adjacencies belonging to an OSPF interface. The **no ip ospf retransmit-interval** command changes the number of seconds between LSA retransmissions for adjacencies belonging to an OSPF interface to the default value.

Use the **ip ospf retransmit-interval** command to establish the time a router sends an LSA to its neighbor. The neighbor keeps the LSA until it receives the acknowledgement.

Group Access

ISP

Command Mode

Interface Configuration

Command Line Usage

ip ospf retransmit-interval <*1-3600*>

no ip ospf retransmit-interval

Command Syntax

1-3600	the amount of time between LSA retransmissions in seconds

Command Default

5

ip ospf transmit-delay

The **ip ospf transmit-delay** command sets the approximate amount of time to transmit an LSA retransmissions for adjacencies belonging to an OSPF interface. The **no ip ospf transmit-delay** command changes the approximate amount of time set to transmit an LSA retransmissions for adjacencies belonging to an OSPF interface.

Use the **ip ospf transmit-delay** command to enable the delay over a link. The delay is defined as the time that it takes for the LSA to propagate over a link.

Before transmission, LSAs in the update packet must have their ages incremented by the amount specified in the *seconds* argument. The value should take into account the transmission and propagation delays for the interface.

If the delay is not added before transmission over a link, the time in which the LSA propagates over the link is not considered. Significance is greater on low-speed links.

Group Access

ISP

Command Mode

Interface Configuration

Command Line Usage

ip ospf transmit-delay *<1-3600>*

no ip ospf transmit-delay

Command Syntax

1-3600	the time it takes to transmit an LSA in seconds

Command Default

1

maximum-paths

The **maximum-paths** command specifies the maximum number of parallel routes an IP routing protocol can support. The **no maximum-paths** command changes or cancels the number of maximum paths.

Group Access

RESTRICTED

Command Mode

Router Configuration

Command Line Usage

maximum-paths <*1-2*>

no maximum-paths

Command Syntax

1-2	the maximum number of parallel routes

network area

The **network area** command defines the interfaces and area ID on which OSPF runs. The **no network area** command deletes the interfaces and area ID on which OSPF runs.

Use the **network area** command to cover IP address(es) for OSPF to operate on an interface. Use the address and *wildcard-mask* as one command to define one or more interfaces for an intended area.

A subnet address may be designated as the area ID if associated areas are used with IP subnets. Each IP subnet is associated with a single area only.

Group Access

ISP

Command Mode

Router Configuration

Command Line Usage

network <*A.B.C.D*> <*A.B.C.D*> **area** {<*0-4294967295*> | <*A.B.C.D*>}

no network <*A.B.C.D*> <*A.B.C.D*> **area** {<*0-4294967295*> | <*A.B.C.D*>}

Command Syntax

A.B.C.D	Network IP address.
A.B.C.D	IP address type mask with wild card bits.
0-4294967295	OSPF area ID as a decimal value
A.B.C.D	OSPF area ID as an IP address if OSPF areas are associated with IP subnets

Command Default

Disabled

passive-interface

The **passive-interface** command disables an interface from sending route updates by prohibiting packets from being transmitted from a specified port. When disabled, the subnet continues advertising to other interfaces. The **no passive-interface** command enables the interface to send route updates.

Group Access

ISP

Command Mode

Router Configuration

Command Line Usage

passive-interface {**cable** <*X/Y*> | **ethernet** <*X/Y*> | **gigaether** <*X/Y*>| **loopback** <*1-64*>}

no passive-interface {**cable** <*X/Y*> | **ethernet** <*X/Y*> | **gigaether** <*X/Y*>| **loopback** <*1-64*>}

Command Syntax

cable *X/Y*	*X* is 0. *Y* is the Cable interface port number.
ethernet *X/Y*	*X* is 0. *Y* is the Ethernet interface port number.
gigaether *X/Y*	*X* is 0. *Y* is the Gigabit Ethernet interface port number.
loopback *1-64*	Loopback interface number

redistribute

The **redistribute** command redistributes routes from one protocol domain to another routing domain. The **no redistribute** command disables route distribution from one protocol domain to another routing domain.

Group Access

ISP

Command Mode

Router Configuration

Command Line Usage

redistribute {**bgp** | **connected** | **rip** | **static**} [**metric** <*1-16777215*>] [**metric-type** {**1** | **2**}] [**route-map** <*WORD*>] [**subnets**] [**tag** <*0-4294967295*>]

no redistribute {**bgp** | **connected** | **rip** | **static**} [**metric** <*1-16777215*>] [**metric-type** {**1** | **2**}] [**route-map** <*WORD*>] [**subnets**] [**tag** <*0-4294967295*>]

Command Syntax

bgp	BGP source protocol
connected	established routes as result of IP enabled on an interface
rip	RIP source protocol
static	IP or OSPF static routes
metric *1-16777215*	metric used for the redistributed route.
metric-type 1 **metric-type 2**	OSPF exterior metric type for redistributed routes
route-map *WORD*	the name of the route-map used to conditionally control the route redistribution
subnets	consider subnets for redistribution into OSPF
tag *0-4294967295*	set a 32-bit tag value for routes redistributed into OSPF

Command Default

Disabled

rfc1583-compatible

The **rfc1583-compatible** enables RFC1583 preference rules on choosing AS-External-LSAs during shortest path first (SPF) calculation according to RFC2328, section 16.4. The **no rfc1583-compatible** command disables RFC1583 preference rules on choosing AS-External-LSAs during SPF calculation according to RFC2238, section 16.4.

Group Access

ISP

Command Mode

Router Configuration

Command Line Usage

rfc1583-compatible

no rfc1583-compatible

Command Default

Disabled

router-id

The **router-id** command overrides a configured OSPF router identifier (IP address) by manually configuring a new identifier. The **no router-id** command restores the initial configuration.

Group Access

ISP

Command Mode

Router Configuration

Command Line Usage

router-id <*A.B.C.D*>

no router-id

Command Syntax

A.B.C.D	the new OSPF router identifier (IP address)

router ospf

The **router ospf** command enables an OSPF routing process. The **no router ospf** command disables the OSPF routing process.

Use the **router ospf** command to designate an OSPF routing process with a unique value.

Group Access

ISP

Command Mode

Global Configuration

Command Line Usage

router ospf

no router ospf

show ip ospf

To display general information about OSPF routing processes, use the **show ip ospf** command.

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show ip ospf [**network**] [| {**begin** | **exclude** | **include**} {<*WORD*>} [| {**count** | **count-only**}]]

show ip ospf [**network**] [| {**count** | **count-only**}]

Command Syntax

network	shows IP OSPF network; displays network area information
|	turns on output modifiers (filters)
begin	filter for output that begins with the specified string
exclude	filter for output that excludes the specified string
include	filter for output that includes the specified string
WORD	the specified string
count	count the number of outputted lines
count-only	count the number of lines while suppressing screen output

show ip ospf database

The **show ip ospf database** command displays list of information related to the OSPF database.

Group Access

All

Command Mode

All Modes except User EXEC

Command Line Usage

show ip ospf [*<0-4294967295>*] **database** [*A.B.C.D* | **adv-router** <*A.B.C.D*> | **asbr-summary** | **database-summary** | **external** | **network** | **nssa-external** | **router** | **self-originate** | **summary**] [| {**begin** | **exclude** | **include**} {*<WORD>*} [| {**count** | **count-only**}]]

show ip ospf [*<0-4294967295>*] **database** [*A.B.C.D* | **adv-router** <*A.B.C.D*> | **asbr-summary** | **database-summary** | **external** | **network** | **nssa-external** | **router** | **self-originate** | **summary**] [| {**count** | **count-only**}]

Command Syntax

0-4294967295	Assigned OSPF area ID number.
A.B.C.D	router links, link state ID always the same as the advertising router, network IP address, value dependent upon advertisement LSA type
adv-router	Displays all LSAs for the specified advertising router.
A.B.C.D	Specifies the advertised router ID.
asbr-summary	Autonomous System Boundary Router (ASBR) summary.
database-summary	summary of the OSPF database
external	external LSAs

network	network LSAs
nssa-external	NSSA external LSA information
router	router LSAs
self-originate	LSAs from the local router
summary	summary LSAs
|	turns on output modifiers (filters)
begin	filter for output that begins with the specified string
exclude	filter for output that excludes the specified string
include	filter for output that includes the specified string
WORD	the specified string
count	count the number of outputted lines
count-only	count the number of lines while suppressing screen output

show ip ospf interface

The **show ip ospf interface** command displays OSPF-related interface information.

Group Access

All

Command Mode

All Modes except User EXEC

Command Line Usage

show ip ospf interface [<*A.B.C.D*> | **cable** <*X*/*Y*> | **ethernet** <*X*/*Y*> | **gigaether** <*X*/*Y*> | **loopback** <*1-64*>] [| {**begin** | **exclude** | **include**} {<*WORD*>} [| {**count** | **count-only**}]]

show ip ospf interface [<*A.B.C.D*> | **cable** <*X*/*Y*> | **ethernet** <*X*/*Y*> | **gigaether** <*X*/*Y*> | **loopback** <*1-64*>] [| {**count** | **count-only**}]

Command Syntax

A.B.C.D	Interface IP address
cable	OSPF information over the Cable interface.
ethernet	OSPF information over the Ethernet/ FastEthernet 802.3 interface.
gigaether	OSPF information over the Gigabit Ethernet interface.
loopback *1-64*	OSPF information over the loopback interface
X/*Y*	*X* is 0. *Y* is the port number.
|	turns on output modifiers (filters)
begin	filter for output that begins with the specified string
exclude	filter for output that excludes the specified string

include	filter for output that includes the specified string
WORD	the specified string
count	count the number of outputted lines
count-only	count the number of lines while suppressing screen output

show ip ospf memory

The **show ip ospf memory** command displays OSPF memory usage information.

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show ip ospf memory [| {**begin** | **exclude** | **include**} {<*WORD*>} [| {**count** | **count-only**}]]

show ip ospf memory [| {**count** | **count-only**}]

Command Syntax

|	turns on output modifiers (filters)
begin	filter for output that begins with the specified string
exclude	filter for output that excludes the specified string
include	filter for output that includes the specified string
WORD	the specified string
count	count the number of outputted lines
count-only	count the number of lines while suppressing screen output

show ip ospf neighbor

The **show ip ospf neighbor** command displays information about all OSPF neighbors.

Use the **show ip ospf neighbor** command to display information for each neighbor.

Group Access

ISP

Command Mode

All modes except User EXEC

Command Line Usage

show ip ospf neighbor [<*A.B.C.D*>] [**detail**] [| {**begin** | **exclude** | **include**} {<*WORD*>} [| {**count** | **count-only**}]]

show ip ospf neighbor [<*A.B.C.D*>] [**detail**] [| {**count** | **count-only**}]

Command Syntax

A.B.C.D	specific OSPF neighbor ID
detail	list of neighbor information in detail
|	turns on output modifiers (filters)
begin	filter for output that begins with the specified string
exclude	filter for output that excludes the specified string
include	filter for output that includes the specified string
WORD	the specified string
count	count the number of outputted lines
count-only	count the number of lines while suppressing screen output

show ip ospf network

The **show ip ospf network** command displays information about OSPF network areas.

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show ip ospf network [| {**begin** | **exclude** | **include**} {<*WORD*>} [| {**count** | **count-only**}]]

show ip ospf network [| {**count** | **count-only**}]

Command Syntax

|	turns on output modifiers (filters)
begin	filter for output that begins with the specified string
exclude	filter for output that excludes the specified string
include	filter for output that includes the specified string
WORD	the specified string
count	count the number of outputted lines
count-only	count the number of lines while suppressing screen output

show ip ospf virtual-links

The **show ip ospf virtual-links** command displays parameters regarding the current state of the OSPF virtual links.

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show ip ospf virtual-links [| {**begin** | **exclude** | **include**} {<*WORD*>} [| {**count** | **count-only**}]]

show ip ospf virtual-links [| {**count** | **count-only**}]

Command Syntax

|	turns on output modifiers (filters)
begin	filter for output that begins with the specified string
exclude	filter for output that excludes the specified string
include	filter for output that includes the specified string
WORD	the specified string
count	count the number of outputted lines
count-only	count the number of lines while suppressing screen output

summary-address

The **summary-address** aggregates external routes at the border of the OSPF domain. The **no summary-address** command deletes aggregated external routes at the border of the OSPF domain.

Use the **summary-address** command to summarize routes from other routing protocols that are redistributed to OSPF. The **area range** command summarizes routes between OSPF areas.

The **summary address** command is responsible for an OSPF autonomous system boundary router to advertise one external route as an aggregate. This applies to all redistributed routes that the address covers.

Group Access

ISP

Command Mode

Router Configuration

Command Line Usage

summary-address <*A.B.C.D*> <*A.B.C.D*> [**tag** <*0-4294967295*>]

no summary-address <*A.B.C.D*> <*A.B.C.D*> [**tag** <*0-4294967295*>]

Command Syntax

A.B.C.D	summary address of range of addresses
A.B.C.D	IP subnet mask for the summary route
tag *0-4294967295*	tag value, can be used as a match value to control redistribution

Command Default

All redistributed routes advertised separately

timers spf

The **timers spf** command configures the amount of time between OSPF topology change receipt and when it starts a shortest path first (SPF) calculation. This includes the hold time between two consecutive SPF calculations. The **no timers spf** command changes the configuration of the amount of time between OSPF topology changes receipt and when it starts an SPF calculation and returns it to the default value.

Use the **timers spf** command to set the delay time and hold time to change routing to a faster path.

Group Access

ISP

Command Mode

Router Configuration

Command Line Usage

timers spf <*0-65535*> <*0-65535*>

no timers spf <*0-65535*> <*0-65535*>

Command Syntax

0-65535	time in seconds between receipt and SPF
0-65535	minimum time in seconds between two consecutive SPF calculations

Command Default

SPF delay = 5 seconds

SPF hold time = 10 seconds

9

IGMP Commands

Introduction

This chapter describes the Internet Group Management Protocol (IGMP) commands used with the BSR 2000™.

Internet Group Management Protocol (IGMP), part of the Internet Protocol (IP) suite, is used between hosts and routers to report dynamic multicast group membership. IP multicasting is the transmission of an IP datagram to a "host group" identified by a single IP destination address. Multicasting directs the same information packets to multiple destinations at the same time, versus unicasting, which sends a separate copy to each individual destination. Because the destinations receive the same source packet at once, delivery of the information takes place in a more timely manner.

As stated in RFC 1112, the membership of a host group is dynamic; that is, hosts may join and leave groups at any time. There is no restriction on the location or number of members in a host group, and a host may be a member of more than one group at a time.

There are three types of messages structures supported by IGMP to communicate with each other about the multicast traffic: “queries”, “reports”, and “leave group” messages. Query messages are used to discover which hosts are in which multicast groups. In response, the hosts sends a report message to inform the querier of a host’s membership. (Report messages are also used by the host to join a new group). Leave group messages are sent when the host wishes to leave the multicast group.

Applications that implement IGMP effectively eliminate multicast traffic on segments that are not destined to receive this traffic, thus limiting the overall amount of traffic on the network.

IGMP Command Descriptions

This section contains an alphabetized list and descriptions of the IGMP commands supported by the BSR.

clear ip igmp counters

The **clear ip igmp counters** command clears IGMP statistics counters on a specific router.

Group Access

ISP

Command Mode

All modes except User EXEC

Command Line Usage

clear ip igmp counters

ip igmp access-group

The **ip igmp access-group** command controls multicast groups that hosts can join. The **no ip igmp access-group** command removes control and allows the hosts to join all groups.

Group Access

ISP

Command Mode

Interface Configuration

Command Line Usage

ip igmp access-group *<1-99> <1300-1999>*

no ip igmp access-group *<1-99> <1300-1999>*

Command Syntax

1-99	standard access list
1300-1999	standard access-list number (expanded range)

Command Default

any group allowed on interface

ip igmp querier-timeout

The **ip igmp querier-interval** command configures the timeout prior to the time the router takes over as the interface querier. The **no ip igmp querier-timeout r**emoves the configured timeout prior to the time the router takes over as the interface querier, and returns it to the default.

Note: Only after the querier has completed the last query, does the router take over as the interface querier after a **no ip igmp querier-timeout** command is issued.

Group Access

ISP

Command Mode

Interface Configuration

Command Line Usage

ip igmp querier-timeout *<1-3600>*

no ip igmp querier-timeout *<1-3600>*

Command Syntax

1-3600	querier timeout value in seconds

Command Default

query value x 2

ip igmp query-interval

The **igmp query-interval** command sets the interval in which the router sends out IGMP queries for that interface. The **no ip igmp query-interval** command removes the set interval in which the router send out IGMP queries for an interface and returns it to the default value.

Use the **ip igmp query-interval** command to configure how often the router solicits the IGMP report responses from all of the multicast hosts on the network.

Group Access

ISP

Command Mode

Interface Configuration

Command Line Usage

ip igmp query-interval *<1-3600>*

no ip igmp query-interval *<1-3600>*

Command Syntax

1-3600	query interval in seconds

Command Default

125 seconds

ip igmp query-max-response-time

The **ip igmp query-max-response-time** command sets the maximum response time advertised in query. Use the **no ip igmp query-max-response-time** command to remove the set maximum response time advertised in query and return it to the default.

Group Access

ISP

Command Mode

Interface Configuration

Command Line Usage

ip igmp query-max-response-time <*1-255*>

no ip igmp query-max-response-time <*1-255*>

Command Syntax

1-255	query response value in tenths of a second

Command Default

10 seconds

ip igmp static-group

The **ip igmp static-group** command connects, or configures, the router as a member of a particular group on the interface. The **no ip igmp static-group** disassociates the router from the group.

The **ip igmp static-group** command is used to give a host (that does not run IGMP) membership in a multicast group.

Group Access

ISP

Command Mode

Interface Configuration

Command Line Usage

ip igmp static-group <*A.B.C.D*>

no ip igmp static-group <*A.B.C.D*>

Command Syntax

A.B.C.D	IP multicast group address that the router is configured to be a member of

Command Default

Disabled

ip igmp version

The **ip igmp version** command configures the specific version used by the router. The **no ip igmp version** removes the configured, specific version used by the router and returns it to the default.

Use the **ip igmp version** command to configure the IGMP version on the interface.

Group Access

ISP

Command Mode

Interface Configuration

Command Line Usage

ip igmp version {*<1-2>*}

no ip igmp version {*<1-2>*}

Command Syntax

1	IGMP Version 1
2	IGMP Version 2

Command Default

Version 2

ip igmp version1-querier

The **ip igmp version1-querier** command configures the router to act as the querier for IGMPv1. This is done by manually assigning the IGMP querier. The **no ip igmp version1-querier** command disables the router from acting as the querier.

Note: The interface is not effected when IGMPv2 is running on the interface. It is recommended that only one querier is enabled in a network segment.

Group Access

ISP

Command Mode

Interface Configuration

Command Line Usage

ip igmp version1-querier

no ip igmp version1-querier

Command Default

Disabled

show ip igmp interface

The **show ip igmp interface** command displays the multicast information for an interface.

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show ip igmp interface [**groups** | **brief**] [| {**begin** | **exclude** | **include**} {<*WORD*>} [| {**count** | **count-only**}]]

show ip igmp interface [**groups** | **brief**] [| {**count** | **count-only**}]

Command Syntax

groups	multicast groups that are joined on each interface
brief	brief summary of IGMP interface
|	turns on output modifiers (filters)
begin	filter for output that begins with the specified string
exclude	filter for output that excludes the specified string
include	filter for output that includes the specified string
WORD	the specified string
count	count the number of outputted lines
count-only	count the number of lines while suppressing screen output

show ip igmp groups

The **show ip igmp groups** command displays multicast groups connected to a specific router using IGMP.

Use the **show ip igmp groups** command to display the following IGMP group information:

Group Address	multicast address
Interface	interface reachable
Uptime	hours, minutes, and seconds multicast known
Expires	hours, minutes, and seconds until the entry is removed from IGMP groups table
Last Reporter	last host of multicast group

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show ip igmp groups [**summary**] [| {**begin** | **exclude** | **include**} {<*WORD*>} [| {**count** | **count-only**}]]

show ip igmp groups [**summary**] [| {**count** | **count-only**}]

Command Syntax

summary	shows summary report of IGMP groups
|	turns on output modifiers (filters)
begin	filter for output that begins with the specified string

exclude	filter for output that excludes the specified string
include	filter for output that includes the specified string
WORD	the specified string
count	count the number of outputted lines
count-only	count the number of lines while suppressing screen output

show ip igmp statistics

The **show ip igmp statistics** command displays statistics for a specified IGMP interface.

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show ip igmp statistics [| {**begin** | **exclude** | **include**} {<*WORD*>} [| {**count** | **count-only**}]]

show ip igmp statistics [| {**count** | **count-only**}]

Command Syntax

|	turns on output modifiers (filters)
begin	filter for output that begins with the specified string
exclude	filter for output that excludes the specified string
include	filter for output that includes the specified string
WORD	the specified string
count	count the number of outputted lines
count-only	count the number of lines while suppressing screen output

10

IP Multicast Commands

Introduction

This chapter describes the IP Multicast Protocol commands used with the BSR. This chapter contains the following sections on the Multicast Routing Table Manager (MRTM), and Multicast Forwarding Manager (MFM) protocols.

- MRTM Command Descriptions
- MFM Command Descriptions

MRTM Command Descriptions

Unlike traditional Internet traffic that requires separate connections for each source-destination pair, IP Multicasting allows many recipients to share the same source. The IP Multicast protocol sends data to distributed servers on the multicast backbone, and MRTM allows different IP protocols to work together on the same router. This means that just one set of packets is transmitted for all destinations. MRTM also manages Multicast Open Shortest Path First (MOSPF), and provides multicast routing support for Resource Reservation Protocol (RSVP). For large amounts of data, IP Multicast is more efficient than normal Internet transmissions because the server can broadcast a message to many recipients simultaneously. This section contains an alphabetized list and descriptions of the MRTM IP multicast commands supported by the BSR.

ip mroute

The **ip mroute** command configures an IP multicast static route. The **no ip mroute** command removes the configuration of an IP multicast static route.

Group Access

ISP

Command Mode

Global Configuration

Command Line Usage

ip mroute <*A.B.C.D*> <*A.B.C.D*> <*A.B.C.D*> [<*1-255*>]

no ip mroute <*A.B.C.D*> <*A.B.C.D*> <*A.B.C.D*> [<*1-255*>]

Command Syntax

A.B.C.D	static source address
A.B.C.D	static network mask
A.B.C.D	RPF neighbor address or route
1-255	administrative distance for mroute

ip mroute static distance

The **ip mroute static distance** command configures a static multicast route. The **no ip mroute static distance** command removes the route.

Group Access

ISP

Command Mode

Global Configuration

Command Line Usage

ip mroute static distance <*1-255*>

no ip mroute static distance <*1-255*>

Command Syntax

1-255	the administrative distance for the multicast route - a lower distance has preference

ip mroute unicast distance

The **ip mroute unicast distance** command configures a unicast multicast route. The **no ip mroute unicast distance** command removes the route.

Group Access

ISP

Command Mode

Global Configuration

Command Line Usage

ip mroute unicast distance <*1-255*>

no ip mroute unicast distance <*1-255*>

Command Syntax

1-255	the administrative distance for the multicast route - a lower distance has preference

ip multicast-routing

The **ip multicast-routing** command enables IP multicast routing. The **no ip multicast-routing** command disables IP multicast routing. This command is used with multicast routing protocols.

Note: Multicast packets are not forwarded unless IP multicast routing is enabled.

Group Access

ISP

Command Mode

Global Configuration

Command Line Usage

ip multicast-routing

no ip multicast-routing

Command Default

Disabled

show ip rpf

The **show ip rpf** command displays how IP multicast routing does Reverse Path Forwarding (RPF).

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show ip rpf <*A.B.C.D*>

Command Syntax

A.B.C.D	displays RPF information for a specified source address

MFM Command Descriptions

MFM supports multicast tools for tracing routes, maintains a multicast forwarding cache and forwards multicast traffic. To forward multicast traffic, each multicast routing protocol must register with the MFM with the APIs for inbound check and outbound check. Parameters such as cache age for the flow, and a time-to-live value for the interface being registered, is included. When MFM receives a data packet that does not have a multicast forwarding cache, the MFM will call the protocol check inbound function, and check the outbound function to the registered protocol to determine the cache.

This section contains an alphabetized list and descriptions of the MFM commands supported by the BSR.

clear ip multicast fwd-cache

The **clear ip multicast fwd-cache** command clears the IP multicast forwarding cache table.

Use the **clear ip multicast fwd-cache** command to clear the multicast forwarding table which is built from the multicast forwarding cache, and then used for forwarding traffic. Once cleared, the Multicast Forwarding Manager regenerates the cache when multicast traffic is received.

Group Access

ISP

Command Mode

All modes except User EXEC

Command Line Usage

clear ip multicast fwd-cache

clear ip multicast proto-cache

The **clear ip multicast proto-cache** command clears the IP multicast protocol cache and also clears the IP multicast forwarding cache.

Note: The MFM manager regenerates the multicast protocol cache when multicast traffic is received.

Group Access

ISP

Command Mode

All modes except User EXEC

Command Line Usage

clear ip multicast proto-cache

mtrace

The **mtrace** command traces the path from a multicast source to a multicast destination branch of a multicast distribution tree.

Group Access

ISP

Command Mode

Privileged EXEC

Command Line Usage

mtrace {<*A.B.C.D (group)*> <*A.B.C.D (hostname)*> <*A.B.C.D (hostname)*>}

Command Syntax

A.B.C.D (group)	group address or group hostname
A.B.C.D (hostname)	destination IP address or destination hostname
A.B.C.D (hostname)	source IP address or source hostname

Command Default

group address or group hostname = 224.2.0.1

show ip multicast cache-summary

The **show ip multicast cache-summary** command displays the number of multicast flows currently passing through the router.

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show ip multicast cache-summary

show ip multicast fwd-cache

The **show ip multicast fwd-cache** command displays all of the multicast forwarding cache on a source group basis.

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show ip multicast fwd-cache [<*A.B.C.D*>] [<*A.B.C.D*>] [**physical**]

Command Syntax

A.B.C.D	only displays the cache for this source or group address
A.B.C.D	only displays the cache for this specified source and group address
physical	displays the cache only in relation to the physical interface - if "physical" is not specified, it will show up with relation to the logical interface.

show ip multicast interface

The **show ip multicast interface** command is used to list the IP address, multicast protocol (PIM or IGMP), and time-to-live (TTL) information that is associated with each multicast interface.

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show ip multicast interface <*A.B.C.D*>

Command Syntax

A.B.C.D	display information only for this interface address

show ip multicast oi-fwd-cache

The **show ip multicast oi-fwd-cache** command is used to display multicast forwarding cache entries that have outgoing interfaces (OIs).

Group Access

ISP

Command Mode

All modes except User EXEC

Command Line Usage

show ip multicast oi-fwd-cache

show ip multicast no-oi-fwd-cache

The **show ip multicast no-oi-fwd-cache** command is used to display multicast forwarding cache entries, which have no outgoing interfaces (OIs).

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show ip multicast no-oi-fwd-cache

show ip multicast proto-cache

The **show ip multicast proto-cache** command is used to display multicast protocol cache entries.

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show ip multicast proto-cache [<*A.B.C.D*>] [<*A.B.C.D*>]

Command Syntax

A.B.C.D	only displays the cache for this source or group address
A.B.C.D	only displays the cache for this specified source and group address

11

CMTS Commands

Introduction

This chapter describes the commands used to configure and manage the Cable Modem Termination System (CMTS). The CMTS permits data to be transmitted and received over a broadband cable TV (CATV) network. Downstream network data traffic flows from the CMTS to connected cable modems (CMs), and upstream network data traffic flows from the CMs to the CMTS.

CMTS Command Descriptions

This section contains an alphabetized list and descriptions of the CMTS commands supported by the BSR.

arp timeout

The **arp timeout** command configures the amount of time an entry stays in the ARP cache. The **no arp timeout** command removes the time configuration an entry stays in the ARP cache.

Use the **show interfaces** command in Privileged EXEC mode to view the ARP time-out value.

Note: If the ARP time-out value is changed, the new value affects all the existing entries in the ARP cache and any entries subsequently added to the ARP cache.

Group Access

MSO

Command Mode

Interface Configuration

Command Line Usage

arp time-out <*4-6000*>

no arp timeout <*4-6000*>

Command Syntax

4-6000	amount of time, in minutes, that an entry is allowed to stay in the ARP cache

Command Default

60 minutes

band

The band command is used to define the start and end frequency band for the Spectrum Group.

Group Access

MSO

Command Mode

Cable Spectrum Group

Command Line Usage

North American DOCSIS

band <*5000000-42000000*> <*5000000-42000000*>

no band <*5000000-42000000*> <*5000000-42000000*>

Euro-DOCSIS

band <*5000000-42000000*> <*5000000-65000000*>

no band <*5000000-42000000*> <*5000000-65000000*>

Command Syntax

5000000-42000000	The start upstream frequency in Hertz for DOCSIS.
5000000-42000000	The end upstream frequency in Hertz for DOCSIS.
5000000-65000000	The start upstream frequency in Hertz for Euro-DOCSIS.
5000000-65000000	The end upstream frequency in Hertz for Euro-DOCSIS.

cable cmts type

The **cable cmts type** command specifies the DOCSIS type supported by all CMTS modules resident in the BSR chassis.

Group Access

MSO

Command Mode

Global Configuration

Command Line Usage

cable cmts type {**Domestic** | **Euro** | **Japan**}

no cable cmts type {**Domestic** | **Euro** | **Japan**}

Command Syntax

Domestic	sets the CMTS module type to the North American DOCSIS standard
Euro	sets the CMTS module type to the Euro-DOCSIS standard
Japan	sets the CMTS module types to the Japan DOCSIS (J-DOCSIS) Standard

Command Default

Domestic

cable concatenation

The **cable concatenation** command enables or disables concatenation for DOCSIS 1.0 or DOCSIS 1.1 cable modems. The **no cable concatenation** command restores the default setting.

Note: Concatenation must be enabled globally with the **cable upstream concatenation** command before any setting specified with the **cable concatenation** command is valid. Once concatenation is enabled globally, the **cable concatenation** command will enable or disable concatentation for DOCSIS 1.0 and 1.1 cable modems only and concatenation will always be enabled for DOCSIS 2.0 cable modems regardless of any setting specified with this command.

Group Access

MSO

Command Mode

Interface Configuration (cable interface only)

Command Line Usage

cable concatenation { **docsis-1.0** | **docsis-1.1** }

no cable concatenation { **docsis-1.0** | **docsis-1.1** }

Command Syntax

docsis-1.0	concatenation is enabled for DOCSIS 1.0 cable modems only
docsis-1.1	concatenation is enabled for DOCSIS 1.1 cable modems only

Command Default

Concatenation is enabled for DOCSIS 1.0, 1.1, and 2.0 cable modems if concatenation is globally enabled with the **cable upstream concatenation** command.

cable deny ip

The **cable deny ip** command allows operators to filter (drop) worm/virus packets on both the upstream and downstream cable interfaces by specifying the IP protocol used by the virus or worm and its packet length (in bytes) to enable a filter for a particular threat. The **no cable deny ip** command disables the filter.

Group Access

All

Command Mode

Interface Configuration (cable interface only)

Command Line Usage

cable deny ip *<0-255> <20-65535>*

no cable deny ip *<0-255> <20-65535>*

Command Syntax

0-255	a numeric value indicating which IP protocol number to drop
20-65535	the length in bytes indicating the size of the IP packet to drop

cable dhcp-giaddr primary

This **cable dhcp-giaddr primary** command forces the BSR to always set the giaddr in host DHCP requests to the primary cable interface IP address.

The **no cable dhcp-giaddr primary** command sets the *giaddr field* in DHCP host requests to the default. When set to the default, the first secondary address, if one is defined, is used in DHCP host requests, otherwise the primary IP address is used.

Group Access

ISP

Command Mode

Interface Configuration (cable interface only)

Command Line Usage

cable dhcp-giaddr primary

no cable dhcp-giaddr primary

Command Default

The giaddr for cable modems is the primary IP address on the cable interface.

The giaddr for Hosts is the first secondary IP address on the cable interface.

cable downstream carrier-only

The downstream carrier-only function is disabled by default and is used for testing purposes only to control downstream output. The **cable downstream carrier-only** command is used optionally as a test function to enable the modulation to the RF carrier of the downstream output. The **no cable downstream carrier-only** command disables the modulation to the RF carrier of the downstream output.

Note: If the **cable downstream carrier-only** command is used, set the rfModulation to 1.

If the **no cable downstream carrier-only** command is used, set the rfModulation to 0.

Group Access

MSO

Command Mode

Interface Configuration (cable interface only)

Command Line Usage

cable downstream [<*0-0*>] **carrier-only**

no cable downstream [<*0-0*>] **carrier-only**

Command Syntax

0-0	Downstream port number.

Command Default

Modulation to the RF carrier is disabled.

cable downstream description

The **cable downstream description** command is used to specify descriptive information for a downstream port on the BSR. This information is limited to 80 characters and single word descriptions are not allowed. Use the characters: _ or - to separate words. For example, if a downstream port served a certain section of a city, the MSO could assign the following description:

```
MOT(config-if)#cable downstream 0 description charlestown_1D
```

Note: The entered description can be seen in the running configuration, and in the command output of **show** commands such as the **show ip interface** and **show running-config** commands.

Command Mode

Interface Configuration (cable interface only)

Command Line Usage

cable downstream <*0-1*> description <*LINE*>

Command Syntax

0-1	is the downstream port number.
LINE	is the text that describes the interface.

cable downstream frequency

The **cable downstream frequency** command is used to set the fixed center downstream frequency for RF output. The **no cable downstream** command returns the fixed center downstream frequency of RF output to the default..

Note: The Japan DOCSIS Standard must be specified with the **cable cmts type** command before a downstream frequency can be selected for any Japan DOCSIS Standard CMTS module.

Note: The digital carrier frequency cannot be the same as the video carrier frequency.

Group Access

MSO

Command Mode

Interface Configuration (cable interface only)

Command Line Usage

North American DOCSIS Standard

cable downstream [*<0-0>*] **frequency** *<91000000-857000000>*

no cable downstream [*<0-0>*] **frequency** *<91000000-857000000>*

Euro-DOCSIS Standard

cable downstream [*<0-0>*] **frequency** *<112000000-858000000>*

no cable downstream [*<0-0>*] **frequency** *<112000000-858000000>*

Japan DOCSIS (J-DOCSIS) Standard

cable downstream [*<0-0>*] **frequency** *<91000000-860000000>*

no cable downstream [*<0-0>*] **frequency** *<91000000-860000000>*

Command Syntax

0-0	Downstream port number.
91000000-857000000	The downstream carrier center frequency. Valid values are from 91000000 to 857000000 Hertz (Hz) for North American DOCSIS.
112000000-858000000	The downstream carrier center frequency. Valid values are from 112000000 to 858000000 Hz for EuroDOCSIS.
91000000-860000000	The downstream carrier center frequency for the Japan DOCSIS (J-DOCSIS) Standard

Command Default

555000000 Hz

cable downstream interleave-depth

The cable operator can protect the downstream path from excess noise or decrease latency on the downstream path by setting the interleave depth. A higher interleave depth provides more protection from noise on the HFC network, but increases downstream latency. A lower interleave depth decreases downstream latency, but provides less protection from noise on the HFC network.

The **cable downstream interleave-depth** command sets the downstream port interleave depth criteria.

Note: A higher interleave depth provides more protection from bursts of noise on the HFC network; however, it increases downstream latency.

Group Access

MSO

Command Mode

Interface Configuration (cable interface only)

Command Line Usage

cable downstream [<*0-0*>] **interleave-depth** {**8** | **16** | **32** | **64** | **128**}

no cable downstream [<*0-0*>] **interleave-depth** {**8** | **16** | **32** | **64** | **128**}

Command Syntax

0-0 Downstream port number.

Review Table 11-1 to determine the appropriate interleave-depth.

Table 11-1 Interleave Depth Criteria

Depth	# of Taps	Increments
8	8	16
12	12	17
16	16	8

Table 11-1 Interleave Depth Criteria

Depth	# of Taps	Increments
32	32	4
64	64	2
128	128	1

Note: The Euro DOCSIS standard requires an interleave depth of 12.

Command Default

The command default is 8 for North American DOCSIS.

cable downstream modulation

The **cable downstream modulation** command sets the modulation rate for a downstream port. The **no cable downstream modulation** command returns the modulation rate setting to the default.

Group Access

MSO

Command Mode

Interface Configuration (cable interface only)

Command Line Usage

cable downstream [<*0-0*>] **modulation** {**256** | **64**}

no cable downstream [<*0-0*>] **modulation** {**256** | **64**}

Command Syntax

0-0	Downstream port number.
256	Modulation rate, 8 bits per downstream symbol.
64	Modulation rate, 6 bits per downstream symbol.

Command Default

64 QAM

cable downstream power-level

The **cable downstream power-level** command sets the power level of a downstream channel. The **no cable downstream power-level** changes the power level setting of a downstream channel to the default.

Use the **cable downstream power-level** command to set the absolute power level in tenths of dBmV. Use **cable downstream power-level** default setting to set the receive power based on the automatic calculation of the necessary power level.

Group Access

MSO

Command Mode

Interface Configuration (cable interface only)

Command Line Usage

cable downstream [<*0-0*>] **power-level** <*450-630*>

no cable downstream [<*0-0*>] **power-level** <*450-630*>

Command Syntax

0-0	Downstream port number.
450-630	An integer between 450 and 630; unit is in tenth-dBmV.

Command Default

550 dBmV

cable downstream pre-equalization

The **cable downstream pre-equalization** command enables pre-equalization adjustment on the downstream port that includes sending pre-equalization coefficients in a ranging response to a CM to compensate for impairment over the transmission line. The **no cable downstream pre-equalization** command disables the pre-equalization function.

Note: Not all CMs support the pre-equalization adjustment. If a CM does not support this adjustment, it may not be able to receive downstream data correctly from the BSR CMTS interface.

Group Access

MSO

Command Mode

Interface Configuration (cable interface only)

Command Line Usage

cable downstream <*NUM*> **pre-equalization <***1-3***>**

no cable downstream <*NUM*> **pre-equalization <***1-3***>**

Command Syntax

NUM	downstream port number (always 0 for the BSR 2000)
1-3	band in the range 1 through 3

cable downstream rate-limit

The **cable downstream rate-limit** command controls whether rate limiting is applied to downstream traffic on a given downstream interface. The **no cable upstream rate-limit** command disables downstream rate limiting. The token-bucket algorithm is used for rate limiting.

Note: If the rate-limit is enabled, downstream traffic is rate-limited according to the cable modems configured. Packets may be buffered at times when any cable modem or the hosts behind the cable modems transmit data exceeding the permitted bandwidth.

Group Access

MSO

Command Mode

Interface Configuration

Command Line Usage

cable downstream <*NUM*> **rate-limit**

no cable downstream <*NUM*> **rate-limit**

Command Syntax

NUM	the downstream port number

Command Default

Disabled

cable downstream schedule

The **cable downstream schedul**e command is used to configure the type of scheduling to be applied on downstream ports.

Group Access

MSO

Command Mode

Interface Configuration (cable interface only)

Command Line Usage

cable downstream schedule {**priority-only** | **priority-wfq**}

Command Syntax

priority-only	specifies the use of straight priority-based scheduling
priority-wfq	specifies the use of priority-based weighted fair queuing scheduling

cable downstream scrambler on

The **cable downstream scrambler on** command enables the scrambler for a downstream port. The **no cable downstream scrambler on** command disables the scrambler for a downstream port.

Group Access

All

Command Mode

Interface Configuration (cable interface only)

Command Line Usage

cable downstream <*NUM*> **scrambler on**

no cable downstream <*NUM*> **scrambler on**

Command Syntax

NUM	the downstream port

cable downstream shutdown

The **cable downstream shutdown** command is used to disable an enabled downstream port when certain downstream parameters require that the downstream port is disabled before these parameters are configured.

The downstream port is disabled by default. Use the **no cable downstream shutdown** command to enable the downstream port after the required downstream parameters are configured for the BSR. The downstream port is not active for data transmission until it is enabled.

Group Access

MSO

Command Mode

Interface Configuration

Command Line Usage

cable downstream [<*0-0*>] **shutdown**

no cable downstream [<*0-0*>] **shutdown**

Command Syntax

0-0	Downstream port number.

Command Default

The downstream port on the cable interface is disabled or "shut down" by default.

cable downstream threshold

The **cable downstream threshold** command specifies downstream channel upper and lower queue thresholds. This command allows an operator to configure "back pressure" parameters for various applications. For example, if the BSR is running both a time critical application (such as Voice Over IP) and best effort service, the **cable downstream threshold** command guarantees that the downstream scheduler can only release bandwidth within a certain specified range to the downstream channel. When a higher priority VOIP packet arrives, the VOIP packet will move ahead of the previously queued downstream non-VOIP data.

Group Access

All

Command Mode

Interface Configuration (cable interface only)

Command Line Usage

cable downstream <*NUM*> **threshold** {**byte** <*500-65535*> <*500-65535*> | **pdu** <*16-256*> <*16-256*>}

no cable downstream <*NUM*> **threshold** {**byte** <*500-65535*> <*500-65535*> | **pdu** <*16-256*> <*16-256*>}

Command Syntax

NUM	the downstream channel number
byte	use the byte count as a threshold unit
500-65535	specify the upper byte threshold
500-65535	specify the lower byte threshold
pdu	use the PDU count as a threshold unit
16-256	specify the upper PDU threshold
16-256	specify the lower PDU threshold

Command Defaults

upper byte threshold = 1000 bytes

lower byte threshold = 500 bytes

upper pdu threshold = 32 PDUs

lower pdu threshold = 16 PDUs

cable downstream trap-enable-if

The **cable downstream trap-enable-if** command enables the *ifLinkUpDownTrapEnable* trap for a downstream channel. The *ifLinkUpDownTrapEnable* trap indicates whether a link up or link down trap should be generated. The **cable downstream no trap-enable-if** command disables the *ifLinkUpDownTrapEnable* trap.

Group Access

All

Command Mode

Interface Configuration (cable interface only)

Command Line Usage

cable downstream <*0-0*> **trap-enable-if**

no cable downstream <*0-0*> **trap-enable-if**

Command Syntax

0-0	Downstream port number.

Command Default

Disabled

cable downstream trap-enable-rdn

The **cable downstream trap-enable-rdn** command enables the *rdnCardIfLinkUpDownEnable* trap for a downstream channel. The *rdnCardIfLinkUpDownEnable* trap indicates whether a link up or link down trap should be generated. The **no cable downstream trap-enable-rdn** command disables the *rdnCardIfLinkUpDownEnable* trap.

Group Access

All

Command Mode

Interface Configuration (cable interface only)

Command Line Usage

cable downstream <*0-0*> **trap-enable-rdn**

no cable downstream <*0-0*> **trap-enable-rdn**

Command Syntax

0-0	Downstream port number.

Command Default

Disabled

cable flap-list aging

The **cable flap-list aging** command specifies the cable flap-list aging in terms of maximum number of minutes a cable modem is kept in the flap-list. Use the **no cable flap-list aging** command to disable cable flap-list aging.

Use this command to keep track of cable modem mac address upstream and downstream traffic for every cable modem having communication problems. Problems can be detected when the cable is inactive. This command will show cable modem registration events, missed ranging packets, upstream power adjustments, and the CMTS physical interface. Monitoring the flap list can not affect cable modem communications.

The user can get the following information with the **cable flap-list aging** *number of days* command:

Upstream performance data.

Quality control installation data.

Cable modem problem isolation and location.

CMTS problems based upon high activity.

Unreliable upstream paths based on high CRC errors.

Unreliable in-home wiring problems based on high CRC errors.

Group Access

MSO

Command Mode

Global Configuration and Interface Configuration (cable interface only)

Command Line Usage

cable flap-list aging <*1-86400*>

no cable flap-list aging <*1-86400*>

Command Syntax

1-86400	maximum number of minutes a cable modem is kept in the flap-list

Command Default

1440 minutes

cable flap-list insertion-time

The **cable flap-list insertion-time command** sets the insertion time interval in seconds. Use the **no** form of this command to disable insertion time.

Use the **cable flap-list insertion-time** command to manage the flapping modem detector and place the cable modem on the flap list if the connection time is outside the insertion time interval.

Note: The insertion-time is the time taken by cable modems to complete their registration.

Group Access

MSO

Command Mode

Global Configuration and Interface Configuration (cable interface only)

Command Line Usage

cable flap-list insertion-time <*1-86400*>

no cable flap-list insertion-time <*1-86400*>

Command Syntax

1-86400	insertion time interval in seconds

Command Default

60 seconds

cable flap-list miss-threshold

The **cable flap-list miss-threshold** command specifies the threshold for missing consecutive polling messages which triggers the polling flap detector. The **no cable flap-list miss-threshold** removes the specified threshold.

Group Access

MSO

Command Mode

Global Configuration and Interface Configuration (cable interface only)

Command Line Usage

cable flap-list miss-threshold <*1-12*>

no cable flap-list miss-threshold <*1-12*>

Command Syntax

1-12	missing consecutive polling messages

Command Default

6

cable flap-list percentage-threshold

The **cable flap-list percentage-threshold** command specifies the CM miss percentage threshold. The **no cable flap-list percentage-threshold** command restores the default threshold value.

If CM miss percentage exceeds the *flapListPercentageThreshold* and the *flapListTrap* is enabled with the **cable flap-list trap-enable** command, a *flapListTrap* will be sent to the CMTS by the SNMP agent.

Group Access

MSO

Command Mode

Global Configuration

Command Line Usage

cable flap-list percentage-threshold <*1-100*>

no cable flap-list percentage-threshold

Command Syntax

1-100	the CM miss threshold percentage

Command Default

10 percent

cable flap-list power-adjust threshold

The **cable flap-list power-adjust threshold** specifies the flap-list power adjustment parameters in dBmV for recording a flap-list event. The **no cable flap-list power-adjust threshold** command disables power-adjust thresholds.

Use the **cable flap-list power-adjust threshold** to manage the flapping modem detector and place the cable modem on the flap-list if the connection exceeds the parameters.

Group Access

MSO

Command Mode

Global Configuration and Interface Configuration (cable interface only)

Command Line Usage

cable flap-list power-adjust threshold <*1-10*>

no cable flap-list power-adjust threshold <*1-10*>

Command Syntax

1-10	threshold in dBmV

Command Default

2 dBmV

cable flap-list size

The **cable flap-list size** command specifies the flap-list size, the maximum number of cable modems in the flap-list. The **no cable flap-list size** command sets the default flap-list table size.

Use the **cable flap-list size** number command to set the number of modems that the cable flap-list table can record.

Group Access

MSO

Command Mode

Global Configuration and Interface Configuration (cable interface only)

Command Line Usage

cable flap-list size <*1-8191***>**

no cable flap-list size <*1-8191*>

Command Syntax

1-8191	number of cable modems that can register to the flap-list table

Command Default

256 cable modems

cable flap-list trap-enable

The **cable flap-list trap-enable** command controls whether a *flapListTrap* will be sent to the CMTS by the SNMP agent if the CM miss percentage exceeds the *flapListPercentageThreshold* specified with the **cable flap-list percentage-threshold** command. The **no cable flap-list percentage-threshold** command disables sending the *flapListTrap*.

Group Access

MSO

Command Mode

Global Configuration

Command Line Usage

cable flap-list trap-enable

no cable flap-list trap-enable

Command Default

Enabled

cable helper-address

The cable helper address function disassembles a DHCP broadcast packet, and reassembles it into a unicast packet so that the packet can traverse the router and communicate with the DHCP server. The **cable helper-address** command enables broadcast forwarding for User Datagram Protocol (UDP) packets.

The **cable helper-address** command can also be used to define the cable helper address to be used for all CPEs whose CMs have an IP address in a particular subnet's address space. This forces the BSR relay agent to forward DHCP requests from a CPE using a selected ISP to a DHCP server configured for that selected ISP.

Note: The **isp-bind** option is only available after selecting the **host** or **mta** options. It is not available for the **cable modem** option.

Note: The **cable helper-address** command allows operators to support *multiple* CM subnets bound to a *single* cable helper-address. Any DHCP requests from clients that are attached to CMs that are part of the Multiple ISP configuration will have their requests relayed to any defined ip helper-addresses.

Group Access

ISP

Command Mode

Interface Configuration (cable and loopback interfaces only)

Command Line Usage

cable helper-address <*A.B.C.D*> {**cable-modem** | **host** [**isp-bind** <*A.B.C.D*>] | **mta** [**isp-bind** <*A.B.C.D*>]}

no cable helper-address <*A.B.C.D*> {**cable-modem** | **host** [**isp-bind** <*A.B.C.D*>] | **mta** [**isp-bind** <*A.B.C.D*>]}

Command Syntax

A.B.C.D	the IP address of the destination DHCP server.
cable-modem	specifies that only CM UDP broadcasts are forwarded.
host	specifies that only CPE UDP broadcasts are forwarded.
mta	specifies that only CPE MTA broadcasts are forwarded.
isp-bind *A.B.C.D*	specifies the secondary IP subnet to which the cable-helper is bound.

cable host authorization range

The **cable host authorization range** command configures an authorization IP address range for Customer Premise's Equipment (CPE) access to the BSR. The **no cable host authorization range** command disables IP address range authorization.

Group Access

MSO

Command Mode

Global Configuration

Command Line Usage

cable host authorization range <*prefix*> <*prefix*>

no cable host authorization range <*prefix*> <*prefix*>

Command Syntax

prefix	starting CPE IP address range
prefix	ending CPE IP address range

cable insert-interval

The **cable insert-interval** command sets the interval at which Initial Maintenance intervals are scheduled in the upstream.These intervals are used by cable modems to send ranging request messages when attempting to join the network. The **no cable insert-interval** command is used to set the default insertion interval.

Note: Ensure that the upstream port is down before setting the insertion interval.

Group Access

MSO

Command Mode

Interface Configuration (cable interface only)

Command Line Usage

cable insert-interval <*0-200*>

no cable insert-interval <*0-200*>

Command Syntax

0-200	The insert interval in hundredths of a second.

Command Default

The default insertion interval is 20 hundredths of a second.

cable intercept

The BSR provides a way to monitor and intercept data originating from a DOCSIS network through the Cable Intercept feature, which provides Multiple System Operators (MSOs) with Lawful Intercept capabilities required by the Communications Assistance for Law Enforcement Act (CALEA) for electronic surveillance. Lawful Intercept capabilities are used by law enforcement agencies to conduct electronic surveillance of circuit and data communications.

Warning: Lawful Intercept capabilities to intercept customer traffic are authorized by either a judicial means to support local laws or through an administrative order governed by service level agreements (SLAs). The proper legal or administrative persons must be contacted first before customer traffic is intercepted and examined.

When the Cable Intercept feature is initiated, copies of the data transmissions from and to a specified Customer Premises Equipment (CPE) MAC address (such as a PC) are sent to an intercept collector, which is a server at a specified IP address and UDP port number.

The BSR 2000 supports a maximum of 16 cable intercept entries in the startup configuration and running configuration files. Only one MAC address per CPE device, such as a PC can be intercepted and only packets from these CPEs are intercepted.

Use the **cable intercept** command to create a cable intercept on the CMTS interface to respond to CALEA requests from law enforcement for traffic regarding a specific user. Use the **no cable intercept** command to delete a cable intercept on the CMTS interface.

Group Access

MSO

Command Mode

Interface Configuration

Command Line Usage

cable intercept <*mac*> <*prefix*> <*0-65535*>

no cable intercept <*mac*> <*prefix*> <*0-65535*>

Command Syntax

mac	The intercept source, which is the MAC address from which traffic is intercepted. Packets with a source or destination MAC address that matches this address are copied and forwarded to the data collection server. Most often, this MAC address is the user's CPE device (such as a PC or VoIP phone), and not the MAC address of the user's CM.
prefix	Specifies the destination IP address for the data collection server that receives copies of the forwarded traffic.
0-65535	The destination User Datagram Port (UDP) port number, which is used exclusively by the data collection server. A default UDP port number is not provided.

Command Default

None

cable modem-aging-timer

The **cable modem-aging-timer** command specifies a cable modem aging timer in minutes. Cable modems that go off-line are automatically removed from the network after the configured time period.

Group Access

MSO

Command Mode

Global Configuration

Command Line Usage

cable modem-aging-timer {*<10-30240>* | **off**}

Command Syntax

10-30240	the cable modem aging timer number in minutes (10 minutes to 21 days)
off	disables the cable modem aging timer

Command Default

Disabled

cable modem dcc

The **cable modem dcc** command allows an operator to manually move DOCSIS 1.1 and 2.0 cable modems ot MTAs to a specified upstream and/or downstream port and logical channel using DOCSIS Dynamic Channel Change (DCC).

Note: The upstream channel must be physically connected for DOCSIS 1.1 and 2.0 cable modems to be manually moved.

When moving a CM or MTA to a different downstream or upstream channel , the upstream channel must be specified first followed by the downstream channel.

The same **init-tech** must be specified for both the upstream and downstream channels.

Group Access

MSO

Command Mode

Privileged EXEC

Command Line Usage

cable modem {<*mac*> | <*prefix*>} **dcc** [**upstream** <*0-7*>/<*0-3*> [**init-tech** <*0-4*>]]

Command Syntax

mac	the cable modem MAC address in the form of xxxx.xxxx.xxxx
prefix	the cable modem IP address

upstream *0-7/0-3*	the upstream port/logical channel
init-tech *0-4*	the ranging technique used for DCC: *0* = re-initialize the MAC *1* = perform broadcast intitial ranging on the new channel before normal operation *2* = perform unicast ranging on the new channel before normal operation *3* = perform either broadcast or unicast ranging on the new channel before normal operation *4* = use the new channel directly without re-intializing or ranging

cable modem qos dsa

The **cable modem qos dsa** command triggers a dynamic service change (DSC) initiated by the CMTS for a specified cable modem. The DSC is in a binary file that conforms to the DOCSIS cable modem configuration file format. This configuration file is saved in the TFTP "boot" directory on a TFTP server with a known IP address. The current implementation has only the change of service based on service-flow (not the flow classifier, nor the payload-header-suppression).

Note: The definition of the dynamic service is defined in a binary file that conforms to the DOCSIS 1.1 cable modem's configuration file format. This configuration file is saved in the TFTP "boot" directory on a TFTP server with known IP address.

Warning: This command should be used with extreme caution as the dynamic service definition in the configuration file will be overwritten.

Group Access

MSO

Command Mode

Privileged EXEC

Command Line Usage

cable modem {<*mac*> | <*prefix*>} **qos dsa** <*prefix*> <*string*>

Command Syntax

mac	The CM Dynamic Service Addition MAC address of the specified cable modem.
prefix	Specified cable modem IP address to create or delete a SID.
prefix	IP address of TFTP server.
string	File name to be configured.

Command Default

none

cable modem qos dsc

The **cable modem qos dsc** command triggers a Dynamic Service Change (DSC) initiated by the CMTS for a specified cable modem (CM).The **cable modem qos dsc** command triggers a dynamic service change (DSC) initiated by the CMTS for a specified cable modem. The definition of the dynamic service is defined in a binary file that conforms to the DOCSIS cable modem's configuration file format. This configuration file is saved in /tftpboot directory on a TFTP server with known IP address. The current implementation only the change of service based on service-flow (not the flow classifier, nor the payload-header-suppression).

The definition of the dynamic service is defined in a binary file that conforms to the DOCSIS cable modem configuration file format. This configuration file is saved in the /tftpboot directory on a TFTP server with a known IP address. The current implementation only is the change of service based on service-flow (not the flow classifier, nor the payload-header-suppression).

Group Access

MSO

Command Mode

Privileged EXEC

Command Line Usage

cable modem {<*mac*> | <*prefix*>} **qos dsc** <*prefix*> <*string*>

Command Syntax

mac	The CM Dynamic Service Addition MAC address of the specified cable modem.
prefix	Specified cable modem IP address to create or delete a SID.
prefix	IP address of TFTP server.
string	File name to be configured.

cable modem qos dsd

The **cable modem qos dsd** command triggers a dynamic service deletion (DSD) initiated by the CMTS for a specified service flow.

Note: The **cable modem qos dsd** command should be used with extreme caution as the correct service-flow identifier must be specified.

Group Access

MSO

Command Mode

Privileged EXEC

Command Line Usage

cable modem qos dsd <*X/Y*> <*1-262143*>

Command Syntax

X/Y	*X* is 0. *Y* is the CMTS port number.
1-262143	Service Flow Identifier (not all values are valid at all times in a running system)

Command Default

none

cable modem max-hosts

The **cable modem max-hosts** command sets the limit for the maximum Customer Premises Equipment (CPE) hosts behind a particular cable modem. The **no cable modem max-hosts** sets the limit to the default value.

Group Access

MSO

Command Mode

Privileged EXEC

Command Line Usage

cable modem {<*mac*> | <*prefix*>} **max-hosts** <*0-32*>

no cable modem {<*mac*> | <*prefix*>} **max-hosts** <*0-32*>

Command Syntax

mac	Cable modem MAC address.
prefix	Cable modem IP address.
0-32	Number of CPE hosts.

cable modem max-hosts-all

The **cable modem max-hosts-all** command sets the limit for the maximum Customer Premises Equipment (CPE) hosts behind all cable modems on the network. The **no cable modem max-hosts-all** sets the limit to the default value.

Group Access

MSO

Command Mode

Global Configuration

Command Line Usage

cable modem max-hosts-all <*0-32*>

no cable modem max-hosts-all <*0-32*>

Command Syntax

0-32	Number of CPE hosts.

cable modem ucc

The **cable modem ucc** command allows an operator to manually move a DOCSIS 1.0 or 1.1 CM or MTA to a different upstream channel within the same MAC domain.

Note: The cable modem will not be moved if the old and new upstream channels are associated to two different Spectrum Groups.

Group Access

MSO

Command Mode

Privileged EXEC

Command Line Usage

cable modem {<*mac*> | <*prefix*>} **ucc** <*0-3*> [**init-tech** <*0-4*> | **logical** <*0-3*>]

Command Syntax

mac	cable modem MAC address in the form of xxxx.xxxx.xxxx
prefix	cable modem IP address
0-3	the upstream physical channel

init-tech *0-4*	the ranging technique used for UCC: *0* = re-initialize the MAC *1* = perform broadcast intitial ranging on the new channel before normal operation *2* = perform unicast ranging on the new channel before normal operation *3* = perform either broadcast or unicast ranging on the new channel before normal operation *4* = use the new channel directly without re-intializing or ranging
logical *0-3*	the upstream logical channel

cable modem updis

The **cable modem updis** command enables the transmission of an an Upstream Transmitter Disable (UP-DIS) MAC layer message that disables a specified cable modem's upstream transmitter. Upon receipt of an UP-DIS message, the cable modem autonomously disables its upstream transmitter. Once disabled through an UP-DIS message, the cable modem's upstream transmitter can only be re-enabled by power cycling the cable modem.

The **cable modem updis** command is not intended to be a replacement for existing mechanisms for controlling a subscriber's service. The **cable modem updis** command provides an additional tool to protect against some forms of denial of service, such as a virus propagated across the Internet, that cannot be controlled with existing management mechanisms.

Group Access

MSO

Command Mode

Privileged EXEC

Command Line Usage

cable modem updis <*mac*>

Command Syntax

mac	the cable modem MAC address in the form of *xxxx.xxxx.xxxx*

cable modulation-profile

The **cable modulation-profile** command navigates to Modulation Profile Configuration Mode. Modulation Profile Configuration Mode provides a series of modulation profile commands that allow an MSO to create or modify a modulation profile.

Warning: Motorola does not recommend modification of modulation profile parameters without a thorough understanding of modulation changes and DOCSIS interface specifications. Modulation profile parameters will affect the physical layer and may cause disruption or degradation of services.

Note: Modulation profiles 1-4, 101-116, 201-205, and 301-310 are pre-configured modulation profiles. To view the configuration of these profiles, use the **show cable modulation-profile** command.

Motorola recommends that user-created modulation profiles use the numbering range of 401-600 to ensure better future portability.

For a complete list and configuration of all 23 pre-defined modulation profiles, refer to *Appendix A, Pre-Defined Modulation Profiles* in the *BSR 64000 Configuration and Management Guide.*

For guidelines on modifying modulation profile parameters, refer to *Appendix B, Understanding and Modifying Modulation Profiles* in the *BSR 64000 Configuration and Management Guide.*

Group Access

MSO

Command Mode

Global Configuration

Command Line Usage

cable modulation-profile {*<1-600>*} [**a-long** | **a-short** | **a-ugs**]

cable modulation-profile {*<1-600>*} [**initial** | **long** | **request** | **short** | **station**] [*<0-10>*] *<16-253> <0-255>* {**16qam** | **qpsk**} {**scrambler** | **no-scrambler**} *<0x0000 - 0x7fff>* {**diff** | **no-diff**} *<64-256>* {**fixed** | **shortened**}

no cable modulation-profile {*<1-600>*} [**a-long** | **a-short** | **a-ugs**]

no cable modulation-profile {*<1-600>*} [**initial** | **long** | **request** | **short** | **station**] [*<0-10>*] *<16-253> <0-255>* {**16qam** | **qpsk**} {**scrambler** | **no-scrambler**} *<0x0000 - 0x7fff>* {**diff** | **no-diff**} *<64-256>* {**fixed** | **shortened**}

Command Syntax

1-600	specify a modulation profile number and enter Modulation Profile Configuration Mode for that modulation profile - the default IUC submode is **request**
a-long	enter the Modulation Profile Configuration Mode **a-long** IUC submode for the specified cable modulation profile number for configuring the advanced PHY long data grant
a-short	enter the Modulation Profile Configuration Mode **a-short** IUC submode for the specified cable modulation profile number for configuring the advanced PHY short data grant
a-ugs	enter the Modulation Profile Configuration Mode **a-ugs** IUC submode for the specified cable modulation profile number for configuring the Unsolicited Grant Service
initial	enter the Modulation Profile Configuration Mode **initial** IUC submode for the specified cable modulation profile number for configuring the Initial Ranging Burst
long	enter the Modulation Profile Configuration Mode **long** IUC submode for the specified cable modulation profile number for configuring the Long Grant Burst

request	enter the Modulation Profile Configuration Mode **request** IUC submode for the specified cable modulation profile number for configuring the Request Burst
short	enter the Modulation Profile Configuration Mode **short** IUC submode for the specified cable modulation profile number for configuring the Short Grant Burst
station	enter the Modulation Profile Configuration Mode **station** IUC submode for the specified cable modulation profile number for configuring the Station Ranging Burst
0-10	the FEC correction value - 0 indicates no Forward Error Correction
16-253	the FEC codeword length in kilobytes
0-255	the maximum burst length in minislots - "0" means no limit
16qam | **qpsk**	the modulation type
scrambler | **no-scrambler**	enable or disable scrambler
0x0000 - 0x7fff	the scrambler seed in hexadecimal format.
diff | **no-diff**	enable or disable differential encoding
64-256	the preamble length in bits
fixed | **shortened**	the handling of FEC for last codeword length

cable modulation-profile copy

The **cable modulation-profile copy** command copies an existing modulation profile from a source modulation profile number to a destination modulation profile number. The destination modulation profile is overwritten by the source modulation profile.

Group Access

MSO

Command Mode

Global Configuration

Command Line Usage

cable modulation-profile copy {*<1-600>*} {*<1-600>*}

no cable modulation-profile copy {*<1-600>*} {*<1-600>*}

Command Syntax

1-600	source modulation profile number
1-600	destination modulation profile number

cable modulation-profile reset

The **cable modulation-profile reset** command resets a modified, pre-defined modulation profile back to the system default.

Group Access

MSO

Command Mode

Global Configuration

Command Line Usage

cable modulation-profile reset {*<1-4>* | *<101-116>* | *<201-205>* | *<301-310>*}

Command Syntax

1-4, *101-116*, *201-205*, *301-310*	the pre-defined modulation profile number

cable multi-ds-override

The **cable multi-ds-override** commands enables downstream frequency override during ranging. Downstream frequency override allows an MSO to instruct a cable modem to move to a specific downstream/upstream pair during ranging by sending an RNG-RSP message with a downstream frequency override that tells a specific cable modem to move to a specific downstream channel. The **no cable multi-ds-override** command disables downstream frequency override during ranging.

Group Access

All

Command Mode

Global Configuration

Command Line Usage

cable multi-ds-override

no cable multi-ds-override

Command Default

Disabled

cable privacy auth life-time

The **cable privacy auth life-time** command sets the authorization key (AK) life-time values for baseline privacy. The **no cable privacy auth life-time** command changes the AK life-time values for baseline privacy back to the default.

Group Access

MSO

Command Mode

Interface Configuration (cable interface only)

Command Line Usage

cable privacy auth life-time <*300-6048000*>

no cable privacy auth life-time <*300-6048000*>

Command Syntax

300-6048000	Length of the key encryption life-time, valid values 300 seconds (5 minutes) to 6048000 seconds (70 days).

Command Default

604800 seconds (7 days)

cable privacy cert

The **cable privacy cert** command allows cable modems to register using self-signed manufacturer certificates, as opposed to a manufacturer certificate that is chained to the DOCSIS root certificate. The **no cable privacy cert** command disables this feature.

Group Access

MSO

Command Mode

Interface Configuration (cable interface only)

Command Line Usage

cable privacy cert {**trust** [**trusted** | **untrusted**] | **valid** [**false** | **true**]}

no cable privacy cert {**trust** [**trusted** | **untrusted**] | **valid** [**false** | **true**]}

Command Syntax

trust [**trusted** | **untrusted**]	set trust for all self-signed manufacturer certificates - default is **untrusted**
valid	enable/disable the checking for a certificate's validity period
false	disable certificate validity checking
true	enable certificate validity checking (default)

Command Default

trust is set to "untrusted"

certificate validity checking is enabled

cable privacy cm-auth life-time

The **cable privacy cm-auth life-time** command sets AK life-time values for a cable modem. The **no cable privacy cm-auth life-time** changes the setting of AK life-time values for a cable modem back to the default.

Group Access

MSO

Command Mode

Interface Configuration (cable interface only)

Command Line Usage

cable privacy cm-auth life-time <*mac*> [<*300-6048000*>]

no cable privacy cm-auth life-time <*mac*>

Command Syntax

mac	cable modem physical address (MAC) in the form xxxx.xxxx.xxxx
300-6048000	length of key encryption life-time in seconds

Command Default

604800 seconds (7 days)

cable privacy cm-auth reset

The **cable privacy cm-auth reset** command resets a Traffic Encryption Key (TEK) before expiration on a grace-time or a life-time value. The **no cable privacy cm-auth reset** command changes the TEK expiration back to the default.

Group Access

MSO

Command Mode

Interface Configuration (cable interface only)

Command Line Usage

cable privacy cm-auth reset <*mac*> <*1-4*>

no cable privacy cm-auth reset

Command Syntax

mac	cable modem MAC address of 6 bytes
1-4	number representing an action: **1** noReset requested - causes CMTS to do nothing **2** invalidateAuth - causes CMTS to invalidate current CM authorization key, does not transmit an Authorization Invalid message to the CM, does not invalidate unicast TEKs **3** sendAuthInvalid - causes CMTS to invalidate current CM authorization key, does not transmit an Authorization invalid message to CM, does not invalidate unicast TEKs **4** invalidateTeks - causes CMTS to invalidate current CM authorization key, to transmit an Authorization Invalid message to the CM, and to invalidate all unicast TEKs related to this CM authorization

Command Default

profile 1

cable privacy cm-tek life-time

The **cable privacy cm-tek life-time** command sets the TEK life-time value for baseline privacy. The **no cable privacy cm-tek life-time** command returns the TEK life-time value to the default value.

Group Access

MSO

Command Mode

Interface Configuration

Command Line Usage

cable privacy cm-tek life-time *<0-16383> <1800-604800>*

no cable privacy cm-tek life-time *<0-16383> <1800-604800>*

Command Syntax

0-16383	CM primary SID.
1800-604800	Traffic encryption life-time value in seconds.

Command Default

43200 seconds

cable privacy cm-tek reset

The **cable privacy cm-tek reset** command resets a CM Traffic Encryption Key (TEK).

Group Access

MSO

Command Mode

Interface Configuration (cable interface only)

Command Line Usage

cable privacy cm-tek reset [<*1-16383*>]

Command Syntax

1-16383	the primary Service Identifier (SID) of the cable modem

cable privacy mcast access

The **cable privacy mcast access** command configures a multicast access list by specifying a cable modem MAC address and the corresponding multicast IP address.

Note: A cable modem MAC address and the corresponding multicast IP address is required.

Group Access

MSO

Command Mode

Interface Configuration (cable interface only)

Command Line Usage

cable privacy mcast access <*H.H.H*> <*A.B.C.D*>

Command Syntax

H.H.H	cable modem physical address (MAC) in the form xxxx.xxxx.xxxx
A.B.C.D	multicast IP address.

cable privacy tek life-time

The **cable privacy tek life-time** command sets the cable privacy Traffic Encryption Key (TEK) life-time value. The **no cable privacy tek life-time** command returns the cable privacy TEK life-time value to the default value.

Note: Baseline privacy is configured with key encryption keys (KEKs), and the TEKs are configured based on the 40 or 56-bit data encryption standard (DES).

A life-time or a grace-time TEK value expires based on a life-time or grace-time value, but a cable modem has to renew its TEK grace-time value before it expires. If a lasting TEK lifetime is needed, use a life-time key.

Group Access

MSO

Command Mode

Interface Configuration (cable interface only)

Command Line Usage

cable privacy tek life-time <*30-604800*>

no cable privacy tek life-time

Command Syntax

30-604800	minimum and maximum traffic encryption life-time value in seconds

Command Default

43200 seconds

cable qos-profile

The **cable qos-profile** command accesses QoS Profile Configuration mode. QoS Profile Configuration mode allows you to create or modify a QoS Profile. The **no cable qos-profile** command deletes a QoS Profile.

Group Access

MSO

Command Mode

Global Configuration and QoS Profile Configuration

Command Line Usage

cable qos-profile <*prof-num*>

no cable qos-profile <*prof-num*>

Command Syntax

prof-num	the QoS Profile identifying number

Note: Only QoS Profile numbers 1-16 can be configured by the user.

cable shared-secret

The **cable shared-secret** command activates or deactivates cable modem authentication with a shared-secret key. The **no cable shared-secret** command sets the cable shared-secret back to the default.

Use the **cable shared-secret** command to authenticate the cable modem such that all cable modems must return a text string to register for access to the network.

If the **no cable shared-secret** command is enabled on the CMTS, secret key checking is not available on any cable modem. If shared-secret is configured on CMTS, cable modems have to use the secret key obtained from the CM configuration files obtained from the TFTP server.

Group Access

MSO

Command Mode

Global Configuration

Command Line Usage

cable shared-secret {**0** <*string*> | **7** <*hex-dump-string*> | <*string*>}

no cable shared-secret {**0** <*string*> | **7** <*hex-dump-string*> | <*string*>}

Command Syntax

0	Specifies an UNENCRYPTED key will follow
7	Specifies an ENCRYPTED key will follow
hex-dump-string	The authentication key in hex number format.
string	The authentication key (enclosed with double quotes if the key contains spaces). The "%" and "!" characters must not be used.

Command Default

null string

cable shared-secondary-secret

The **cable shared-secondary-secret** command activates or deactivates cable modem authentication with a shared-secondary-secret key. The **no cable shared-secondary-secret** command sets the cable shared-secondary-secret back to the default.

Use the **cable shared-secondary-secret** command to authenticate the cable modem such that all cable modems must return a text string to register for access to the network.

If the **no cable shared-secondary-secret** command is enabled on the CMTS, secret key checking is not available on any cable modem. If shared-secondary-secret is configured on CMTS, cable modems have to use the secret key obtained from the CM configuration files obtained from the TFTP server.

Group Access

MSO

Command Mode

Global Configuration

Command Line Usage

cable shared-secondary-secret {**0** <*string*> | **7** <*hex-dump-string*> | <*string*>}

no cable shared-secondary-secret {**0** <*string*> | **7** <*hex-dump-string*> | <*string*>}

Command Syntax

0	Specifies an UNENCRYPTED key will follow
7	Specifies an ENCRYPTED key will follow
hex-dump-string	The authentication key in hex number format.
string	The authentication key (enclosed with double quotes if the key contains spaces). The "%" and "!" characters must not be used.

Command Default

null string

cable spectrum-group

The **cable spectrum-group** command is used to create a cable spectrum group and enter Cable Spectrum Group mode in which to configure a cable spectrum group. All of the cable spectrum parameters are configured from Cable Spectrum Group mode.

Group Access

MSO

Command Mode

Global Configuration

Command Line Usage

cable spectrum-group <*WORD*>

no cable spectrum-group <*WORD*>

Command Syntax

WORD	The cable spectrum group name.

cable sync-interval

The synchronization message interval is the interval between successive synchronization message transmissions from the BSR CMTS interface to the CMs. The **cable sync-interval** command sets the synchronization interval between transmission of successive SYNC messages from the CMTS to CMs. The **no cable sync-interval** returns the interval setting to transmit SYNC messages to the default.

Note: Ensure that you disable the cable interface using the **cable shutdown** command before using the **cable sync-interval** command.

Group Access

MSO

Command Mode

Interface Configuration (cable interface only)

Command Line Usage

cable sync-interval <*0-200*>

no cable sync-interval

Command Syntax

0-200	synchronization interval in milliseconds.

cable ucd-interval

The **cable ucd-interval** command sets the interval between transmission of successive Upstream Channel Descriptor (UCD) messages. The **no cable ucd-interval** changes the interval setting to transmit UCD messages back to the default.

Note: Ensure that you disable the cable interface using the **cable shutdown** command before using the **cable ucd-interval** command.

Group Access

MSO

Command Mode

Interface Configuration (cable interface only)

Command Line Usage

cable ucd-interval <*0-2000*>

no cable ucd-interval

Command Syntax

0-2000	UCD interval in *milliseconds*

Command Default

1000

cable upstream active-codes

The **cable upstream active-codes** command specifies the number of active codes allowed for an S-CDMA channel type. The active codes value must be a non prime number. Increasing the number of allowed active codes provides more transmission channel capacity. Reducing the number of active codes takes advantage of the S-CDMA spreader processing gain at the expense of channel capacity.

Group Access

MSO

Command Mode

Interface Configuration (cable interface only)

Command Line Usage

cable upstream <*X*/*Y*> **active-codes** <*64-128*>

no cable upstream <*X*/*Y*> **active-codes** <*64-128*>

Command Syntax

X/*Y*	the upstream port and logical channel number (0-3)
64-128	the total number of allowed active codes

cable upstream channel-type

The **cable upstream channel-type** command allows you to specify the channel type for the default upstream channel (0) or specify the channel type for up to four logical channels (0-3).

Group Access

MSO

Command Mode

Interface Configuration (cable interface only)

Command Line Usage

cable upstream {<*NUM*> | <*X*/*Y*>} **channel-type** {**tdma** | **atdma** | **mtdma** | **scdma**}

no cable upstream {<*NUM*> | <*X*/*Y*>} **channel-type** {**tdma** | **atdma** | **mtdma** | **scdma**}

Command Syntax

NUM	the upstream port (default channel number = 0)
X/*Y*	the upstream port number and logical channel number (0-3)
tdma	DOCSIS 1.0 or 1.1 channel type
atdma	DOCSIS 2.0 channel type
mtdma	DOCSIS 1.0, 1.1, 2.0 TDMA channel type
scdma	DOCSIS 2.0 channel type only used for logical channel configurations

cable upstream channel-width

The **cable upstream channel-width** command specifies an upstream channel width for an upstream port. The **no cable upstream channel-width** command returns the default value.

Group Access

MSO

Command Mode

Interface Configuration (cable interface only)

Command Line Usage

cable upstream <*NUM*> **channel-width** [**1600000** | **200000** | **3200000** | **400000** | **800000**]

no cable upstream <*NUM*> **channel-width** [**1600000** | **200000** | **3200000** | **400000** | **800000**]

Command Syntax

NUM	Upstream port number - *0,1,2,3*
1600000	1600000 - channel width 1600 kHz
200000	200000 - channel width 200 kHz
3200000	3200000 - channel width 3200 kHz
400000	400000 - channel width 400 kHz
800000	800000 - channel width 800 kHz

cable upstream codes-minislot

The **cable upstream codes-minislot** command specifies the number of active codes allowed for each minislot on an S-CDMA channel. The number active codes allowed for each minislot determines the minislot capacity and sets the granularity of the upstream grants.

Group Access

MSO

Command Mode

Interface Configuration (cable interface only)

Command Line Usage

cable upstream <*X*/*Y*> **codes-minislot** <*2-32*>

no cable upstream <*X*/*Y*> **codes-minislot** <*2-32*>

Command Syntax

X/*Y*	the upstream port and logical channel number (0-3)
2-32	the number of codes allowed per minislot

cable upstream concatenation

The **cable upstream concatenation** command enables CMTS concatenation capabilities. The **no cable upstream concatenation** command disables CMTS concatenation capabilities.

Note: Concatenation must be enabled globally with the **cable upstream concatenation** command before any setting specified with the **cable concatenation** command is valid. Once concatenation is enabled globally, the **cable concatenation** command will enable or disable concatentation for DOCSIS 1.0 and 1.1 cable modems only and concatenation will always be enabled for DOCSIS 2.0 cable modems regardless of any setting specified with this command.

Group Access

MSO

Command Mode

Interface Configuration (cable interface only)

Command Line Usage

cable upstream <*NUM*> **concatenation**

no cable upstream <*NUM*> **concatenation**

Command Syntax

NUM	the upstream port number

Command Default

Enabled

cable upstream data-backoff

Use the **cable upstream data-backoff** command sets data back-off value to assign automatic or fixed start and stop values. The **no cable upstream data-backoff** command returns to the default data back-off value.

Note: The automatic setting is recommended.

Group Access

MSO

Command Mode

Interface Configuration (cable interface only)

Command Line Usage

cable upstream <*NUM*> **data-backoff** {<*0-15*> <*0-15*> | **automatic**}

no cable upstream <*NUM*> **data-backoff** {<*0-15*> <*0-15*> | **automatic**}

Command Syntax

NUM	Upstream port number
0-15	Start of data backoff
0-15	End of data backoff
automatic	Automatic data-backoff.

cable upstream description

The **cable upstream description** command is used to specify descriptive information for a upstream port on the BSR. This information is limited to 80 characters and single word descriptions are not allowed. Use the characters: _ or - to separate words. For example, if a upstream port served a certain section of a city, the MSO could assign the following description:

```
MOT(config-if)#cable upstream 0 description charlestown_1U
```

Note: The entered description can be seen in the running configuration, and in the command output of **show** commands such as the **show ip interface** and **show running-config** commands.

Command Mode

Interface Configuration (cable interface only)

Command Line Usage

cable upstream <*NUM***> description <***LINE***>**

Command Syntax

NUM	is the upstream port number.
LINE	is the text that describes the interface.

cable upstream force-frag

The **cable upstream force-frag** command is used as a traffic shaping tool that forces the CM to fragment large upstream packets. When a CM sends a request to the CMTS for a large data grant that exceeds the configured minislot threshold, the CMTS grants the CM the configured minislot threshold, which forces the CM to make another data grant request for the remaining data, thereby causing data packets in the original grant to be fragmented by the CM.

Group Access

MSO

Command Mode

Interface Configuration (cable interface only)

Command Line Usage

cable upstream <*NUM***> force-frag** <*0-255*>

no cable upstream <*NUM***> force-frag** <*0-255*>

Command Syntax

NUM	Upstream port number
0-255	Configured minislot threshold without fragmentation for large data grants from 0 to 255.

Command Default

The force fragmentation feature is set to 0 for no forced fragmentation of large data grants.

cable upstream frequency

The **cable upstream frequency** command sets the fixed frequency for the upstream cable port in Hz. The **no cable upstream frequency** command returns the default upstream frequency value. The cable interface does not operate until a fixed upstream frequency is set. The RF upstream frequency must comply with the expected CM output frequency.

Note: The Japan DOCSIS Standard must be specified with the **cable cmts type** command before an upstream frequency can be selected for any Japan DOCSIS Standard CMTS module.

Note: Make sure that the upstream frequency selected does not interfere with the frequencies used for any other upstream applications running in the cable plant.

Group Access

MSO

Command Mode

Interface Configuration (cable interface only)

Command Line Usage

North American DOCSIS Standard

cable upstream <*NUM*> **frequency** <*5000000-42000000*>

no cable upstream <*NUM*> **frequency** <*5000000-42000000*>

Euro-DOCSIS Standard

cable upstream <*NUM*> **frequency** <*5000000-65000000*>

no cable upstream <*NUM*> **frequency** <*5000000-65000000*>

Japan DOCSIS (J-DOCSIS) Standard

cable upstream <*NUM*> **frequency** <*10000000-55000000*>

no cable upstream <*NUM*> **frequency** <*10000000-55000000*>

Command Syntax

NUM	Upstream port number
5000000-42000000	The upstream frequency value; valid entries are from 5000000 to 42000000 Hertz (Hz) for DOCSIS.
5000000-65000000	The upstream frequency value; valid entries are from 5000000 to 65000000 Hz for Euro-DOCSIS.
10000000-55000000	The upstream frequency value for the Japan DOCSIS (J-DOCSIS) Standard

Command Default

none

cable upstream hopping-seed

The **cable upstream hopping-seed** command specifies the 15 bit S-CDMA hopping seed value used for the code hopping sequence initialization.

Note: The logical channel must be disabled to specify a new hopping seed value.

Group Access

MSO

Command Mode

Interface Configuration (cable interface only)

Command Line Usage

cable upstream <*X*/*Y*> **hopping-seed** <*0-32767*>

no cable upstream <*X*/*Y*> **hopping-seed** <*0-32767*>

Command Syntax

X/*Y*	the upstream port and logical channel number (0-3)
0-32767	the hopping seed value (0 disables code hopping)

cable upstream ingress-canceller enable

The **cable upstream ingress-canceller enable** command enables the ingress canceller feature for an upstream cable port. Ingress cancellation is a DOCSIS 2.0 feature that protects against worst case plant impairments such as common path distortion (CPD), citizen band (CB), short-wave radio, and ham radio by opening unused portions of the upstream Spectrum. The **no cable upstream ingress-canceller enable** command disables the ingress canceller feature for an upstream cable port.

Group Access

All

Command Mode

Interface Configuration (cable interface only)

Command Line Usage

cable upstream <*NUM*> **ingress-canceller enable**

Command Syntax

NUM	the upstream port

cable upstream ingress-canceller idle-interval

The **cable upstream ingress-canceller idle-interval** command configures the idle interval for the ingress canceller feature.

Group Access

All

Command Mode

Interface Configuration (cable interface only)

Command Line Usage

cable upstream <*NUM*> **ingress-canceller idle-interval** <*256-512*> **frequency** <*1-20*>

no cable upstream <*NUM*> **ingress-canceller idle-interval** <*256-512*> **frequency** <*1-20*>

Command Syntax

NUM	the upstream port
256-512	the range of the idle interval in symbols
frequency *1-20*	the range of the idle frequency

cable upstream invited-range-interval

The **cable upstream invited-range-interval** command is used to define the amount of time in milliseconds allowed by the CMTS between ranging requests transmitted by the cable modem (CM). The **no cable upstream invited-range-interval** command returns to the default value.

Group Access

MSO

Command Mode

Interface Configuration (cable interface only)

Command Line Usage

cable upstream <*NUM*> **invited-range-interval** <*0-30000*>

no cable upstream <*NUM*> **invited-range-interval** <*0-30000*>

Command Syntax

NUM	the upstream port number
0-30000	the time in milliseconds allowed by the CMTS between ranging requests transmitted by the cable modem

Command Default

10000 milliseconds

cable upstream iuc11-grant-size

The **cable upstream iuc11-grant-size** command specifies the size of the Interval Usage Code (IUC) 11 Advanced Unsolicited Grant burst descriptor when configuring a DOCSIS 2.0 upstream logical channel.

Note: If a modulation profile for an upstream channel does not support IUC 11, the configuration of the IUC 11 byte size will be not be allowed. If a modulation profile for an upstream channel is changed and the new modulation profile does not support IUC 11, the IUC 11 byte size muset be reset to "0".

Group Access

MSO

Command Mode

Interface Configuration (cable interface only)

Command Line Usage

cable upstream <*X*/*Y*> **iuc11-grant-size** [<*0-1024*>]

no cable upstream <*X*/*Y*> **iuc11-grant-size** [<*0-1024*>]

Command Syntax

X/*Y*	the upstream port and logical channel number (0-3)
0-1024	the grant size in bytes

Command Default

0 bytes

cable upstream maintain-power-density on

The **cable upstream maintain-power-density on** command enables the Maintain Power Spectral Density feature for each logical channel. If Maintain Power Spectral Density is enabled and the modulation rate is different from the previous UCD, the cable modem must change its transmit power level to keep the power spectral density as close as possible to what it was prior to the modulation rate change. The **no cable upstream maintain-power-density on** command disables the Maintain Power Spectral Density feature. If Maintain Power Spectral Density is disabled, the cable modem maintains the same power level that it was using prior to the modulation rate change.

Group Access

MSO

Command Mode

Interface Configuration (cable interface only)

Command Line Usage

cable upstream <*X*/*Y*> **maintain-power-density on**

no cable upstream <*X*/*Y*> **maintain-power-density on**

Command Syntax

X/*Y*	the upstream port and logical channel number (0-3)

cable upstream map-interval

The **cable upstream map-interval** command is used to determine the time interval in microseconds for bandwidth maps messages (MAP) to be used by the CM to allocate upstream time slots. The **no cable upstream map-interval** command resets the upstream interval to the default.

Group Access

MSO

Command Mode

Interface Configuration (cable interface only)

Command Line Usage

cable upstream <*NUM*> **map-interval** <*2000-16000*>

no cable upstream <*NUM*> **map-interval** <*2000-16000*>

Command Syntax

NUM	Upstream port number
2000-16000	Interval value in microseconds.

Command Default

4000 microseconds

cable upstream max-calls

The Maximum Assigned Bandwidth (MAB) feature is used on the cable interface to regulate the number of Voice-over-IP (VOIP) calls that are available on a particular upstream channel for Unsolicited Grant Service (UGS) and Unsolicited Grant Service with Activity Detection UGS-AD constant bit rate (CBR) data flows. A definitive limit on the number of voice calls ensures that bandwidth resources are not overused on an upstream channel.

Use the **cable upstream max-calls** command to configure the maximum number of voice calls for an upstream channel. The **no cable upstream max-calls** command returns the maximum number of voice calls to the default value.

Group Access

MSO

Command Mode

Interface Configuration (cable interface only)

Command Line Usage

cable upstream <*NUM*> **max-calls** <*0-255*>

no cable upstream <*NUM*> **max-calls** <*0-255*>

Command Syntax

NUM	Upstream port number
0-255	Number of voice calls permitted on the upstream channel.

Command Default

The default maximum number of calls is 0.

cable upstream minislot-size

Use the **cable upstream minislot-size** command to set the number of 6.25 microsecond ticks in each upstream minislot. The **no cable upstream minislot-size** command returns the minislot size to the default value.

Group Access

MSO

Command Mode

Interface Configuration (cable interface only)

Command Line Usage

cable upstream <*NUM*> **minislot-size** [**2** | **4** | **8** | **16** | **32** | **64** | **128**]

no cable upstream <*NUM*> **minislot-size** [**2** | **4** | **8** | **16** | **32** | **64** | **128**]

Command Syntax

NUM	the upstream port number

2	Channel Width	Valid Minislot Sizes
4	3200000 Hz	2,4,8 ticks
8	1600000 Hz	4,8,16 ticks
16	800000 Hz	8,16,32 ticks
32	400000 Hz	16,32,64 ticks
64	200000 Hz	32,64,128 ticks
128		

Command Defaults

Channel Width	Minislot Size
3200000 Hz	4 ticks
1600000 Hz	8 ticks
800000 Hz	16 ticks
400000 Hz	32 ticks
200000 Hz	64 ticks

cable upstream modem-ranging-delay

The **cable upstream modem-ranging-delay** command specifies the maximum cable modem ranging delay in microseconds (usec). The ranging delay of a modem is the timing adjustment that would be sent to the modem if it were located next to the CMTS. For example, if a modem is located next to the CMTS and the **show cable modem** command indicates a timing offset of 1800 (10MHz clock units), the ranging delay for the modem is (1800 x 100)/1024 = 175-microseconds. The maximum modem ranging delay is used in sizing Initial Maintenance intervals in the upstream and is used for no other purpose. Initial Maintenance is the upstream interval that a cable modem uses to send its initial ranging request message when it wants to join the network. The **no cable upstream modem-ranging-delay** command restores the default value.

Group Access

MSO

Command Mode

Interface Configuration (cable interface only)

Command Line Usage

cable upstream <*NUM*> **modem-ranging-delay** <*0-600*>

no cable upstream <*NUM*> **modem-ranging-delay**

Command Syntax

NUM	Upstream port number
0-600	The maximum ranging timing offset in microseconds.

Command Default

250 microseconds

cable upstream modulation-profile

The **cable upstream modulation-profile** is used to apply an upstream modulation profile to an upstream channel. The **no cable upstream modulation-profile** command returns the modulation profile to modulation profile 1.

Group Access

MSO

Command Mode

Interface Configuration (cable interface only)

Command Line Usage

cable upstream <*NUM*> **modulation-profile <***1-600*>

no cable upstream <*NUM*> **modulation-profile <***1-600*>

Command Syntax

NUM	Upstream port number
1-600	Modulation profile number from 1 to 600.

Command Default

modulation profile 1

cable upstream physical-delay

The CMTS physical delay function is used to specify the maximum round-trip propagation delay between the CMTS and cable modems (CMs). The CMTS can optionally set the physical delay automatically.

The **cable upstream physical-delay** command is used to set fixed or automatic physical delay parameters. You can use the following options to adjust the physical delay function:

- A single fixed time can be set for physical delay.
- Physical delay parameters can be configured so that they are adjusted automatically by the BSR when you specify the automatic option with a specified minimum and maximum microsecond range.
- If you do not want to specify a range for the automatic option, select the automatic option only.

The **no cable upstream physical-delay** command changes the physical delay setting back to the default value.

Group Access

MSO

Command Mode

Interface Configuration (cable interface only)

Command Line Usage

cable upstream <*NUM*> **physical-delay** {<*10-1600*> | **automatic** [<*10-1600*> <*10-1600*>]}

no cable upstream <*NUM*> **physical-delay** {<*10-1600*> | **automatic** [<*10-1600*> <*10-1600*>]}

Command Syntax

NUM	Upstream port number
10-1600	Fixed physical delay in microseconds.
automatic	Automatic physical delay in microseconds.

10-1600	Automatic minimum physical delay in microseconds - the default is 200 microseconds
10-1600	Automatic maximum physical delay in microseconds - the default is 1600 microseconds

Command Default

The fixed physical delay is 400 microseconds

cable upstream power-level

The BSR CMTS interface controls CM output power levels to meet the desired CMTS upstream input power level. Input power level adjustments to an upstream port compensate for CMTS signal degradation between the optical receiver and the upstream RF port.

The **cable upstream power-level** command is used to set the upstream input power level in *absolute* mode. In *absolute* mode, the input power level does not change when the upstream channel width is changed. Defining the input power level in *absolute* mode could possibly cause upstream return lasers to clip on a completely populated upstream channel.

Caution: If the power level is not explicitly set on the upstream interfaces, they default to 0 dBmV in absolute mode with a 3.2 MHz, 2560 kilosymbols per second rate. Ensure that the correct power level is set on each upstream channel.

Table 11-2 describes how the upstream channel bandwidth corresponds to the input power-level range and default power-level range for a specific upstream channel.

Table 11-2 Upstream Input Power Level Range Parameters

Upstream Channel Bandwidth	Default Power-level Range	Power-level Range
200 KHz	-1 dBmV	-16 to +14 dBmV
400 KHz	+2 dBmV	-13 to +17 dBmV
800 KHz	+5 dBmV	-10 to +20 dBmV
1.6 MHz	+8 dBmV	-7 to +23 dBmV
3.2 MHz	+11 dBmV	-4 to +26 dBmV

Caution: Use caution when increasing the input power level in *absolute* mode. The CMs on the HFC network increase their transmit power level by 3 dB for every incremental upstream channel bandwidth change, causing an increase in the total power on the upstream channel. This may violate the upstream return laser design parameters

Group Access

MSO

Command Mode

Interface Configuration (cable interface only)

Command Line Usage

cable upstream <*NUM***> power-level** <*-160 - +290*>

no cable upstream <*NUM***> power-level** <*-160 - +290*>

Command Syntax

NUM	Upstream port number
-160 - +290	The input power level, expressed in tenths of a dB.

Command Default

0 dB

Command Example

The following example shows how to use the **cable upstream power-level** command to set the upstream input power level to +5 dBmV in *absolute* mode, which keeps the input power level at +5 dBmV regardless of the upstream channel bandwidth setting, as shown below:

```
MOT(config-if)#cable upstream 0 power-level 50
```

cable upstream power-level default

The BSR CMTS interface controls CM output power levels to meet the desired CMTS upstream input power level. Input power level adjustments to an upstream port compensate for CMTS signal degradation between the optical receiver and the upstream RF port.

The **cable upstream power-level default** command is used to set the upstream input power level in *relative* mode, which means that the input power level changes when the upstream channel width is changed. For example, if the input power level is +11 dBmV for a DOCSIS 3.2 MHz upstream channel bandwidth setting in *relative* mode and is changed to 1.6 MHz, the default receive power is +8 dBmV. The default power levels for the 3.2 MHz and 1.6 MHz channels are equal *relative* to their respective channel bandwidth settings

Caution: If the power level is not explicitly set on the upstream interfaces, they default to 0 dBmV in absolute mode with a 3.2 MHz, 2560 kilosymbols per second rate. Ensure that the correct power level is set on each upstream channel.

Table 11-3 describes how the upstream channel bandwidth corresponds to the input power-level range and default power-level range for a specific upstream channel.

Table 11-3 Upstream Input Power Level Range Parameters

Upstream Channel Bandwidth	Default Power-level Range	Power-level Range
200 KHz	-1 dBmV	-16 to +14 dBmV
400 KHz	+2 dBmV	-13 to +17 dBmV
800 KHz	+5 dBmV	-10 to +20 dBmV
1.6 MHz	+8 dBmV	-7 to +23 dBmV
3.2 MHz	+11 dBmV	-4 to +26 dBmV

Group Access

MSO

Command Mode

Interface Configuration (cable interface only)

Command Line Usage

cable upstream <*NUM*> **power-level default** {<*-150 - +150*>}

no cable upstream <*NUM*> **power-level default** {<*-150 - +150*>}

Command Syntax

NUM	Upstream port number
-150 - +150	The number of dB above or below the default input power level.

Command Default

0 dB

Command Example

The following example shows how to use the **cable upstream power-level default** command to set the input power level for a 3.2 MHz channel in *relative* mode from +11 dBmV to +5 dBmV:

```
MOT(config-if)#cable upstream 0 power-level default -60
```

The default input power level is reduced by 6 dB. The power level is now +5 dBmV.

The following example shows how to use the **cable upstream power-level default** command to set the input power level for a 3.2 MHz channel in *relative* mode from +11 dBmV to 0 dBmV, as shown below:

```
MOT(config-if)#cable upstream 0 power-level default -110
```

The default input power level is reduced by 11 dB.

cable upstream pre-equalization

The **cable upstream pre-equalization** command enables pre-equalization adjustment on the upstream port that includes sending pre-equalization coefficients in a ranging response to a CM to compensate for impairment over the transmission line. The **no cable upstream pre-equalization** command disables the pre-equalization function.

Note: Not all CMs support the pre-equalization adjustment. If a CM does not support this adjustment, the BSR CMTS interface may not be able to receive upstream data correctly from the CM.

Group Access

MSO

Command Mode

Interface Configuration (cable interface only)

Command Line Usage

cable upstream <*NUM*> **pre-equalization**

no cable upstream <*NUM*> **pre-equalization**

Command Syntax

NUM	Upstream port number

cable upstream range-backoff

Use the **cable upstream range-backoff** command to set the start and end upstream range-backoff values for a CM or re-establish a CM if a power outage occurs. Use the **no cable upstream range-backoff** command return the ranging back-off default value. If you choose automatic, the system sets the upstream data-backoff start and end values.

Group Access

MSO

Command Mode

Interface Configuration (cable interface only)

Command Line Usage

cable upstream <*NUM*> **range-backoff** {<*0-15*> <*0-15*> | **automatic**}

no cable upstream <*NUM*> **range-backoff** {<*0-15*> <*0-15*> | **automatic**}

Command Syntax

NUM	Upstream port number
0-15	Start of range backoff
0-15	End of range backoff
automatic	Automatic range backoff.

Command Default

start 0, end 4

cable upstream range-forced-continue

The **cable upstream range-forced-continue** command forces a ranging response to continue for all CMs. The no **cable upstream range-forced-continue** command disables forcing a ranging response/

Group Access

MSO

Command Mode

Interface Configuration (cable interface only)

Command Line Usage

cable upstream <*NUM*> **range-forced-continue**

no cable upstream <*NUM*> **range-forced-continue**

Command Syntax

NUM	Upstream port number

cable upstream range-power-override

The **cable upstream range-power-override** command enables CM power adjustment. The **no cable upstream range-power-override** command disables CM power adjustment.

Group Access

MSO

Command Mode

Interface Configuration (cable interface only)

Command Line Usage

cable upstream <*NUM*> **range-power-override**

no cable upstream <*NUM*> **range-power-override**

Command Syntax

NUM	Upstream port number

cable upstream rate-limit

The **cable upstream rate-limit** command controls whether rate-limiting is applied to any CM sending upstream data to the CMTS on a given upstream interface. The **no cable upstream rate-limit** command changes the rate limit applied to a cable modem sending upstream data to the CMTS back to the default which is disabled. The token-bucket algorithm is used for rate-limiting.

Note: If the rate-limit is enabled, data received from cable modems are rate-limited according to the cable modems configured. Packets may be buffered at times when any cable modem or the hosts behind the cable modems transmit data exceeding the permitted bandwidth.

Group Access

MSO

Command Mode

Interface Configuration

Command Line Usage

cable upstream <*NUM*> **rate-limit**

no cable upstream <*NUM*> **rate-limit**

Command Syntax

NUM	Upstream port number

Command Default

Disabled

cable upstream snr-offset

The **cable upstream snr-offset** command configures the display an SNR value with an offset. The offset can be configured for each upstream port up to a value of 100 (10 dB) in 10 (1 dB) increments. The offset value will be added to the SNR value when it is displayed with the **show controllers** and **show interfaces cable upstream signal-quality** CLI commands and through SNMP. The offset value will not be added to the actual SNR reading that is used by critical tasks such as Spectrum Management.

Group Access

MSO

Command Mode

Interface Configuration (cable interface only)

Command Line Usage

cable upstream <*NUM*> **snr-offset** {**10** | **20** | **30** | **40** | **50** | **60** | **70** | **80** | **90** | **100**}

no cable upstream <*NUM*> **snr-offset** {**10** | **20** | **30** | **40** | **50** | **60** | **70** | **80** | **90** | **100**}

Command Syntax

NUM	the upstream port number
	the offset value in increments of 10 (1 dB):
10	offset SNR value by 10
20	offset SNR value by 20
30	offset SNR value by 30
40	offset SNR value by 40
50	offset SNR value by 50
60	offset SNR value by 60
70	offset SNR value by 70
80	offset SNR value by 80
90	offset SNR value by 90
100	offset SNR value by 100

cable upstream spectrum-group

The **cable upstream spectrum-group command** is used to apply a spectrum group to an upstream port. The **no cable upstream spectrum-group command removes the spectrum group.**

Group Access

MSO

Command Mode

Interface Configuration (cable interface only)

Command Line Usage

cable upstream <*NUM*> **spectrum-group** <*WORD*>

no cable upstream <*NUM*> **spectrum-group** <*WORD*>

Command Syntax

NUM	Upstream port number
WORD	The exact group name applied to the upstream port.

cable upstream shutdown

The **cable upstream shutdown** command administratively disables the upstream port.The **no cable upstream shutdown** command enables an upstream port.

Note: Ensure that each upstream port is enabled after the port is properly configured and ready for use.

Group Access

MSO

Command Mode

Interface Configuration (cable interface only)

Command Line Usage

cable upstream <*NUM*> **shutdown**

no cable upstream <*NUM*> **shutdown**

Command Syntax

NUM	Upstream port number

Command Default

Each upstream port is disabled.

cable upstream spread-interval

The **cable upstream spread-interval** specifies the spreading interval for an S-CDMA frame. A spreading interval is the time that it takes to transmit one symbol per code across all 128 codes in an S-CDMA frame. The time duration of an S-CDMA frame is determined by a configurable number of spreading intervals and the signaling rate.

Group Access

MSO

Command Mode

Interface Configuration (cable interface only)

Command Line Usage

cable upstream <*X*/*Y*> **spread-interval** <*1-32*>

no cable upstream <*X*/*Y*> **spread-interval** <*1-32*>

Command Syntax

X/*Y*	the upstream port and logical channel number (0-3)
1-32	the spreading interval value

cable upstream trap-enable-cmts

The **cable upstream trap-enable-cmts** command enables the *rdnCmtsLinkUpDownTrapEnable* trap for an upstream port. The *rdnCmtsLinkUpDownTrapEnable* trap indicates whether a CMTS link up or link down trap should be generated. The **no cable upstream trap-enable-rdn** command disables the *rdnCmtsLinkUpDownTrapEnable* trap.

Group Access

All

Command Mode

Interface Configuration (cable interface only)

Command Line Usage

cable upstream <*NUM*> **trap-enable-cmts**

no cable upstream <*NUM*> **trap-enable-cmts**

Command Syntax

NUM	Upstream port number

Command Default

Disabled

cable upstream trap-enable-if

The **cable upstream trap-enable-if** command enables the *ifLinkUpDownTrapEnable* trap for an upstream port. The *ifLinkUpDownTrapEnable* trap indicates whether a link up or link down trap should be generated. The **cable upstream no trap-enable-if** command disables the *ifLinkUpDownTrapEnable* trap.

Group Access

All

Command Mode

Interface Configuration (cable interface only)

Command Line Usage

cable upstream <*NUM*> **trap-enable-if**

no cable upstream <*NUM*> **trap-enable-if**

Command Syntax

NUM	Upstream port number.

Command Default

Disabled

cable upstream trap-enable-rdn

The **cable upstream trap-enable-rdn** command enables the *rdnCardIfLinkUpDownEnable* trap for an upstream port. The *rdnCardIfLinkUpDownEnable* trap indicates whether a link up or link down trap should be generated. The **no cable upstream trap-enable-rdn** command disables the *rdnCardIfLinkUpDownEnable* trap.

Group Access

All

Command Mode

Interface Configuration (cable interface only)

Command Line Usage

cable upstream <*NUM*> **trap-enable-rdn**

no cable upstream <*NUM*> **trap-enable-rdn**

Command Syntax

NUM	Upstream port number.

Command Default

Disabled

cable utilization-interval

The **cable utilization-interval** command specifies the upstream or downstream channel utilization calculation interval. The **no cable utilization-interval** returns the channel utilization calculation interval to the default value of "0" (disabled).

Group Access

MSO

Command Mode

Global Configuration

Command Line Usage

cable utilization-interval <*0-86400*>

no cable utilization-interval <*0-86400*>

Command Syntax

0-86400	the channel utilization interval in seconds, 0 is disabled

Command Default

0 = disabled

channel-type

The **channel-type** command specifies the channel type for a modulation profile. There are four possible channel-types:

- TDMA - DOCSIS 1.1 channel type
- ATDMA - DOCSIS 2.0 channel type
- MTDMA - DOCSIS 1.1 or DOCSIS 2.0 channel type
- S-CDMA - DOCSIS 2.0 channel type only used for logical channel configurations

Group Access

MSO

Command Mode

Modulation Profile Configuration

Command Line Usage

channel-type {**tdma** | **atdma** | **scdma** | **mtdma**}

no channel-type {**tdma** | **atdma** | **scdma** | **mtdma**}

Command Syntax

tdma	TDMA, Time Division Multiple Access - valid for **initial**, **long**, **request**, **short**, and **station** IUC codes
atdma	Advanced TDMA, Time Division Multiple Access - valid for **a-long**, **a-short**, **a-ugs**, **initial**, **request**, and **station** IUC codes
scdma	S-CDMA Synchronous CDMA, Code Division Multiple Access - valid for **a-long**, **a-short**, **a-ugs**, **initial**, **request**, and **station** IUC codes
mtdma	TDMA-A-TDMA - valid for **a-long**, **a-short**, **a-ugs**, **initial**, **request**, and **station** IUC codes

clear cable dcc-stats

The **clear cable dcc-stats** command clears all Dynamic Channel Change (DCC) statistics for all CMTS modules in the BSR chassis or a CMTS module in a specified slot.

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

clear cable dcc-stats [<*X*/*Y*>]

Command Syntax

X/*Y*	*X* is 0. *Y* is the CMTS MAC domain.

clear cable flap-list

The **clear cable flap-list** command clears the cable flap-list. You can either clear the flap-list of a specific cable modem by specifying its MAC address or clear the flap-lists of all the cable modems by using the **all** option.

Group Access

MSO

Command Mode

Privileged EXEC

Command Line Usage

clear cable flap-list {<*mac*> | **all**}

Command Syntax

mac	MAC address in the form of xxxx.xxxx.xxxx
all	apply to all MAC addresses

clear cable modem

The **clear cable modem** command is used to either clear the traffic counters or reset a single cable modem or all cable modems connected to the BSR. The **clear cable modem** command options can be used to do the following:

- Clear or reset a single cable modem by using its MAC address.
- Clear or reset specific group of cable modems.
- Clear or reset a single cable modem by using its IP address.
- Clear or reset all cable modems.

Group Access

MSO

Command Mode

Privileged EXEC

Command Line Usage

clear cable modem {<*mac*> [<*mac*>] | <*prefix*> | **all** } {**counters** | **reset** }

Command Syntax

mac	the cable modem's MAC address
mac	a MAC address mask that specifies a group of cable modems
prefix	the cable modem's IP address
all	clear the cable modem traffic counters or reset all cable modems
counters	clear the cable modem traffic counters
reset	reset the cable modem

clear cable modem offline

The clear cable modem offline command removes a cable modem from the list of offline cable modems. This command allows you to do the following:

- remove a single offline cable modem from the offline list
- remove all offline cable modems in a single CMTS from the offline list
- remove all offline cable modems from the offline list

Note: The **cable modem aging timer** removes offline cable modems from the list after the configured timeout period has expired. The **clear cable modem offline** command is useful if you need to remove a modem before the cable modem aging timer has expired or if you are not using the cable modem aging timer feature.

Group Access

MSO

Command Mode

Privileged EXEC

Command Line Usage

clear cable modem offline [<*mac*> | <*X*/*Y*>]

Command Syntax

mac	the cable modem's MAC address
X/*Y*	*X* is 0. *Y* is the port number.

clear cable qos svc-flow statistics

The **clear cable qos svc-flow statistics** command clears all statistics relating to downstream rate-limiting for a particular service flow. This is the same information displayed with the **show cable qos svc-flow statistics** command.

Group Access

MSO

Command Mode

All modes except User EXEC

Command Line Usage

clear cable qos svc-flow statistics [<*X/Y*>] [<*1-4292967295*>]

Command Syntax

X/Y	*X* is 0. *Y* is the CMTS port number.
1-4292967295	service flow ID

clear cable ucc-stats

The **clear cable ucc-stats** command clears all UCC statistics for all CMTS modules in the BSR chassis or a CMTS module in a specified slot.

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

clear cable ucc-stats [<*X*/*Y*>]

Command Syntax

X/*Y*	*X* is 0. *Y* is the CMTS MAC domain.

clear counters cable

The **clear counters cable** clears counters for a cable interface.

Group Access

All

Command Mode

All modes except User EXEC.

Command Line Usage

clear counters cable <*X/Y*>

Command Syntax

X/*Y*	*X* is 0. *Y* is the CMTS port number.

codes-subframe

The **codes-subframe** command specifies the sub-frame size for an S-CDMA channel type. The sub-frame size establishes the boundaries over which interleaving is accomplished

Group Access

MSO

Command Mode

Modulation Profile Configuration

Command Line Usage

codes-subframe <*1-128*>

no codes-subframe <*1-128*>

Command Syntax

1-128	the sub-frame size

collect interval

The **collect interval** command configures the interval rate at which data collection is performed by the spectrum manager.

Group Access

MSO

Command Mode

Cable Spectrum Group

Command Line Usage

collect interval <*60-65535*>

Command Syntax

60-65535	The time interval in seconds

collect resolution

The **collect resolution** command is used to configure the frequency resolution rate that the spectrum manager performs.

Group Access

MSO

Command Mode

Cable Spectrum Group

Command Line Usage

collect resolution <*200000-400000*>

Command Syntax

200000-400000	The resolution in Hertz.

Command Default

200000 Hz

dhcp leasequery authorization on

The **dhcp leasequery authorization on** command enables the exchange of DHCP lease query messages between the CMTS and a DHCP server. The **no dhcp leasequery authorization on** command disables this exchange.

When an IP packet is either received from or destined to a Host/CPE which does not have an entry in the BSR's DHCP Lease table, the DHCP Lease Query feature will attempt to identify the Host/CPE. If the DHCP Lease Query attempt fails, packets associated with this Host/CPE are discarded.

Group Access

System Administrator

Command Mode

Interface Configuration (cable interface only)

Command Line Usage

dhcp leasequery {**authorization** {**on**}}

no dhcp leasequery {**authorization** {**on**}}

Command Syntax

authorization	Authorization configuration
on	Turn on the authorization (Disables Proxy ARP)

dhcp throttle on

The **dhcp throttle on** command enables DHCP Rate Limiting for all CMs or CPEs. The **no dhcp throttle on** command disables DHCP Rate Limiting for all CMs or CPEs.

Note: Once enabled for either CPEs, CMs, or both types of devices, rate limiting applies to all DHCP Request/Discover packets on a per device basis. The DHCP Rate Limiting feature does not support specifying a particular device for which rate limiting will be applied.

Group Access

All

Command Mode

Interface Configuration (cable interface only)

Command Line Usage

dhcp throttle {**cm** | **cpe**} **on**

no dhcp throttle {**cm** | **cpe**} **on**

Command Syntax

cm	enable DHCP packet rate limiting for all CMs.
cpe	enable DHCP packet rate limiting for all CPEs.

Command Default

Disabled

dhcp throttle window

The **dhcp throttle window** command configures the rate of one DHCP Request/Discover packet per number of seconds for a CM or CPE. The **no dhcp throttle window** command restores the DHCP Request/Discover packet rate per number of seconds to the default value for all CMs or CPEs.

Note: DHCP Rate Limiting must be enabled with the **dhcp throttle on** command for a new DHCP Request/Discover packet rate limit setting (other than the default) to take effect.

Group Access

All

Command Mode

Interface Configuration (cable interface only)

Command Line Usage

dhcp throttle {**cm** | **cpe**} **window** <*20-30000*>

no dhcp throttle {**cm** | **cpe**} **window** <*20-30000*>

Command Syntax

cm	configure a DHCP packet rate limit per millisecond for all CMs.
cpe	configure a DHCP packet rate limit per millisecond for all CPEs.
20-30000	the number of milliseconds for each DHCP Request/Discover packet

Command Default

one DHCP Request packet every 5000 milliseconds (five seconds)

differential-encoding on

The **differential-encoding on** command specifies whether or not differential encoding is used in this modulation profile. Differential encoding is a technique where data is transmitted according to the phase change between two modulation symbols instead of by the absolute phase of a symbol. Differential encoding makes the absolute phase of the received signal insignificant and has the effect of doubling the BER for the same C/N. The **no differential-encoding on** command disables differential encoding for this modulation profile.

Note: Differential encoding is applicable only to TDMA bursts that use QPSK or 16QAM modulation.

Group Access

MSO

Command Mode

Modulation Profile Configuration

Command Line Usage

differential-encoding on

no differential-encoding on

docstest

The **docstest** command globally enables or disables DOCSIS 2.0 test mode on the BSR through the DOCSIS 2.0 Testing MIB (SP-TestMIBv2.0-D02-030530). The DOCSIS 2.0 Testing MIB is used to test DOCSIS 2.0 protocol compliance through a set of objects used to manage DOCSIS 2.0 Cable Modem (CM) and Cable Modem Termination System (CMTS) programmable test features.

Note: The DOCSIS 2.0 Testing MIB is considered to be an adjunct to the DOCSIS 2.0 Specification rather than a part of that specification. Support for this MIB does not indicate compliance with the DOCSIS 2.0 specification. Conversely, lack of support for this MIB does not indicate non-compliance with the DOCSIS 2.0 specification. However, support for this MIB is mandatory for all DOCSIS 2.0 compliant CMs and CMTSs that are submitted for Certification and Qualification by CableLabs.

Once DOCSIS 2.0 test mode is enabled with the **docstest enable** command, the BSR remains in DOCSIS 2.0 test mode until the test mode is disabled with the **docstest disable** command or the system is rebooted.

Group Access

MSO

Command Mode

Privileged EXEC

Command Line Usage

docstest {**disable** | **enable**}

Command Syntax

disable	disable DOCSIS 2.0 test mode
enable	enable DOCSIS 2.0 test mode

Command Default

Disabled

docstest type

The **docstest type** command allows you to specifiy the type of DOCSIS 2.0 test to be used through a series of enumerated test modes. The enumerated test mode selected with the **docstest type** command corresponds to an integer "TYPE" field in the DOCSIS 2.0 Testing MIB's CM/CMTS TLV Table.

Note: DOCSIS 2.0 test mode must be enabled with the **docstest enable** command before a DOCSIS 2.0 test type can be specified.

Group Access

MSO

Command Mode

Privileged EXEC

Command Line Usage

docstest type {<*1-112*>{<*Slot*/*Port*>}} [*LINE*]

no docstest type {<*1-112*>{<*Slot*/*Port*>}} [*LINE*]

Command Syntax

1-112	the enumerated test mode corresponding to an integer "TYPE" field in the DOCSIS 2.0 Testing MIB's CM/CMTS TLV Table
Slot/*Port*	*Slot* is always 0 for the BSR 2000. *Port* is the CMTS port number.
LINE	specifies the data required for the test - up to 510 characters can be entered with first two characters being the length and value of the data that follows - the length and value correspond to the LENGTH and VALUE fields from the DOCSIS 2.0 Testing MIB's CM/CMTS TLV Table

fec-codeword

This **fec codeword** command specifies the number of information bytes for each FEC codeword.

Group Access

MSO

Command Mode

Modulation Profile Configuration

Command Line Usage

fec-codeword <*16-253*>

no fec-codeword <*16-253*>

Command Syntax

16-253	the number of information bytes for each FEC codeword

fec-correction

The **fec-correction** command specifies the number of bytes that can be corrected per Forward Error Correction (FEC) code word. This is the number of bytes that the FEC decoder can correct within a codeword. A FEC codeword consists of information and parity bytes for error correction. The number of parity bytes is equal to two times the number of correctable errors. The size of correctable errors is dictated by channel impairments.

Group Access

MSO

Command Mode

Modulation Profile Configuration

Command Line Usage

fec-correction <*0-10*>

no fec-correction <*0-10*>

Command Syntax

0-10	the FEC correction value - 0 indicates no Forward Error Correction

fft display

The **fft display** command displays the FFT power level measurement data to the console or telnet session in one of the two formats: table or graph (ASCII plot). Power level measurement data is retrieved either from an operational CMTS module or a file system. The user specifies a frequency range for which power level measurement data is to be displayed.

Group Access

MSO

Command Mode

Privileged EXEC

Command Line Usage

fft display {*Slot*/*Port* | **nvram**: <*WORD*> | **flash**: <*WORD*>} **startfreq** {*<0-81920000>*} **endfreq** {*<0-81920000>*} {**table** | **graph**}

Command Syntax

Slot/*Port*	*Slot* is always 0 for the BSR 2000. *Port* is a valid upstream port number.
nvram:	retrieve the power level measurement data from the NVRAM file system
flash:	retrieve the power level measurement data from the flash file system
WORD	power level measurement data filename - limit of 20 characters excluding the "`.fft`" filename extension
startfreq *0-81920000*	start of the frequency range (0 Hz - 81.92 MHz)
endfreq *0-81920000*	end of the frequency range (0 Hz - 81.92 MHz)
table | **graph**	specify table or graph display format

fft setup

The **fft setup** command can be used to configure the FFT processor on the BCM3138/ BCM3140 chip set or to display the current FFT processor configuration.

Group Access

MSO

Command Mode

Privileged EXEC

Command Line Usage

fft setup <*Slot*/*Port*> [**sample** {<*256-2048*>} **mode** {**Tap-in**} **window** {**blackman** | **blackman-harris** | **hamming** | **hanning** | **rectangular**}]

Command Syntax

Slot/*Port*	*Slot* is always 0 for the BSR 2000. *Port* is a valid upstream port number.
sample *256-2048*	number of samples of the power level measurement
mode Tap-in	RF Sentry operational mode
window	window coefficient to shape the output of the power level measurement (**rectangular**, **hamming**, **hanning**, **blackman**, or **blackman-harris**)

Command Defaults

sample = 2048

window = **rectangular**

fft start

The **fft start** command initiates the power level measurement using the FFT algorithm via the RF Sentry.

Note: The **sample**, **mode**, and **window** arguments are optional with the **fft start** command but can be used to override the current FFT processor configuration specified with the **fft setup** command and initiate power level measurement with a new FFT processor configuration.

Group Access

MSO

Command Mode

Privileged EXEC

Command Line Usage

fft start <*Slot*/*Port*> [**sample** {<*256-2048*>}] [**mode** {**Tap-in**}] [**window** {**rectangular** | **hamming** | **hanning** | **blackman** | **blackman-harris**}]

Command Syntax

Slot/*Port*	*Slot* is always 0 for the BSR 2000. *Port* is a valid upstream port number.
sample *256-2048*	number of samples of the power level measurement
mode Tap-in	RF Sentry operational mode
window	window coefficient to shape the output of the power level measurement (**rectangular**, **hamming**, **hanning**, **blackman**, or **blackman-harris**)

fft store

The **fft store** command saves the latest FFT power level measurement data for a CMTS module to a file system. The user specifies a particular slot and port, the file system (NVRAM or Flash), and a file name without any extension to be used to store the FFT power level measurement data. An extension of ".fft" will be automatically added to the file name.

Group Access

MSO

Command Mode

Privileged EXEC

Command Line Usage

fft store *Slot*/*Port* {**nvram**: <*WORD*> | **flash**: <*WORD*>}

Command Syntax

Slot/*Port*	*Slot* is always 0 for the BSR 2000. *Port* is a valid upstream port number.
nvram:	store the power level measurement data to the NVRAM file system
flash:	store the power level measurement data to the Flash file system
WORD	power level measurement data filename - limit of 20 characters not including any filename extension

guard-band

The **guard-band** command is used to define the minimum spectrum separation or spacing between upstream channels in the same spectrum group.

Group Access

MSO

Command Mode

Cable Spectrum Group

Command Line Usage

guard-band {*<0-37000000>* | *<0-60000000>*}

no guard-band {*<0-37000000>* | *<0-60000000>*}

Command Syntax

0-37000000	The guard band separation size in Hertz for North America.
0-60000000	The guard band separation size in Hertz for Europe.

Command Default

North America = 0 Hz

Europe = 0 Hz

hop action band

The **hop action band** command is used to determine the search order for each frequency band during the frequency hop action.

Group Access

MSO

Command Mode

Cable Spectrum Group

Command Line Usage

hop action band <*5000000-42000000*> <*5000000-42000000*> [**priority** <*1-255*>]

no hop action band <*5000000-42000000*> <*5000000-42000000*> [**priority** <*1-255*>]

Command Syntax

5000000-42000000	The start upstream frequency band in Hertz.
5000000-42000000	The end upstream frequency band in Hertz.
1-255	The upstream band priority number.The lower number takes precedence.

Command Default

upstream band priority = 128

hop action channel-width

The **hop action channel-width** command is used to change the upstream channel-width setting before a frequency hop action.

Group Access

MSO

Command Mode

Cable Spectrum Group

Command Line Usage

hop action channel-width {**1600000** | **200000** | **3200000** | **400000** | **800000**} [**priority** *<1-255>*]

no hop action channel-width {**1600000** | **200000** | **3200000** | **400000** | **800000**} [**priority** *<1-255>*]

Command Syntax

	The upstream channel width setting.
1600000	**1600000** = Channel width of 1600 kHz
200000	**200000** = Channel width of 200 kHz
3200000	**3200000** = Channel width of 3200 kHz
400000	**400000** = Channel width of 400 kHz
800000	**800000** = Channel width of 800 kHz
1-255	The upstream band priority number.The lower number takes precedence.

Command Default

upstream band priority = 128

hop action frequency

The **hop action frequency** command is used to determine the frequency search order for either discrete center frequencies or frequency bands during the frequency hop action.

Group Access

MSO

Command Mode

Cable Spectrum Group

Command Line Usage

hop action frequency <*5000000-42000000*> [**priority** <*1-255*>]

no hop action frequency <*5000000-42000000*> [**priority** <*1-255*>]

Command Syntax

5000000-42000000	The upstream frequency in Hertz
1-255	The upstream band priority number.The lower number takes precedence.

Command Default

upstream band priority = 128

hop action modulation-profile

The **hop action modulation-profile** command is used to change the modulation profile setting before a frequency hop action.

Group Access

MSO

Command Mode

Cable Spectrum Group

Command Line Usage

hop action modulation-profile <*1-16*> [**priority** <*1-255*>]

no hop action modulation-profile <*1-16*> [**priority** <*1-255*>]

Command Syntax

1-16	The modulation profile number.
1-255	The upstream band priority number.The lower number takes precedence.

Command Default

modulation profiles = 1 or 2

upstream band priority = 128

hop action power-level

The hop action power-level command is used to change the power-level setting before a frequency hop action.Table 11-4 describes how the upstream channel bandwidth corresponds to the input power-level range and default power-level range for a specific upstream channel.

Table 11-4 Upstream Input Power Level Range Parameters

Upstream Channel Bandwidth	Default Power-level Range	Power-level Range
200 KHz	-1 dBmV	-16 to +14 dBmV
400 KHz	+2 dBmV	-13 to +17 dBmV
800 KHz	+5 dBmV	-10 to +20 dBmV
1.6 MHz	+8 dBmV	-7 to +23 dBmV
3.2 MHz	+11 dBmV	-4 to +26 dBmV

Group Access

MSO

Command Mode

Cable Spectrum Group

Command Line Usage

hop action power-level {<*-160 - +290*> | **default** < *-150 - +150*>} [**priority** <*1-255*>]

no hop action power-level {<*-160 - +290*> | **default** < *-150 - +150*>} [**priority** <*1-255*>]

Command Syntax

<*-160 - +290*>	The input power level, expressed in tenths of a dB.

default *-150 - +150*	The number in tenths of a dB above or below the default input power level.
1-255	The upstream band priority number.The lower number takes precedence.

Command Default

upstream band priority = 128

hop action roll-back

The **hop action roll-back** command is used to return the upstream channel width or modulation profile setting, that was adjusted during a hop action, to the original configuration when upstream channel conditions improve.

Group Access

MSO

Command Mode

Cable Spectrum Group

Command Line Usage

hop action roll-back

no hop action roll-back

Command Default

Disabled

hop period

The **hop period** command is used to prevent excessive frequency hops on an upstream port.

Group Access

MSO

Command Mode

Cable Spectrum Group

Command Line Usage

hop period <*30-3600*>

no hop period <*30-3600*>

Command Syntax

30-3600	The rate at which the frequency hop takes place in seconds.

Command Default

300 seconds

hop threshold flap

A frequency hopping threshold is configured to prevent unnecessary frequency hops in instances when one or a minimal number of cable modems (CMs) lose their connection with the BSR. The frequency hopping threshold is determined by the percentage of CMs that lose their connectivity. The **hop threshold flap** command is used to trigger the hop threshold flap when a greater than a set percentage of CMs lose their connectivity.

Group Access

MSO

Command Mode

Cable Spectrum Group

Command Line Usage

hop threshold flap *<1-100>*

no hop threshold flap *<1-100>*

Command Syntax

1-100	The threshold percentage of CMs that can lose connectivity before the hop threshold flap is triggered.

Command Default

Disabled

interface cable

The **interface cable** command is used to enter cable interface configuration mode.

Group Access

MSO

Command Mode

Global Configuration

Command Line Usage

interface cable <*X/Y*>

Command Syntax

X/Y	*X* is 0. *Y* is the CMTS port number.

interleaver-block-size

The **interleaver-block-size** command specifies the interleaver block size for an ATDMA or MTDMA channel. Interleaving is a technique which improves the error correction of channel noise such as burst errors. The interleaver re-arranges transmitted data and distributes it among different interleaver blocks. At the receiver end, the interleaved data is arranged back into the original sequence by a de-interleaver. By intermixing the transmitted data and reassembling it on the receiver end, any transmission errors are spread out over a greater transmission time.

Forward error correction (FEC) is very effective on errors that are spread out. Interleaving spreads bursts of errors over several blocks so that the maximum number of errors in each block stays within the number of correctable errors. Since most errors occur in bursts, this is an efficient way to improve the error rate. Interleaver transmissions do not transmit each codeword by itself, but instead send bits from multiple codewords at the same time, so that a noise burst affects the minimum number of bits per codeword. This allows the FEC algorithm a greater chance of detecting and correcting any transmission errors.

Group Access

MSO

Command Mode

Modulation Profile Configuration

Command Line Usage

interleaver-block-size <*32-2048*>

no interleaver-block-size <*32-2048*>

Command Syntax

32-2048	the ATDMA or MTDMA interleaver block size value

interleaver-depth

The **interleaver-depth** command specifies the interleaver depth for an ATDMA or MTDMA channel. This command sets the interleaver minimum latency. A higher interleaver depth provides more protection from bursts errors by spreading out the bits for each codeword over a greater transmission time. However, a higher depth also increases downstream latency, which may slow TCP/IP throughput for some configurations.

DOCSIS 2.0 specifies five different interleaver depths - 128:1 is the highest amount of interleaving and 8:16 is the lowest.

- 128:1 indicates that 128 codewords made up of 128 symbols each will be intermixed on a 1 for 1 basis
- 8:16 indicates that 16 symbols will be kept in a row per codeword and intermixed with 16 symbols from 7 other codewords.

Group Access

MSO

Command Mode

Modulation Profile Configuration

Command Line Usage

interleaver-depth <*0-128*>

no interleaver-depth <*0-128*>

Command Syntax

0-128	the ATDMA or MTDMA interleaver depth value

interleaver-step-size

The **interleaver-step-size** command specifies the interleaver step size for an S-CDMA channel. The interleaver step size is the amount time that symbols are dispersed in time within the frame due to interleaving .

Group Access

MSO

Command Mode

Modulation Profile Configuration

Command Line Usage

interleaver-step-size <*1-31*>

no interleaver-step-size <*1-31*>

Command Syntax

1-31	the interleaver step size value

ip address

The **ip address** command configures a primary or secondary IP address for an interface or defines the Gateway IP address (giaddr) for Customer Premises Equipment (CPE), Multimedia Telephone Adapter (MTA), or cable modem DHCP requests. The **no ip address** command is used to remove an IP address from the interface. When configuring the cable interface IP address two additional options are supported; the **host** and **mta** options.

The additional options are only available from cable interface configuration mode when selecting an IP address. During the DHCP process, the relay agent requests an IP address in a particular subnet by inserting the IP address of the interface into the DHCP requests from CMs, hosts, and MTAs. The primary address is always inserted in cable modem DHCP requests. If a secondary address or a secondary host address is defined, then the first secondary or secondary host IP address in the list is inserted into DHCP requests from hosts. If one or multiple secondary mta IP address are defined, then the first secondary mta IP address defined is inserted into DHCP requests from secondary MTA devices. The **ip dhcp relay information option** command must be enabled to allow the BSR to determine what type of device originated the DHCP request. By default, the primary address will be inserted into DHCP requests.

When an operator wants to support multiple ISP providers, the **ip address** command can be used to group secondary subnets together. Basically one secondary is defined for CMs and another secondary subnet is defined for CPEs. The CM subnet and the CPE subnet are bound through the use of the isp-bind option of the ip address command. First the secondary subnet for CMs is defined and then the secondary subnet for CPE's is defined using **isp-bind** option. To bind the CPE subnet with the CM subnet, the CM subnet address is entered after the **isp-bind** option is entered while configuring the secondary subnet for CPE's.

Note: Supporting multiple ISPs on the BSR requires significant coordination between the operator provisioning system and the configuration of the BSR. Refer to *Selecting a Specific ISP* in the *BSR 2000 Configuration and Management Guide*.

Note: You must configure a primary IP address before configuring a secondary IP address.

Note: The **host** or **mta** optional parameters can be specified with a secondary IP address on a loopback interface. However, these parameters will have no effect unless the loopback interface is configured as a virtual cable bundle master.

Group Access

System Administrator

Command Mode

Interface Configuration (cable or loopback interfaces only)

Command Line Usage

ip address <*A.B.C.D*> <*A.B.C.D*> [**secondary** [**host** | **mta**][**isp-bind** <*A.B.C.D*>]]]

no ip address <*A.B.C.D*> <*A.B.C.D*> [**secondary** [**host** | **mta**][**isp-bind** <*A.B.C.D*>]]]

Command Syntax

A.B.C.D	the IP address
A.B.C.D	the subnetwork mask for the IP address - the BSR supports up to a 30-bit subnetwork IP address mask
secondary	designates the specified IP address as a secondary IP address - on a cable interface, defines this IP address as the IP address to be inserted into host DHCP requests

host	defines the IP address for the cable interface as the giaddr for host DHCP requests - on the cable interface, defines this IP address as the IP address to be inserted into host DHCP requests (this option is only available on the cable interface)
mta	defines the IP address for the cable interface as the giaddr for all MTA DHCP requests - on the cable interface, defines this IP address as the IP address to be inserted into MTA DHCP requests (this option is only available on the cable interface)
isp-bind *A.B.C.D*	specifies the secondary IP subnet to which this secondary address is bound.

ip dhcp relay information option

The IP DHCP relay function is used only when multiple subnetworks are configured on the same cable interface. The IP DHCP relay function gathers broadcast DHCP MAC discovery packets from a DHCP host, such as a CM or Customer Premises Equipment (CPE), and redirect the packets to their corresponding DHCP server or DHCP server profile if there is only one DHCP server. The DHCP server assigns an IP address to the CM or CPE that requested the IP address.

Use the **ip dhcp relay information option** command to enable the DHCP option-82 relay-agent on the cable interface. Use the **no ip dhcp relay information option** command to disable the DHCP option-82 relay-agent on the cable interface.

Group Access

ISP

Command Mode

Interface Configuration

Command Line Usage

ip dhcp relay information option

no ip dhcp relay information option

Command Default

DHCP option-82 disabled

iuc

The **iuc** command is used to completely configure a modulation profile without having to enter individual IUC submodes.

Group Access

MSO

Command Mode

Modulation Profile Configuration

Command Line Usage

iuc {**a-long** | **a-short** | **a-ugs** | **initial** | **long** | **request** | **short** | **station**} [**atdma** | **mtdma** | **scdma** | **tdma**] {**128qam** | **16qam** | **256qam** | **32qam** | **64qam** | **8qam** | **qpsk**} {*<0-16>*} {*<16-253>*} {**fixed** | **short**} {*<0-255>*} {**off** | **on**} {*<0x0-0x7fff>*} {**off** | **on**} {**none** | **qpsk0** | **qpsk1**} {*<0-1536>*} {*<0-2048>*} {*<0-2048>*} {*<0-32>*} {**off** | **on**} {*<0-128>*} {**off** | **on**}

no iuc {**a-long** | **a-short** | **a-ugs** | **initial** | **long** | **request** | **short** | **station**} [**atdma** | **mtdma** | **scdma** | **tdma**] {**128qam** | **16qam** | **256qam** | **32qam** | **64qam** | **8qam** | **qpsk**} {*<0-16>*} {*<16-253>*} {**fixed** | **short**} {*<0-255>*} {**off** | **on**} {*<0x0-0x7fff>*} {**off** | **on**} {**none** | **qpsk0** | **qpsk1**} {*<0-1536>*} {*<0-2048>*} {*<0-2048>*} {*<0-32>*} {**off** | **on**} {*<0-128>*} {**off** | **on**}

last-codeword-length

The **last-codeword-length** command specifies fixed or shortened handling of FEC for last code word.

Group Access

MSO

Command Mode

Modulation Profile Configuration

Command Line Usage

last-codeword-length {**fixed** | **shortened**}

no last-codeword-length {**fixed** | **shortened**}

Command Syntax

fixed	fixed handling of FEC for last code word
shortened	shortened handling of FEC for last code word

load-balancing static

Static upstream load balancing evenly distributes cable modems across multiple upstream channels serving the same geographical community or Spectrum Group. Load balancing is based on the cable modem count on each upstream channel. Static load balancing means that the BSR will only attempt to move a cable modem to another upstream channel after the modem's registration process is complete.

The **load-balancing static** command enables static load balancing for a Spectrum Group. The **no load-balancing static** command disables static load balancing.

Group Access

MSO

Command Mode

Cable Spectrum Group

Command Line Usage

load-balancing static

no load-balancing static

Command Default

Disabled

Note: The **load-balancing static** command cannot move cable modems registered with a TLV type 2. To move cable modems registered with a TLV type 2, you must use the **cable modem ucc** command.

max-burst

The **max-burst** command is used to specify the maximum burst length in minislots. The maximum burst length is used to determine the breakpoint between packets that use the short data grant burst profile and packets that use the long data grant burst profile. If the required upstream time to transmit a packet is greater than this value, the long data grant burst profile is used. If the time is less than or equal to this value, the short data grant burst profile is used.

Group Access

MSO

Command Mode

Modulation Profile Configuration

Command Line Usage

max-burst <*0-255*>

no max-burst <*0-255*>

Command Syntax

0-255	the maximum burst value in minislots

modulation-type

The **modulation-type** command specifies the digital frequency modulation technique used in a modulation profile.

- Quadrature Phase Shift Keying (QPSK) is a digital frequency modulation technique is used primarily for sending data from the cable subscriber upstream.
- Quadrature Amplitude Modulation (QAM) is a digital frequency modulation technique is primarily used for sending data downstream.

Group Access

MSO

Command Mode

Modulation Profile Configuration

Command Line Usage

modulation-type {**qpsk** | **16qam** | **8qam** | **32qam** | **64qam | 128qam | 256qam**}

no modulation-type {**qpsk** | **16qam** | **8qam** | **32qam** | **64qam | 128qam | 256qam**}

Command Syntax

qpsk
16qam
8qam
32qam
64qam
128qam
256qam

qpsk creates a default QPSK modulation type where all bursts are sent using QPSK

16qam creates a default 16-QAM modulation type where all bursts are sent using 16-QAM

8qam is used for DOCSIS 2.0 ATDMA or S-CDMA channel types only - creates a default 8-QAM modulation type where all bursts are sent using 8-QAM

32qam is used for DOCSIS 2.0 ATDMA or S-CDMA channel types only - creates a default 32-QAM modulation type where all bursts are sent using 32-QAM

64qam used for DOCSIS 2.0 ATDMA or S-CDMA channel types only - creates a default 64-QAM modulation type where all bursts are sent using 64-QAM

128qam is used for DOCSIS 2.0 ATDMA or S-CDMA channel types only - creates a default 128 -QAM modulation type where all bursts are sent using 128-QAM.

256qam is used for DOCSIS 2.0 ATDMA or S-CDMA channel types only - creates a default 256 -QAM modulation type where all bursts are sent using 256-QAM.

ping docsis

The **ping docsis** command is used to "ping" a cable modem (CM) on the network at the MAC layer to determine if the CM is online by entering the CM's MAC or IP address.

When a DOCSIS ping is initiated, the BSR sends a test packet downstream towards the CM to test its connection. In most instances, this command is used to determine if a particular CM is able to communicate at the MAC address layer when a cable modem has connectivity problems at the network layer. For example, if a CM is unable to register and obtain an IP address, the ping DOCSIS command can help you determine if there are provisioning problems associated with the CM.

Group Access

MSO

Command Mode

Privileged EXEC and Interface Configuration

Command Line Usage

ping docsis {<*mac*> | <*prefix*>} [<*1-100*>]

Command Syntax

mac	The MAC address of the CM in the form of xxxx.xxxx.xxxx.
prefix	The IP address of the CM.
1-100	The number of ping test packets to be sent to the cable modem.

preamble-length

The **preamble-length** command is used to specify the preamble length in bits. The preamble length is used to define a synchronizing string of modulation symbols that is used to allow the receiver to find the phase and timing of the transmitted burst.

Group Access

MSO

Command Mode

Modulation Profile Configuration

Command Line Usage

preamble-length <*0-1536*>

no preamble-length <*0-1536*>

Command Syntax

0-1536	the preamble length in bits - 0 indicates no preamble: *0-1536* is used for DOCSIS 2.0 bursts *0-1024* is used for DOCSIS 1.x bursts

preamble-type

The **preamble-type** command specifies the preamble format for DOCSIS ATDMA. MTDMA, and S-CDMA channel type modulation profiles. The preamble format is specified through the Quadrature Phase-Shift Keying (QPSK) digital modulation technique.

Group Access

MSO

Command Mode

Modulation Profile Configuration

Command Line Usage

preamble-type {**qpsk0** | **qpsk1**}

no preamble-type {**qpsk0** | **qpsk1**}

Command Syntax

qpsk0	low power QPSK preamble
qpsk1	high power QPSK preamble

scrambler-mode

The **scrambler-mode** command enables or disables the scrambler. The scrambler is used to generate an almost random sequence of transmission symbols. This ensures an even distribution of transmissions through the channel.

Group Access

MSO

Command Mode

Modulation Profile Configuration

Command Line Usage

scrambler-mode {**off** | **on**}

no scrambler-mode {**off** | **on**}

Command Syntax

off	disable the scrambler
on	enable the scrambler

scrambler-seed

The **scramber-seed** command specifies a scrambler seed value as a hexidecimal number. The scrambler seed is the initial value that is used to start the scrambler's pseudo-randomizer to scramble the bits. As the transmitter and receiver know the scrambler seed value, scrambling can be reversed at the receiver leaving only the original data.

Group Access

MSO

Command Mode

Modulation Profile Configuration

Command Line Usage

scrambler-seed <*0x00-0x7fff*>

no scrambler-seed <*0x00-0x7fff*>

Command Syntax

0x00-0x7fff	the scrambler seed value

show cable dcc-stats

The **show cable dcc-stats** command displays DOCSIS Dynamic Channel Change (DCC) statistics for a MAC domain. The following is an example of typical screen output from the **show cable dcc-stats** command:

```
CMTS Slot: 0  MAC Domain: 0  Interface index: 32513
Number of DCC Reqs          :  0
Number of DCC Rsps          :  0
Number of DCC Rsps(Depart)  :  0
Number of DCC Rsps(Arrive)  :  0
Number of DCC Acks          :  0
Number of DCC               :  0
Number of DCC Fails         :  0

CMTS Slot: 3  MAC Domain: 0  Interface index: 229121
Number of DCC Reqs          :  0
Number of DCC Rsps          :  0
Number of DCC Rsps(Depart)  :  0
Number of DCC Rsps(Arrive)  :  0
Number of DCC Acks          :  0
Number of DCC               :  0
Number of DCC Fails         :  0

CMTS Slot: 3  MAC Domain: 1  Interface index: 229122
Number of DCC Reqs          :  0
Number of DCC Rsps          :  0
Number of DCC Rsps(Depart)  :  0
Number of DCC Rsps          :  0
Number of DCC Rsps(Depart)  :  0
Number of DCC Rsps(Arrive)  :  0
Number of DCC Acks          :  0
Number of DCC               :  0
Number of DCC Fails         :  0
```

Group Access

All

Command Mode

Interface Configuration (cable interface only)

Command Line Usage

show cable dcc-stats [<*X*/*Y*>]

Command Syntax

X/*Y*	*X* is 0. *Y* is the CMTS MAC domain.

show cable downstream

The **show cable downstream** command displays the following downstream cable information:

ifIndex	interface index
annex	the downstream MPEG framing format
frequency	radio frequency carrier center frequency
rfModulation	radio frequency enabled
interleaveDepth	depth of interleaving to provide protection from noise
qamMode	downstream modulation type
channelWidth	radio frequency channel width
powerLevel	downstream transmit power level in units of whole dB to one decimal place
Reserved BW	the amount of reserved downstream bandwidth configured
Spectrum Group	the associated Spectrum Group names

The following is an example of typical screen output from the **show cable downstream** command:

```
ifIndex:          98305
description:
annex:            B
frequency:        327000000
rfModulation:     true
interleaveDepth:  32
qamMode:          256
channelWidth:     6000000
powerLevel:       600 (10th of dB)
Spectrum Group:
```

Group Access

All

Command Mode

Interface Configuration

Command Line Usage

show cable downstream [<*0-0*>]

Command Syntax

0-0	MAC domain identification

show cable flap-list

The **show cable flap-list** command displays the cable flap-list and provides the following information:.

MAC ID	Customer account or street address.
Cable IF	Upstream port.
Hit	Number of times modem responds to mac layer keep alive messages, minimum hit rate one time/30 seconds, can indicate intermittent upstream, laser clipping, or common-path distortion. Count should be much higher than Miss count, if not, modem having problem maintaining the connection due to upstream problem, flap count increments each time the system transitions from a Hit to a Miss.
Miss	Number of times modem misses the mac layer keep-alive message, 8% normal, can indicate intermittent upstream, laser clipping, common path distortion.
Ins	Number of times the modem comes up and connect to the network, number of times RF link reestablished more frequently than time period configured in the **cable flap-list insertion time** command.
P-Adj	Number of times the CMTS instructed the modem to adjust transmit (TX) power beyond threshold configured with the **cable flap-list power-adjust threshold** command, can indicate unacceptable connections, thermal sensitivity.
Flap	Total of P-Adj and Ins values, high flap-count modems have high SIDs and may not register.
Rng	Number of times the modem exceeded the missed ranging threshold.

Type	Specifies the type of flap (ranging, timing, or power)
Time	Most recent time modem dropped connection.

The following is an example of typical screen output from the **show cable flap-list** command:

```
MAC ID       CableIF Hit  Miss  Ins  Pow  Rng  Flap   Type Time
000b.0643.3b60  4/0 U1 1469  7    0    0   1   1     Rng  FRI NOV 05 11:59:39
000b.0643.36c8  4/0 U1 1469  7    0    0   1   1     Rng  FRI NOV 05 11:59:40
000b.0643.3b78  4/0 U1 1469  6    0    0   1   1     Rng  FRI NOV 05 11:59:40
```

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show cable flap-list [**sort-flap** | **sort-interface** | **sort-time**]

Command Syntax

sort-flap	Sort by number of times cable modem flapped.
sort-interface	Sort cable modem flaps by interface.
sort-time	Sort most recent time cable modem flapped.

show cable insert-interval

The **show cable insert-interval** command shows the period (in hundredths of a second) with which Initial Maintenance intervals are scheduled in the upstream. The following is an example of typical screen output from the **show cable insert-interval** command:

```
Cable insert-interval: 20
```

Group Access

All

Command Mode

Interface Configuration

Command Line Usage

show cable insert-interval

show cable modem

The **show cable modem** command is used to gather a variety of cable modem (CM) statistical information used to evaluate network performance, troubleshoot registration problems, and learn specific registration and ranging information on modems connected to a specific interface.

Use the **show cable modem** command to see detailed modem configuration information for a specific head-end modem. The following information is provided:

Interface	CM interface with active connection
Upstream IF Index	Upstream interface to which the cable modem belongs.
Downsteam IF Index	Downstream interface to which the cable modem belongs.
Prim SID	Primary Service Identifier number.
Connectivity State	Describes the connectivity state of a cable modem. The table below describes the 20 cable modem connectivity states supported on the BSR.
Timing offset	CM current timing adjustment.
Rec Power	CM receive downstream receive power level in units of whole dB to one decimal place
IP address	CM IP address
MAC address	Media Access Control layer address

Cable modem connectivity states are as follows:

init(o)	Option file transfer was started.
init(t)	Time-of-day (TOD) exchange was started.
init(r1)	CM sent initial ranging parameters.
init(r2)	CM is ranging.
init(rc)	Ranging is complete.

dhcp(d)	DHCP Discover was sent by CM.
dhcp(o)	DHCP Offer was received.
dhcp(req)	DHCP Request was sent by CM.
dhcp(ack)	DHCP Ack was received, IP address was assigned by DHCP server.
online	CM registered; enabled for data.
online(d)	CM registered, but network access for the CM is disabled.
online(un)	CM registered, but not enabled data. Fail to verify modem's identity by BPI module.
online(pk)	CM registered; baseline privacy interface (BPI) enabled, and key encryption key (KEK) is assigned.
online(pt)	CM registered; BPI enabled, and traffic encryption key (TEK) is assigned.
reject(m)	CM did attempt to register; registration was refused due to bad mic.
reject(c)	CM did attempt to register; registration was refused due to bad COS.
reject(r)	CM did attempt to register, registration was refused due to unavailable resource.
reject(pk)	KEK modem key assignment is rejected.
reject(pt)	TEK modem key assignment is rejected.
offline	CM is considered to be offline.

The following is an example of typical screen output from the **show cable modem** command:

```
Interface        Prim Connect     Timing Rec   Ip Address      Mac Address
                 Sid  State       Offset Power
Cable  4/1/D1U1 5    online(pt)  572    0.0   150.31.101.14   000b.0643.36c8
Cable  4/1/D1U1 1    online(pt)  573    -.2   150.31.101.44   000b.0643.3716
Cable  4/1/D1U1 4    online(pt)  576    0.0   150.31.101.45   000b.0643.3b60
Cable  4/1/D1U1 3    online(pt)  586    0.0   150.31.101.46   000b.0643.3b72
Cable  4/1/D1U1 9    online(pt)  581    0.2   150.31.101.50   000b.0643.3b78
Cable  4/1/D1U1 7    online(pt)  573    0.3   150.31.101.21   000b.0643.3b84
Cable  4/1/D1U1 8    online(pt)  581    0.3   150.31.101.17   000b.0643.3b90
Cable  4/1/D1U1 10   online(pt)  583    0.1   150.31.101.12   000b.0643.3b9a
Cable  4/1/D1U1 2    online(pt)  578    0.3   150.31.101.15   000b.0643.3bb2
```

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show cable modem [| {**begin** | **exclude** | **include**} {<*WORD*>} [| {**count** | **count-only**}]]

show cable modem [| {**count** | **count-only**}]

Command Syntax

|	turns on output modifiers (filters)
begin	filter for output that begins with the specified string
exclude	filter for output that excludes the specified string
include	filter for output that includes the specified string
WORD	the specified string

count	count the number of outputted lines
count-only	count the number of lines while suppressing screen output

show cable modem cpe

The **show cable modem cpe command displays the following** Customer Premises Equipment (CPE) information for all cable interfaces, a particular upstream port, or a specific CPE:

Interface	the downstream cable interface and upstream port the cable modem is connected to
PSID	the upstream Primary SID number associated with this cable modem
CM MAC	the cable modem's MAC address
CM IP	the cable modem's IP address
CPE MAC	the MAC address of a CPE device connected to the cable modem displayed in the command output
CPE IP	the IP address of a CPE device connected to the cable modem displayed in the command output
Count	the CPE count per cable modem

The following is an example of typical screen output from the **show cable modem cpe** command:

```
Interface       Prim Connect    Timing Rec   Ip Address      Mac Address
                Sid  State      Offset Power
Cable  4/1/D1U1 2    online(pt) 578    0.3   150.31.101.15   000b.0643.3bb2
Number of Hosts = 0
```

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show cable modem <*mac*> **cpe** [| {**begin** | **exclude** | **include**} {<*WORD*>} [| {**count** | **count-only**}]]

show cable modem <*mac*> **cpe** [| {**count** | **count-only**}]

show cable modem cpe <*X*/*Y*> [**upstream** <*NUM*>] [| {**begin** | **exclude** | **include**} {<*WORD*>} [| {**count** | **count-only**}]]

show cable modem cpe <*X*/*Y*> [**upstream** <*NUM*>] [| {**count** | **count-only**}]

Command Syntax

mac	the cable modem's MAC address
X/*Y*	*X* is 0. *Y* is the CMTS port number.
upstream *NUM*	the upstream port number
|	turns on output modifiers (filters)
begin	filter for output that begins with the specified string
exclude	filter for output that excludes the specified string
include	filter for output that includes the specified string
WORD	the specified string
count	count the number of outputted lines
count-only	count the number of lines while suppressing screen output

show cable modem detail

The **show cable modem detail** command displays information for a SID assigned to a cable modem on a specific CMTS interface or a specific CM connected to a specific interface. The QoS Profile the cable modem used for registration is displayed in the "QoS Profile Index" field. The device type is displayed in the device type field: CM = cable modem, eSTB = embedded Set Top Box. The following is typical output from the **show cable modem detail** command.

```
CM Record (index 1) Dump:
Psid                        1
Config                      0x2
Status                      regComplete
BPI Enabled                 No
MAC Address                 0012.2503.52ac
IP Addr                     150.31.83.15
US Chan                     1
DS Chan                     0
Vendor Id                   00 00 00
MAX Classifier              0
MAX CPEs                    1
Qos Profile                 0
Device type                 CM
--Ranging State--
State                       0x4
Retry                       0
NoReqCount                  0
Pending                     0
Rx Power                    2
Freq Offset                 26
Timing Offset               1791
Last Invited                1567669(ms)
Max Interval                10003(ms)
Max Req Delay               398(ticks)
Equalization Data:
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
##CM Capability:##
Concatenation:              1
DOCSIS Version:             DOCSIS 2.0
Fragmentation:              1
PHS:                        1
BPI:                        1
US SIDs:                    4
Transmit Equilizer:         1(Taps/Symbol)
Xmit Equilizer Taps:        24
DCC Support:                1
```

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show cable modem detail {<*X/Y*> <*NUM*>} {<*MAC*>} [| {**begin** | **exclude** | **include**} {<*WORD*>} [| {**count** | **count-only**}]]

show cable modem detail {<*X/Y*> <*NUM*>} {<*MAC*>} [| {**count** | **count-only**}]

Command Syntax

X/Y	*X* is 0. *Y* is the CMTS port number.
NUM	The Service Identifier assigned to a CM.
MAC	The cable modem's MAC address.
|	turns on output modifiers (filters)
begin	filter for output that begins with the specified string
exclude	filter for output that excludes the specified string
include	filter for output that includes the specified string
WORD	the specified string
count	count the number of outputted lines
count-only	count the number of lines while suppressing screen output

show cable modem hosts

The **show cable modem hosts** command displays the number of Customer Premises Equipment (CPE) hosts connected to a specific CM.

```
MAC Address     MAC      Prim Ver     Frag Concat PHS Priv   DS     US
                State    SID                                 Saids  Sids
0090.833d.bba0 online   6    DOC1.0  no    yes   no   BPI     0      0
```

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show cable modem {<*mac*> | <*prefix*>} **hosts** [| {**begin** | **exclude** | **include**} {<*WORD*>} [| {**count** | **count-only**}]]

show cable modem {<*mac*> | <*prefix*>} **hosts** [{**count** | **count-only**}]

Command Syntax

mac	cable modem MAC address
prefix	cable modem IP address
|	turns on output modifiers (filters)
begin	filter for output that begins with the specified string
exclude	filter for output that excludes the specified string
include	filter for output that includes the specified string
WORD	the specified string

count	count the number of outputted lines
count-only	count the number of lines while suppressing screen output

show cable modem loadbalance-group

The **show cable modem loadbalance-group** command displays cable modem load balancing group assignments. The following is typical output from the **show cable modem loadbalance-group** command:

```
Cable                   Mac Address           Load Balance
Interface                                     Group Name
Cable  1/0/D0/U0/C0      0008.0e10.3cb2        lbg-1
Cable  1/0/D0/U1/C0      0010.1848.2004        lbg-1
Cable  1/0/D0/U3/C0      0010.9518.f403        lbg-1
Cable  1/0/D0/U3/C0      0012.c90b.cff8        lbg-1
Cable  1/0/D0/U0/C0      0020.4094.e238        lbg-1
Cable  1/0/D0/U1/C0      0050.04b2.f8e0        Not Assigned
```

Group Access

ALL

Command Mode

All modes except User EXEC

Command Line Usage

show cable modem loadbalance-group [| {**begin** | **exclude** | **include**} {<*WORD*>} | {**count** | **count-only**}]

show cable modem loadbalance-group [| {**count** | **count-only** } {<*WORD*>}]

Command Syntax

|	turns on output modifiers (filters)
begin	filter for output that begins with the specified string
count	count the number of outputted lines

count-only	count the number of lines while suppressing screen output
exclude	filter for output that excludes the specified string
include	filter for output that includes the specified string
WORD	the specified string

show cable modem mac

The **show cable modem mac** command displays the following MAC layer (layer 2) information for all cable modems attached to the BSR, cable modems on a specific CMTS module, or a specific cable modem:

MAC Address	the cable modem's MAC address
MAC State	the stage of connectivity that the cable modem has achieved with the CMTS - **offline** or in one of a number of **online, init**, or **reject** states
Prim SID	the Primary SID number associated with this cable modem
Version	the version of the DOCSIS specification that this cable modem supports (DOC1.0, DOC1.0+, DOC1.1, DOC2.0) - this field does not indicate the DOCSIS version that a cable modem is running. If the modem is offline, a default version of DOCSIS 1.0 is displayed.
QoS Prov	the version of DOCSIS for which the cable modem is registered and provisioned
Frag	**yes** indicates that this cable modem is capable of performing DOCSIS 1.1 style fragmentation
Concat	**yes** indicates that this cable modem is capable of performing concatenation
PHS	**yes** indicates that this cable modem is capable of performing DOCSIS 1.1 style Payload Header Suppression (PHS)
Priv	**BPI+** indicates that this Cable Modem is capable of supporting BPI+ encryption if not, it displays **BPI**

DS Saids	the number of BPI+ style downstream Security Association Identifiers (SAIDs) that this cable modem supports (DOCSIS 1.1 modems only)
US Sids	the number of upstream Service IDentifiers (SIDs) that this cable modem supports (DOCSIS 1.1 modems only)
Dev.	the device type field: CM = cable modem eSTB = embedded Set Top Box

If the cable modem supports DOCSIS 1.0+, it will be displayed in the "Version" field of the command output. The following is typical output from the **show cable modem mac** command:

```
MAC Address    MAC     Prim   Ver   QoS    Frag  Concat   PHS Priv DS    US    Dev.
               State    SID          Prov                          Saids Sids
000b.0643.36c8 online(pt) 5    DOC1.1 DOC1.0  no    no     no  BPI  0     0    CM
000b.0643.3716 online(pt) 1    DOC1.0 DOC1.0  no    no     no  BPI  0     0    eSTB
000b.0643.3b60 online(pt) 4    DOC1.1 DOC1.0  no    no     no  BPI  0     0    CM
000b.0643.3b72 online(pt) 3    DOC1.1 DOC1.0  no    no     no  BPI  0     0    CM
000b.0643.3b78 online(pt) 9    DOC1.1 DOC1.0  no    no     no  BPI  0     0    CM
000b.0643.3b84 online(pt) 7    DOC1.1 DOC1.0  no    no     no  BPI  0     0    CM
000b.0643.3b90 online(pt) 8    DOC1.1 DOC1.0  no    no     no  BPI  0     0    CM
000b.0643.3b9a online(pt) 10   DOC1.1 DOC1.0  no    no     no  BPI  0     0    CM
000b.0643.3bb2 online(pt) 2    DOC1.0+ DOC1.0  no    no     no  BPI  0     0    CM
```

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show cable modem <*mac*> **mac** [| {**begin** | **exclude** | **include**} {<*WORD*>} [| {**count** | **count-only**}]]

show cable modem <*mac*> **mac** [| {**count** | **count-only**}]

show cable modem mac [<*X/Y*>] [| {**begin** | **exclude** | **include**} {<*WORD*>} [| {**count** | **count-only**}]]

show cable modem mac [<*X/Y*>] [| {**count** | **count-only**}]

Command Syntax

mac	the cable modem's MAC address
X/*Y*	*X* is 0. *Y* is the CMTS port number.
|	turns on output modifiers (filters)
begin	filter for output that begins with the specified string
exclude	filter for output that excludes the specified string
include	filter for output that includes the specified string
WORD	the specified string
count	count the number of outputted lines
count-only	count the number of lines while suppressing screen output

show cable modem maintenance

The **show cable modem maintenance** command displays the following station maintenance error statistics for all cable modems attached to the BSR, cable modems on a specific CMTS module, or a specific cable modem:

Mac Address	the MAC address of the cable modem
I/F	the interface on which the cable modem has an active connection
Prime Sid	the primary service identifier assigned to the modem
SM Exhausted Count - Time	the number of times a CM was dropped because it did not reply to station maintenance requests
SM Aborted Count - Time	the number of times the CM was dropped because its operational parameters were unacceptable including power level outside of the acceptable range, or the timing offset changes

The following is typical output from the **show cable modem maintenance** command:

```
MAC Address   I/F      Prim    SM Exhausted           SM Aborted
                       Sid     Count - Time           Count - Time
000b.0643.36c8 C4/1/U1  5      0     xxx xx xx:xx:xx  0     xxx xx xx:xx:xx
000b.0643.3716 C4/1/U1  1      0     xxx xx xx:xx:xx  0     xxx xx xx:xx:xx
000b.0643.3b60 C4/1/U1  4      0     xxx xx xx:xx:xx  0     xxx xx xx:xx:xx
000b.0643.3b72 C4/1/U1  3      0     xxx xx xx:xx:xx  0     xxx xx xx:xx:xx
000b.0643.3b78 C4/1/U1  9      0     xxx xx xx:xx:xx  0     xxx xx xx:xx:xx
000b.0643.3b84 C4/1/U1  7      0     xxx xx xx:xx:xx  0     xxx xx xx:xx:xx
000b.0643.3b90 C4/1/U1  8      0     xxx xx xx:xx:xx  0     xxx xx xx:xx:xx
000b.0643.3b9a C4/1/U1  10     0     xxx xx xx:xx:xx  0     xxx xx xx:xx:xx
000b.0643.3bb2 C4/1/U1  2      0     xxx xx xx:xx:xx  0     xxx xx xx:xx:xx
```

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show cable modem <*mac*> **maintenance** [| {**begin** | **exclude** | **include**} {<*WORD*>} [| {**count** | **count-only**}]]

show cable modem <*mac*> **maintenance** [| {**count** | **count-only**}]

show cable modem maintenance [<*X/Y*>] [| {**begin** | **exclude** | **include**} {<*WORD*>} [| {**count** | **count-only**}]]

show cable modem maintenance [<*X/Y*>] [| {**count** | **count-only**}]

Command Syntax

mac	the cable modem's MAC address
X/*Y*	*X* is 0. *Y* is the CMTS port number.
|	turns on output modifiers (filters)
begin	filter for output that begins with the specified string
exclude	filter for output that excludes the specified string
include	filter for output that includes the specified string
WORD	the specified string
count	count the number of outputted lines
count-only	count the number of lines while suppressing screen output

show cable modem offline

The **show cable modem offline** command provides the following information about cable modems that are offline:

Interface	cable modem interface with active connection
Prim Sid	Primary Service Identifier number
Mac address	cable modem Media Access Control layer address
DeRegistration Timestamp	the time at which the modem deregistered in *month,date,hh:mm:ss* format
lastTxBytes	the size of the last transmitted data
lastRxBytes	the size of the last received data

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show cable modem offline [<*0-0*> | <X/Y> | <*mac*>] [| {**begin** | **exclude** | **include**} {<*WORD*>} [| {**count** | **count-only**}]]

show cable modem offline [<*0-0*> | <X/Y> | <*mac*>] [| {**count** | **count-only**}]

Command Syntax

0-0	This number is always 0 for the BSR 2000.
X/Y	*X* is 0. *Y* is the CMTS port number.
mac	the cable modem MAC address
|	turns on output modifiers (filters)

begin	filter for output that begins with the specified string
exclude	filter for output that excludes the specified string
include	filter for output that includes the specified string
WORD	the specified string
count	count the number of outputted lines
count-only	count the number of lines while suppressing screen output

show cable modem phy

The **show cable modem phy** command displays the following physical hardware information for or all cable modems attached to the BSR, cable modems on a specific CMTS module, or a specific cable modem:

Mac Address	the MAC address of the cable modem
I/F	the channel number
USPwr (dBmV)	the upstream power level in dBmV as measured at the CMTS upstream port for this cable modem
USSNR (tenthdB)	the estimated upstream signal to noise ratio of signals generated by this cable modem as measured at the CMTS upstream port
Timing Offset	the ranging time offset for the cable modem
Mod Type	the modulation type for the cable modem - possible types are: TDMA - DOCSIS 1.X capable modems or DOCSIS 2.0 modems with TLV39 DOCSIS 2.0 Mode disabled ATDMA - DOCSIS 2.0 modems on an ATDMA or MTDMA channel. SCDMA - DOCSIS 2.0 modems on an SCDMA channel

The following is typical output from the **show cable modem phy** command:

```
MAC Address          I/F           USPwr  USSNR        Timing Mod
                                   (dBmV) (tenthdB)    Offset Type
0008.0e10.3cb2       C1/0/U0 2     323          1494   TDMA
0010.1848.2004       C1/0/U1 2     343          1788   TDMA
0010.9518.f403       C1/0/U3 1     356          1872   TDMA
0012.c90b.cff8       C1/0/U3 2     356          1787   TDMA
0020.4094.e238       C1/0/U0 0     321          1908   TDMA
0050.04b2.f8e0       C1/0/U1 -1    343          2088   TDMA
```

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show cable modem <*mac*> **phy** [| {**begin** | **exclude** | **include**} {<*WORD*>} | {**count** | **count-only**}]

show cable modem <*mac*> **phy** [| {**count** | **count-only** } {<*WORD*>}]

show cable modem phy [<*X/Y*>] [| {**begin** | **exclude** | **include**} {<*WORD*>} | {**count** | **count-only**}]

show cable modem phy [<*X/Y*>] [| {**count** | **count-only** } {<*WORD*>}]

Command Syntax

mac	the cable modem's MAC address
X/*Y*	*X* is 0. *Y* is the CMTS port number.
|	turns on output modifiers (filters)
begin	filter for output that begins with the specified string
count	count the number of outputted lines

count-only	count the number of lines while suppressing screen output
exclude	filter for output that excludes the specified string
include	filter for output that includes the specified string
WORD	the specified string

show cable modem registered

The **show cable modem registered** command displays the following information about registered cable modems:

Interface	cable modem interface with active connection
Prim Sid	Primary Service Identifier number
Connect State	describes the connectivity state of a cable modem. The table below describes the 20 cable modem connectivity states supported on the BSR
Timing Offset	current cable modem timing adjustment.
Rec Power	cable modem receive downstream power level in dbmv
Ip address	cable modem IP address
Mac address	cable modem Media Access Control layer address

The following is typical output from the **show cable modem registered** command:

```
Interface        Prim Connect     Timing Rec   Ip Address      Mac Address
                 Sid  State       Offset Power
Cable  4/1/D1U1 4    online(pt) 580    0.2   150.31.101.14   000b.0643.36c8
Cable  4/1/D1U1 6    online(pt) 581    0.1   150.31.101.44   000b.0643.3716
Cable  4/1/D1U1 9    online(pt) 581    0.0   150.31.101.45   000b.0643.3b60
Cable  4/1/D1U1 7    online(pt) 580    0.0   150.31.101.46   000b.0643.3b72
Cable  4/1/D1U1 5    online(pt) 579    0.1   150.31.101.50   000b.0643.3b78
Cable  4/1/D1U1 1    online(pt) 583    0.4   150.31.101.21   000b.0643.3b84
Cable  4/1/D1U1 2    online(pt) 583    0.2   150.31.101.17   000b.0643.3b90
Cable  4/1/D1U1 3    online(pt) 579    0.1   150.31.101.12   000b.0643.3b9a
Cable  4/1/D1U1 8    online(pt) 581    0.0   150.31.101.15   000b.0643.3bb2
```

Cable modem connectivity states are as follows:

online	CM registered; enabled for data.
online(d)	CM registered, but network access for the CM is disabled.

online(un)	CM registered, but not enabled data. Fail to verify modem's identity by BPI module.
online(pk)	CM registered; baseline privacy interface (BPI) enabled, and key encryption key (KEK) is assigned.
online(pt)	CM registered; BPI enabled, and traffic encryption key (TEK) is assigned.
reject(r)	CM did attempt to register, registration was refused due to unavailable resource.
reject(pk)	KEK modem key assignment is rejected.
reject(pt)	TEK modem key assignment is rejected.

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show cable modem registered [| {**begin** | **exclude** | **include**} {<*WORD*>} [| {**count** | **count-only**}]]

show cable modem registered [| {**count** | **count-only**}]

Command Syntax

|	turns on output modifiers (filters)
begin	filter for output that begins with the specified string
exclude	filter for output that excludes the specified string
include	filter for output that includes the specified string
WORD	the specified string

count	count the number of outputted lines
count-only	count the number of lines while suppressing screen output

show cable modem stats

The **show cable modem stats** command displays the following statistics for each cable modem on a CMTS module. This includes cable modems that are off-line.

Interface	cable modem interface with active connection
Prim Sid	Primary Service Identifier number
Connect State	describes the connectivity state of a cable modem. The table below describes the 20 cable modem connectivity states supported on the BSR.
Mac Address	cable modem Media Access Control layer address
Registration Time	the length of time a cable modem has been registered in *ddd:hh:mm:ss format*
TxKbytes	the number of unicast Kbytes that have been transmitted
RxKbytes	the number of unicast Kbytes that have been received

The following is an example of typical screen output from the **show cable modem stats** command:

```
Interface        Prim Connect    Mac Address    Registration  Tx        Rx
                 Sid  State                     Time          Kbytes    Kbytes
Cable  4/1/D1U1   8  online(pt) 000b.0643.3bb2   000:19:08:35       154     269
```

Cable modem connectivity states are as follows:

init(r1)	CM sent initial ranging parameters.
init(r2)	CM is ranging.
init(rc)	ranging is complete.
dhcp(d)	DHCP Discover was sent by CM.
dhcp(o)	DHCP Offer was received.
dhcp(req)	DHCP Request was sent by CM.

dhcp(ack)	DHCP Ack was received, IP address was assigned by DHCP server.
init(o)	option file transfer was started.
init(t)	Time-of-day (TOD) exchange was started.
online	CM registered; enabled for data.
online(d)	CM registered, but network access for the CM is disabled.
online(un)	CM registered, but not enabled data. Fail to verify modem's identity by BPI module.
online(pk)	CM registered; baseline privacy interface (BPI) enabled, and key encryption key (KEK) is assigned.
online(pt)	CM registered; BPI enabled, and traffic encryption key (TEK) is assigned.
reject(m)	CM did attempt to register; registration was refused due to bad mic.
reject(c)	CM did attempt to register; registration was refused due to bad COS.
reject(r)	CM did attempt to register, registration was refused due to unavailable resource.
reject(pk)	KEK modem key assignment is rejected.
reject(pt)	TEK modem key assignment is rejected.
offline	CM is considered to be offline.

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show cable modem {*<X/Y>* | *<mac>* | *<prefix>*} **stats** [| {**begin** | **exclude** | **include**} {*<WORD>*} [| {**count** | **count-only**}]]

show cable modem {<*X/Y*> | <*mac*> | <*prefix*>} **stats** [| {**count** | **count-only**}]

Command Syntax

X/Y	*X* is 0. *Y* is the port number.
mac	the cable modem MAC address
prefix	the IP address
|	turns on output modifiers (filters)
begin	filter for output that begins with the specified string
exclude	filter for output that excludes the specified string
include	filter for output that includes the specified string
WORD	the specified string
count	count the number of outputted lines
count-only	count the number of lines while suppressing screen output

show cable modem summary

The **show cable modem summary** command displays cable modem information for each cable interface on the BSR. The following is an example of typical screen output from the **show cable modem summary** command and descriptions of the output fields:

```
Interface                    Cable Modem
                  Total  Registered  Unregistered  Offline  SpecGrp
Cable  1/0/U0   227     134          3             90       Mansfield
Cable  1/0/U1   163     130          0             33       Mansfield
Cable  1/0/U2   151     137          0             14       Mansfield
Cable  1/0/U3   286     230          2             54       Mansfield
Cable  4/0/U0   57      45           0             12       Tewksbury
Cable  4/0/U1   83      49           0             34       Tewksbury
```

Interface	the BSR 2000 CMTS slot (always 0 for the BSR 2000), port, and upstream port number
Total	the total number of active, registered, and offline cable modems
Registered	the number of cable modems which have reached the Online(d), Online (pk), Online(pt) or Online(un) states
Unregistered	the number of cable modems in any Init, DHCP, Reject state or substate
Offline	the number of cable modems which have no state and are not communicating but were previously provisioned - these modems are assumed to be powered off
SpecGrp	the Spectrum Group name for each upstream channel.

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show cable modem summary [<*X/Y*> [**downstream** {<*NUM*>} | **total**]] [| {**begin** | **exclude** | **include**} {<*WORD*>} [| {**count** | **count-only**}]]

show cable modem summary [<*X/Y*> [**downstream** <*NUM*> | **total**]] [| {**count** | **count-only**}]

Command Syntax

X/*Y*	*X* is 0. *Y* is the port number.
|	turns on output modifiers (filters)
begin	filter for output that begins with the specified string
exclude	filter for output that excludes the specified string
include	filter for output that includes the specified string
WORD	the specified string
count	count the number of outputted lines
count-only	count the number of lines while suppressing screen output

show cable modem summary total

The **show cable modem summary total** command displays cable modem information for each cable interface on the BSR. The following is an example of typical screen output from the **show cable modem summary total** command and descriptions of the output fields:

```
Interface          Total          Active         Registered    SpecGrp
                   Modems         Modems         Modems        Name
Cable   2/0/U0     5              0              5             Mansfield
Cable   2/0/U1     2              0              2             Mansfield
Cable   3/0/U1     1              0              1             Tewksbury
Cable   3/0/U2     1              0              1             Tewksbury
Total              9              0              9
```

Interface	the BSR 2000 CMTS slot (always 0 for the BSR 2000), port, and upstream port number
Total Modems	the total number of active, registered, and offline cable modems
Active Modems	the number of cable modems in any Init, DHCP, Reject state or substate
Registered Modems	the number of cable modems which have reached the Online(d), Online (pk), Online(pt) or Online(un) states
SpecGrp	the Spectrum Group name for each upstream channel.

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show cable modem summary total [| {**begin** | **exclude** | **include**} {<*WORD*>} [| {**count** | **count-only**}]]

show cable modem summary total [| {**count** | **count-only**}]

Command Syntax

|	turns on output modifiers (filters)
begin	filter for output that begins with the specified string
exclude	filter for output that excludes the specified string
include	filter for output that includes the specified string
WORD	the specified string
count	count the number of outputted lines
count-only	count the number of lines while suppressing screen output

show cable modem svc-flow-id

The **show cable modem svc-flow-id** command displays the following information for all of the service flows associated with a specific MAC address:

Service flow id	the service flow identifier number
Interface	cable modem interface with active connection
Flow Direction	the flow direction for this service flow
Flow Max Rate	the maximum sustained traffic rate allowed for this service flow in bits/sec - no traffic rate limit for this service flow is indicated by "no restriction"

The following is typical output from the **show cable modem svc-flow-id** command:

```
Service flow id  Interface   Flow Direction   Flow Max Rate
              9  cable  0/1  Upstream                96000
             10  cable  0/1  Downstream                 10
```

Command Mode

All modes except User EXEC

Command Line Usage

show cable modem <*mac*> **svc-flow-id** [| {**begin** | **exclude** | **include**} {<*WORD*>} [| {**count** | **count-only**}]]

show cable modem <*mac*> **svc-flow-id** [| {**count** | **count-only**}]

Command Syntax

mac	cable modem Media Access Control layer address
|	turns on output modifiers (filters)
begin	filter for output that begins with the specified string
exclude	filter for output that excludes the specified string
include	filter for output that includes the specified string

WORD	the specified string
count	count the number of outputted lines
count-only	count the number of lines while suppressing screen output

show cable modem time-registered

The **show cable modem time-registered** command displays how long a cable modem has been registered. This command can be used to specify individual cable modems, cable modems associated with a particular BSR 2000 chassis slot, or cable modems associated with a particular Spectrum Group. The following information is provided:

Interface	cable modem interface with active connection
Connect State	describes the connectivity state of a cable modem. The table below describes the 20 cable modem connectivity states supported on the BSR.
Mac Address	cable modem Media Access Control layer address
Registration Time	the length of time a cable modem has been registered in *ddd:hh:mm:ss format*
Spectrum Group	the associated Spectrum Group name

Cable modem connectivity states are as follows:

online	CM registered; enabled for data.
online(d)	CM registered, but network access for the CM is disabled.
online(un)	CM registered, but not enabled data. Fail to verify modem's identity by BPI module.
online(pk)	CM registered; baseline privacy interface (BPI) enabled, and key encryption key (KEK) is assigned.
online(pt)	CM registered; BPI enabled, and traffic encryption key (TEK) is assigned.
reject(m)	CM did attempt to register; registration was refused due to bad mic.

reject(c)	CM did attempt to register; registration was refused due to bad COS.
reject(r)	CM did attempt to register, registration was refused due to unavailable resource.
reject(pk)	KEK modem key assignment is rejected.
reject(pt)	TEK modem key assignment is rejected.

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show cable modem time-registered {<*mac*> | <*X/Y*> | **slot** [<*NUM*>] | **spectrum-group** {<*WORD*>} } [| {**begin** | **exclude** | **include**} {<*WORD*>} [| {**count** | **count-only**}]]

show cable modem time-registered {<*mac*>| <*X/Y*> | **slot** [<*NUM*>] | **spectrum-group** {<*WORD*>} } [| {**count** | **count-only**}]

Command Syntax

mac	the MAC address of a particular cable modem
X/Y	*X* is 0. *Y* is the port number.
slot *NUM*	This number is always 0 for the BSR 2000.
spectrum-group *WORD*	the Spectrum Group name
|	turns on output modifiers (filters)
begin	filter for output that begins with the specified string
exclude	filter for output that excludes the specified string
include	filter for output that includes the specified string

WORD	the specified string
count	count the number of outputted lines
count-only	count the number of lines while suppressing screen output

show cable modem timing-offset

This **show cable modem timing-offset** command allows the user to select which cable modems are displayed on the console based on their timing offset value. The timing offset stored at the cable modem is the accumulation of all the timing adjustments sent to the cable modem. The cable modem starts at an initial timing offset which takes into account the cable modem's internal delays. The BSR cannot determine at what timing offset a particular cable modem starts and therefore the values stored and displayed by the BSR are the summation of the adjustments from the cable modem's initial timing offset. Since most manufacturers use a different initial timing offset value, the values stored by the BSR will vary per cable modem based on the manufacturer.

Note: The true timing offset that a CM is using should be read at the CM using SNMP. A CM with the highest recorded timing offset could be the furthest unit away from the BSR and be functioning correctly.

The **show cable modem timing-offset** command displays the following information about a cable modem:

Interface	cable modem interface with active connection
Prim Sid	Primary Service Identifier number
Connect State	describes the connectivity state of a cable modem. The table below describes the 20 cable modem connectivity states supported on the BSR
Timing Offset	current cable modem timing adjustment
Rec Power	cable modem receive downstream power level in dbmv
Ip address	cable modem IP address
Mac address	cable modem Media Access Control layer address

The following is typical output from the **show cable modem timing-offset** command:

```
Interface      Prim  Connect     Timing Rec    Ip Address      Mac Address
               Sid   State       Offset  Power
Cable  4/1/D1U1 6    online(pt)  581     0.1   150.31.101.44   000b.0643.3716
Cable  4/1/D1U1 9    online(pt)  581     0.1   150.31.101.45   000b.0643.3b60
Cable  4/1/D1U1 1    online(pt)  583     0.3   150.31.101.21   000b.0643.3b84
Cable  4/1/D1U1 2    online(pt)  583     0.1   150.31.101.17   000b.0643.3b90
Cable  4/1/D1U1 8    online(pt)  581     0.0   150.31.101.15   000b.0643.3bb2
```

Cable modem connectivity states are as follows:

init(r1)	CM sent initial ranging parameters.
init(r2)	CM is ranging.
init(rc)	ranging is complete.
dhcp(d)	DHCP Discover was sent by CM.
dhcp(o)	DHCP Offer was received.
dhcp(req)	DHCP Request was sent by CM.
dhcp(ack)	DHCP Ack was received, IP address was assigned by DHCP server.
init(o)	option file transfer was started.
init(t)	Time-of-day (TOD) exchange was started.
online	CM registered; enabled for data.
online(d)	CM registered, but network access for the CM is disabled.
online(un)	CM registered, but not enabled data. Fail to verify modem's identity by BPI module.
online(pk)	CM registered; baseline privacy interface (BPI) enabled, and key encryption key (KEK) is assigned.
online(pt)	CM registered; BPI enabled, and traffic encryption key (TEK) is assigned.
reject(m)	CM did attempt to register; registration was refused due to bad mic.

reject(c)	CM did attempt to register; registration was refused due to bad COS.
reject(r)	CM did attempt to register, registration was refused due to unavailable resource.
reject(pk)	KEK modem key assignment is rejected.
reject(pt)	TEK modem key assignment is rejected.
offline	CM is considered to be offline.

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show cable modem timing offset {**above | below**} *<0-500000>* [*<X/Y>*] [| {**begin | exclude | include**} {*<WORD>*} [| {**count** | **count-only**}]]

show cable modem timing offset {**above | below**} *<0-500000>* [*<X/Y>*] [| {**count** | **count-only**}]

Command Syntax

above	identify all cable modems with a timing offset above the entered number
below	identify all cable modems with a timing offset below the entered number
0-500000	the timing offset value
X/Y	*X* is 0. *Y* is the port number.
|	turns on output modifiers (filters)
begin	filter for output that begins with the specified string
exclude	filter for output that excludes the specified string

include	filter for output that includes the specified string
WORD	the specified string
count	count the number of outputted lines
count-only	count the number of lines while suppressing screen output

show cable modem unregistered

The **show cable modem unregistered** command displays the following information about unregistered cable modems:

Interface	cable modem interface with active connection
Prim Sid	Primary Service Identifier number
Connect State	describes the connectivity state of a cable modem. The table below describes the 20 cable modem connectivity states supported on the BSR.
Timing Offset	current cable modem timing adjustment
Rec Power	cable modem receive downstream power level in dbmv
Ip address	cable modem IP address
Mac address	cable modem Media Access Control layer address

Cable modem connectivity states are as follows:

init(r1)	CM sent initial ranging parameters.
init(r2)	CM is ranging.
init(rc)	ranging is complete.
dhcp(d)	DHCP Discover was sent by CM.
dhcp(o)	DHCP Offer was received.
dhcp(req)	DHCP Request was sent by CM.
dhcp(ack)	DHCP Ack was received, IP address was assigned by DHCP server.
init(o)	option file transfer was started.
init(t)	Time-of-day (TOD) exchange was started.
offline	CM is considered to be offline.

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show cable modem unregistered [| {**begin** | **exclude** | **include**} {<*WORD*>} [| {**count** | **count-only**}]]

show cable modem unregistered [| {**count** | **count-only**}]

Command Syntax

|	turns on output modifiers (filters)
begin	filter for output that begins with the specified string
exclude	filter for output that excludes the specified string
include	filter for output that includes the specified string
WORD	the specified string
count	count the number of outputted lines
count-only	count the number of lines while suppressing screen output

show cable modulation-profile

The **show cable modulation-profile** command displays all configured modulation profiles on the BSR. A modulation profile contains six burst profiles sent out in a UCD message to configure CM transmit parameters. The following is typical screen output from the **show cable modulation-profile** command:

```
Cable Modulation Profile 1
+--------------+------+------+------+------+------+------+------+------+
|              |  1   |  3   |  4   |  5   |  6   |  9   |  10  |  11  |
|          IUC | Req  | Init | Per  | Short| Long |  Adv |  Adv |  Adv |
|              |      | Maint| Maint| Data | Data | Short| Long |  UGS |
+--------------+------+------+------+------+------+------+------+------+
     Modulation   qpsk   qpsk   qpsk  16qam  16qam  64qam  64qam   XXXX
  Diff Encoding    OFF    OFF    OFF    OFF    OFF    OFF    OFF   XXXX
   Preamble Len     64    128    128    384    384    120    120   XXXX
    FEC Err CRC      0      5      5      5     10     12     16   XXXX
     FEC CW Len     16     34     34     78    235     75    220   XXXX
 Scrambler Seed    338    338    338    338    338    338    338   XXXX
      Max Burst      0      0      0      8      0      6      0   XXXX
     Guard Time      8     48     48      8      8      8      8   XXXX
  Last Codeword  FIXED  FIXED  FIXED  SHORT  SHORT  SHORT  SHORT   XXXX
      Scrambler     ON     ON     ON     ON     ON     ON     ON   XXXX
    Intlv Depth      1      1      1      1      1      1      1   XXXX
   Intlv Blk Sz   1536   1536   1536      0      0   1536   1536   XXXX
  Preamble Type  QPSK0  QPSK0  QPSK0   NONE   NONE  QPSK1  QPSK1   XXXX
 SCDMA Spreader    OFF    OFF    OFF    OFF    OFF    OFF    OFF   XXXX
   Codes Subfrm      0      0      0      0      0      0      0   XXXX
   Intlv Stp Sz      0      0      0      0      0      0      0   XXXX
   TCM Encoding    OFF    OFF    OFF    OFF    OFF    OFF    OFF   XXXX
   Channel Type  mtdma  mtdma  mtdma  mtdma  mtdma  mtdma  mtdma   XXXX
```

The **show cable modulation-profile** command displays the following modulation profile group information::

Modulation	the upstream modulation type
Diff Encoding	indicates if differential encoding is enabled/disabled
Preamble Len	the preamble length in bits
FEC Err CRC	the number of corrected Forward Error Correction (FEC) errors
FEC CW Len	the FEC code word length in bytes
Scrambler Seed	the scrambler seed in decimal format
Max Burst	the maximum burst length in minislots
Guard Time	Guard time size
Last Codeword	Last codeword shortened
Scrambler	Scramble enabled indication
Intlv Depth	the interleaver depth value
Intlv Blk Sz	the interleaver block size value
Preamble Type	the preamble type: NONE, QPSK0, QPSK1
SCDMA Spreader	enabled/disabled SCDMA spreader
Codes Subfrm	the codes subframe value
Intlv Stp Sz	the interleaver step size value
TCM Encoding	enabled/disabled TCM encoding
Channel Type	the channel type: atdma, mtdm, scdma, tdma

Note: For a complete list and configuration of all 23 pre-defined modulation profiles, refer to Appendix A, Pre-Defined Modulation Profiles of the *BSR 2000 Configuration and Management Guide*.

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show cable modulation-profile [<*1-600*> [<*1-11*>]]

Command Syntax

1-600	the modulation profile number
1-11	a specific IUC code: 1 = Request Burst 3 = Initial Maintenance 4 = Station Maintenance 5 = Short Grant Burst 6 = Long Grant Burst 9 = Advanced PHY Short Data Grant 10 = Advanced PHY Long Data Grant 11 = Unsolicited Grant Service

show cable modulation-profile brief

The **show cable modulation-profile brief** command displays cursory information for all configured modulation profiles on the BSR. The **show cable modulation-profile brief** command displays which modulation profiles are pre-defined, pre-defined but modified by the user, or user configured as shown in the sample commnad output below:

```
Profile     Chan-type  Config-status          In-use
1           tdma       pre-defined            yes
2   to 4    tdma       pre-defined
5           tdma       user-configured
6           tdma       user-configured
101         mtdma      pre-defined, changed
102 to 104  mtdma      pre-defined
201 to 205  atdma      pre-defined
301 to 310  scdma      pre-defined
```

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show cable modulation-profile brief

show cable privacy auth

The **show cable privacy auth** command displays the AK grace time and life time values, in seconds. The following is an example of typical screen output from the **show cable privacy auth** command:

```
Interface Cable 0/0
 Auth grace time: 600
 Auth life  time: 604800
```

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show cable privacy auth

show cable privacy cm-auth

The **show cable privacy cm-auth** command displays baseline privacy (BPI) authorization key (AK) information for an individual cable modem (CM) using its MAC address.

Group Access

All

Command Mode

Interface Configuration (cable interface only)

Command Line Usage

show cable privacy cm-auth [<*mac*>]

Command Syntax

mac	Cable modem's MAC address in the form of xxxx.xxxx.xxxx.

show cable privacy cmts

The **show cable privacy cmts** command displays all the baseline privacy statistics specified by the MIB for the cable interface.

The following is an example of typical screen output from the **show cable privacy cmts** command:

```
authGraceTime: 600
authLifeTime: 604800
tekGraceTime: 3600
tekLifeTime: 43200
certTrust: 2
certVerPeriod: 1
authCmtsReqs: 9
authCmtsReplys: 9
authCmtsRejects: 0
authCmtsInvalids: 0
authenInfos: 0
saMapReqs: 0
saMapReplys: 0
saMapRejects: 0
```

Group Access

All

Command Mode

Interface Configuration (cable interface only)

Command Line Usage

show cable privacy cmts

show cable privacy tek

The **show cable privacy tek** command shows Traffic Encryption Key (TEK) grace time and life-time values.

The following is an example of typical screen output from the **show cable privacy tek** command:

```
Interface Cable 0/0
 Tek grace time: 3600
 Tek life  time: 43200

Interface Cable 0/1
 Tek grace time: 3600
 Tek life  time: 43200
```

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show cable privacy tek

show cable qos profile

The **show cable qos profile** command displays the following information for all QoS Profiles or a selected user configurable QoS Profile:

Note: This command is only valid for DOCSIS 1.0, DOCSIS 1.0+, and Euro-DOCSIS 1.0 cable modems.

Prof Idx	the QoS Profile identifying number
Pri	the relative priority number assigned to upstream traffic by this QoS profile with 7 being the highest priority.
Max UP BW	the maximum upstream bandwidth
Guar UP BW	the guaranteed minimum upstream bandwidth
Max DOWN BW	the maximum downstream bandwidth.
Max tx burst	the maximum transmit burst size in bytes - valid range is from 0 (the default) to the largest 16-bit integer
BPI Mode	"true" indicates that Baseline Privacy is enabled for this QoS profile - "false" indicates that Baseline Privacy is not enabled for this Qos profile
Flow Count	the number of cable modems that have registered using this QoS Profile - active Qos Profiles are those with Flow Count = 0
Tos Mask	overwrites the Type of Service (TOS) field in IP datagrams received on the upstream before forwarding them downstream if the value is **not** "0"

Tos Value	the overwrite value substituted for the received TOS value.
Created By	"Oper" indicates a user configured QoS Profile and "Modem" indicates a QoS Profile learned from the cable modem during registration

The following is typical output from the **show cable qos profile** command:

```
Prof  Pri  Max      Guar     Max      Max      BPI    Flow  Tos   Tos    Created
Idx       UP       UP       DOWN     Tx       Mode   Count Mask  Value  By
          BW       BW       BW       Burst
1     1    0        0        0        0        false  0     0     0      Oper
3     1    0        0        0        0        false  0     0     0      Oper
```

Note: The "Prof Idx" field output indicates a *user configured* QoS Profile's unique identifying number in the range of 1-16. All QoS Profile identifying numbers in the range of 17-32 indicate a QoS Profile that was learned from cable modem registrations.

When using the **show cable qos profile** command to view the class of service configuration for DOCSIS 1.0, DOCSIS 1.0+, and Euro-DOCSIS 1.0 cable modems, you will obtain inconsistent results under the following conditions:

- If you have not given each user configurable QoS Profile a unique identifying number (in the range of 1 through 16) in the CM configuration file.
- When you modify a CM's configuration file and specify parameter values that are already in use by other registered modems and fail to change the QoS Profile identifying number to a unique value.

Note: All registered CMs are using the QoS parameters as defined in their respective configuration files and only the output from the **show cable qos profile** command is inconsistent.

Once all DOCSIS 1.0, DOCSIS 1.0+, and Euro-DOCSIS 1.0 cable modems have a a unique QoS Profile number, the display of the **show cable qos profile** command is accurate.

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show cable qos profile [<*NUM*> [<*1-32*> [**mac**]]]

Note: The **show cable qos profile** command without any argumanets displays all user-configured QoS profiles on the BSR regardless of whether they are in use. The **show cable qos profile** command without arguments does not display any QoS profiles that have been learned via modem registration.

The **show cable qos profile** command with the <*NUM*> argument displays all active Qos Profiles either user-configured or learned via modem registration for the specified CMTS slot.

Command Syntax

NUM	This number is always 0 for the BSR 2000.
1-32	the QoS Profiles's identifying number based on a valid range of defined service classes - numbers 1-16 are user configured and numbers 17-32 are learned by the CMTS during cable modem registration
mac	adds the MAC addresses of the cable modems to the display

show cable qos svc-flow classifier

A service flow classifier matches a packet to a service flow using a service flow reference. The service flow reference associates a packet classifier encoding with a service flow encoding to establish a SFID. Classifiers have the following features:

- Classifiers are loosely ordered by priority.
- Several classifiers can refer to the same service flow.
- More than one classifier may have the same priority.
- The CMTS uses a downstream classifier to assign packets to downstream service flows.
- The CM uses an upstream classifier to assign packets to upstream service flows.

The **show cable qos svc-flow classifier** command is used to display the packet classifiers of a service flow configured on the cable interface.

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show cable qos svc-flow classifier [<*X/Y*> [<*1-4292967295*> [<*1-65535*>]]]

Note: If the Classifier ID is not given, all the classifiers with the given SFID are listed.

Command Syntax

X/Y	*X* is 0. *Y* is the CMTS port number.
1-4292967295	SFID
1-65535	Classifier identification

show cable qos svc-flow dynamic-stat

The show cable qos svc-flow dynamic-stat command displays the statistics for dynamic service additions, deletions, and changes for both upstream and downstream service flows.

The following is typical output from the **show cable qos svc-flow dynamic-stat** command:

```
Interface index:  294658
Qos DS Direction: 1
Qos DSA Reqests:  0
Qos DSA Rsps:     0
Qos DSA Acks:     0
Qos DSC Reqs:     0
Qos DSC Rsps:     0
Qos DSC Acks:     0
Qos DSD Reqs:     0
Qos DSD Rsps:     0
Qos dynamic adds:          0
Qos dynamic add fails:     0
Qos dynamic changes:       0
Qos dynamic change fails:  0
Qos dynamic deletes:       0
Qos dynamic delete fails:  0
```

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show cable qos svc-flow dynamic-stat

show cable qos svc-flow log

The **show cable qos svc-flow log** command displays the time that the service flow was created or deleted, the total number of packets counted, and the MAC address of the cable modem (CM) that used the service flow.

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show cable qos svc-flow log

show cable qos svc-flow param-set

The **show cable qos svc-flow param-set** command displays parameter settings for all service classes configured on an individual CMTS slot and port or all CMTS modules on the BSR.

The following is typical output from the **show cable qos svc-flow param-set** command:

```
Interface index:                294658
Qos service flow id:            1
Qos parameter set type:         Active
Qos parameter set bit map:      0xdc800000
Qos active timeout:             0
Qos admitted timeout:           200
Qos scheduling type:            Best Effort
Qos traffic priority:           5
Qos max traffic rate:           96000
Qos max traffic burst:          3044
Qos min reserved rate:          64000
Qos min reserved pkt size:      300
Qos max concatenated burst:     1522
Qos tos AND mask:               0xff
Qos tos OR mask:                0x0
Qos req/trans policy:           0x0
```

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show cable qos svc-flow param-set [*X*/*Y*] [*<1-4292967295>*]

Command Syntax

X/*Y*	*X* is 0. *Y* is the port number.
1-4292967295	service flow ID

show cable qos svc-flow phs

The **show cable qos svc-flow phs** command displays the payload header suppression (PHS) configured for an interface that is used for a specific service flow.

Note: If the PHS is not specified, all PHS entries with the specified SFIDs are listed.

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show cable qos svc-flow phs [<*X/Y*> [<*1-4292967295*> [<*1-65535*>]]]

Command Syntax

X/Y	*X* is 0. *Y* is the CMTS port number.
1-4292967295	SFID
1-65535	Classifier identification

show cable qos svc-flow statistics

The **show cable qos svc-flow statistics** command is used to determine the number of dropped packets due to downstream rate-limiting for a particular service flow.

The following is typical output from the **show cable qos svc-flow statistics** command:

```
Interface index:                        294658
Qos service flow id:                    1
Qos service flow packets:               605
Qos service flow octets:                321040
Qos service flow time created:          12906
Qos service flow time active:           79778
Qos service flow PHS unknowns:          0
Qos service flow policed drop packets:  0
Qos service flow policed delay packets: 0
Qos service flow class:                 DefRRUp
Qos service flow admit status:          Success
Qos service flow admit restrict time:   0
```

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show cable qos svc-flow statistics [<*X/Y*> [<*1-4292967295*>]]

Command Syntax

X/Y	*X* is 0. *Y* is the CMTS port number.
1-4292967295	SFID

show cable qos svc-flow summary

The **show cable qos svc-flow summary** command displays the service flow information, including the SID, and QoS parameters sets associated with the service flow.

The following is typical output from the **show cable qos svc-flow summary** command:

Group Access

```
Interface index:            294658
Qos service flow id:        1
Qos service flow SID:       2
Qos service flow direction: Upstream
Qos service flow primary:   True

Interface index:            294658
Qos service flow id:        2
Qos service flow SID:       0
Qos service flow direction: Downstream
Qos service flow primary:   True
```

All

Command Mode

All modes except User EXEC

Command Line Usage

show cable qos svc-flow summary [<*X/Y*> [<*1-4292967295*>]]

Command Syntax

X/Y	*X* is 0. *Y* is the CMTS port number.
1-4292967295	SFID

show cable qos svc-flow upstream-stat

The **show cable qos svc-flow upstream-stat** command is used to display the number of fragmented packets, incomplete fragmented packets, and the number of concatenated bursts counted on the service flow.

The following is typical output from the **show cable qos svc-flow upstream-stat** command:

```
Interface index:                294658
Qos service flow SID:           1
Qos upstream frag packets:      0
Qos upstream incomplete packets: 0
Qos upstream concat bursts:     0

Interface index:                294658
Qos service flow SID:           2
Qos upstream frag packets:      0
Qos upstream incomplete packets: 0
Qos upstream concat bursts:     0
```

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show cable qos svc-flow upstream-stat [<X/Y> [<*1-16383*>]]

Command Syntax

X/Y	*X* is 0. *Y* is the CMTS port number.
1-16383	Classifier identification

show cable spectrum-group

The **show cable spectrum-group** command is used to verify if the spectrum group that you assigned is activated for the upstream port.

The following is typical output from the **show cable qos svc-flow spectrum-group** command:

```
Spectrum Group: sg1
Member channels:

Schedule   Band                Schedule
Id         (Mhz)               From Time     To Time
1           5.000 - 42.000
```

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show cable spectrum-group [<*WORD*> [**map** | **schedule**]]

Command Syntax

WORD	The exact group name applied to the upstream port.
map	Show spectrum allocation map
schedule	Show spectrum schedule

show cable spectrum-group load-balance summary

This **show cable spectrum-group load-balance summary** command displays a summary of cable modem distribution and load balancing statistics for the spectrum group. The following is an example of typical screen output from the **show cable spectrum-group load-balance summary** command:

```
Spectrum Group: Mansfield
Static Load Balancing: enabled
Interface        Registered   Move      Move
                 Modems       Success   Failure
Cable   2/0/U0   3            1         0
Cable   2/0/U1   1            1         0
Cable   2/0/U2   6            3         0
Cable   2/0/U3   2            1         0
Total           12            6         0
```

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show cable spectrum-group <*WORD*> **load-balance summary**

Command Syntax

WORD	The Spectrum Group name.

show cable sync-interval

The **show cable sync-interval** command shows the configured sync-interval value between CMTS transmission of successive SYNC messages.

The following is an example of typical screen output from the **show cable sync-interval** command:

```
Cable sync-interval: 10
```

Group Access

All

Command Mode

Interface Configuration (cable interface only)

Command Line Usage

show cable sync-interval

show cable ucc-stats

The **show cable ucc-stats** command displays DOCSIS Upstream Channel Change (UCC) statistics for a MAC domain. The following is an example of typical screen output from the **show cable ucc-stats** command:

```
CMTS Slot:  0   MAC Domain: 1  Interface index: 58654976
Number of UCC Reqs  : 0
Number of UCC Rsps  : 0
Number of UCC       : 0
Number of UCC Fails : 0

CMTS Slot:  0  MAC Domain: 0  Interface index: 176095232
Number of UCC Reqs  : 0
Number of UCC Rsps  : 0
Number of UCC       : 0
Number of UCC Fails : 0

CMTS Slot:  0  MAC Domain: 1  Interface index: 176095488
Number of UCC Reqs  : 0
Number of UCC Rsps  : 0
Number of UCC       : 0
Number of UCC Fails : 0

CMTS Slot:  0  MAC Domain: 0  Interface index: 243204096
Number of UCC Reqs  : 0
Number of UCC Rsps  : 0
Number of UCC       : 0
Number of UCC Fails : 0
```

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show cable ucc-stats [<*X*/*Y*>]

Command Syntax

X/*Y*	*X* is 0. *Y* is the CMTS port number.

show cable ucd-interval

The **show cable usd-interval** command shows configured ucd-interval between transmission of successive UCD messages.

The following is an example of typical screen output from the **show cable ucd-interval** command:

```
Cable ucd-interval: 1000
```

Group Access

All

Command Mode

Interface Configuration (cable interface only)

Command Line Usage

show cable ucd-interval

show cable upstream

The **show cable upstream** command displays the following upstream cable information:

ifIndex	interface index
description	displays the user-defined description of the upstream port
centerFreq	center frequency for cable modem use
rng_back_st	initial ranging backoff fixed start value
rng_back_en	initial ranging backoff fixed end value
data_back_st	initial data backoff fixed start value
data_back_en	initial data backoff fixed end value
channelWidth	radio frequency channel width
powerLevel	power level in units of whole dB to one decimal place
slotSize	port minislot size in number of time ticks
force-frag	forced fragmentation enabled
map-interval	configured map interval value
pre-equalization	pre-equalization adjustment enabled
invited-range-interval	the number of invited range interval requests configured for this upstream channel
range-forced-continue	range forced continue enabled
range-power-override	specifies whether range power override is enabled (true) or disabled (false)
concatenation	specifies whether concatenation is on (true) or off (false).
physical-delay	the upstream physical delay configuration
rate-limit	upstream data transmission rate-limit

modulation-profile	physical layer profile characteristics
max-calls	the maximum number of voice calls configured for this upstream channel
Spectrum Group	displays the associated Spectrum Group name
modem ranging delay	the maximum ranging timing offset for a modem that is co-located with (next to) the CMTS, in microseconds.The range, 0 to 600 (with a default of 250), corresponds to ranging timing offsets in REFCLK units of 0 to 6144 (with a default of 2560).

The following is an example of typical screen output from the **show cable downstream** command:

```
ifIndex:                295173
description:
centerFreq:             22800000
rng_back_st:            0
rng_back_en:            4
data_back_st:           2
data_back_en:           8
channelWidth:           3200000
powerLevel:             0 (10th of dB)
slotSize:               4
force-frag:             0
map-interval:           4000
pre-equalization:       0
invited-range-interval: 10000
range-forced-continue:  0
range-power-override:   false
concatenation:          true
physical-delay:         Mode 0, Min 400, Max 1600
rate-limit:             0
modulation-profile:     1
max-calls:              0
Spectrum Group:
modem ranging delay:    250 (usec)
```

Group Access

All

Command Mode

Interface Configuration (cable interface only)

Command Line Usage

show cable upstream {<*NUM*> | <*X*/*Y*>}

Command Syntax

NUM	the upstream channel number
X/*Y*	*X* is 0. *Y* is the CMTS port number.

show docsis-version

The **show docsis-version** command displays the DOCSIS version of a slot in the BSR 2000 chassis. Returned values are DOCSIS 1.X (DOCSIS 1.0 or DOCSIS 1.1) and DOCSIS 2.0.

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show docsis-version <*0-0*>

Command Syntax

0-0	This number is always 0 for the BSR 2000.

show docstest

The **show docstest** command displays DOCSIS 2.0 testing information. A displayed value of "0" indicates that no test has been initiated.

Note: DOCSIS 2.0 test mode must be enabled with the **docstest enable** command before DOCSIS 2.0 testing information can be displayed.

Group Access

MSO

Command Mode

Privileged EXEC

Command Line Usage

show docstest

show interfaces cable

The **show interfaces cable** command displays the following cable interface information:

cable port up/ administratively down	cable modem active or taken down by administrator
up/administratively down	determines if software processes handling lineup/protocol down interface is operational or taken down by the administrator
hardware	hardware type and address
internet address	internet address then subnet mask
MTU	interface maximum transmission unit (MTU)
BW	bandwidth (BW) in kilobits per second
received broadcast	total number of broadcast or multicast packets that interface receives
cable	downstream interface location
downstream up/ administratively down	interface administrative state
packets output	number of packets transmitted from the interface
bytes	number of bytes transmitted from the interface
discarded	number of packets discarded
output errors	errors that prevented downstream transmission of packets from the interface
cable	upstream cable location
upstream up/ administratively down	upstream interface administrative status
received broadcasts	upstream interface broadcast packets received

multicasts	upstream interface multicast packets received
unicasts	upstream interface unicast packets received
discards	upstream interface discarded packets
errors	total errors preventing upstream interface transmission through interface
unknown protocol	upstream interface packets received through interface
packets input	upstream interface packets received through interface with no errors
corrected	upstream interface packets that were uncorrected
uncorrectable	upstream interface packets that were corrected
noise	corrupted packet as a result of line noise
microreflections	corrupted packets as a result of microreflections
guaranteed-rate	number of bandwidth requests queued in the guarantee-rate queue from modems that have minimum upstream rates for their class of service
best-effort service	number of bandwidth requests queued in the best-effort queue depth queue from modems without a reserved rate on the upstream interface
total modems	modems, active or inactive, sharing upstream channel on this channel
current total	reserved for modems sharing an upstream channel interface

bandwidth	requiring the QoS for that modem. Each time the modem connects to an upstream channel, the value for the guaranteed upstream value increments by the QoS rate.
snmp out packets	number of SNMP packets sent by the other router modem
packets too big	larger than maximum packet size sent by the router modem
no such name errors	name errors non-existent number, undefinable MIB
bad values errors	number of set requests that detail an invalid value for a MIB object
general errors	number of requests failed due to some other error, excluding a noSuchName error, badValue error, or any of the other specific errors
response	number of responses
trap	number of traps sent

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show interfaces cable <*X*/*Y*> [| {**begin** | **exclude** | **include**} {<*WORD*>} [| {**count** | **count-only**}]]

show interfaces cable <*X*/*Y*> [| {**count** | **count-only**}]]

Command Syntax

X/Y	*X* is 0. *Y* is the CMTS port number
|	turns on output modifiers (filters)
begin	filter for output that begins with the specified string
exclude	filter for output that excludes the specified string
include	filter for output that includes the specified string
WORD	the specified string
count	count the number of outputted lines
count-only	count the number of lines while suppressing screen output

show interfaces cable downstream

The **show interfaces cable downstream** command displays the following downstream cable information:

cable	downstream cable location
upstream up/ administratively down	downstream interface administrative status
packets output	number of packets transmitted from the interface
bytes	number of bytes transmitted from the interface
discarded	number of packets discarded
total active modems	total active cable modems on this downstream channel
Spectrum Group	the associated upstream Spectrum Group names

The following is an example of typical screen output from the **show interfaces cable downstream** command:

```
Cable 3/0: Downstream 0 is administratively down
  0 packet output, 0 bytes, 0 discarded
  0 total active modems
  Spectrum Group: N/A
```

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show interfaces cable <*X*/*Y*> **downstream** [<*0-0*>] [| {**begin | exclude | include**} {<*WORD*>} [| {**count** | **count-only**}]]

show interfaces cable <*X*/*Y*> **downstream** [<*0-0*>] [| {**count** | **count-only**}]

Command Syntax

X/*Y*	*X* is 0. *Y* is the port number
0-0	downstream port number
|	turns on output modifiers (filters)
begin	filter for output that begins with the specified string
exclude	filter for output that excludes the specified string
include	filter for output that includes the specified string
WORD	the specified string
count	count the number of outputted lines
count-only	count the number of lines while suppressing screen output

show interfaces cable intercept

Use the **show interfaces cable intercept** command to view statistical information for each intercepted Customer Premises Equipment (CPE) MAC address.

The **show interfaces cable intercept** command displays the following CPE information:

MAC Address	MAC (hardware) address of a CPE, such as a customer's PC or VoIP phone.
Destination IP Address	IP address of the data collection server.
Destination UDP Port	UDP Port number that is used exclusively by the data collection server.
Packets	The total number of packets that have been intercepted from each specified CPE on this CMTS interface.
Bytes	The total number of bytes that have been intercepted from each specified CPE on this CMTS interface.

Group Access

MSO

Command Mode

All modes except User EXEC mode.

Command Line Usage

show interfaces cable <*X*/*Y*> **intercept**

Command Syntax

X/*Y*	*X* is 0. *Y* is the CMTS port number

Command Default

None

show interfaces cable service-class

The **show interfaces cable service-class** command displays interface level service class information for all downstream and upstream service classes, downstream service classes, or upstream service classes. The following is an example of typical screen output from the **show interfaces cable service-class** command:

```
Dir Ch ClassName Pri Thr CAP MAB FreeBW Defer Succe Restr HighPri
================================================================
 Dn  0 DefBEDown   1   0   0   1   100%     0     0     0        0
 Dn  0 DefRRDown   1   0   0   1   100%     0     0     0        0
 Dn  0 DefEMDown   1   0   0   1   100%     0     0     0        0
 Dn  0    mass11   1   0   0  48   100%     0     0     0        0
 Dn  0    mass12   1   0   0  30   100%     0     0     0        0
 Dn  0    mass13   1   0   0  18   100%     0     0     0        0
----------------------------------------------------------------
 Up  0   DefBEUp   1   0   0   1   100%     0     0     0        0
 Up  0   DefRRUp   1   0 100   1   100%     0     0     0        0
 Up  0    DefUGS   1  20 100   1   100%     0     0     0        0
 Up  0  DefUGSAD   1   0  80   1   100%     0     0     0        0
 Up  0   DefRTPS   1   0 100   1   100%     0     0     0        0
 Up  0  DefNRTPS   1   0 100   1   100%     0     0     0        0
 Up  0   DefEMUp   1   0 100   1   100%     0     0     0        0
 Up  0     mass1   1   0   0  49   100%     0     0     0        0
 Up  0     mass2   1   0   0  30   100%     0     0     0        0
 Up  0     mass3   1   0   0  14   100%     0     0     0        0
----------------------------------------------------------------
 Up  1   DefBEUp   1   0   0   1   100%     0     0     0        0
 Up  1   DefRRUp   1   0 100   1   100%     0     0     0        0
 Up  1    DefUGS   1  20 100   1   100%     0     0     0        0
 Up  1  DefUGSAD   1   0  80   1   100%     0     0     0        0
 Up  1   DefRTPS   1   0 100   1   100%     0     0     0        0
 Up  1  DefNRTPS   1   0 100   1   100%     0     0     0        0
 Up  1   DefEMUp   1   0 100   1   100%     0     0     0        0
 Up  1     mass1   1   0   0  49   100%     0     0     0        0
 Up  1     mass2   1   0   0  30   100%     0     0     0        0
 Up  1     mass3   1   0   0  14   100%     0     0     0        0
```

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show interfaces cable <*X*/*Y*> **service-class** [**all** | **downstream** | **upstream**] [| {**begin** | **exclude** | **include**} {<*WORD*>} [| {**count** | **count-only**}]]

show interfaces cable <*X*/*Y*> **service-class** [**all** | **downstream** | **upstream**] [| {**count** | **count-only**}]

Command Syntax

X/*Y*	*X* is 0. *Y* is the CMTS port number.
all	display both upstream and downstream service class information
downstream	display downstream service class information only
upstream	display upstream service class information only
|	turns on output modifiers (filters)
begin	filter for output that begins with the specified string
exclude	filter for output that excludes the specified string
include	filter for output that includes the specified string
WORD	the specified string
count	count the number of outputted lines
count-only	count the number of lines while suppressing screen output

show interfaces cable upstream

The **show interfaces cable upstream** command displays the following upstream cable interface information:

Cable	upstream cable location
Upstream up/ administratively down	upstream interface administrative status
Received broadcasts	upstream interface broadcast packets received
Received multicasts	upstream interface multicast packets received
Received unicasts	upstream interface unicast packets received
discarded	upstream interface discarded packets
errors	total errors preventing upstream transmission of packets
unknown protocol	packets received that were generated using a protocol unknown to the BSR 2000
Avg upstream channel utilization	the average percentage of upstream channel utilization
packets input	total packets received through the upstream interface with no errors
Total Modems On This Upstream Channel	active or inactive cable modems on this upstream channel
Spectrum Group	the associated Spectrum Group name

The following is an example of typical screen output from the **show interfaces cable upstream** command:

```
Cable 0/1: Upstream 1 is up
  Received 0 broadcasts, 0 multicasts, 0 unicasts
  0 discarded, 0 errors, 0 unknown protocol
  Avg upstream channel utilization : 0
  0 packets input
  Total Modems On This Upstream Channel: 0
  Spectrum Group:
```

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show interfaces cable <*X*/*Y*> **upstream** <*NUM*> [**signal-quality** | **spectrum** <*5000000-42000000*> <*5000000-42000000*>| **stats**] [| {**begin** | **exclude** | **include**} {<*WORD*>} [| {**count** | **count-only**}]]

show interfaces cable <*X*/*Y*> **upstream** <*NUM*> [**signal-quality** | **spectrum** <*5000000-42000000*> <*5000000-42000000*>| **stats**] [| {**count** | **count-only**}]

Command Syntax

X/*Y*	*X* is 0. *Y* is the port number.
NUM	the upstream channel number - 0,1,2,3,4,5,6,7
signal-quality	display signal-quality information
spectrum	view the noise power level for the whole spectrum.
5000000-42000000	start frequency in Hz
5000000-42000000	end frequency in Hz
stats	display upstream statistical information

|	turns on output modifiers (filters)
begin	filter for output that begins with the specified string
exclude	filter for output that excludes the specified string
include	filter for output that includes the specified string
WORD	the specified string
count	count the number of outputted lines
count-only	count the number of lines while suppressing screen output

show stats cmts

The **show stats cmts** command displays the following upstream and downstream statistical information:

Upstream Statistics

cable	upstream cable location
upstream up/ administratively down	upstream interface administrative status
Received broadcasts	upstream interface broadcast packets received
Received multicasts	upstream interface multicast packets received
Received unicasts	upstream interface unicast packets received
discarded	upstream interface discarded packets
errors	total errors preventing upstream transmission of packets
unknown protocol	packets received that were generated using a protocol unknown to the BSR 2000
Total Modems On This Upstream Channel	total active or inactive cable modems on this upstream channel
Spectrum Group	the associated Spectrum Group name

Downstream Statistics

cable	downstream cable location
downstream up/ administratively down	downstream interface administrative status
packets output	number of packets transmitted from the interface
bytes	number of bytes transmitted from the interface

discarded	number of packets discarded
total active modems	total active cable modems on this downstream channel
Spectrum Group	the associated upstream Spectrum Group names

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show stats <*NUM*> **cmts** [| {**begin | exclude | include**} {<*WORD*>} [| {**count** | **count-only**}]]

show stats <*NUM*> **cmts** [| {**count** | **count-only**}]

Command Syntax

NUM	This number is always 0 for the BSR 2000.
|	turns on output modifiers (filters)
begin	filter for output that begins with the specified string
exclude	filter for output that excludes the specified string
include	filter for output that includes the specified string
WORD	the specified string
count	count the number of outputted lines
count-only	count the number of lines while suppressing screen output

show stats summary error

The **show stats summary error** command displays the following statistical information on FEC (forward error correction) errors:

MAC Address	MAC Address of the cable modem
I/F	interface on which the cable modem has an active connection
SID	Service ID number
CorrFec Count	the number of correctable forward error correction (FEC) errors
CorrFec Ratio	correctable forward error correction ratio
UnCorrFec Count	the number of uncorrectable forward error correction (FEC) errors
UnCorrFec Ratio	correctable forward error correction ratio

The following is an example of typical screen output from the **show stats summary error** command:

```
MAC Address     I/F     SID    CorrFec    CorrFec     UnCorrFec    UnCorrFec
                                Count       Ratio       Count        Ratio
000b.0643.36c8  0/0/U2  5      0          0.00000000  0            0.00000000
000b.0643.3716  0/0/U2  8     0          0.00000000  6330272      0.00000000
000b.0643.375a  0/0/U3  20     0          0.00000000  0            0.00000000
000b.0643.3766  0/0/U3  6      0          0.00000000  0            0.00000000
000b.0643.3ac6  0/0/U3  11     0          0.00000000  0            0.00000000
000b.0643.3b60  0/0/U0  12     0          0.00000000  0            0.00000000
000b.0643.3b72  0/0/U2  10     0          0.00000000  6330272      0.00000000
000b.0643.3b78  0/0/U1  7      0          0.00000000  0            0.00000000
000b.0643.3b84  0/0/U1  15     0          0.00000000  0            0.00000000
000b.0643.3b90  0/0/U1  13     0          0.00000000  0            0.00000000
000b.0643.3b9a  0/0/U0  14     0          0.00000000  0            0.00000000
000b.0643.3bb2  0/0/U0  9      0          0.00000000  0            0.00000000
000b.063b.b320  0/1/U7  7      0          0.00000000  0            0.00000000
000b.0643.33fc  0/1/U4  2      0          0.00000000  0            0.00000000
000b.0643.361a  0/1/U5  19     0          0.00000000  0            0.00000000
000b.0643.3718  0/1/U4  5      0          0.00000000  0            0.00000000
000b.0643.3bb0  0/1/U5  4      0          0.00000000  0            0.00000000
0020.4027.a15c  0/1/U7  6      0          0.00000000  0            0.00000000
0020.409a.24f0  0/1/U6  3      0          0.00000000  0            0.00000000
0020.409a.760c  0/1/U6  17     0          0.00000000  0            0.00000000
```

Group Access

All

Command Mode

Privileged EXEC

Command Line Usage

show stats summary error [**sid** *<1-2049>*]

Command Syntax

sid *1-2049*	the Service ID number

snr display

The **snr display** command displays SNR measurement data to a console or telnet session. SNR measurement data is retrieved either from an operational CMTS module or a file system.

Group Access

MSO

Command Mode

Privileged EXEC

Command Line Usage

snr display {<*NUM*>{<*NUM*>}} | **flash:**<**filename**> <*WORD*> | **loop-data** {<*NUM*>{<*NUM*>}} | **nvram:**<**filename**> <*WORD*>}

Command Syntax

NUM	This number is always 0 for the BSR 2000.
NUM	valid upstream port number
flash:<**filename**>	retrieve the SNR measurement data from the Flash file system
loop-data	displays SNR loop measurement data
nvram:<**filename**>	retrieve the SNR measurement data from the NVRAM file system
WORD	SNR measurement data filename - limit of 20 characters excluding the "`.snr`" filename extension

snr loop

The **snr loop** command allows an operator to perform SNR measurements for a specified number of times on one particular frequency.

Group Access

MSO

Command Mode

Privileged EXEC

Command Line Usage

snr loop {<*NUM*>} {<*NUM*>}{<*NUM*>}{<*NUM*>}{<*frequency*>} {**1600000** | **200000** | **3200000** | **400000** | **6400000** | **800000**} [<*mac*> | **equalization** {**off** | **on**} | **ingress-cancel** {**off** | **on**} | **modulation-type** {**16qam** | **qpsk**}]

Command Syntax

NUM	This number is always 0 for the BSR 2000.
NUM	valid upstream port number (0-3)
NUM	the number SNR measurement repetitions (1-100)
NUM	a ranging pattern number used to look up a certain pattern to be used for SNR measurement
frequency	the particular frequency to perform SNR measurements on
1600000	channel width 1600 kHz
200000	channel width 200 kHz
3200000	channel width 3200 kHz
400000	channel width 400 kHz
6400000	channel width 6400 kHz
800000	channel width 800 kHz

mac	the MAC address, in the form of xxxx.xxxx.xxxx, of a device to perform SNR measurements on
equalization	**off -** perform SNR measurements without equalization **on -** eperform SNR measurements with equalization
ingress-cancel	**off -** perform SNR measurements without ingress cancellation **on -** perform SNR measurements with ingress cancellation
modulation-type	**16qam** - perform SNR measurements for 16qam mode **qpsk** - perform SNR measurements for QPSK mode

snr setup

The **snr setup** command is used to configure SNR measurement on the BCM3138/ BCM3140 chip set.

Group Access

MSO

Command Mode

Privileged EXEC

Command Line Usage

snr setup {*<NUM>*{*<NUM>*}} {*<5000000-42000000>* | *<5000000-65000000>* | *<5000000-55000000>*} {*<5000000-42000000>* | *<5000000-65000000>* | *<5000000-55000000>*} {**1600000** | **200000** | **3200000** | **400000** | **6400000** | **800000**} [**equalization** {**auto** | **off** | **on**}| **ingress-cancel** {**auto** | **off** | **on**} | **modulation-type** {**16qam** | **auto** | **qpsk**}]

Note: Depending on the configuration of the BSR 2000, the start and end frequencies will reflect the North American DOCSIS, EURODOCSIS, or J-DOCSIS standards

Command Syntax

NUM	This number is always 0 for the BSR 2000.
NUM	valid upstream port number
5000000-42000000	is the North America standard start frequency in Hz
5000000-42000000	is the North America standard end frequency in Hz.
5000000-65000000	is the EURODOCSIS standard start frequency in Hz
5000000-65000000	is the EURODOCSIS standard start frequency in Hz

5000000-55000000	is the J-DOCSIS standard start frequency in Hz
5000000-55000000	is the J-DOCSIS standard end frequency in Hz.
1600000	channel width 1600 kHz
200000	channel width 200 kHz
3200000	channel width 3200 kHz
400000	channel width 400 kHz
6400000	channel width 6400 kHz
800000	channel width 800 kHz
equalization	**auto -** evaluate the SNR with and without equalization **off -** evaluate the SNR without equalization **on -** evaluate the SNR with equalization
ingress-cancel	**auto** evaluate the SNR with and without ingress cancellation **off -** evaluate the SNR without ingress cancellation **on -** evaluate the SNR with ingress cancellation
modulation-type	**16qam** - evaluate the SNR for 16qam mode **auto** - evaluate the SNR for both QPSK and 16QAM modes **qpsk** - evaluate the SNR for QPSK mode

snr setup-get

The **snr setup-get** command dispalys the current SNR measurement feature configuration.

Group Access

MSO

Command Mode

Privileged EXEC

Command Line Usage

snr setup-get [<*NUM*> [<*NUM*>]]

Command Syntax

NUM	This number is always 0 for the BSR 2000.
NUM	valid upstream port number

snr start

The **snr start** command initiates SNR measurement via the RF Sentry

Group Access

MSO

Command Mode

Privileged EXEC

Command Line Usage

snr start {<*NUM*>{<*NUM*>}} [<*mac*>]

Command Syntax

NUM	This number is always 0 for the BSR 2000.
NUM	valid upstream port number
mac	MAC address of the reference modem in the form of `xxxx.xxxx.xxxx`

snr store

The **snr store** command saves the latest SNR measurement data for a 2x8 CMTS module to a file system. The user specifies a particular slot and port, the file system (NVRAM or Flash), and a file name without any extension to be used to store the SNR measurement data. An extension of ".snr" will be automatically added to the file name.

Group Access

MSO

Command Mode

Privileged EXEC

Command Line Usage

snr store {<*NUM*>{<*NUM*>}} {**flash:**<**filename**> <*WORD*> | **nvram:**<**filename**> <*WORD*>}

Command Syntax

NUM	This number is always 0 for the BSR 2000.
NUM	valid upstream port number
flash:<**filename**>	store the SNR measurement data from the Flash file system
nvram:<**filename**>	store the SNR measurement data from the NVRAM file system
WORD	SNR measurement data filename - limit of 20 characters excluding the "`.snr`" filename extension

spreader on

The **spreader on** command enables or disables the spreader for this S-SDMA channel.

Group Access

MSO

Command Mode

Modulation Profile Configuration

Command Line Usage

spreader on

no spreader on

tcm-encoding on

The **tcm encoding on** command enables trellis-coded modulation (TCM) for this S-CDMA channel. The trellis-coded modulation technique partitions the constellation into subsets called cosets so as to maximize the minimum distance between pairs of points in each coset. The **no tcm encoding on** command disables trellis-coded modulation (TCM) for this S-CDMA channel.

Group Access

MSO

Command Mode

Modulation Profile Configuration

Command Line Usage

tcm encoding on

no tcm encoding on

time band

The **time band** command is used to schedule when a spectrum group band is available. The spectrum group band can be made available on either a daily or weekly schedule.

Group Access

MSO

Command Mode

Cable Spectrum Group

Command Line Usage

time {*<day>* | *<hh:mm:ss>*} **band** *<5000000-42000000> <5000000-42000000>*

no time {*<day>* | *<hh:mm:ss>*} **band** *<5000000-42000000> <5000000-42000000>*

Command Syntax

day	The three letter abbreviation for day of the week.
hh:mm:ss	The time during the day when the band becomes available.
5000000-42000000	The start upstream frequency in Hertz.
5000000-42000000	The end upstream frequency in Hertz.

time delete

The **time delete** command can be used to schedule the time when the spectrum group band is removed on a daily or weekly basis.

Group Access

MSO

Command Mode

Cable Spectrum Group

Command Line Usage

time {*<day> <hh:mm:ss>*} **delete** *<5000000-42000000> <5000000-42000000>*

no time {*<day> <hh:mm:ss>*} **delete** *<5000000-42000000> <5000000-42000000>*

Command Syntax

day	The three letter abbreviation for day of the week.
hh:mm:ss	*The time during the day when the band is removed.*
5000000-42000000	The start upstream frequency in Hertz.
5000000-42000000	The end upstream frequency in Hertz.

12

BGP Commands

Introduction

This chapter describes the Border Gateway Protocol version 4 (BGP-4) commands used with the BSR.

BGP is an Inter-Autonomous System (AS) routing protocol that exchanges network availability information with any other router speaking BGP. The information for a network is the complete list of ASs that traffic must transport to reach that network and is then used to assure loop-free paths. This information is used to construct a graph of AS connectivity from which routing loops may be pruned, and some policy decisions at the AS level may be enforced.

BGP Command Descriptions

This section contains an alphabetized list and descriptions of the BGP commands supported by the BSR.

aggregate-address

The **aggregate-address** command creates an entry in the BGP routing table. The **no aggregate-address** command disables this function. Use the **aggregate-address** command to implement aggregate routing by redistributing the route in BGP.

Group Access

ISP

Command Mode

Router Configuration

Command Line Usage

aggregate-address <*A.B.C.D*> <*A.B.C.D*> [**advertise-map** <*WORD*>] [**as-set**] [**attribute-map** <*WORD*>] [**summary-only**] [**suppress-map** <*WORD*>]

no aggregate-address <*A.B.C.D*> <*A.B.C.D*> [**advertise-map** <*WORD*>] [**as-set**] [**attribute-map** <*WORD*>] [**summary-only**] [**suppress-map** <*WORD*>]

Command Syntax

A.B.C.D	aggregate address in routing table
A.B.C.D	aggregate mask in routing table
advertise-map *WORD*	name of route map to choose the routes to include into the aggregate and generate associated attributes if **as-set** is specified
attribute-map *WORD*	route map name to establish aggregate route attribute
as-set	generates AS set path information
summary-only	creates aggregate route and suppresses advertisements of all aggregated, more specific routes
suppress-map *WORD*	suppresses chosen, specific routes

Command Default

Disabled

auto-summary

The **auto-summary** command returns the user back to the automatic summarization default of subnet routes into network-level routes. The **no auto-summary** command disables this function.

When the route is summed up, it reduces the amount of routing information in the routing tables. Use the **network** command or the **no auto-summary** command to advertise and transmit subnet routes in BGP. BGP will not accept subnets distributed from IGP.

If a **network** command is not entered, and auto-summarization is disabled, network routes will not be advertised for networks with subnet routes unless they contain a summary route.

Group Access

ISP

Command Mode

Router Configuration

Command Line Usage

auto-summary

no auto-summary

Command Default

Enabled

bgp always-compare-med

The **bgp always-compare-med** command enables comparison of the Multi-exit Discriminator (MED) from path entries from different ASs. The **no bgp always-compare-med** command stops comparisons.

Use the **bgp always-compare** MED command to change the default, allowing comparison of MEDs, which are received from any autonomous system. By default, during the best-path selection process, MED comparison is done only among paths from the same autonomous system. This command changes the default behavior by allowing comparison of MEDs among paths regardless of the autonomous system from which the paths are received.

The MED path, considered the best path, is the parameter used when selecting the paths compared to many other options. The preference between a path with a lower MED and a path with a higher MED, is the lower MED path.

Group Access

ISP

Command Mode

Router Configuration

Command Line Usage

bgp always-compare-med

no bgp always-compare-med

bgp confederation identifier

The **bgp confederation identifier** command configures a BGP confederation identifier. The **no bgp confederation identifier** command removes a BGP confederation identifier.

Use the **bgp confederation identifier** command to reduce the IBGP mesh which splits an autonomous system into many autonomous systems. They are then grouped into an individual confederation. Each autonomous system is entirely engaged and has a small number of connections to other autonomous systems in the identical confederation. The confederation appears to be an individual autonomous system to all else.

Group Access

ISP

Command Mode

Router Configuration

Command Line Usage

bgp confederation identifier <*1-65535***>**

no bgp confederation identifier *<1-65535>*

Command Syntax

1-65535	autonomous system number to identify confederation as a whole

bgp confederation peers

The **bgp confederation peers** command configures the ASs that belong to the confederation. The **no bgp confederation peer** command removes an AS from the confederation.

Use the **bgp confederation peers** command to configure the ASs that belong to a confederation. Autonomous systems specified in this command are visible internally to a confederation. Each autonomous system is fully meshed within itself. The BGP confederation identifier command specifies the confederation to which the autonomous systems belong.

Group Access

ISP

Command Mode

Router configuration

Command Line Usage

bgp confederation peers <*1-65535*>

no bgp confederation peers <*1-65535*>

Command Syntax

1-65535	autonomous system number

bgp dampening

The **bgp dampening** command enables BGP route dampening. The **no bgp dampening** command to sets the default values or disables this function.

Note: The penalty is halved after the half-life period when a route is flapping. The router configured for damping (dampening) assigns a penalty to a route when a route flaps. Penalties are cumulative and are stored in the BGP routing table. A flapping route is suppressed when its penalty exceeds the suppress limit. A suppressed route is reused when its decayed penalty falls below the reuse limit.

Group Access

ISP

Command Mode

Router Configuration

Command Line Usage

bgp dampening [*<1-45> <1-20000> <1-20000> <1-255>*| **route-map <***WORD***>**]

no bgp dampening

Command Syntax

1-45	half-life period in minutes, each time a route is assigned a penalty, the penalty is decreased by half after the half-life period in 5 second intervals, with penalties being cumulative
1-20000	allows route to be reused if penalty for flapping route falls below reuse value
1-20000	route suppresses when its penalty exceeds this value
1-255	maximum suppression time in minutes
route-map *WORD*	route map name

Command Default

half life	=	15 minutes
route reuse	=	750
route suppression	=	2000
maximum suppression time	=	4 times the half-life

bgp default local-preference

The **bgp default local-preference** command changes the default local preference value which is sent to all routers in the local ASs. The **no bgp default local-preference** command configures a default local preference value.

Group Access

ISP

Command Mode

Router Configuration

Command Line Usage

bgp default local-preference <*0-4294967295*>

no bgp default local-preference <*0-4294967295*>

Command Syntax

0-4294967295	local preference value (higher values receive preference)

bgp permit

The **bgp permit** command permits updates with either the AGGREGATOR attribute set to the 0 Autonomous System (AS) or with the 0.0.0.0 address in the BGP routing process. The **no bgp permit** command disables the updates.

Group Access

ISP

Command Mode

Router Configuration

Command Line Usage

bgp permit [**aggregator-AS-0** | **aggregator-address-0**]

no bgp permit [**aggregator-AS-0** | **aggregator-address-0**]

Command Syntax

aggregator-AS-0	permits updates to AGGREGATOR attribute set with an AS of 0.
aggregator-address-0	permits updates with the AGGREGATOR attribute set with a 0.0.0.0 address.

Command Default

Disabled

bgp router-id

The **bgp router-id** command overrides a configured BGP router identifier (IP address) by manually configuring a new identifier. The **no bgp router-id** command restores the initial configuration.

Group Access

ISP

Command Mode

Router Configuration

Command Line Usage

bgp router-id <*A.B.C.D*>

no bgp router-id

Command Syntax

A.B.C.D	the new BGP router identifier (IP address)

clear ip bgp

The **clear ip bgp** command resets a BGP connection using soft reconfiguration.

Group Access

ISP

Command Mode

All Modes except User EXEC

Command Line Usage

clear ip bgp {***** | <*A.B.C.D*> | <*WORD*>}[**soft** [**in** | **out**]]

Command Syntax

*****	resets active BGP sessions
A.B.C.D	IP address of BGP neighbor to clear
WORD	name of a specific BGP peer group to clear the state
soft	reapply any export policies and sends refresh updates without clearing the state
in	inbound soft reconfiguration; reapply any import policies and send refresh updates without clearing the state
out	outbound soft reconfiguration

Command Default

Disabled

clear ip bgp dampening

The **clear ip bgp dampening** command clears route dampening information and unsuppress the suppressed routes.

Group Access

ISP

Command Mode

All Modes except User EXEC

Command Line Usage

clear ip bgp dampening [<*A.B.C.D*> | <*A.B.C.D*>]

Command Syntax

A.B.C.D	IP address of the network about which to clear dampening information
A.B.C.D	network mask applied to the above address

clear ip bgp flap-statistics

The **clear ip bgp flap-statistics** clears BGP flap statistics.

Group Access

ISP

Command Mode

All Modes except User EXEC

Command Line Usage

clear ip bgp flap-statistics [<*A.B.C.D*> | **filter-list** <*1-199*> | **regexp** <*LINE*>]

Command Syntax

A.B.C.D	network to clear flap statistics
filter-list	clear flap statistics for all the paths that pass the access list
1-199	clear flap statistics for all the paths that match the regular expression
regexp	clear flap statistics for all the paths that match the regular expression.
LINE	a regular-expression to match the BGP AS paths

default-information originate

The **default-information originate** command generates a default route into the BGP database. The **no default-information originate** command disables default route generation.

Group Access

ISP

Command Mode

Router Configuration

Command Line Usage

default-information originate

no default-information originate

Command Default

Disabled

default-metric

The default metric feature is used to eliminate the need for separate metric definitions for each routing protocol redistribution.The **default-metric** command forces the BGP routing protocol to use the same metric value for all distributed routes from other routing protocols. The **no default-metric** command removes or changes the default metric value for the BGP routing protocol.

Group Access

ISP

Command Mode

Router Configuration

Command Line Usage

default-metric <*1-4294967295*>

no default-metric

Command Syntax

1-4294967295	Default metric value.

distance bgp

The **distance bgp** command sets external, internal, and local administrative distances for routes to function. The **no distance bgp** command sets the default values.

Use the **distance bgp** command to administer distance based on the preferred routing information source received from a router or group of routers. This enables the system to prioritize protocols dependant upon the distances between 1 to 255, where 0 is the best route, and the most unreliable route is 255. The **bgp distance** command has an influence on whether the BGP-learned routes are installed in the routing table.

Note: It is recommended that the administrative distance not be changed.

Group Access

ISP

Command Mode

Router Configuration

Command Line Usage

distance bgp [*<1-255> < 1-255> <1-255>*]

no distance bgp

Command Syntax

1-255	administrative distance for routes external to the AS
1-255	administrative distance for routes external to the AS - routes with a distance of 255 are not installed in the routing table
1-255	administrative distance for local route

Command Default

external distance	=	20
internal distance	=	200
local distance	=	200

distribute-list in

The **distribute-list in** command filters networks received in routing updates. The **no distribute-list in** command changes or cancels the filters received in updates.

Group Access

ISP

Command Mode

Router Configuration

Command Line Usage

distribute-list *<1-199> <1300-2699>* **in**

no distribute-list *<1-199> <1300-2699>* **in**

Command Syntax

1-199	access list number
1300-2699	extended access list number
in	applies access list to incoming route updates

Command Default

Disabled

distribute-list out

The **distribute-list out** command prevents networks from being advertised in updates. The **no distribute-list out** command enables update advertisements.

Use the **distribute-list out** command to apply the access list to outgoing route updates.

Group Access

ISP

Command Mode

Router Configuration

Command Line Usage

distribute-list *<1-199> <1300-2699>* **out**

no distribute-list *<1-199> <1300-2699>* **out**

Command Syntax

1-199	access list number
1300-2699	extended access list number
out	applies access list to outgoing route updates

Command Default

Disabled

ip as-path access-list

The **ip as-path access-list** command creates or modifies a BGP related access list and its elements. The **no ip as-path access** command deletes the corresponding list element.

Use the **no ip as-path access-list** command to modify elements and add to the IP as-path access list of corresponding elements. Use the **ip as-path access-list** and the **neighbor filter-list** commands to use as-path filters to filter BGP advertisements.

Group Access

ISP

Command Mode

Global Configuration

Command Line Usage

ip as-path access-list <*1-199*> {**permit** <*LINE*> | **deny** <*LINE*>}

no ip as-path access <*1-199*>

Command Syntax

1-199	access list number
permit	permits access for matching conditions
deny	denies access to matching conditions
LINE	regular expression describing the as-paths to be matched

ip community-list

The **ip community-list** command creates a BGP related access list and its elements.There are two types of community lists: standard and extended. The standard community lists have a list number from 1 to 99. The extended community lists have a list number from 100 to 199. The **ip community-list** deletes the community lists and all associated elements.

The community lists are used in the **match community-list** command and the set communities' **set comm-list delete** commands. The route maps are used for inbound and outbound filtering.

Note: The community lists are related to the respective elements, and are of the standard and extended types:

Standard community lists:

To create a standard community list and its elements, use the **ip community-list** command. To delete the list element use the **no ip community-list** command.

If there is no elements left in the list, the list will be removed too. To delete the community list and all its elements use the **no ip community-list** command.

Extended community lists:

To create an extended community list and its elements use the **ip community-list** command. To delete the list element use the **no ip community-list** command. If there are no elements left in the list, the list will be removed too.

Group Access

ISP

Command Mode

Global Configuration

Command Line Usage

ip community-list *<1-99> <100-199>*{**permit** | **deny**} [*<1-4294967295>* | **internet** | **local-AS** | **no-export** | **no-advertise**]

no ip community-list *<1-99> <100-199>*{**permit** | **deny**} [*<1-4294967295>* | **internet** | **local-AS** | **no-export** | **no-advertise**]

Command Syntax

1-99	standard access list number,
100-199	extended access list number
permit	allows access for matching
deny	prevents access for matching
1-4294967295	a community number - you can specify a single number or multiple numbers separated by a space
internet	internet community
local-AS	do not advertise this route to peers outside of the local autonomous system
no-export	routes with this community are sent to peers in other sub-autonomous systems within a confederation
no-advertise	do not advertise this route to any peer internal or external

match as-path

The **match as-path** command matches a BGP autonomous system path access list match entries or appends new list numbers to the existing match entry. The **no match as-path** command removes the list numbers from the match entry used in the command.

Use the **match as-path** command to match a BGP autonomous system path to advertise on the route-map. Values can be set using the **match as-path** command.

Use the **match as-path** command to match at least one BGP autonomous system path to ensure advertisement on the route-map.

Use the **match as-path** command to globally replace values matched and set with the **match as-path c**ommand and the **set weight** command to supersede weights established with the **neighbor weight** and the **neighbor filter-list** commands.

The values set by the **match** and **set** commands override global values. For example, the weights assigned with the **match as-path** and **set weight** route-map commands override the weights assigned using the **neighbor weight** and **neighbor filter-list** commands. The implemented weight is established by the initial autonomous system match.

Group Access

ISP

Command Mode

Route-map Configuration

Command Line Usage

match as-path [<*1-199*>]

no match as-path [<*1-199*>]

Command Syntax

1-199	as-path list number - you can specify a single number or multiple numbers separated by a space

match community

The **match community** command creates a BGP autonomous system community access list match entry or appends new list numbers to the existing match entry. The **no match community** command removes the match entry completely. The no match community command removes the list numbers or the **exact-match** attribute from the match entry use the command

Use the **match community-list** command to ensure that the route is advertised for outbound and inbound route-maps. If a change to some of the information is to match is needed, configure a second route-map with specifics.

Group Access

ISP

Command Mode

Route-map Configuration

Command Line Usage

match community [*<1-99> <100-199>*] **exact-match**]

no match community [*<1-99> <100-199>*] **exact-match**]

Command Syntax

1-99	standard community list number
100-199	extended community list number
exact-match	exact match required; all of the communities and only those communities in the community list must be present

maximum-paths

The **maximum-paths** command specifies the maximum number of parallel routes an IP routing protocol can support. The **no maximum-paths** command changes or cancels the number of maximum paths.

Group Access

RESTRICTED

Command Mode

Router Configuration

Command Line Usage

maximum-paths <*1-2*>

no maximum-paths

Command Syntax

1-2	the maximum number of parallel routes

neighbor advertisement-interval

The **neighbor advertisement-interval** command sets the minimum amount of time between sending BGP routing updates. Use the **no neighbor advertisement-interval** form of this command to delete an entry.

Use the **neighbor advertisement-interval** command to configure all the members of the peer group with the same attributes.

Group Access

ISP

Command Mode

Router Configuration

Command Line Usage

neighbor {<*A.B.C.D*> | <*WORD*>} **advertisement-interval** <*0-600*>

no neighbor {<*A.B.C.D*> | <*WORD*>} **advertisement-interval** <*0-600*>

Command Syntax

A.B.C.D	neighbor IP address
WORD	neighbor peer-group-name
0-600	amount of time in seconds

Command Default

30 seconds for external peers

5 seconds for internal peers

neighbor confed-segment

The **neighbor confed-segment** command allows you configure a neighbor to use either AS confederation sequence or AS confederation set as the path segment type in the AS path attribute. The **no neighbor confed-segment** command disables the AS confederation path segment type attribute.

Group Access

ISP

Command Mode

Router Configuration

Command Line Usage

neighbor {<*A.B.C.D*>} **confed-segment** {**sequence** | **set**}

no neighbor {<*A.B.C.D*>} **confed-segment** {**sequence** | **set**}

Command Syntax

A.B.C.D	neighbor IP address
sequence	convert to AS_CONFED_SEQUENCE (rfc3065: value 3)
set	convert to AS_CONFED_SET (rfc3065: value 4)

Command Default

AS confederation path segment type attribute is disabled.

neighbor default-originate

The **neighbor default-originate** command allows a BGP speaker to send the default route 0.0.0.0 to a neighbor for the neighbor's default. The **no neighbor default-originate** command sends no route as a default.

The **neighbor default-originate** command does not require the presence of 0.0.0.0 in the local router, and when used with a route map, the default route 0.0.0.0 is injected only if the route map contains a **match ip address** clause and there is a route that matches the IP access list exactly. The route map can contain other match clauses also.

The user can use standard or extended access lists with the **neighbor default-originate** command.

Group Access

ISP

Command Mode

Router Configuration

Command Line Usage

neighbor {<*A.B.C.D*> | <*WORD*>} **default-originate** [**route-map** <*WORD*>]

no neighbor {<*A.B.C.D*> | <*WORD*>} **default-originate** [**route-map** <*WORD*>]

Command Syntax

A.B.C.D	neighbor IP address
WORD	peer group name
WORD	route map name

neighbor description

The **neighbor description** command provides a neighbor a description. The **no neighbor description** clears the provided neighbor description.

Group Access

ISP

Command Mode

Router Configuration

Command Line Usage

neighbor {<*A.B.C.D*> | <*WORD*>} **description** [*LINE*]

no neighbor {<*A.B.C.D*> | <*WORD*>} **description** [*LINE*]

Command Syntax

A.B.C.D	neighbor IP address
WORD	name of a BGP peer group
LINE	up to 80 characters in length to describe neighbor

neighbor distribute-list

The **neighbor distribute-list** command distributes BGP neighbor information based on the access list. The **no neighbor distribute-list** command deletes an entry.

Use the **neighbor distribute-list** command to filter BGP advertisements. Also, use the **ip as-path access-list** and the **neighbor filter-list** commands to use as-path filters to filter BGP advertisements. If a BGP peer group is specified, all members of that group are associated. Specifying the neighbor distribute-list command with an IP address to replace the value already in the peer group.

Group Access

ISP

Command Mode

Router Configuration

Command Line Usage

neighbor {*<A.B.C.D>* | *<WORD>*} **distribute-list** *<1-199>* *<1300-2699>* {**in** | **out**}

no neighbor {*<A.B.C.D>* | *<WORD>*} **distribute-list** *<1-199>* *<1300-2699>* {**in** | **out**}

Command Syntax

A.B.C.D	neighbor IP address
WORD	name of a BGP peer group
1-199	standard access list number between 1 and 199
1300-2699	expanded range access list number between 1300 and 2699
in	within the group
out	outside the group

neighbor ebgp-multihop

The **neighbor ebgp-mulithop** command accepts route updates from external peers residing on the network that are not directly connected. The **no neighbor ebgp-mulithop** command blocks route updates.

Use the **neighbor ebgp-multihop** command to modify BGP peer groups for unified configuration by specifying a peer-group-name.

Group Access

ISP

Command Mode

Router Configuration

Command Line Usage

neighbor {<*A.B.C.D*> | <*WORD*>} **ebgp-multihop** <*1-255*>

no neighbor {<*A.B.C.D*> | <*WORD*>} **ebgp-multihop** <*1-255*>

Command Syntax

A.B.C.D	IP address of external peer, BGP neighbor
WORD	external BGP group name
1-255	the maximum hop count - if no value is entered, the default value of 255 is used

neighbor filter-list

The **neighbor filter-list** command creates a BGP filter. The **no neighbor filter-list command** disables this function.

Use the **neighbor filter-list** command to create filters on both inbound and outbound BGP routes. Unlimited weight filters are accepted on a per-neighbor principle, but only one inbound or one outbound filter is accepted, not both. Route selection rules determine the weight of a route.

Weight assignment is based on the initial autonomous system path, or as-path. Weights announced override weights assigned by global **neighbor** commands. This happens when the initial match is made. Therefore, weights assigned using **match as-path** and **set weight** commands override weights assigned by the **neighbor weight** and **neighbor filter-list** commands.

Members of a peer group realize configured specifics when the *peer-group-name* argument is used with the **neighbor filter-list** command. If the **neighbor filter-list** command is used with a specified IP address, then the IP address overrides the value from the peer group.

Note: Using the command in the form, **no neighbor** {**ip-address** | **peer-group**} **filter-list** <*access-list-number*> **weight** [<*weight*>], the optional [<*weight*>] argument has no effect.

Using the command in the form, neighbor {**ip-address** | **peer-group**} **filter-list** [<*access-list-number*>] {**in** | **out** }, the optional [<*access-list-number*>] argument has no effect.

Group Access

ISP

Command Mode

Router Configuration

Command Line Usage

neighbor {<*A.B.C.D*> | <*WORD*>} **filter-list** <*1-199*> {**in** | **out** | **weight** <*0-65535*>}

no neighbor {<*A.B.C.D*> | <*WORD*>} **filter-list** <*1-199*> {**in** | **out** | **weight** <*0-65535*>}

Command Syntax

A.B.C.D	neighbor IP address
WORD	BGP peer group
1-199	filter list number
in	access list to incoming routes
out	access list to outgoing routes
weight *0-65535*	BGP weight metric assigned for competing incoming routes; accepted values are 0 to 65535; the largest weight is preferred

Command Default

Disabled

neighbor maximum-prefix

The **neighbor maximum-prefix** command controls the number of prefixes accepted from a neighbor. The **no neighbor maximum-prefix** command stops the controlled number of prefixes accepted from a neighbor.

Use the **neighbor maximum-prefix** command to manage the number of prefixes accepted from a neighbor.

Note: A prefix is a classless route or a route with a particular starting point and length, with unlimited prefixes. Therefore, 198.7.97.0/27 and 198.7.97.0/20 are **not** the same prefix (route). If the maximum number of acceptable prefixes configured is exceeded, the router ends peering, which is the default.

Group Access

ISP

Command Mode

Router Configuration

Command Line Usage

neighbor {*<A.B.C.D>* | *<WORD>*} **maximum-prefix** *<1-65536>* [*<1-100 >* | **warning-only**]

no neighbor {*<A.B.C.D>* | *<WORD>*} **maximum-prefix** *<1-65536>* [*<1-100>* | **warning-only**]

Command Syntax

A.B.C.D	neighbor IP address
WORD	name of BGP peer-group
1-65536	maximum number of configured prefixes allowed from specific neighbor

1-100	integer specifying what percentage of the maximum number that the router generates a warning message
warning-only	only generate a warning message when the maximum number is exceeded

Command Default

Disabled

Threshold default, 75%

neighbor next-hop-self

The **neighbor next-hop-self** command disables BGP processing updates. The **no neighbor next-hop-self** command enables BGP processing updates.

Note: Members of a peer group realize configured specifics when the *peer-group-name* argument is used with the **neighbor next-hop-self** command.

Specifying the command with an IP address will override the value inherited from the peer group. Use the **set ip next-hop** command for additional control.

Group Access

ISP

Command Mode

Router Configuration

Command Line Usage

neighbor {<*A.B.C.D*> | <*WORD*>} **next-hop-self**

no neighbor {<*A.B.C.D*> | <*WORD*>} **next-hop-self**

Command Syntax

A.B.C.D	neighbor IP address
WORD	name of neighbor peer-group

Command Default

Disabled

neighbor password

The **neighbor password** command enables the Message Digest 5 (MD5) authentication on a TCP connection between two BGP peers. The **no neighbor password** command disables the Message Digest 5 (MD5) authentication on a TCP connection between two BGP peers.

Use the **neighbor password** command to authenticate and to verify TCP connections between two BGP peers, of which the same password is configured. This command begins the MD5 generation for outgoing packets and check every segment on a TCP connection for incoming packets.

Group Access

ISP

Command Mode

Router Configuration

Command Line Usage

neighbor {<*A.B.C.D*> | <*WORD*>} **password** {**0** | **7** }<*LINE*>

no neighbor {<*A.B.C.D*> | <*WORD*>} **password** {**0** | **7**} <*LINE*>

Command Syntax

A.B.C.D	neighbor IP address
WORD	name of neighbor peer-group
0	specifies an UNENCRYPTED password will follow
7	specifies an ENCRYPTED password will follow
LINE	the unencrypted password, 1-32 ASCII characters or the encrypted password, 18-80 hex digits (even number of digits)

Command Default

Disabled

neighbor peer-group (assigning members)

The **neighbor peer-group** (assigning members) command configures a BGP neighbor to be a member a BGP peer group. The **no neighbor peer-group** (assigning members) command removes the neighbor from the peer group.

The **neighbor peer-group** creates a new member of a peer-group. If there is no such peer, it will be created and assigned to the group. If there is such peer already, and it does not belong to any other group, it will be assigned to the group and inherit its AS number and all its policies. If an existing peer belongs to another group, it must be removed from that group first with **no neighbor peer-group** command.

The neighbor at the IP address specified completes all of the configuration options of the peer group.

Group Access

ISP

Command Mode

Router Configuration

Command Line Usage

neighbor <*A.B.C.D*> **peer-group** <*WORD*>

no neighbor <*A.B.C.D*> **peer-group** <*WORD*>

Command Syntax

A.B.C.D	address of the BGP neighbor
WORD	the name of the peer-group

neighbor peer-group (creating)

The **neighbor peer-group** (creating) command creates a BGP peer group. The **no neighbor peer-group** (creating) command removes the peer group and all of its members.

Group Access

ISP

Command Mode

Router Configuration

Command Line Usage

neighbor <*WORD*> **peer-group**

no neighbor <*WORD*> **peer-group**

Command Syntax

WORD	peer group name

neighbor remote-as

The **neighbor remote-as** command performs many functions as described below. Use the **neighbor remote-as number** command to assign a BGP router to an autonomous system.

Group Access

ISP

Command Mode

Router Configuration

Command Line Usage

neighbor <*A.B.C.D*> **remote-as** <*1-65535*>

creates a new BGP peer and assigns an AS number to it. If such peer does not exist already, it assigns a new AS number to existing peer. Such assignment can be done for the existing peer only if it is not a member of any peer-group.

no neighbor <*A.B.C.D*> [**remote-as** [<*1-65535*>]]

deletes the corresponding peer, regardless if it is peer-group member or not.

neighbor <*WORD*> **remote-as** <*1-65535*>

assigns a new AS number to existing peer-group. If the peer-group has an AS number already, it will be replaced with the new one. All existing peer-group members will inherit this AS number too.

no neighbor <*WORD*> **remote-as** [<*1-65535*>]

removes the peer-group and all its members.

Command Syntax

A.B.C.D	BGP peer address
WORD	name of BGP peer group
1-65535	neighbor autonomous system number

neighbor remove-private-as

The **neighbor remove-private-as** command triggers the removal of private AS numbers from outbound updates. Use **no neighbor remove-private-as** command to stops such removal.

Group Access

ISP

Command Mode

Router Configuration

Command Line Usage

neighbor {<*A.B.C.D*> | <*WORD*>} **remove-private-as**

no neighbor {<*A.B.C.D*> | <*WORD*>} **remove-private-as**

Command Syntax

A.B.C.D	address of the BGP neighbor
WORD	name of neighbor peer-group

Command Default

No removal

neighbor route-map

The **neighbor route-map** command applies a route map to incoming or outgoing routes. The **no neighbor route-map** command clears a route map for incoming and outgoing routes.

Group Access

ISP

Command Mode

Router Configuration

Command Line Usage

neighbor {<*A.B.C.D*> | <*WORD*>} **route-map** <*WORD*> {**in** | **out**}

no neighbor {<*A.B.C.D*> | <*WORD*>} **route-map** <*WORD*> {**in** | **out**}

Command Syntax

A.B.C.D	neighbor IP address
WORD	name of BGP peer group
WORD	name of route-map
in	apply to incoming routes
out	apply to outgoing routes

neighbor route-reflector-client

The **neighbor route-reflector-client** command configures the router as a BGP route-reflector. The **no neighbor route-reflector-client** command configures a router back to a BGP route-reflector.

Use the **neighbor route-reflector-client** command to establish a local router to act as the route-reflector with the specified neighbor as a client.

Note: When all clients are disabled, the local router is no longer a route-reflector.

Group Access

ISP

Command Mode

Router Configuration

Command Line Usage

neighbor {<*A.B.C.D*> | <*WORD*>} **route-reflector-client**

no neighbor {<*A.B.C.D*> | <*WORD*>} **route-reflector-client**

Command Syntax

A.B.C.D	neighbor IP address
WORD	name of BGP peer group

neighbor send-community

The **neighbor send-community** command will allow a communities attribute, if any, to be sent in outbound updates to a neighbor. The **no neighbor send-community** command stops sending communities attribute.

Group Access

ISP

Command Mode

Router Configuration

Command Line Usage

neighbor {<*A.B.C.D*> | <*WORD*>} **send-community** [**both** | **extended** | **standard**]

no neighbor {<*A.B.C.D*> | <*WORD*>} **send-community** [**both** | **extended** | **standard**]

Command Syntax

A.B.C.D	neighbor IP address
WORD	name of BGP peer group
both	Send both standard and extended community attributes
extended	Send extended community attribute
standard	Send standard community attribute

Command Default

Send standard community attribute

neighbor shutdown

The **neighbor shutdown** command disables a neighbor or peer group. The **no neighbor shutdown** command enables a neighbor or peer group.

Use the **neighbor shutdown** command to end an session for a particular neighbor or peer group. This removes all routing information associated.

Use the **show ip bgp summary** command for a list of neighbors and peer-group connection. Those neighbors with an Idle status and the Administrative entry have been disabled by the **neighbor shutdown** command.

Group Access

ISP

Command Mode

Router Configuration

Command Line Usage

neighbor {<*A.B.C.D*> | <*WORD*>} **shutdown**

no neighbor {<*A.B.C.D*> | <*WORD*>} **shutdown**

Command Syntax

A.B.C.D	neighbor IP address
WORD	name of BGP peer group

neighbor soft-reconfiguration inbound

The **neighbor soft-reconfiguration inbound** command starts the storage of incoming updates without any modification. The **no neighbor soft-reconfiguration inbound** command stops this storage and releases the memory used for them.

Use the **neighbor soft-reconfiguration inbound** command to start update story required to enable inbound software configuration with the **clear ip bgp soft** [**in**] command. Outbound BGP soft-reconfiguration does not need inbound software configuration.

Outbound BGP soft-reconfiguration does not need inbound software configuration.

Note: When the **neighbor soft-reconfiguration inbound** command is issued, the peer will first be disabled and then enabled again. The no form of this command doesn't bring the peer down.

Group Access

ISP

Command Mode

Router Configuration

Command Line Usage

neighbor {<*A.B.C.D*> | <*WORD*>} **soft-reconfiguration inbound**

no neighbor {<*A.B.C.D*> | <*WORD*>} **soft-reconfiguration inbound**

Command Syntax

A.B.C.D	neighbor IP address
WORD	name of BGP peer group
inbound	specific inbound update

Command Default

No storage

neighbor timers

The **neighbor timers** command sets the timers for a particular BGP peer or peer group. The **no neighbor timers** command clears the timers for a particular BGP peer or peer group.

Use the **neighbor timers** command to configure a specific neighbor or peer-group timers values to bypass the timers configured for all BGP neighbors using the **timers bgp** command.

Note: If, during the negotiated holdtime (which is the smallest of configured hold time and the holdtime advertised by the neighbor), no messages arrive, the peer will be brought down. If the negotiated holdtime is 0, then the peer will never be brought down, because it hasn't received any messages. If the value of the keepalive timer is 0, then no keepalive messages will be sent.

Group Access

ISP

Command Mode

Router Configuration

Command Line Usage

neighbor {<*A.B.C.D*> | <*WORD*>} **timers** {<*0-21845*>} [<*0-65535*>]

no neighbor {<*A.B.C.D*> | <*WORD*>} **timers**

Command Syntax

A.B.C.D	neighbor IP address
WORD	name of BGP peer group
0-21845	frequency of keepalive messages to peers in seconds
0-65535	amount of time passed when no keepalive message is sent, in seconds

Command Default

keepalive = 60 seconds

hold time = 180 seconds

neighbor update-source loopback

The **neighbor update-source loopback** command allows an internal BGP session to use any loopback interface for the TCP session. The **no neighbor update-source loopback** command blocks a BGP session from using a loopback interface for the TCP session.

Group Access

ISP

Command Mode

Router Configuration

Command Line Usage

neighbor {<*A.B.C.D*> | <*WORD*>} **update-source loopback** <*1-64*>

no neighbor {<*A.B.C.D*> | <*WORD*>} **update-source loopback** <*1-64*>

Command Syntax

A.B.C.D	neighbor IP address
WORD	name of BGP peer group
loopback	loopback interface
1-64	loopback interface number

Command Default

Best local address

neighbor weight

The **neighbor weight** command establishes a weight to a neighbor connection. The **no neighbor weight** command removes a weight to a neighbor connection.

Note: Initially, all routes learned from this neighbor will have the assigned weight. The route with the highest weight is chosen as the choice route when multiple routes are available on the network.

Group Access

ISP

Command Mode

Router Configuration

Command Line Usage

neighbor {<*A.B.C.D*> | <*WORD*>} **weight** <*0-65535*>

no neighbor {<*A.B.C.D*> | <*WORD*>} **weight** <*0-65535*>

Command Syntax

A.B.C.D	neighbor IP address
WORD	name of BGP peer group
0-65535	weight assignment

Command Default

learned routes = 0

routes sourced by local router = 32768

network

The **network** command specifies the list of networks for the BGP routing process. The **no network** command deletes the entry.

Use the **network** command to control what networks are originated. be included in the BGP updates. Network types are learned from connected routes, dynamic routing, and static route sources. Because BGP can handle subnetting and supernetting, the mask is used. The maximum number of network commands is based on the configured nvram or ram.

Group Access

ISP

Command Mode

Router Configuration

Command Line Usage

network <*A.B.C.D*> [**mask** <*A.B.C.D*>]

no network <*A.B.C.D*> [**mask** <*A.B.C.D*>]

Command Syntax

A.B.C.D	network that BGP will advertise
A.B.C.D	network or subnetwork mask address

redistribute

The **redistribute** command redistributes routes from one protocol domain to another routing domain. The **no redistribute** command disables route distribution from one protocol domain to another routing domain.

Group Access

ISP

Command Mode

Router Configuration

Command Line Usage

redistribute {**connected** | **ospf** [**match** {**internal** | **external** | **external 1** | **external 2**}] | **rip** | **static**} [**metric** *<0-4294967295>*] [**route-map** *<WORD>*] [**weight** *<0-65535>*]

no redistribute {**connected** | **ospf** [**match** {**internal** | **external** | **external 1** | **external 2**}] | **rip** | **static**} [**metric** *<0-4294967295>*] [**route-map** *<WORD>*] [**weight** *<0-65535>*]

Command Syntax

connected	established routes as result of IP enabled on an interface
ospf	OSPF source protocol
match	the criteria by which OSPF routes are redistributed into BGP
internal	routes that are internal to an autonomous system
external	routes external to an autonomous system, but are imported into OSPF as either Type 1 or Type 2 external route
external 1	routes that are external to an autonomous system, but are imported into OSPF as Type 1 external route

external 2	routes that are external to an autonomous system, but are imported into OSPF as Type 2 external route
rip	RIP source protocol
static	IP or BGP static routes
metric *0-4294967295*	metric value used for the redistributed route.
route-map *WORD*	the name of the route-map used to conditionally control the route redistribution
weight *0-65535*	set a network weight value when redistributing into BGP

Command Default

Disabled

route-map

The **route-map** command creates or modifies route-maps and their sequences. The **no route-map** command removes the corresponding sequence from the route-map.If there are no sequences left in the route-map, the route-map will be deleted too.

Use the **route-map** command, and the **match** and **set** commands to configure the rules for redistributing routes from one routing protocol to another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the match criteria, which are the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the set actions, the particular redistribution actions to perform if the criteria enforced by the **match** commands are met. The **no route-map** command deletes the route map.

Note: If the optional sequence number [<*0-65535*>] is omitted, the default sequence number 10 is used. If the optional access value [**permit** | **deny**] is omitted, the default value permit is used.

These two commands create a route-map with the <*route-map-name*> name, if it does not exist, and the sequence specified by the sequence number and access value, there is no such sequence. Otherwise, the access value of the existing sequence is set to the new access value.

Group Access

ISP

Command Mode

Global Configuration

Command Line Usage

route-map <*WORD*> [**deny** | **permit**] [<*0-65535*>]

route-map <*WORD*> [**deny** | **permit**] [<*0-65535*>]

Command Syntax

WORD	route-map name
0-65535	route-map sequence number
deny	denies access for matching conditions
permit	permits access for matching conditions

router bgp

The **router bgp** command configures the BGP routing process. Use the **no router bgp** command clears BGP routing process configuration.

Use the **router bgp** command to establish a distributed routing core that automatically guarantees the loop-free exchange of routing information between AS's.

Group Access

ISP

Command Mode

Global Configuration

Command Line Usage

router bgp <*1-65535*>

no router bgp <*1-65535*>

Command Syntax

1-65535	number of the autonomous system identifying the router to other BGP routers

set as-path prepend

The **set as-path prepend** command modifies AS system path attributes for the matched BGP routes. The **no set as-path prepend** command ends modification of a system path for BGP routes.

Use the **set as-path prepend** command to guide the path information to control the BGP decision process.

Group Access

ISP

Command Mode

Route Map Configuration

Command Line Usage

set as-path prepend <*1-65535*>

no set as-path prepend <*1-65535*>

Command Syntax

1-65535	prepend string - you can specify a single number or multiple numbers separated by a space

set comm-list

The **set comm-list** command deletes communities from the community attribute of an inbound or outbound update. The **no set comm-list** command deletes the entry.

Use the **set comm-list** command to delete communities from the community attribute of inbound or outbound updates using a route map to filter and determine the communities to be deleted.

If the standard list is referred in the **set comm-list delete** command, only the elements with the single community number or no community number in them will be used. All others will be quietly ignored. Any element specified with the 'internet' keyword is equivalent to element without community number.

If the **set community comm** and **set comm-list list-num delete** commands are configured in the same sequence of a route-map attribute, the deletion operation (set comm-list list-num delete) is performed before the set operation (set community comm).

Note: If the **set community** and **set comm-list delete** commands are configured in the same sequence of a route-map attribute, the deletion operation (**set comm-list delete**) is performed before the set operation (**set community**).

Group Access

ISP

Command Mode

Route-map Configuration

Command Line Usage

set comm-list {*<1-99>* | *<100-199>*} **delete**

no set comm-list {*<1-99>* | *<100-199>*} **delete**

Command Syntax

1-99	standard community list number
100-199	extended community list number
delete	delete inbound or outbound communities from the community attribute

set community

The **set community** command add or replace communities from the community attribute of an inbound or outbound update. Use the **no set community** command removes the specified communities from the set.

Use the **route-map** command, and the match and set commands to configure the rules for redistributing routes from one routing protocol to another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the match criteria, which are the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the set actions, the particular redistribution actions to perform if the criteria enforced by the **match** commands are met. The **no route-map** command deletes the route map.

Note: The communities could be specified as numbers; the result will be the same; none removes community attribute from the update unless additive is specified for the set entry. In this case it doesn't modify update community attributes.

In other words, the **no set community** command, if the entry had some community numbers in it before removal, and as the result of the removal no numbers are left, then the entry itself is deleted.

The command **set community none** removes all community numbers from set entry, if any, but leaves the value of the additive attribute intact.

Group Access

ISP

Command Mode

Route-map Configuration

Command Line Usage

set community {*<1-4294967295>* | **local-AS** | **no-advertise** | **no-export** | **additive** | **none**}

no set community {*<1-4294967295>* | **local-AS** | **no-advertise** | **no-export** | **additive** | **none**}

Command Syntax

1-4294967295	community number
additive	add to the existing community
local-AS	do not advertise this route to peers outside of the local autonomous system
no-advertise	do not advertise this route to any peer internal or external
no-export	routes with this community are sent to peers in other sub-autonomous systems within a confederation
none	no community attribute

set ip next-hop

The **set ip next-hop** command establishes a next-hop value for the AS path. The **no ip next-hop** command deletes the entry.

Use the **ip policy route-map** interface configuration command, the **route-map** global configuration command, and the **match** and **set** route-map configuration commands, to define the conditions for policy routing packets. The **ip policy route-map** command identifies a route map by name. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the *match criteria*---the conditions under which policy routing occurs. The **set** commands specify the *set actions*---the particular routing actions to perform if the criteria enforced by the **match** commands are met.

If the interface associated with the first next hop specified with the **set ip next-hop** command is down, the optionally specified IP addresses are tried in turn.

Group Access

ISP

Command Mode

Route-map Configuration

Command Line Usage

set ip next-hop <*A.B.C.D*>

no set ip next-hop

Command Syntax

A.B.C.D	IP address of the next hop to which packets are output; address of the adjacent router

Command Default

Disabled

set local-preference

The **set-local preference** command establishes a preference value for the AS system path. Use the **set local-preference** command to send the local-preference to all routers in the local autonomous system.

Use the **no set-local preference** form of this command to delete the entry.

Note: In the **no set-local preference** command, the optional *<0-4294967295>* argument has no effect.

Group Access

ISP

Command Mode

Route-map Configuration

Command Line Usage

set local-preference *<0-4294967295>*

no set local-preference *<0-4294967295>*

Command Syntax

0-4294967295	local preference value

set metric-type

The **set metric-type** command sets the destination routing protocol. The **no set metric-type** command returns the default.

Use the **set metric-type** command, and the match and set commands to configure the rules for redistributing routes from one routing protocol to another. Each **set metric-type** command has a list of **match** and **set** commands associated with it. The **match** commands specify the match criteria, which are the conditions under which redistribution is allowed for the current **set metric-type** command. The **set** commands specify the set actions, the particular redistribution actions to perform if the criteria enforced by the **match** commands are met. The **no set metric-type** command deletes the route map.

Group Access

ISP

Command Mode

Route-map configuration

Command Line Usage

set metric-type {**internal** | **external** | **type-1** | **type-2**}

no set metric-type {**internal** | **external** | **type-1** | **type-2**}

Command Syntax

internal	internal metric
external	external metric
type-1	OSPF external type 1 metric
type-2	OSPF external type 2 metric

Command Default

Disabled

set origin

The **set origin** command configures the conditions for redistributing routes from any protocol to any protocol. The **no set origin** command deletes the BGP origin code.

When the **set origin** command configures redistributing routes from any protocol to any protocol, any match clause is necessary which includes pointing to a “permit everything” to set tags.

Group Access

ISP

Command Mode

Route-map Configuration

Command Line Usage

set origin {**egp | igp** | **incomplete**}

no set origin {**egp | igp** | **incomplete**}

Command Syntax

egp	remote EGP
igp	local IGP
incomplete	unknown heritage

set tag

The **set tag** command sets the value of the destination routing protocol. The **no set tag** command removes the value.

The **route-map** global configuration command and the **match** and **set** route-map configuration commands are used together to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the conditions for redistribution for the current **route-map** command. The **set** commands specify the particular redistribution actions to perform if the criteria enforced by the **match** commands are met. The **no route-map** command deletes the route map.

Group Access

ISP

Command Mode

Route-map Configuration

Command Line Usage

set tag <*0-4294967295*>

no set tag <*0-4294967295*>

Command Syntax

0-4294967295	tag value

Command Default

If not specified, tag is forwarded to the new destination protocol.

set weight

The **set-weight** command to set the route weight on the network. The first autonomous system match determines the weight to be set.

Use the **set weight** command to set the route weight on the network. The first AS match determines the weight to be set. The route with the highest weight is chosen as the choice route when multiple routes are available on the network. Weights spoken when an as path is matched, override any weight set by the **neighbor** command. Any match clause is necessary which includes pointing to a “permit everything” to set tags

Group Access

ISP

Command Mode

Route-map Configuration

Command Line Usage

set weight <*0-65535*>

no set weight

Command Syntax

0-65535	weight value

show ip as-path-access-list

The **show ip as-path-access-list** command displays configured AS path access lists and their elements.

Use the **show ip as-path-access-list** command to display configured as-path access lists and their elements.

With the optional access list number argument, it displays the specified as-path access list, if such list exists. Without it, it displays all configured as-path access lists.

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show ip as-path-access-list [<*1-199*>]

Command Syntax

1-199	AS path access list number

show ip bgp

The **show ip bgp** command displays entries in the routing table. Use the **show ip bgp** command to determine whether the session is active or not.

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show ip bgp [<*A.B.C.D*>] [<*A.B.C.D*>] [**longer-prefixes**] [| {**begin** | **exclude** | **include**} {<*WORD*>} [| {**count** | **count-only**}]]

show ip bgp [<*A.B.C.D*>] [<*A.B.C.D*>] [**longer-prefixes**] [| {**count** | **count-only**}]

Command Syntax

A.B.C.D	network address in the BGP routing table to display
A.B.C.D	displays all BGP routes matching the network address/network mask pair
longer-prefixes	displays route and more specific routes
|	turns on output modifiers (filters)
begin	filter for output that begins with the specified string
exclude	filter for output that excludes the specified string
include	filter for output that includes the specified string
WORD	the specified string

count	count the number of outputted lines
count-only	count the number of lines while suppressing screen output

show ip bgp cidr-only

The **show ip bgp cidr-only** command displays routes without natural network masks, or Classless Inter-domain Routing (CIDR) routes.

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show ip bgp cidr-only [| {**begin** | **exclude** | **include**} {<*WORD*>} [| {**count** | **count-only**}]]

show ip bgp cidr-only [| {**count** | **count-only**}]

Command Syntax

|	turns on output modifiers (filters)
begin	filter for output that begins with the specified string
exclude	filter for output that excludes the specified string
include	filter for output that includes the specified string
WORD	the specified string
count	count the number of outputted lines
count-only	count the number of lines while suppressing screen output

show ip bgp community

The **show ip bgp community** command display routes that belong to specified BGP communities.

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show ip bgp community [<*1-4294967295*> | <*LINE*> | **exact-match** <*LINE*> | **expanded** | **local-AS** | **no-advertise** | **no-export**] [| {**begin** | **exclude** | **include**} {<*WORD*>} [| {**count** | **count-only**}]]

show ip bgp community [<*1-4294967295*> | <*LINE*> | **exact-match** <*LINE*> | **expanded** | **local-AS** | **no-advertise** | **no-export**] [| {**count** | **count-only**}]

Command Syntax

1-4294967295	the community number
LINE	an ordered list as a regular expression
exact-match	display routes that have an exact match
expanded	extended access list format
local-AS	do not advertise this route to peers outside of the local autonomous system
no-advertise	do not advertise this route to any peer internal or external
no-export	routes with this community are sent to peers in other sub-autonomous systems within a confederation
|	turns on output modifiers (filters)

begin	filter for output that begins with the specified string
exclude	filter for output that excludes the specified string
include	filter for output that includes the specified string
WORD	the specified string
count	count the number of outputted lines
count-only	count the number of lines while suppressing screen output

show ip bgp community-list

The **show ip bgp community-list** command display routes that are permitted by the BGP community list.

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show ip bgp community-list {*<1-99> <100-199>*} [**exact-match**] [| {**begin** | **exclude** | **include**} {*<WORD>*} [| {**count** | **count-only**}]]

show ip bgp community-list {*<1-99> <100-199>*} [**exact-match**] [| {**count** | **count-only**}]

Command Syntax

1-99	the standard community list number
100-199	the expanded community list number
exact-match	display routes that have an exact match
|	turns on output modifiers (filters)
begin	filter for output that begins with the specified string
exclude	filter for output that excludes the specified string
include	filter for output that includes the specified string
WORD	the specified string
count	count the number of outputted lines
count-only	count the number of lines while suppressing screen output

show ip bgp dampened-paths

The **show ip bgp dampened-paths** command displays BGP dampened routes.

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show ip bgp dampened-paths [| {**begin** | **exclude** | **include**} {<*WORD*>} [| {**count** | **count-only**}]]

show ip bgp dampened-paths [| {**count** | **count-only**}]

Command Syntax

|	turns on output modifiers (filters)
begin	filter for output that begins with the specified string
exclude	filter for output that excludes the specified string
include	filter for output that includes the specified string
WORD	the specified string
count	count the number of outputted lines
count-only	count the number of lines while suppressing screen output

show ip bgp flap-statistics

The **show ip bgp flap-statistics** command displays BGP flap statistics.

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show ip bgp flap-statistics [<*A.B.C.D*>] [<*A.B.C.D*>] [**longer-prefixes**] [**filter-list** <*1-199*>] [**regexp** <*LINE*>] [| {**begin** | **exclude** | **include**} {<*WORD*>} [| {**count** | **count-only**}]]

show ip bgp flap-statistics [<*A.B.C.D*>] [<*A.B.C.D*>] [**longer-prefixes**] [**filter-list** <*1-199*>] [**regexp** <*LINE*>] [| {**count** | **count-only**}]

Command Syntax

A.B.C.D	network address in the BGP routing table to display
A.B.C.D	displays all BGP routes matching the network address/network mask pair
longer-prefixes	displays route and more specific routes
filter-list *1-199*	number of an autonomous system path access list
regexp *LINE*	a regular-expression to match the BGP autonomous system paths
|	turns on output modifiers (filters)
begin	filter for output that begins with the specified string
exclude	filter for output that excludes the specified string

include	filter for output that includes the specified string
WORD	the specified string
count	count the number of outputted lines
count-only	count the number of lines while suppressing screen output

show ip bgp memory

The **show ip bgp memory** command displays BGP memory usage information.

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show ip bgp memory [| {**begin** | **exclude** | **include**} {<*WORD*>} [| {**count** | **count-only**}]]

show ip bgp memory [| {**count** | **count-only**}]

Command Syntax

|	turns on output modifiers (filters)
begin	filter for output that begins with the specified string
exclude	filter for output that excludes the specified string
include	filter for output that includes the specified string
WORD	the specified string
count	count the number of outputted lines
count-only	count the number of lines while suppressing screen output

show ip bgp neighbors

The **show ip bgp neighbors** command displays information about TCP and BGP connections to neighbors.

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show ip bgp neighbors [<*WORD*> | **global** | **ipv4**] [**advertised-routes** | **dampened-routes** | **received-routes** | **routes**] [| {**begin** | **exclude** | **include**} {<*WORD*>} [| {**count** | **count-only**}]]

show ip bgp neighbors [<*WORD*> | **global** | **ipv4**] [**advertised-routes** | **dampened-routes** | **received-routes** | **routes**] [| {**count** | **count-only**}]

Command Syntax

A.B.C.D	the IP address of a neighbor; if not specified, all neighbors are displayed
global	Global routing/forwarding
ipv4	Neighbors active in this family
advertised-routes	displays all routes advertised to a BGP neighbor
dampened-routes	displays all dampened routes received from a neighbor
received-routes	displays all received routes (both accepted and filtered) from a specific neighbor
routes	displays all routes that were received and accepted for the specified neighbor
|	turns on output modifiers (filters)

begin	filter for output that begins with the specified string
exclude	filter for output that excludes the specified string
include	filter for output that includes the specified string
WORD	the specified string
count	count the number of outputted lines
count-only	count the number of lines while suppressing screen output

show ip bgp paths

The **show ip bgp paths** command displays all BGP paths in the database.

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show ip bgp paths [<*LINE*>] [| {**begin** | **exclude** | **include**} {<*WORD*>} [| {**count** | **count-only**}]]

show ip bgp paths [<*LINE*>] [| {**count** | **count-only**}]

Command Syntax

LINE	regular expression to match BGP autonomous systems paths
|	turns on output modifiers (filters)
begin	filter for output that begins with the specified string
exclude	filter for output that excludes the specified string
include	filter for output that includes the specified string
WORD	the specified string
count	count the number of outputted lines
count-only	count the number of lines while suppressing screen output

show ip bgp peer-group

The **show ip bgp peer-group** command displays information about BGP peer groups.

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show ip bgp peer-group [<*WORD*> | **global** | **ipv4**] [| {**begin** | **exclude** | **include**} {<*WORD*>} [| {**count** | **count-only**}]]

show ip bgp peer-group [<*WORD*> | **global** | **ipv4**] [| {**count** | **count-only**}]

Command Syntax

WORD	display information about a specific peer-group; number of peers and groups
global	Global routing/forwarding
ipv4	Neighbors active in this family
|	turns on output modifiers (filters)
begin	filter for output that begins with the specified string
exclude	filter for output that excludes the specified string
include	filter for output that includes the specified string
WORD	the specified string
count	count the number of outputted lines
count-only	count the number of lines while suppressing screen output

show ip bgp regexp

The **show ip bgp regexp** command displays routes matching the regular expression.

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show ip bgp regexp {<*LINE*>} [| {**begin** | **exclude** | **include**} {<*WORD*>} [| {**count** | **count-only**}]]

show ip bgp regexp {<*LINE*>} [| {**count** | **count-only**}]

Command Syntax

LINE	regular expression to match the BGP autonomous system paths
|	turns on output modifiers (filters)
begin	filter for output that begins with the specified string
exclude	filter for output that excludes the specified string
include	filter for output that includes the specified string
WORD	the specified string
count	count the number of outputted lines
count-only	count the number of lines while suppressing screen output

show ip bgp summary

The **show ip bgp summary** command displays the status of all BGP connections.

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show ip bgp summary [**global** | **ipv4**] [| {**begin** | **exclude** | **include**} {<*WORD*>} [| {**count** | **count-only**}]]

show ip bgp summary [**global** | **ipv4**] [| {**count** | **count-only**}]

Command Syntax

global	Global routing/forwarding
ipv4	Neighbors active in this family
|	turns on output modifiers (filters)
begin	filter for output that begins with the specified string
exclude	filter for output that excludes the specified string
include	filter for output that includes the specified string
WORD	the specified string
count	count the number of outputted lines
count-only	count the number of lines while suppressing screen output

show ip community-list

The **show ip community-list** command displays a configured community access list and the associated elements.

Use the **show ip community access list** command to display configured community access lists and their elements.

With the optional access list number argument, it displays the specified community access list, if such list exists. Without it, it displays, all configured community access lists.

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show ip community-list [<*1-99*> | <*100-199*>]

Command Syntax

1-99	standard community list number
100-199	expanded community list number

synchronization

The **synchronization** command enables IGP synchronization. The **no synchronization** command disables IGP synchronization.

Group Access

ISP

Command Mode

Router Configuration

Command Line Usage

synchronization

no synchronization

timers bgp

The **timers bgp** command adjusts BGP network timers. The **no timers bgp** command resets the BGP timing defaults values.

Group Access

ISP

Command Mode

Router Configuration

Command Line Usage

timers bgp <*0-21845*> [<*0-65535*>]

no timers bgp <*0-21845*>

Command Syntax

0-21845	the frequency, in seconds, at which the software sends keepalive messages to its peer
0-65535	the holdtime interval, in seconds, which, after not receiving a keepalive message, that the software declares a BGP peer dead - the holdtime value is always three times the keepalive value

Command Syntax

keepalive = 60 seconds

holdtime = 180 seconds

13

PIM Commands

Introduction

This chapter describes the Protocol-Independent Multicast (PIM) commands that are supported on the BSR 2000. The BSR supports PIM in sparse mode.

PIM Command Descriptions

This section contains an alphabetized list and descriptions of the PIM commands supported by the BSR.

ip pim border

Use the **ip pim border** command to configure a PIM domain boundary on the interface of a border router peering with one or more neighbors outside the PIM domain.

Group Access

ISP

Command Mode

Interface Configuration

Command Line Usage

ip pim border

no ip pim border

ip pim dr-priority

The **ip pim dr-priority** command sets the priority by which a router is elected as the designated router (DR). When a Designated Router (DR) is an election candidate, the router with the highest priority is elected as the DR. The DR priority is configured on the router's interface. If a DR priority is assigned on multiple router interfaces, then the router with the highest IP address is used as the DR.

If a router does not advertise its priority in its hello messages, the router has the highest priority and is elected as the DR. If multiple routers have this priority status, then the router with the highest IP address configured on an interface is elected to be the DR.

The **no ip pim dr-priority** command removes a router from the list of Designated Routers.

Group Access

ISP

Command Mode

Interface Configuration

Command Line Usage

ip pim dr-priority *<1-255>*

no ip pim dr-priority *<1-255>*

Command Syntax

1-255	the priority of the router to be selected as the DR. Higher value indicates higher priority.

Command Default

The default DR priority for the BSR is 1, which means that the BSR is the DR.

ip pim message-interval

Use the **ip pim message-interval** command to specify the PIM router join/prune messages interval. The **no ip pim message-interval** command sets the join/prune message interval to the default value.

Group Access

ISP

Command Mode

Interface Configuration

Command Line Usage

ip pim message-interval *<1-65535>*

no ip pim message-interval

Command Syntax

1-65535	join/prune interval in seconds

Command Default

60 seconds

ip pim query-interval

The **ip pim query-interval** command adjusts how often PIM router query messages are sent to other PIM routers to control the DR process. IP multicast routers send PIM query "Hello" messages to determine which router is the Designated Router (DR) for each LAN segment (subnetwork). The DR sends Internet Group Management Protocol (IGMP) host query messages to all hosts on the directly connected LAN. When PIM operates in sparse mode, the DR sends source registration messages to the Rendezvous Point (RP). The **no ip pim query-interval** command sets the PIM router query messages to the default interval; it does **not** disable the query messages.

Group Access

ISP

Command Mode

Interface Configuration

Command Line Usage

ip pim query-interval <*1-65535*>

no ip pim query-interval

Command Syntax

1-65535	the PIM query message interval in seconds

Command Default

30 seconds

ip pim spt-threshold lasthop

The **ip pim spt-threshold lasthop** command configures when a PIM leaf router should join the shortest path source tree. This is determined by specifying a network traffic threshold at which the router switches to the shortest path source tree after the last hop. The **no ip pim spt-threshold lasthop** command restores the default value or changes the setting.

Group Access

ISP

Command Mode

Global Configuration

Command Line Usage

ip pim spt-threshold lasthop {*<0-4294967294>* | **infinity**}

no ip pim spt-threshold lasthop [*<0-4294967294>* | **infinity**]

Command Syntax

0-4294967294	the traffic rate in kilobits per second
infinity	never switch to the shortest path source tree - indicates that the rendezvous point (RP) is always used

Command Default

1024 kbps

network

The PIM version of the **network** command enables IP networks for the PIM routing process. The **no network** command disables networks for the PIM routing process.

Group Access

ISP

Command Mode

Router Configuration

Command Line Usage

network <*prefix*> <*A.B.C.D*>

no network <*prefix*> <*A.B.C.D*>

Command Syntax

prefix	IP address of directly connected network
A.B.C.D	PIM wild card bits

pim accept-rp

The **pim accept-rp** command configures a router to accept only Join or Prune messages destined for a specified rendezvous point (RP) and for a specific list of groups. The **no pim accept-rp** command disables accepting only Join or Prune messages so that all Join and Prune messages are processed.

The group address must be in the range specified by the access list. If no access list is provided, the default is all class D group addresses. When the address is one of the system's addresses, the system will be the RP only for the specified group range specified by the access list. When the group address is not in the group range, the RP will not accept Join or Register messages and will respond immediately to Register messages with Register-Stop messages.

Group Access

ISP

Command Mode

Router Configuration

Command Line Usage

pim accept-rp <*A.B.C.D*> [*1-99*]

no pim accept-rp <*A.B.C.D*> [*1-99*]

Command Syntax

A.B.C.D	The rendezvous point address of the RP allowed to send Join and Prune messages to groups in the range specified by the group access list.
1-99	The access list number that defines which groups are subject to be checked for only Join and Prune messages. If not specified, the whole class D groups are subject to the check.

Command Default

Disabled

pim register-checksum

Use the **pim register-checksum** command to register a packet checksum type.

Group Access

ISP

Command Mode

Router Configuration

Command Line Usage

pim register-checksum [**new** | **old**]

Command Syntax

new	use only IP and PIM Control Headers
old	use complete IP packet length

Command Default

Complete IP packet length

pim rp-address

The **pim rp-address** command configures the address of a static PIM rendezvous point (RP) for a particular group. The **no pim rp-address** command removes an RP address for a particular group.

Note: You must configure the IP address of RPs on all routers (including the RP router) if you use static RP.

First-hop routers send register packets to the RP address on behalf of source multicast hosts. Routers also use this address on behalf of multicast hosts that want to become members of a group. These routers send Join and Prune messages towards the RP. The RP must be a PIM router but does not require any special configuration to recognize that it is the RP. RPs are not members of the multicast group but serve as a "meeting place" for multicast sources and group members. You can configure a single RP for more than one group. The access list determines which groups the RP can be used for. If no access list is configured, the RP is used for all groups. A PIM router can use multiple RPs, but only one per group. Statically configured RP will take precedence over RP learned though a dynamic mechanism such as the bootstrap mechanism.

Group Access

ISP

Command Mode

Router Configuration

Command Line Usage

pim rp-address <*A.B.C.D*> [*1-99*]

no ip pim rp-address <*A.B.C.D*>

Command Syntax

A.B.C.D	The IP address of the router to be a statically configured PIM RP. This is a unicast IP address in four-part, dotted notation.
1-99	The number of an access list that defines for which multicast groups the RP should use. This is a standard IP access list. If no number is entered, then the default is the whole class D group range.

Command Default

No PIM rendezvous points are preconfigured.

pim unicast-route-lookup

The **pim unicast-route-lookup** command retrieves routes from the BSR's unicast routing table.

Group Access

ISP

Command Mode

Router Configuration

Command Line Usage

pim unicast-route-lookup

no pim unicast-route-lookup

router pim

Use the **router pim** command to enter Router Configuration mode from Global Configuration mode and enable PIM routing.

Group Access

ISP

Command Mode

Global Configuration

Command Line Usage

router pim

show ip pim

The **show ip pim** command displays various PIM routing information. Use the **show ip pim** command to determine whether the session is active or not.

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show ip pim bsr-router

show ip pim interface [**cable** <*X/Y*> | **count** | **ethernet** <*X/Y*> | **gigaether** <*X/Y*> | **loopback** <*1-64*>]

show ip pim neighbor [<*A.B.C.D*> | **cable** <*X/Y*> | **detail | ethernet** <*X/Y*> | **gigaether** <*X/Y*> | **loopback** <*1-64*>]

show ip pim rp [<*A.B.C.D*> | **mapping**]

show ip pim rp-hash <*A.B.C.D*>

show ip pim unresolved-groups

Command Syntax

bsr-router	Bootstrap router (v2) information
interface	PIM interface information
cable *X/Y*	Cable interface
count	Internet multicast packet count
ethernet *X/Y*	Ethernet interface
gigaether *X/Y*	Gigabit Ethernet interface
loopback *1-64*	Loopback interface
neighbor	PIM neighbor information
A.B.C.D	IP address of a specific neighbor

detail	Shows all joins/prunes towards this neighbor
rp	PIM Rendezvous Point (RP) information
A.B.C.D	IP group address
mapping	show group-to-RP mappings
rp-hash	RP to be chosen based on group selected information
unresolved-groups	unresolved groups information
|	turns on output modifiers (filters)
begin	filter for output that begins with the specified string
exclude	filter for output that excludes the specified string
include	filter for output that includes the specified string
WORD	the specified string
count	count the number of outputted lines
count-only	count the number of lines while suppressing screen output

14

Service Class Commands

Introduction

Service levels provide a means of defining service flows with specific QoS parameters (such as maximum, minimum, or reserved traffic rates, priority, and service scheduling types) and binding them to a named service class. The concept of maximum assigned bandwidth, in the context of a service class, provides a means for controlling the amount of bandwidth that a particular service class can use on an interface. This allows a user to configure levels of service to support applications with specific bandwidth and priority requirements such as voice, video, and data and to further permit users to provide differentiated levels of service.

Admission control is an authorization mechanism that provides a method of controlling the admission of service flows belonging to specific service classes on individual interfaces. Admission control is determined by the bandwidth percentage (maximum assigned bandwidth) and the amount of over-booking (configured active percent) allowed for a service class on an interface.

The creation of service classes involves assigning service flows to a service class and providing all flows belonging to that class with a defined Quality of Service. DOCSIS 1.1 has defined a set of QoS parameters, a means for associating specific QoS parameter values to a service flow, and assigning service flows their QoS parameters by referencing a service class name. A set of pre-defined, default service classes are provided with the BSR 2000 and a user has the capability of modifying these default service class parameters.

Entering Service Class Configuration Mode

Service Class Configuration mode provides access to the service class commands described in this section. To enter Service Class Configuration mode, do the following:

1. From Global Configuration mode, enter **cable service-class** and press the <**Enter**> key:

   MOT(config)# **cable service-class** <**Enter**>

   The command line prompt changes to:

   MOT(config-srvclass)#

To return to Global Configuration mode:

2. Enter the **end** or **exit** press the <**Enter**> key:

   MOT(config-srvclass)# **end**/**exit** <**Enter**>

Service Class Command Descriptions

This section contains an alphabetized list and descriptions of the service class commands supported by the BSR.

activity-timeout

The **activity-timeout** command specifies the timeout for active QoS parameters which is the maximum duration that resources may remain unused on an active service flow. The **no activity-timeout** command restores the default value.

Group Access

All

Command Mode

Service Class Configuration

Command Line Usage

activity-timeout <*WORD*> <*0-65535*>

no activity-timeout <*WORD*> <*0-65535*>

Command Syntax

WORD	the user-defined service class name created with the **name** command
0-65535	the activity timeout value in seconds

Command Default

0

admission-timeout

The **admission-timeout** command specifies the timeout for admitted QoS parameters which is the duration that the CMTS must hold resources for a service flow's admitted QoS parameter set while they are in excess of its active QoS parameter set. The **no admission-timeout** command a restores the default value.

Group Access

All

Command Mode

Service Class Configuration

Command Line Usage

admission-timeout <*WORD*> <*0-65535*>

no admission-timeout <*WORD*> <*0-65535*>

Command Syntax

WORD	the user-defined service class name created with the **name** command
0-65535	the admission timeout value in seconds

Command Default

200

admitted-bw-threshold

The **admitted-bw-threshold** command specifies the amount of admitted bandwidth, in percentage, for a service class on an interface. If this bandwidth threshold is exceeded, an event will be generated. The **no admitted-bw-threshold** command restores the default value.

Group Access

All

Command Mode

Service Class Configuration

Command Line Usage

admitted-bw-threshold <*WORD*> <*0-100*>

no admitted-bw-threshold <*WORD*> <*0-100*

Command Syntax

WORD	the user-defined service class name created with the **name** command
0-100	the percentage of admitted bandwidth

Command Default

0

allow-share

The **allow-share** command provides the ability to share bandwidth between different service level classes. Enabling bandwidth sharing, allows the bandwidth of a service level class to be used as a bandwidth "pool" that can be shared by multiple service level classes.

Group Access

All

Command Mode

Service Class Configuration

Command Line Usage

allow-share <*WORD*> <*0-1*>

no allow-share <*WORD*> <*0-1*>

Command Syntax

WORD	the name of the service class
0	disables bandwidth sharing
1	enables bandwidth sharing

Command Default

Disabled for every service class.

cable service-class

The **cable service-class** command enters Service Class Configuration mode from Global Configuration mode. To return to Global Configuration mode, use the **end** command.

Group Access

All

Command Mode

Global Configuration

Command Line Usage

cable service-class

cap

The **cap** command specifies the configured active percent (CAP) parameter for a service flow. This parameter controls overbooking for a service class. The **no cap** command restores the default value.

The configured active percent of a service class is an estimation of what fraction, expressed as a percentage, of service flows belonging to that service class that will be simultaneously active on an interface.

Group Access

All

Command Mode

Service Class Configuration

Command Line Usage

cap <*WORD*> <*0-100*>

no cap <*WORD*> <*0-100*>

Command Syntax

WORD	the user-defined service class name created with the **name** command
0-100	the configured active percentage value

Command Default

BE-UP = 0

BE-DOWN = 0

UGS = 100

UGS-AD = 80

RTPS = 5

NRTPS = 5

clear cable srvclass-stats

The **clear cable srvclass-stats** command clears service class statistics on the BSR. These are the same service class statistics displayed with the show cable srvclass-stats command.

Group Access

All

Command Mode

Service Class Configuration

Command Line Usage

clear cable srvclass-stats [<*0-0*> <*0-3*> [**DOWN** | **UP** | <*WORD*>]]

Command Syntax

0-0	This number is always 0 for the BSR 2000.
0-3	the port number
DOWN	clear downstream service class statistics
UP	clear upstream service class statistics
WORD	the user-defined service class name created with the **name** command

enforce-cmts-qos

The **enforce-cmts-qos** command enforces all service level parameters for all cable modems belonging to a service class regardless of the parameters specified in the cable modem's configuration file. When MAB, CAP, and the maximum or minimum reserve rates are configured for a given service class, these parameters are overriden by a cable modem's configuration file if the cable modem was configured after the service class was set up.

The **enforce-cmts-qos** command overrides the cable modem's configuration file QoS settings with the CMTS's service class configuration. The **no enforce-cmts-qos** command disables the cable modem's configuraion file override.

Note: The **enforce-cmts-qos** command will not override service flow TLV settings in cable modem configuration files for dynamically created service flows.

Group Access

All

Command Mode

Service Class Configuration

Command Line Usage

enforce-cmts-qos <*WORD*>

no enforce-cmts-qos <*WORD*>

Command Syntax

WORD	the name of the service class

Command Default

Disabled

grant-interval

The **grant-interval** command specifies the nominal time between grants. The **no grant-interval** command restores the default value.

Note: Specifying a grant interval is only relevant for service flows using Unsolicited Grant Service (UGS) or Unsolicited Grant Service with Activity Detection (UGS-AD) scheduling.

Group Access

All

Command Mode

Service Class Configuration

Command Line Usage

grant-interval <*WORD*> <*0-4294967295*>

no grant-interval <*WORD*> <*0-4294967295*>

Command Syntax

WORD	the user-defined service class name created with the **name** command
0-4294967295	the grant interval in microseconds

Command Default

UGS = 10000

UGS-AD = 10000

grant-jitter

The **grant-jitter** command specifies the tolerated grant jitter which is the maximum amount of time that the transmission opportunities may be delayed from the nominal periodic schedule for this service flow. The **no grant-jitter** command restores the default value.

Note: Specifying a tolerated grant jitter is only relevant for service flows using Unsolicited Grant Service (UGS) or Unsolicited Grant Service with Activity Detection (UGS-AD) scheduling.

Group Access

All

Command Mode

Service Class Configuration

Command Line Usage

grant-jitter <*WORD*> <*0-4294967295*>

no grant-jitter <*WORD*> <*0-4294967295*>

Command Syntax

WORD	the user-defined service class name created with the **name** command
0-4294967295	the tolerated grant jitter in microseconds

Command Default

UGS = 2000

UGS-AD = 2000

grant-size

The **grant-size** command specifies the unsolicited grant size. Grant size includes the entire MAC frame data PDU from the Frame Control byte to end of the MAC frame. The **no grant-size** command restores the default value.

Note: Specifying an unsolicited grant size is only relevant for service flows using Unsolicited Grant Service (UGS) or Unsolicited Grant Service with Activity Detection (UGS-AD) scheduling.

Group Access

All

Command Mode

Service Class Configuration

Command Line Usage

grant-size <*WORD*> <*0-65535*>

no grant-size <*WORD*> <*0-65535*>

Command Syntax

WORD	the user-defined service class name created with the **name** command
0-65535	the unsolicited grant size in bytes

Command Default

UGS = 152

UGS-AD = 152

grants-per-interval

The **grants-per-interval** command specifies the number of data grants per grant interval. The **no grants-per-interval** command restores the default value.

Note: Specifying the number of data grants per grant interval is only relevant for service flows using Unsolicited Grant Service (UGS)or Unsolicited Grant Service with Activity Detection (UGS-AD) scheduling:

- for UGS, the value of this parameter indicates the actual number of data grants per Nominal Grant Interval
- for UGS-AD, the value of this parameter indicates the maximum number of Active Grants per Nominal Grant Interval

Group Access

All

Command Mode

Service Class Configuration

Command Line Usage

grants-per-interval <*WORD*> <*0-127*>

no grants-per-interval <*WORD*> <*0-127*>

Command Syntax

WORD	the user-defined service class name created with the **name** command
0-127	the number of grants

Command Default

1

mab

The **mab** command specifies the Maximum Assigned Bandwidth (MAB) which is the amount of bandwidth a service class is permitted to use on an interface. It is expressed as a percentage of the total interface bandwidth capacity. The MAB of a service class is applied during admission control to determine whether to admit a new service flow and again by the packet schedulers to provide a class-based weighting to the scheduler. The **no mab** command restores the default value.

Note: For scheduling purposes, each service class gets its bandwidth based on its MAB fraction relative to other classes, not based on the absolute value of the MAB. For example, if there are only two active service classes and both have the same MAB, each service class would get 50% of the bandwidth. The absolute value of the MAB is only used for admission control not scheduling.

Group Access

All

Command Mode

Service Class Configuration

Command Line Usage

mab <*WORD*> <*1-100*>

no mab <*WORD*> <*1-100*>

Command Syntax

WORD	the user-defined service class name created with the **name** command
1-100	the percentage of bandwidth a service class is permitted to use on an interface

Command Default

The default value is 1 for user-created classes.

max-burst

The **max-burst** command specifies the maximum traffic burst size for flows belonging to a specific service class. The **no max-burst** command restores the default value.

Group Access

All

Command Mode

Service Class Configuration

Command Line Usage

max-burst <*WORD*> <*1522-4294967295*>

no max-burst <*WORD*> <*1522-4294967295*>

Command Syntax

WORD	the user-defined service class name created with the **name** command
1522-4294967295	the token bucket size in bytes for this service flow - the minimum value is the larger of 1522 bytes or the value of Maximum Concatenated Burst size

Command Default

BE-DOWN = 3044

BE-UP = 3044

RTPS = 3044

NRTPS = 3044

max-concat-burst

The **max-concat-burst** command specifies the maximum concatenated burst in bytes which a service flow is allowed. The maximum concatenated burst is calculated from the FC byte of the Concatenation MAC Header to the last CRC in the concatenated MAC frame. The **no max-concat-burst** command restores the default value.

Note: Specifying a maximum concatenated burst is only relevant for upstream service flows.

Group Access

All

Command Mode

Service Class Configuration

Command Line Usage

max-concat-burst <*WORD*> <*0-65535*>

no max-concat-burst <*WORD*> <*0-65535*>

Command Syntax

WORD	the user-defined service class name created with the **name** command
0-65535	the maximum concatenated burst in bytes - a value of "0" means there is no limit

Command Default

1522

max-latency

The **max-latency** command specifies the maximum allowable time for sending a packet from a CMTS network interface to an RF interface starting at the point the packet is received on the network interface. The **no max-latency** command restores the default value.

Note: Specifying a maximum latency value is only relevant for downstream service flows.

Group Access

All

Command Mode

Service Class Configuration

Command Line Usage

max-latency <*WORD*> <*0-4294967295*>

no max-latency <*WORD*> <*0-4294967295*>

Command Syntax

WORD	the user-defined service class name created with the **name** command
0-4294967295	the latency value in microseconds

Command Default

0

max-rate

The max-rate command specifies the maximum data rate the CM must adhere to and the CMTS must enforce. The **no max-rate** command restores the default value.

Group Access

All

Command Mode

Service Class Configuration

Command Line Usage

max-rate <*WORD*> <*0-4294967295*>

no max-rate <*WORD*> <*0-4294967295*>

Command Syntax

WORD	the user-defined service class name created with the **name** command
0-4294967295	the maximum data rate value in bits per second

Command Default

0

min-pkt-size

The **min-pkt-size** command specifies the minimum packet size in bytes reserved for a service flow. The minimum reserved rate (**min-rate**) must be set in conjunction with the minimum packet size for this service flow. The **no min-pkt-size** command restores the default value.

Group Access

All

Command Mode

Service Class Configuration

Command Line Usage

min-pkt-size <*WORD*> <*64-1522*>

no min-pkt-size <*WORD*> <*64-1522*>

Command Syntax

WORD	the user-defined service class name created with the **name** command
64-1522	the minimum packet size in bytes

Command Default

128

min-rate

The **min-rate** command specifies the minimum reserved traffic rate reserved for this service flow. The minimum packet size (**min-pkt-size**) must be set in conjunction with the minimum reserved traffic rate for this service flow.The **no min-rate** command restores the default value.

Group Access

All

Command Mode

Service Class Configuration

Command Line Usage

min-rate <*WORD*> <*0-4294967295*>

no min-rate <*WORD*> <*0-4294967295*>

Command Syntax

WORD	the user-defined service class name created with the **name** command
0-4294967295	the minimum reserved traffic rate in bits-per-second

Command Default

0

name

The **name** command creates a service class record with a user-specified name that is entered on the command line. The **no name** command deletes this service class record. Commands for specifying configuration parameters will use the service class name as the key word for distinguishing which service class record is being configured.

Group Access

All

Command Mode

Service Class Configuration

Command Line Usage

name <*WORD*> [**schedtype** [**be-down** | **be-up** | **non-rtps** | **rtps** | **ugs** | **ugs-ad**]]

no name <*WORD*>

Command Syntax

WORD	the user-defined service class name, 1-15 characters in length
schedtype	specifies which upstream scheduling service is used for upstream transmission requests and packet transmissions
be-down	best effort service on the downstream port
be-up	best effort service on the upstream port
non-rtps	non-real-time polling
rtps	real-time polling
ugs	unsolicited grant service
ugs-ad	unsolicited grant service with activity detection

poll-interval

The **poll-interval** command specifies the nominal polling interval between successive unicast request opportunities for this service flow on the upstream channel. The **no poll-interval** command restores the default value.

Note: Specifying a nominal polling interval is only relevant for service flows using Unsolicited Grant Service with Activity Detection (UGS-AD), Real-Time Polling Service (RTPS), or Non-Real-Time Polling Service (NRTPS) scheduling.

Group Access

All

Command Mode

Service Class Configuration

Command Line Usage

poll-interval <*WORD*> <*0-4294967295*>

no poll-interval <*WORD*> <*0-4294967295*>

Command Syntax

WORD	the user-defined service class name created with the **name** command
0-4294967295	the nominal polling interval in microseconds

Command Default

UGS-AD = 10000

RTPS = 50000

NRTPS = 50000

poll-jitter

The **poll-jitter** command specifies the maximum amount of time that the unicast request interval may be delayed from the nominal periodic schedule for this service flow. The **no poll-jitter** command restores the default value.

Note: Specifying a poll jitter value is only relevant for service flows using Unsolicited Grant Service with Activity Detection (UGS-AD) or Real-Time Polling Service (RTPS) scheduling.

Group Access

All

Command Mode

Service Class Configuration

Command Line Usage

poll-jitter <*WORD*> <*0-4294967295*>

no poll-jitter <*WORD*> <*0-4294967295*>

Command Syntax

WORD	the user-defined service class name created with the **name** command
0-4294967295	maximum amount of delay in microseconds

Command Default

UGS-AD = 5000

RTPS = 25000

req-trans-policy

The **req-trans-policy** command specifies:

- which IUC opportunities the CM uses for upstream transmission requests and packet transmissions for this service flow
- whether requests for this Service Flow may be piggybacked with data
- whether data packets transmitted on this service flow can be concatenated, fragmented, or have their payload headers suppressed

For UGS, it also specifies how to treat packets that do not fit into the UGS grant. The **no req-trans-policy** command restores the default value.

Note: Specifying a **req-trans-policy** value is only relevant for upstream service flows.

Group Access

All

Command Mode

Service Class Configuration

Command Line Usage

req-trans-policy <*WORD*> <*0x0-0x7fff*>

no req-trans-policy <*WORD*> <*0x0-0x7fff*>

Command Syntax

WORD	the user-defined service class name created with the **name** command
0x0-0x7fff	the Request/Transmission Policy bit mask

Command Default

BE-UP = 0

UGS = 0x7f

UGS-AD = 0x7f

RTPS = 0x1f

NRTPS = 0

restricted admission disabled

The **restricted admission disabled** command disables the admission of service flows in the admission restricted state. The admission restricted state is when a service flow is admitted when there is insufficient resources to meet its reserved rate and, subsequently, the flow only receives best effort service. The **no restricted admission disabled** command enables the admission of service flows in the admission restricted state.

Group Access

All

Command Mode

Service Class Configuration

Command Line Usage

restricted admission disabled

no restricted admission disabled

Command Default

Restricted admission is enabled by default.

schedpriority

The **schedpriority** command assigns a scheduling priority for a service class. The **no schedpriority** command a restores the default value.

Each service class must be assigned a scheduling priority to determine the order in which service flows are serviced for transmitting packets (downstream) and generating data grants (upstream). Schedule priority is separate from the traffic priority parameter which is specified to differentiate priority for service flows with identical QoS parameter sets.

Group Access

All

Command Mode

Service Class Configuration

Command Line Usage

schedpriority <*WORD*> <*1-32*>

no schedpriority <*WORD*> <*1-32*>

Command Syntax

WORD	the user-defined service class name created with the **name** command
1-32	the scheduling priority value

Command Default

1

show cable service-class

The **show cable service-class** command displays a configuration summary for all service classes, including all default service classes, that are active on the BSR.The complete configuration of an individual service class can also be displayed. The following default service classes are supported:

DefBEDown	downstream service class, no minimum rate
DefRRDown	downstream service class, non-zero minimum rate
DefBEUp	upstream best-effort service class, no minimum rate
DefRRUp	upstream best-effort service class, non-zero minimum rate
DefUGS	upstream unsolicited grant service class
DefUGSAD	upstream unsolicited grant service with activity detection service class
DefRTPS	upstream real-time polling service class
DefNRTPS	upstream non-real-time polling service class
DefEMUp	upstream emergency call service class
DefEMDown	downstream emergency call service class
DefMCDown	downstream multicast service class

The following is an example of typical screen output from the **show cable service-class** command:

```
Upstream Service Classes

Service Class        mab       cap       priority  allowShared
-------------------------------------------------------------
DefBEUp              10        50        1         0
DefRRUp              5         100       5         0
DefUGS               70        100       1         0
DefUGSAD             1         80        1         0
DefRTPS              1         5         1         0
DefNRTPS             1         5         1         0
DefEMUp              1         100       1         0
upPing               1         0         1         0

Total assigned bandwidth (mab sum): 90%


Downstream Service Classes

Service Class        mab       cap       priority  allowShare
-------------------------------------------------------------
DefBEDown            10        50        1         0
DefRRDown            85        100       5         0
DefEMDown            1         100       1         0
dnPing               1         0         1         0

Total assigned bandwidth (mab sum): 97%
```

The following is an example of typical screen output for an individual service class from the **show cable service-class** <*WORD*> command:

```
service class name:                DefBEUp
direction:                         upstream
schedule type:                     best effort
maximum assigned bandwidth:        10
configured active percent:         50
scheduling priority:               1
admitted bw threshold:             0
traffic priority:                  0
maximum sustained rate:            0
maximum traffic burst:             3044
minimum reserved rate:             0
assumed minimum rate packet size:  128
maximum concatenated burst:        1522
active QoS parameter timeout:      0
admitted QoS parameter timeout:    200
tos overwrite AND mask:            0xff
tos overwrite OR mask:             0x0
request/transmission policy:       0x0
```

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show cable service-class [<*WORD*>]

Command Syntax

WORD	Display the complete configuration of a user-defined service class created with the **name** command or one of the default service classes.

show cable srvclass-stats

The **show cable srvclass-stats** command displays service class statistics for a specified service class on a specified interface.

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show cable srvclass-stats {<*0-0*>} {<*0-3*>} {<*WORD*>}

Command Syntax

0-0	This number is always 0 for the BSR 2000.
0-3	the port number
WORD	the user-defined service class name created with the **name** command

tos-overwrite

The **tos-overwrite** command provides an "AND" and "OR" mask which the CMTS must use to overwrite the "type of service" field on all upstream IP packets on a service flow. If this parameter is omitted, then the TOS field will not be modified by the CMTS. The **no tos-overwrite** command restores the default value.

Group Access

All

Command Mode

Service Class Configuration

Command Line Usage

tos-overwrite <*WORD*> <*0x0-0xff*> <*0x0-0xff*>

no tos-overwrite <*WORD*> <*0x0-0xff*> <*0x0-0xff*>

Command Syntax

WORD	the user-defined service class name created with the **name** command
0x0-0xff	TOS AND mask
0x0-0xff	TOS OR mask

Command Default

TOS AND mask	TOS OR mask
BE-UP = 0xff	BE-UP = 0
UGS = 0xff	UGS = 0
UGS-AD = 0xff	UGS-AD = 0
RTPS = 0xff	RTPS = 0
NRTPS = 0xff	NRTPS = 0

trafpriority

The **trafpriority** command specifies the relative priority of service flows that have identical QoS parameters. The **no trafpriority** command restores the default value.

Group Access

All

Command Mode

Service Class Configuration

Command Line Usage

trafpriority <*WORD*> <*0-7*>

no trafpriority <*WORD*> <*0-7*>

Command Syntax

WORD	the user-defined service class name created with the **name** command
0-7	the service flow priority value

Command Default

0

15

Secure Shell Server Commands

Introduction

Secure Shell server (SSH) is a program that allows remote hosts to login to the BSR over a non-secure network and execute commands in a secure manner. SSH provides strong authentication and secure communications over non-secure networks such as the public Internet.

The SSH protocol uses TCP as the transport layer. An SSH server listens for connections from SSH clients on a well-known TCP port. An SSH client is launched from a remote host and connects to the SSH server. The SSH server and SSH client then handle key exchange, encryption, authentication, command execution, and data exchange.

Secure Shell Server Command Descriptions

This chapter contains an alphabetized list and descriptions of the SSH commands supported by the BSR.

show ssh config

The **show ssh config** command displays the following configuration information for an SSH session.

SSH2 Secure Shell	the SSH version number
sshTaskId	the task identifier for this SSH session
debugMode	"0" indicates that SSH debugging is turned off - "1" indicates that SSH debugging is turned on
quiet_mode	"1" indicates that SSH debugging is turned off - "0" indicates that SSH debugging is turned on
idle_timeout	the inactivity timeout value (in seconds) for SSH sessions to time out a specified with the **ssh timeout** command
portStr	the defined TCP port number for SSH to listen for incoming connections as specified with the **ssh port** command
max_connections	the maximum number of allowed, simultaneous SSH sessions specified with the **ssh session-limit** command
password_guesses	the number of authentication attempts that will be allowed for an SSH client attempting a connection as specified with the **ssh password-guesses** command
macs	the message authentication (data integrity) algorithm used for SSH sessions as specified with the **ssh message-authentication** command
ciphers	the cipher for the encryption of SSH session data as specified with the **ssh ciphers** command

subsystemString	the type of SSH server
Private HostKey file	the private hostkey authentication filename
Public HostKey file	the public hostkey authentication filename

Note: To display modifications to the default SSH configuration, use the following command:

show running-config | include ssh

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show ssh config

Command Default

Restricted admission is enabled by default.

show ssh hostkey-fingerprint

The **show ssh hostkey-fingerprint** command displays the fingerprint of a public key.

Note: The SSH server must be disabled to execute this command.

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show ssh hostkey-fingerprint {**nvram:** <*filename*>}

Command Syntax

nvram: *filename*	display fingerprint of public hostkey file stored in NVRAM

show users ssh

The **show users ssh** command displays information about active SSH sessions including SSH resource use and active calls.

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show users ssh

ssh ciphers

The **ssh ciphers** command configures a cipher for the encryption of SSH session data.

Group Access

ISP

Command Mode

Global Configuration

Command Line Usage

ssh ciphers [**3des-cbc** | **aes128-cbc** | **aes192-cbc** | **aes256-cbc** | **any** | **arcfour** | **blowfish-cbc** | **cast128-cbc** | **none** | **twofish-cbc** | **twofish192-cbc** | **twofish256-cbc**]

no ssh ciphers

Command Syntax

3des-cbc	three-key triple DES in cbc mode, with 168-bit keys
aes128-cbc	Advanced Encryption standard (AES) with 128-bit keys
aes192-cbc	Advanced Encryption standard (AES) with 192-bit keys
aes256-cbc	Advanced Encryption standard (AES) with 256-bit keys
any	attempt all possible Ciphers, none excluded
arcfour	stream cipher with 128-bit keys
blowfish-cbc	Blowfish in CBC mode, with 128-bit keys
cast128-cbc	CAST cipher in cbc mode
none	no encryption
twofish-cbc	alias for twofish128-cbc

twofish192-cbc	Twofish in cbc mode with 192-bit keys
twofish256-cbc	Twofish in cbc mode with 256-bit keys

ssh enable

The **ssh enable** command enables an SSH process. The **no ssh enable** command disables the SSH process. If SSH is disabled, all existing SSH sessions will be terminated.

Group Access

ISP

Command Mode

Global Configuration

Command Line Usage

ssh enable

no ssh enable

ssh-keygen2

The **ssh-keygen2** tool generates authentication key files for the BSR 2000 Secure Shell Server. Host keys are required for the SSH Server and can either be generated in the BSR 2000 or generated on another BSR and copied over.

Note: The SSH Server must be disabled on the BSR 2000 before running the ssh-keygen2 tool.

Caution: The BSR 2000 Secure Shell Server only accepts host key files generated with the ssh-keygen2 tool. Keys files generated using the OpenSSH ssh-keygen tool will not work with the BSR 2000 Secure Shell Server.

The ssh-keygen2 tool resolves interoperability problems associated with OpenSSH. A key file must be generated using the ssh-keygen2 tool for the BSR 2000 Secure Shell Server to interoperate properly with OpenSSH Secure Shell clients.

Group Access

System Administrator

Command Mode

Privileged EXEC

Command Line Usage

ssh-keygen2 [**bits** <*512-1024*> | **hostkeyfile** { **nvram:** <*filename*>} | **passphrase** <*WORD*>| **type** {**dsa** | **rsa**}]

Command Syntax

bits *512-1024*	specify the key strength in bits
hostkeyfile nvram: *filename*	create private hostkey file name stored in NVRAM

passphrase <*WORD*>	Sets a passphrase for SSH connections. The password can be up to 31 characters maximum.
type dsa	Digital Signature Algorithm key type
type rsa	Rivest-Shamir-Adleman public-key algorithm key type

Command Default

bits = 1024

hostkeyfile = **nvram:** *hostkey*

type = **dsa**

ssh load-host-key-files

The **ssh load-host-key-files** command specifies a new private or public hostkey authentication file. The default hostkey authentication file names are "`hostkey` and `hostkey.pub`". These two files must exist and must be valid key files. Use the UNIX **ssh-keygen2** tool to generate a new hostkey authentication file.

Note: If the hostkey authentication files are invalid, SSH will not run.

Group Access

ISP

Command Mode

Global Configuration

Command Line Usage

ssh load-host-key-files {**nvram:**} {<*filename*>}

no ssh load-host-key-files

Command Syntax

nvram:	specifies Non-volatile Random Access Memory (NVRAM) as the location of the hostkey authentication file
filename	filename of the hostkey authentication file stored in Flash or NVRAM

Command Default

hostkey = *hostkey*.pub

ssh logout session-id

The **ssh logout session-id** command will terminate an SSH session in progress. This command can be used when a user wants to reconnect using new configuration parameters.

Group Access

System Administrator

Command Mode

Privileged EXEC

Command Line Usage

ssh logout session-id <*0-3*>

Command Syntax

0-3	the session-id number - the session-id is the number displayed with the **show users ssh ssh** command

ssh message-authentication

The **ssh message-authentication** command specifies the message authentication (data integrity) algorithm used for SSH sessions.

Group Access

ISP

Command Mode

Global Configuration

Command Line Usage

ssh message-authentication [**any** | **hmac-md5** | **hmac-md5-96** | **hmac-sha1** | **hmac-sha1-96** | **none**]

no ssh message-authentication

Command Syntax

any	attempt all possible MAC algorithms except "none"
hmac-md5	digest length = key length = 20
hmac-md5-96	first 96 bits of HMAC-MD5 (digest length=12, key length=16)
hmac-sha1	digest length = key length = 20
hmac-sha1-96	first 96 bits of HMAC-SHA1 (digest length=12, key length=20)
none	no message authentication

Command Default

any

ssh password-authentication radius

The **ssh password-authentication radius** command enables RADIUS services to be used for password authentication. The **no ssh password-authentication radius** command disables this feature.

Group Access

System Administrator

Command Mode

Global Configuration

Command Line Usage

ssh password-authentication radius [**local-password**]

no ssh password-authentication radius [**local-password**]

Command Syntax

local-password	authenticate with a locally configured password if there is no response from the RADIUS server

ssh password-guesses

The **ssh password-guesses** command specifies how many authentication attempts (login and password exchange) will be allowed for an SSH client attempting a connection.

Group Access

ISP

Command Mode

Global Configuration

Command Line Usage

ssh password-guesses <*1-5*>

no ssh password-guesses

Command Syntax

1-5	password guess attempt number

Command Default

3

ssh port

The **ssh port** command configures SSH to listen for incoming connections on a defined TCP port number.

Group Access

ISP

Command Mode

Global Configuration

Command Line Usage

ssh port <*1-65535*>

no ssh port

Command Syntax

1-65535	port number

Command Default

22

ssh session-limit

The **ssh session-limit** command specifies the maximum number of simultaneous SSH sessions that the BSR accepts.

Group Access

ISP

Command Mode

Global Configuration

Command Line Usage

ssh session-limit <*0-4*>

no ssh session-limit

Command Syntax

0-4	number of simultaneous SSH sessions

Command Default

4

ssh timeout

The **ssh timeout** command specifies an inactivity timeout value for SSH sessions to time out. Specifying a value of "0" will disable time-out for SSH sessions.

Group Access

ISP

Command Mode

Global Configuration

Command Line Usage

ssh timeout <*0-60*>

Command Syntax

0-60	the timeout value in minutes

Command Default

5 minutes

16

PacketCable Commands

Overview

The BSR fully supports the Cablelabs® PacketCable™ 1.*x* specification, including VoIP telephony services.

Command Descriptions

This chapter contains an alphabetized list and descriptions of PacketCable commands used with the BSR.

cable dynamic-service authorization-mode

The **cable dynamic-service authorization-mode** command allows the cable interface to accept dynamic service. The **no cable dynamic-service command** rejects dynamic service on the cable interface.

Group Access

All

Command Mode

Interface Configuration (cable interface only)

Command Line Usage

cable dynamic-service authorization-mode {**auth_no_ecn02064** | **authorize** | **disable** | **unauthorize**}

Command Syntax

auth_no_ecn02064	authorize Dynamic Service based on DQoS gates without PacketCable ECN 2064 support
authorize	authorize CM initiated Dynamic Service based on DQoS gates, which only accepts DOCSIS DSX MAC management message types (DSA-REQ, DSC-REQ, DSD-REQ) from the CM that is authorized through DQoS. This argument is required when DQoS is enabled.
disable	reject all Dynamic Service
unauthorize	accept all Dynamic Service

Note: ECN 2064 (dqos-n-02064) places additional requirements on the authorization of dynamic service requests by an MTA. Set this value if the MTAs connected to the cable interface do not support this ECN.

Command Default

Disabled

cable dynamic-service active-timeout

CMs dynamically allocate resources such as service identifiers (SIDs) and bandwidth by using a Dynamic Service Addition (DSA) transaction. If the CM fails to issue a Dynamic Service Deletion Request (DSD-REQ) to the cable interface or the DSD-REQ is being dropped for any reasons (e.g. due to noise), these resources could be held by the cable interface indefinitely. For this reason, an active timeout interval could be configured on the cable interface so that the cable interface can remove the dynamic service flows by issuing the DSD-REQs to the CM when the timer expires.

The **cable dynamic-service active-timeout** command specifies an active timeout for dynamic service flows. The active timeout is the time since the dynamic service was used. As long as the dynamic service continues to receive at least one packet within this interval, the service is not deleted.

Group Access

All

Command Mode

Interface Configuration (cable interface)

Command Line Usage

cable dynamic-service active-timeout <*0-65535*>

Command Syntax

0-65535	active timeout value in seconds - "0" disables the active timer

Note: If the CM requests an active timeout for that dynamic service flow in the DSA-REQ, this active timer starts using the timeout value specified in the DSA-REQ.

Command Default

0

clear configuration

The **clear configuration** command resets the COPS, Dynamic QoS, event message, or electronic surveillance configuration parameters to the default settings.

Group Access

All

Command Mode

PacketCable Configuration

Command Line Usage

clear configuration [**cops** | **dqos** | **em** | **es**]

Command Syntax

cops	set all COPS configuration parameters to their default values
dqos	set all DQoS configuration parameters to their default values
em	set all event message configuration parameters to their default values
es	set the electronic surveillance feature to the default value.

clear cops pdp-ip all

The **clear cops pdp-ip all** command removes all Policy Decision Point (PDP) IP addresses.

Group Access

All

Command Mode

PacketCable Configuration

Command Line Usage

clear cops pdp-ip all

clear counters ipsec

The **clear counters ipsec** command clears the IPSec statistical counters.

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

clear counters ipsec

clear packet-cable gate

The **clear packet-cable gate** command releases reserved or committed DQoS and Multimedia gates.

Group Access

All

Command Mode

Privileged EXEC

Command Line Usage

clear packet-cable gate [**all** | **dqos** | **cops** <*0-3*> | **slot** <*NUM*> | **modem** <*mac*> | **subscriber** <*A.B.C.D*> | **identifier** <*0x00000000-0xffffffff*>]

Command Syntax

all	releases all gates
dqos	releases all DQoS gates
cops <*0-3*>	releases a gate for a specified *COPS Client handle*
slot <*NUM*>	Releases all gates associated with a specified slot number. This number is always 0 for the BSR 2000.
modem <*mac*>	*CM MAC address*
subscriber <*A.B.C.D*>	MTA or Client IP address.
identifier *0x00000000-0xffffffff*	Gate Identifier in hexadecimal notation

clear packet-cable statistics

The **clear packet-cable statistics** command clears event messages, gate, or electronic surveillance statistical counters.

Group Access

All

Command Mode

Privileged EXEC

Command Line Usage

clear packet-cable statistics [**em** | **gate** | **es** {**identifier** <*0x00000000-0xffffffff*>}]

Command Syntax

em	event message statistics
gate	specify gate statistics
es	ES duplicated packet and byte counts
identifier *0x00000000-0xffffffff*	clear a specific ES identifier

cmts-ip

The **cmts-ip** command specifies the network or loopback interface IP address used for the PacketCable protocols.

Group Access

All

Command Mode

PacketCable Configuration

Command Line Usage

cmts-ip <*A.B.C.D*>

no cmts-ip <*A.B.C.D*>

Command Syntax

A.B.C.D	network or loopback interface IP address

Command Default

Any network or loopback IP address

cops client-timer

If the **show packet-cable statistics gate** command output for the Client-Open Sent field in the COPS Statistics section is incrementing, the network and the PDP server need to be examined to determine the reason for the COPS Client timeouts. The COPS Client Timer (which is the response timer for sending the COPS Client-Open message) can be specified if COPS connections time out before receiving a Client-Accept message.

The **cops client-timer** command specifies the time permitted for the BSR to receive the Client-Accept message from the PDP before terminating the COPS connection. The **no cops client-timer** command restores the default setting.

Group Access

All

Command Mode

PacketCable Configuration

Command Line Usage

cops client-timer <*1-3600000*>

no cops client-timer <*1-3600000*>

Command Syntax

1-3600000	COPS Client timer value in milliseconds

Command Default

3000 milliseconds

cops pdp-ip

The **cops pdp-ip** command restricts COPS connections to a specific Policy Decision Point (PDP). A PDP is either the Call Management Server in the PacketCable architecture or the Policy Server in the PacketCable Multimedia architecture where a Client/MTA policy request is either serviced or rejected. The **no cops pdp-ip** command removes an IP address from the list.

Note: If one or more PDP IP addresses are configured, only connections from these PDP IP addresses are accepted. Up to 100 “trusted” PDP IP addresses can be configured.

Group Access

All

Command Mode

PacketCable Configuration

Command Line Usage

cops pdp-ip *<A.B.C.D>*

no cops pdp-ip *<A.B.C.D>*

Command Syntax

A.B.C.D	PDP IP address

Command Default

Any PDP IP address is allowed to make a COPS connection.

cops pep-id

The **cops pep-id** command specifies the default Policy Enforcement Point (PEP) text string, that is used in COPS messaging, to uniquely identify the BSR within the PacketCable/PacketCable Multimedia domain

The **no cops pep-id** command restores the default value.

Group Access

All

Command Mode

PacketCable Configuration

Command Line Usage

cops pep-id <*string*>

no cops pep-id <*string*>

Command Syntax

string	COPS PEP ID string that is between 1 and 32 characters.

Command Default

"Motorola CMTS"

cops status-trap-enable

The **cops status-trap-enable** command enables or disables the COPS status SNMP trap through the *DQoSCopsTrap* SNMP MIB object. If the COPS status SNMP trap is enabled, the BSR generates an SNMP trap when one or more of the following conditions are occur:

- a keep alive timeout
- the COPS connection is disconnected
- a failure to establish a TCP connection
- a COPS connection is established
- an unauthorized PDP attempt to establish a COPS connection

Group Access

All

Command Mode

PacketCable Configuration

Command Line Usage

cops status-trap-enable {**disable** | **enable**}

Command Syntax

disable	disables COPS status SNMP trap (if previously enabled).
enable	enables COPS status SNMP trap. The default is disabled.

Command Default

Disabled

debug packet-cable gate

The **debug packet-cable gate** command displays DQoS and Multimedia gate state transition information. The **no debug packet-cable gate** command turns off this debugging function.

Group Access

All

Command Mode

Privileged EXEC

Command Line Usage

debug packet-cable gate

no debug packet-cable gate

Command Default

Disabled

debug packet-cable trace cops

The **debug packet-cable trace cops** command dumps COPS messages in hexidecimal format to the console. The **no debug packet-cable trace cops** command turns off this debugging function.

Group Access

All

Command Mode

Privileged EXEC

Command Line Usage

debug packet-cable trace cops

no debug packet-cable trace cops

Command Default

Disabled

debug packet-cable trace em

The **debug packet-cable trace em** command dumps event messages in hexidecimal format to the console. The **no debug packet-cable trace em** command turns off this debugging function.

Group Access

All

Command Mode

Privileged EXEC

Command Line Usage

debug packet-cable trace em

no debug packet-cable trace em

Command Default

Disabled

debug ipsec

The **debug ipsec** command displays all realtime IP security (IPSec) debugging information to the console. The **no debug ipsec** command turns off this debugging function.

Note: Debugging for IPSec can only occur when IPSec is not shutdown.

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

debug ipsec {**ike** [**chan-agent** | **del-msg** | **info-msg** | **key-exg** | **main** | **quick**] | **ipsec** | **sadb** | **spd**}

no debug ipsec {**ike** [**chan-agent** | **del-msg** | **info-msg** | **key-exg** | **main** | **quick**] | **ipsec** | **sadb** | **spd**}

Command Syntax

ike	enables the debugging of the Internet Key Exchange (IKE) channel agent information, delete messages, informational messages, key exchanges, main mode (IKE phase 1) and quick mode (IKE phase 2) information to the console. Disabling this parameter shuts down all six of the IKE debug printing categories.
chan-agent	enables the debugging of the channel agent information and prints it to the console
del-msg	enables the debugging of delete messages and prints them to the console

info-msg	enables the debugging of informational messages and prints them to the console
key-exg	enables the debugging of key exchanges and prints them to the console
main	enables the debugging Internet Security Association Key Management Protocol (ISAKMP) exchange statements and prints them to the console
quick	enables the debugging of ISAKMP IKE Security Association (SA) exchange statements and prints them to the console
ipsec	enables the debugging of IPSec information and prints it to the console
sadb	enables the debugging of Security Association Database (SADB) information and prints it to the console
spd	enables the debugging of the IPSec Security Policy Database (SPD) information and prints it to the console

Command Default

Disabled

dqos emergency-trap-enable

The **dqos emergency-trap-enable** command enables or disables an SNMP trap for Emergency Calls through the *rdnPktDQoSEmergencyTrapEnable* SNMP MIB object. If the Emergency Call SNMP trap is enabled, the BSR generates an SNMP trap if an Emergency Call is initiated.

Group Access

All

Command Mode

PacketCable Configuration

Command Line Usage

dqos emergency-trap-enable {**disable** | **enable**}

Command Syntax

disable	disable Emergency Call SNMP trap (if previously enabled)
enable	enable Emergency Call SNMP trap

Command Default

Disabled

dqos res-req-trap-enable

The **dqos res-req-trap-enable** command enables or disables a Resource Request SNMP trap through the *DQoSResReq* SNMP MIB object. If the Resource Request SNMP trap is enabled, the BSR generates an SNMP trap if a Resource Request from an MTA is invalid. This would include one or more of the following conditions:

- an invalid gate ID (DSA-REQ contains an unknown gate ID)
- a missing gate ID (DSA-REQ is missing gate ID)
- requested resources are exceeded

Group Access

All

Command Mode

PacketCable Configuration

Command Line Usage

dqos res-req-trap-enable {**disable** | **enable**}

Command Syntax

disable	disable Resource Request SNMP trap (if previously enabled)
enable	enable Resource Request SNMP trap

Command Default

Disabled

dqos shutdown

The **dqos shutdown** command disables Dynamic QoS (DQoS) and COPS operation on the BSR.The **no dqos shutdown** command enables DQoS and the COPS operation on the BSR.

Group Access

All

Command Mode

PacketCable Configuration

Command Line Usage

dqos shutdown

no dqos shutdown

Command Default

Disabled

dqos t0-timer/t1-timer

If T0 and T1 timeouts are being counted in the **show packet-cable statistics gate** command output, the network and the PDP server need to be examined. T0 and T1 timers may need to be increased from their default values to avoid T0 and T1 timeouts.

The **dqos t0-timer** and **dqos t1-timer** commands configure the T0 and T1 timers. The T0 timer specifies the period of time that a gate is allocated without being authorized. The T1 timer specifies the time that can elapse between the authorization and commit. The **no dqos t0-timer** and **no dqos t1-timer** commands restore the default values.

Group Access

All

Command Mode

PacketCable Configuration

Command Line Usage

dqos {**t0-timer** | **t1-timer**} *<1-3600>*

Command Syntax

t0-timer	time, in seconds, that a gate ID can remain allocated without any specified gate parameters
t1-timer	time, in seconds, that an authorization for a gate can remain valid
1-3600	number of seconds

Command Default

t0-timer = 30 seconds

t1-timer = 250 seconds

em element-number

The **em element-number** command specifies a unique event message Element ID for the BSR. The **no em element-number** command restores the default setting.

Group Access

All

Command Mode

PacketCable Configuration

Command Line Usage

em element-number <*0-99999*>

no em element-number <*0-99999*>

Command Syntax

0-99999	Element ID number

Command Default

0

em event-disable-mask

The **em event-disable-mask** command specifies a hexidecimal mask to disable event messages. The **no em event-disable-mask** command restores the default setting.

The following table describes the QoS event message bit definitions. These hexidecimal values can also be combined. For example, QoS_Release and QoS_Commit event messages can be disabled by entering the hexidecimal number: 0x00040080.

Event Message	Bit Definition (1 Based)	Hexidecimal value
QoS_Reserve	7	0x00000040
QoS_Release	8	0x00000080
Time_Change	17	0x00010000
QoS_Commit	19	0x00040000

Group Access

All

Command Mode

PacketCable Configuration

Command Line Usage

em event-disable-mask <*0x00000000-0xffffffff*>

Command Syntax

0x00000000-0xffffffff	set bits correspond to event message IDs being disabled

Command Default

0x00000000 (which is no mask)

em event-priority

The **em event-priority** command specifies the priority of event messages generated from the BSR relative to other events. The **no em event-priority** command restores the default setting.

Group Access

All

Command Mode

PacketCable Configuration

Command Line Usage

em event-priority <*0-255*>

no em event-priority <*0-255*>

Command Syntax

0-255	event message priority value

Command Default

128

em flag-override

The Call Management Server directs the BSR (for PacketCable only) to send event messages to the Record Keeping Server in either batch mode (putting event messages together in a packet) or in realtime mode (sending event messages in packets as they come). The event flag, which tells the BSR to send event messages to the Record Keeping Server can be overridden.

The **em flag-override** command forces the BSR to use realtime mode or batch mode regardless of what the Call Manager Server directs the BSR to do. The **no em flag-override** command disables event flag override.

Note: PacketCable Multimedia supports realtime mode only.

Group Access

All

Command Mode

PacketCable Configuration

Command Line Usage

em flag-override {**batch** | **realtime**}

no em flag-override

Command Syntax

batch	send the event message in batch mode
realtime	send the event message in realtime mode

Command Default

Disabled

em max-batch-events

Event messages are batched together before being sent to the Record Keeping Server. The **em max-batch-events** command specifies the amount of event messages that are batched. The **no em max-batch-events** command restores the default setting. The collected messages are sent when the **em max-batch-time** parameter expires.

Group Access

All

Command Mode

PacketCable Configuration

Command Line Usage

em max-batch-events <*2-32*>

no em max-batch-events <*2-32*>

Command Syntax

2-32	maximum number of batched event messages

Command Default

6

em max-batch-time

The hold-time for batched event messages can be specified to allow more time so that multiple event messages are combined into one packet to reduce network traffic.

The **em max-batch-time** command specifies the interval that the batched event messages are held before they are sent to the Record Keeping Server. The **no em max-batch-time** command restores the default setting.

Group Access

All

Command Mode

PacketCable Configuration

Command Line Usage

em max-batch-time <*1-60*>

no em max-batch-time <*1-60*>

Command Syntax

1-60	maximum time in seconds

Command Default

10

em qos-descriptor-disable

The QoS Descriptor attribute can be disabled if an MSO administrator decides it does not need it because it wants to reduce the event message size for network traffic management purposes.

The QoS descriptor attribute contains the Service Class profile name and QoS parameters. The **em qos-descriptor-disable** command disables the QoS Descriptor attribute. The **no em qos-descriptor-disable command enables** the QoS Descriptor.

Group Access

All

Command Mode

PacketCable Configuration

Command Line Usage

em qos-descriptor-disable

no em qos-descriptor-disable

Command Default

Enabled

em retry-count

If an Accounting-Response event message is not received by the BSR from the Record Keeping Server, the BSR sends the event message again. Once all retries are exhausted, the BSR tries an alternate Record Keeping Server (if one is available). The network and the Record Keeping Server should be examined to determine the reason for these timeouts.

The event message retry count can be specified depending on the amount of network congestion and the distance between the BSR and the Record Keeping Server. For example, if network congestion causes reported timeouts in the Account Request Failure field in the **show packet-cable statistics** command output, the event message retry count may need to be changed.

The **em retry-count** command specifies the number of retries that should occur before the BSR tries an alternate Record Keeping Server. The **no em retry-count** command restores the default setting.

Group Access

All

Command Mode

PacketCable Configuration

Command Line Usage

em retry-count <*0-16*>

no em retry-count <*0-16*>

Command Syntax

0-16	maximum number of retransmissions for each Record Keeping Server

Command Default

3

em retry-interval

The event message retry interval can be configured depending on the amount of network congestion and the distance between the BSR and the Record Keeping Server. For example, if the distance caused a time delay, the event message retry interval can be extended from the default value to allow more time for the BSR to receive an Accounting-Response message. The network and the Record Keeping Server should be examined to determine the reason for these timeouts. In most cases the **em retry-count** command parameter should be increased before the **em retry-interval** command parameter is modified.

The **em retry-interval** command specifies the event message retry interval for receiving an Accounting Response. The **no em retry-interval** command restores the default value.

Group Access

All

Command Mode

PacketCable Configuration

Command Line Usage

em retry-interval <*1-3600*>

no em retry-interval

Command Syntax

1-3600	retry interval in seconds

Command Default

2

em shutdown

The **em shutdown** command disables event messages generated from the BSR if they are not needed. The **no em shutdown** command enables event messages.

Group Access

All

Command Mode

PacketCable Configuration

Command Line Usage

em shutdown

no em shutdown

Command Default

Enabled

em udp-port

If the default UDP port is already in use, another UDP port can be specified for PacketCable event messages. A different UDP port can also be specified for event messages because of security reasons.

The **em udp-port** command specifies a UDP port number for event messages. The **no em udp-port** command restores the default setting.

Group Access

All

Command Mode

PacketCable Configuration

Command Line Usage

em udp-port <*1-65535*>

no em udp-port <*1-65535*>

Command Syntax

1-65535	UDP port number for event messages.

Command Default

1813

es

The **no es shutdown** command enables electronic surveillance. The **es shutdown** command disables electronic surveillance.

The **es trap-enable enable** command enables the electronic surveillance SNMP trap. The **no es trap-enable disable** command disables the electronic surveillance SNMP trap.

Note: Electronic surveillance conforms to Communications Assistance for Law Enforcement Act (CALEA) requirements.

Group Access

All

Command Mode

PacketCable Configuration

Command Line Usage

es {**shutdown** | **trap-enable** {**disable** | **enable**}}

no es {**shutdown** | **trap-enable** {**disable** | **enable**}}

Command Syntax

shutdown	Shutdown electronic surveillance functionality
trap-enable {**disable** | **enable**}	Enable/disable the electronic surveillance SNMP trap

Command Default

Disabled

ike client-addr

The **ike client-addr** command specifies the IP address used by the BSR for its source address during IKE protocol exchanges.

Group Access

All

Command Mode

IPSec Configuration

Command Line Usage

ike client-addr <*A.B.C.D*>

Command Syntax

A.B.C.D	host IP address used for IKE

ike phase1

The IKE Phase 1 Lifetime Interval and IKE Phase 1 Lifesize can be specified to enhance security. These settings determine how long the key is exposed. For example, an MSO administrator can decide to update this key on a regular basis to prevent successful hacking.

The **ike phase1** command specifies the IKE phase 1 lifetime value and the lifesize value that can either trigger or prevent the expiration of the IKE security association:

Group Access

All

Command Mode

IPSec Configuration

Command Line Usage

ike phase1 lifetime <*0, 300-2592000***>** [**lifesize <***0, 10240-4190000***>**]

Command Syntax

0, 300-2592000	lifetime interval value in seconds. Zero indicates an unlimited lifetime.
0, 10240-4190000	lifesize value in kilobytes

Command Default

Lifetime is 28800.

Lifesize is 0, which indicates an unlimited size in kilobytes.

ike phase2

The IKE Phase 2 Lifetime Interval and IKE Phase 2 Lifesize can be specified to enhance security. These settings determine how long the key is exposed. For example, an MSO administrator can decide to update this key on a regular basis to prevent successful hacking.

The **ike phase2** command specifies the IKE phase 2 lifetime value and lifesize value for the lifetime:

Group Access

All

Command Mode

IPSec Configuration

Command Line Usage

ike phase2 lifetime <*300-2592000*> [**lifesize** <*0, 10240-4190000*>]

Command Syntax

300-2592000	lifetime interval value in seconds. Zero indicates an unlimited time.
0, 10240-4190000	lifesize value in kilobytes

Command Default

Lifetime is 28800

Lifesize is 0, which indicates an unlimited size in kilobytes.

ike retries

The number of IKE retries can be specified for network problems. Observe the number of IKE retries in the **show ipsec ike** command output. If the number of IKE retries is increasing, then the network and server should be examined to determine the reason for the excessive number of IKE retries.

The **ike retries** command specifies the number of IKE retries.

Group Access

All

Command Mode

IPSec Configuration

Command Line Usage

ike retries <*1-10*>

Command Syntax

1-10	number of retransmissions

Command Default

3

ike timeout

The IKE retransmission timeout interval can be specified for network problems. Observe the number of IKE timeouts in the **show ipsec ike** command output. If the number of IKE timeouts is increasing, then the network and server should be examined to determine the reason for the excessive number of IKE timeouts.

The **ike timeout** command specifies the IKE retransmission timeout interval.

Group Access

All

Command Mode

IPSec Configuration

Command Line Usage

ike timeout <*1-20*>

Command Syntax

1-20	timeout value in seconds

Command Default

10

ipsec

The **ipsec** command accesses IPSec Configuration mode from Global Configuration mode.

Group Access

All

Command Mode

Global Configuration and PacketCable Configuration

Command Line Usage

ipsec

ipsec shutdown

The **ipsec shutdown** command disables IPSecIKE for the BSR.The **no ipsec shutdown** command enables IPSec/IKE for the BSR.

Note: For the initial configuration of IPSec/IKE, the IPSec configurable parameters should be configured, before IPSec is enabled. At a minimum, the **ike client-addr** command should be configured prior to enabling IPSec.

Group Access

All

Command Mode

IPSec Configuration

Command Line Usage

ipsec shutdown

no ipsec shutdown

Command Default

Disabled

packet-cable

The **packet-cable** command is used to access PacketCable Configuration mode from Global Configuration mode.

Group Access

All

Command Mode

Global Configuration

Command Line Usage

packet-cable

show cable dynamic-service

The **show cable dynamic-service** command displays the dynamic service configuration status for the cable interfaces.

The following provides typical screen output from the **show cable dynamic-service** command:

```
Cable dynamic-service auth-mode: authorize
Cable dynamic-service active-timeout: 0
```

Group Access

All

Command Mode

Interface Configuration

Command Line Usage

show cable dynamic-service

show ipsec

The **show ipsec** command displays the configuration of IKE, IPSec, Security Association Database (SADB), Security Policy Database (SPD), SPD preshared-keys, or SPD Policies.

The following provides typical screen output from the **show ipsec ipsec** command:

```
IPsec:
    Initialized = false
    IPsec Retain DF bit = disabled

    IPsec Bypass       : 0          Ipsec Discard     : 0
    IPsec Outbound Ah  : 0          IPsec Inbound Ah  : 0
    IPsec Outbound ESP : 0          IPsec Inbound ESP : 0
    IPsec Output(total): 0          IPsec Input(total): 0
```

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show ipsec {**ike** | **ipsec** | **sadb** | **spd** [**policy** | **preshared-key**]}

Command Syntax

ike	display IKE-specific configuration
ipsec	display IPSec-specific configuration
sadb	display the Security Association Database (SADB) configuration
spd	display SPD-specific configuration
policy	display SPD policy configuration
preshared-key	display SPD preshared-key and IP address configuration

show packet-cable configuration

The **show packet-cable configuration** command displays COPS, DQoS, event messaging, electronic surveillance, and PacketCable Multimedia configuration information.

The following provides typical screen output from the **show packet-cable configuration** command and output field descriptions:

```
PacketCable Configuration
-------------------------
CMTS IP address: 150.31.50.10

COPS Configuration
------------------
PEP ID: Motorola CMTS
Client Timer: 4000 milliseconds
Status trap: disabled

Dynamic QoS Configuration
-------------------------
DQoS is enabled
T0 Timer: 30  seconds
T1 Timer: 60  seconds
Resource Request trap: disabled
Emergency trap: disabled
```

PacketCable Configuration	display the cable (CMTS) interface IP address.
COPS Configuration	display the PEP ID, Client Timer, and if the Status SNMP trap is enabled or disabled.
PDP IP Address	display the Policy Decision Point (PDP) for one or more Call Management Servers (PacketCable architecture).

Dynamic QoS Configuration	displays if DQoS is enabled or disabled, T0 and T1 timer parameters, and whether the COPS status and Resource Request SNMP traps are enabled or disabled.
Event Message Configuration	displays if event messages are enabled or disabled and other event message configuration parameters
Electronic Surveillance Configuration	displays if ES is enabled or disabled and if the ES status SNMP trap is enabled or disabled.

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show packet-cable configuration [**dqos** | **em** | **es**]

Command Syntax

cops	display the COPS configuration and status information
dqos	display DQoS configuration and status information
em	display event message configuration and status information
es	display electronic surveillance configuration and status information

show packet-cable cops

The **show packet-cable cops** command display all COPS connections, which includes the COPS Client handle, PDP IP address, port number, keep-alive timeout, and duration time.

The following provides typical screen output from the **show packet-cable cops** command and output field descriptions:

```
COPS Connection Information
 ------------------------------------------------------------------------------
| Handle | Type |  IP Address    | Port | Keep-Alive Timeout | Connected Time |
 ------------------------------------------------------------------------------
     0      DQoS      172.50.1.100  52287            60              01:05:02
     1      DQoS      150.31.1.143  46351            30              01:05:02
     4      DQoS      150.31.1.140  59970            60              00:49:25
```

Handle	COPS handle ID
CMS IP Address	PDP IP address
Port Number	Socket connection port number.
Keep-Alive Timeout	Keep-Alive timeout interval between when a Keep-Alive packet is sent and received for a COPS connection.
Duration Time	time (days and hours) the COPS connection has been active. If a COPS handle has been disconnected it display "disconnected".

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show packet-cable cops [**inactive**]

Command Syntax

inactive	specify the COPS Client(s) that are inactive

show packet-cable gate

The **show packet-cable gate** command display the gate ID in hexidecimal notation, CM MAC address, CPE (subscriber) IP address, cable slot number, upstream and downstream Service Flow Identifier (SFID) number, status and committed time gate summary information

The following provides typical screen output from the **show packet-cable gate** command:

```
DQoS Gates:     2
-------------------------------------------------------------------------------
 GateID |    Modem     |  Subscriber   |CM|   SFID    |Pri|  Status   |Committed
  (0x)  | MAC Address  |  IP Address   |TS| Up  | Dn  |   |           |  Time
-------------------------------------------------------------------------------
00000D3C 0011.8065.f57a   150.31.55.101  0    57    58 Low   Committed 00:21:58
00000E86 0011.8065.f580   150.31.55.102  0    55    56 Low   Committed 00:21:58
```

The following provides the **show packet-cable gate** command output field descriptions:

GateID (0x)	display the gate Identifier in hexadecimal notation
Modem MAC Address	cable modem (CM) MAC address
Subscriber IP Address	Client IP address
CMTS	This number is always 0 for the BSR 2000.
SFID	display the upstream (Up) SFID number, and the downstream (Dn) Service Flow Identifier (SFID) number.
Pri	gate priority, which is either high or low.
Status	gate status
Committed Time	time at which the gate was committed

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show packet-cable gate [**dqos** | **cops** <*0-3*> | **identifier** <*0x00000000-0xffffffff*> | **modem** <*mac*> | **slot** <*NUM*> | **subscriber** <*A.B.C.D*>]

Command Syntax

dqos	specify all DQoS gates
cops *0-3*	specify a COPS connection and COPS handle to display
identifier *0x00000000-0xffffffff*	Gate Identifier in hexadecimal notation to display detailed information about the DQoS or Multimedia gate.
modem *mac*	specify a cable modem MAC address to display
slot *NUM*	This number is always 0 for the BSR 2000.
subscriber *A.B.C.D*	specify a CPE (subscriber) IP address to display

show packet-cable statistics

The **show packet-cable statistics** command displays COPS statistics, DQoS gate statistics, PacketCable Multimedia gate statistics, event message statistics, DQoS event message statistics, and electronic surveillance event message statistics.

The following provides typical screen output from the **show packet-cable statistics gate** command:

```
COPS Statistics
-------------------------------------------------------------------------
COPS Established:                   6  Client-Open Sent:                  6
COPS Terminated:                    3  Client-Accept Received:            6
COPS Unauthorized:                  0  Request Sent:                      6
Keep-Alive Sent:                  519  Client-Close Received:             0
Keep-Alive Received:              519  Client-Close Sent:                 0
Keep-Alive Timeout:                 0  Sync-State-Req Received:           0
Del-Req-State Sent:                 0  Sync-State-Comp Sent:              0

DQoS Gate Statistics
-------------------------------------------------------------------------
Gate-Alloc Count:                   3  Gate-Open Count:                   4
Gate-Alloc-Ack Count:               3  Gate-Close Count:                  2
Gate-Alloc-Err Count:               0  T0 Timeout:                        0
Gate-Set Count:                     4  T1 Timeout:                        0
Gate-Set-Ack Count:                 4  T7 Timeout:                        0
Gate-Set-Err Count:                 0  T8 Timeout:                        0
Gate-Delete Count:                  1  CM Delete:                         2
Gate-Delete-Ack Count:              1  CM Dereg:                          0
Gate-Delete-Err Count:              0  Admin Delete:                      0
Gate-Info Count:                    0
Gate-Info-Ack Count:                0
Gate-Info-Err Count:                0
```

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show packet-cable statistics [**em** | **es** {**identifier** <*0x00000000-0xffffffff*>} | **gate** [**cops** [<*0-99*>]]]

Command Syntax

em	display event message statistics
es	display electronic surveillance statistics
identifier *0x00000000-0xffffffff*	gate identifier in hexadecimal notation
gate	display gate statistics
cops	gate statistics per COPS connection
0-99	COPS handle

spd allow-dynamic-rsp

The **spd allow-dynamic-rsp** command allows a dynamic response from a peer to negotiate Internet Key Exchange (IKE) even though the SPD policy setting is other than the "APPLY" policy setting.

The **no spd allow-dynamic-rsp** command is used to return the default setting.

Group Access

All

Command Mode

IPSec Configuration

Command Line Usage

spd allow-dynamic-rsp

no spd allow-dynamic-rsp

Command Default

BSR strictly follows the configured SPD.

spd override

The **spd override** command is used to override IP addresses, ports, or protocols that are configured in the IPSec Security Policy Database (SPD).

The **no spd override** is used to remove the address, port, or protocol override.

Group Access

All

Command Mode

IPSec Configuration

Command Line Usage

spd override [**addr-selector** | **port-selector** | **protocol-selector**]

no spd override [**addr-selector** | **port-selector** | **protocol-selector**]

Command Syntax

addr-selector	SPD overrides a specific IP address within a range of IP addresses or a wild card IP address set in the SPD.
port-selector	SPD overrides a specific port with a range of port(s) or wild card set in the SPD.
protocol-selector	SPD overrides a specific protocol with a range of protocol or wild card of protocol set in the SPD.

Command Default

No SPD override address selector is configured.

SPD override port selector is configured.

SPD override protocol selector is configured.

spd policy

The **spd policy** command specifies a security policy for the given peers IPSec Security Policy Database (SPD). The SPD policy is priority based. The lower number index has a higher priority. Data packets are compared against rules in the SPD policy, starting with the first index. When a match is found, that rule is applied and no further comparisons are made against the SPD policy for that data packet. When deleting entries, a single rule or all the rules in the table can be deleted at once.

Group Access

All

Command Mode

IPSec Configuration

Command Line Usage

spd policy <*ipAddr*{*-ipAddr2*|*:ipMask*}> <*ipAddr*{*-ipAddr2*|*:ipMask*}> <*num*> <*0-65535*> <*0-65535*> {**apply** | **bypass** | **discard**} **transport** [**after** <*num*>]

no spd policy {<*num*> | **all**}

Command Syntax

ipAddr{*-ipAddr2*|*:ipMask*}	source network IP address followed by a colon and subnetwork mask. If a hyphen is used between *ipAddr* and *ipAddr2*, this specifies a range of source network IP addresses.
ipAddr{*-ipAddr2*|*:ipMask*}	destination network IP address followed by a colon and subnetwork mask. If a hyphen is used between *ipAddr* and *ipAddr2*, this specifies a range of destination network IP addresses.

num	transport protocol number which is the IP protocol from the IP protocol header. The format is a decimal number. A value of "0" represents any protocol. For example, the Call Management Server/Gate Controller or Call Management Server/Policy Server can use TCP Port 6 and the Record Keeping Server can use UDP Port 17.
0-65535	*source* TCP/UDP *port number*. "0" represents any port.
0-65535	*destination* TCP/UDP *port number*. "0" represents any port
apply transport	used if the packet matches the rule for this policy (i.e., *ipAddr*, *ipAddr2*, num, source port, or destination port matches the packet being processed), then apply transport mode IPSEC to the IP Packet.
bypass	used if the packet matches the rule for this policy (i.e., *ipAddr*, *ipAddr2*, *num*, source port, or the destination port matches the packet being processed), then the IPSEC processing is bypassed and the IP packet is processed.
discard	used if the packet matches the rule for this policy (i.e., *ipAddr*, *ip Addr2*, *num*, source port, or destination port matches the packet being processed), then discard this IP packet.
after	allows a rule to be inserted after an existing rule in the SPD. If the **after** is not present, the new rule is added to the first index.
num	policy security index number from the **show ipsec** spd policy command. The index numbering begins at "1".

spd preshared-key

The **spd preshared-key** command specifies the Pre-shared Key IP address to allow a Pre-shared secret key to be passed between parties in a communication flow to authenticate their mutual identities. The **no spd preshared-key** removes the Pre-shared Key IP address.

Group Access

All

Command Mode

IPSec Configuration

Command Line Usage

spd preshared-key <*A.B.C.D*> <*string*>

no spd preshared-key <*A.B.C.D*>

Command Syntax

A.B.C.D	cable interface IP address
string	Pre-shared Key name which is between 1 to 128 characters

17

VLAN Tagging Commands

Introduction

This chapter describes the commands used to configure and manage the VLAN Tagging on the BSR. VLAN Tagging allows the BSR to forward traffic received from a CPE connected to a bridging CM to a uniquely numbered VLAN using the 802.1Q industry-standard trunking encapsulation on a selected "bridge mode trunk" port.

VLAN Tagging Command Descriptions

This section contains an alphabetized list and descriptions of the VLAN Tagging commands supported by the BSR.

bridge cable modem

The **bridge cable modem** command designates a particular cable modem as a bridging CM and associates its CPE traffic to a specified VLAN.

Group Access

All

Command Mode

Global Configuration

Command Line Usage

bridge cable modem <*mac*> <*2-4094*> [**stackable**]

Command Syntax

mac	cable modem MAC Address in the form xxxx.xxxx.xxxx
2-4094	the VLAN ID
stackable	allows stacking of multiple IEEE 802.1Q tags

Note: VLAN ID 1 is reserved for use by the attached Layer 2 switch/router for management purposes and as the default "native" VLAN for that equipment. VLAN ID 1 may not be configured on the BSR for Ethernet port tagged routing or for cable modem Layer 2 bridging.

bridge mode trunk

The **bridge mode trunk** command enables VLAN tagged bridging on a network interface. Only the Ethernet Network Interface is permitted to be configured for VLAN Tagging.

Group Access

All

Command Mode

Interface Configuration (Ethernet and Gigaether only)

Command Line Usage

bridge mode trunk [**priority** <*0-255*>]

Command Syntax

0-255	the optional priority value for the "bridge mode trunk "port - if multiple network ports are configured with **bridge mode trunk** command, the BSR selects the port with the highest priority value for forwarding VLAN tagged layer 2 packets. If not specified, the default priority value is 128.

clear bridge vlan counters

The **clear bridge vlan counters** command clears all receive and transmit statistics for all VLANs associated with a VLAN cable modem. These are the same statistics displayed with the **show bridge vlan counters** command.

Group Access

All

Command Mode

Privileged EXEC

Command Line Usage

clear bridge vlan counters [<*2-4094*>]

Command Syntax

2-4094	the VLAN ID - if omitted, all VLAN counters are cleared

encapsulation dot1q

The **encapsulation dot1q** command configures tagged routing on a bridge trunk port. This means that all layer 3 packets routed by the BSR that egress the port are tagged with a particular 802.1Q VLAN ID tag. The **no encapsulation dot1q** disables VLAN tagged routing.

Group Access

All

Command Mode

Interface Configuration

Command Line Usage

encapsulation dot1q *<2-4094>*

no encapsulation dot1q *<2-4094>*

Command Syntax

2-4094	the VLAN ID for routed traffic

Note: VLAN ID 1 is reserved for use by the attached Layer 2 switch/router for management purposes and as the default "native" VLAN for that equipment. VLAN ID 1 may not be configured on the BSR for Ethernet port tagged routing or for cable modem Layer 2 bridging.

The **encapsulation dot1q** command can be used only if "bridge mode trunk" has already been entered on the interface with the **bridge mode trunk** command.

show bridge vlan

The **show bridge vlan** command displays bridge VLAN statistics including associated bridging cable modems and receive and transmit counts. The following is typical screen output from the **show bridge vlan** command:

```
Selected Network Bridge Port: ethernet 0/0
Vlan CM
---- --------------

   2 0000.0000.0065
   3 0000.0000.0066
```

The **show bridge vlan counters** command displays statistical counters for all VLANs or a specific VLAN associated with a network bridge port. The following is typical screen output from the **show bridge vlan counters** command:

```
VLAN  Upstream  Upstream       Downstream  Downstream
ID    Packets   Discards       Packets     Discards
----  --------  -------------  ----------  ----------

2          714             23         922           34
3           50              0          45            0
```

Group Access

All

Command Mode

All modes except User EXEC

Command Line Usage

show bridge vlan

show bridge vlan counters [<*2-4094*>]

Command Syntax

counters	display statistical counters for all VLANs or a specific VLAN associated with a network bridge port
2-4094	the VLAN ID - if omitted, all VLANs are displayed

Note: VLAN ID 1 is reserved for use by the attached Layer 2 switch/router for management purposes and as the default "native" VLAN for that equipment. VLAN ID 1 may not be configured on the BSR for Ethernet port tagged routing or for cable modem Layer 2 bridging.

A

Command Defaults

This Appendix provides a list of default values or default states for BSR 2000 commands. Those commands for which the **Default** column is left blank do not have a default value associated with them.

Table A-1 System Administration Commands

Command	Default
aaa accounting commands default	
aaa accounting exec default	
aaa authentication login default	
aaa authentication enable	
aaa authentication local-override	Disabled
aaa authorization commands default	
aaa authorization exec default	
aaa new-model	Disabled
alias	
banner motd	
boot system	

Table A-1 System Administration Commands

Command	Default
batch	
broadcast	
chkdsk	
clear evt	
clear log	
clock set	
clock timezone	UTC
configure	
console authentication radius	
copy	
delete	
description	
dir	NVRAM
disable	
duplex	Auto negotiation enabled
enable	
enable authentication radius	
enable password	
enable secret	
encapsulation snap	
erase	
exception	
exit	
forced-download	
format	
help	
history size	10 lines in the history buffer
hostname	
ip ftp password	

Table A-1 System Administration Commands

Command	Default
ip ftp username	
ip netmask-format	bitcount
ip tacacs source-interface	
ip tftp source-interface loopback	
logging	
logging admin-status	
logging buffered	Notifications, log file is 256 Kbytes
logging console	Notifications
logging control docsis	No logging control docsis
logging default	
logging disable bpi_auth_invalid_messages	Logging of these messages is enable by default
logging disable bpi_auth_reject_messages	Logging of these messages is enable by default
logging disable bpi_map_reject_messages	Logging of these messages is enable by default
logging disable cm_ranging_fail_r103_0	Logging of these messages is enable by default
logging evt clear	
logging evt set	
logging facility	local 7
logging on	Disabled
logging rate-limit	
logging reporting	
logging reporting default	
logging session	
logging snmp-trap	
logging source-interface loopback	
logging trap	Notifications level (severity=5)
login	
logout	
memory checkzero	
message	

Table A-1 System Administration Commands

Command	Default
more	
page	on
password	
privilege restricted	
radius-server	
radius-server source-interface loopback	
redundancy cmts	redundancy enabled
reload	
repeat	
service password-encryption	No encryption
session-timeout	5 minutes for telnet sessions 0 for console sessions (session maintained indefinitely)
show aliases	
show boot	
show clock	
show evt	
show history	
show log	
show logging evt	
show logging reporting	
show logging syslog	
show memory	32 bit
show pool	
show process	
show process cpu	Frequency = 60 Hz
show process memory	All display output is shown in bytes. Sorting is disabled
show process msg-q-info	

Table A-1 System Administration Commands

Command	Default
show process semaphores	
show process stack	
show running-config	
show startup-config	
show tacacs	
show tacacs statistics	
show tech	
show user-group	
show users	
show version	
speed	Auto negotiation enabled
sync file	
tacacs-server host	
tacacs-server key	
tacacs-server port	global port number 49
tacacs-server reset-connections	
tacacs-server retry	3 retries
tacacs-server timeout	10 seconds
telnet	
telnet authentication radius	
telnet session-limit	64 concurrent telnet sessions
username	
username privilege	
username user-group	

Table A-2 IP Commands

Command	Default
arp	No entries in table arpa (ethernet ARP)
arp timeout	
cable helper-address	
clear arp-cache	
clear counters	
clear host	
clear ip route	
clear ip traffic	
host authorization	Disabled
interface	
ip access-group	No access groups defined
ip address	
ip broadcast-address	
ip dhcp relay information	
ip domain-list	
ip domain-lookup	Enabled
ip domain-name	No domain is configured.
ip forward-protocol udp	
ip helper-address	
ip host	No hosts configured
ip irdp	**holdtime = 1800 seconds** **maxadvertinterval = 600 seconds** **minadvertinterval = 450 seconds** **preference =** *-2147483648-2147483647*
ip mask-reply	Enabled
ip mtu	1496 bytes
ip name-server	

Table A-2 IP Commands

Command	Default
ip proxy-arp	Disabled
ip rarp-server	Disabled
ip redirects	
ip route	administrative distance = 1
ip routing	Enabled
ip source-route	
ip unreachables	Enabled
passive-interface	Routing updates are transmitted over the router.
ping	
show controllers	
show host authorization	
show host authorization cpe	
show host authorization interface cable	
show host authorization summary	
show host unauthorized cpe	
show hosts	
show interfaces	
show ip arp	
show ip dhcp stats	
show ip interface	
show ip irdp	
show ip protocols	
show ip route	
show ip traffic	
show sntp	
show tcp brief	
show tcp statistics	
shutdown	
sntp authenticate	

Table A-2 IP Commands

Command	Default
sntp authentication-key	
sntp broadcastdelay	3000 microseconds
sntp broadcast client	
sntp disable	Enabled
sntp server	SNTP traffic not accepted from a time server
sntp timer	
sntp trusted-key	No trusted keys defined
traceroute	**timeout** = 3 seconds **nprobes** = 3 **minhops** = 1 **maxhops** = 64 **port** = 32868 **tos** = 0 **df** = disabled
trap-enable-if	Disabled
trap-enable-rdn	Disabled

Table A-3 SNMP Commands

Command	Default
show snmp	
snmp-server access	
snmp-server chassis-id	Defaults to chassis serial number
snmp-server community	
snmp-server community-table	*snmpCommunityStatus* = active *snmpCommunityStorageType* = nonvolatile
snmp-server contact	no contact set
snmp-server context	
snmp-server convert	

Table A-3 SNMP Commands

Command	Default
snmp-server docs-trap-control	
snmp-server enable informs	Disabled
snmp-server enable traps	Disabled
snmp-server engineID	
snmp-server group	
snmp-server host	No hosts configured
snmp-server location	
snmp-server notify	*snmpNotifyRowStatus* = active *snmpNotifyStorageType* = nonvolatile
snmp-server notify-filter	*snmpNotifyFilterMask* = empty *snmpNotifyFilterRowStatus* = active *snmpNotifyFilterStorageType* = nonvolatile
snmp-server notify-filter-profile	*snmpNotifyFilterProfileRowStatus* = active *snmpNotifyFilterProfileStorType* = nonvolatile
snmp-server packetsize	1400 bytes
snmp-server port number	UDP port number 161
snmp-server shutdown	Disabled
snmp-server sysname	
snmp-server target-addr	*snmpTargetAddrMMS* = 484 *snmpTargetAddrRowStatus* = active *snmpTargetAddrStorageType* = nonvolatile
snmp-server target-params	*snmpTargetParamsRowStatus* = active *snmpTargetParamsStorageType* = nonvolatile
snmp-server trap rate-limit	
snmp-server trap-source loopback	
snmp-server user	
snmp-server view	

Table A-4 Debug Commands

Command	Default
debug aps	
debug arp	
debug cable cra	
debug cable err	
debug cable keyman	
debug cable mac	
debug cable map	
debug cable modem-select	
debug cable privacy	
debug cable qos	
debug cable range	
debug cable reg	
debug cable ucc	
debug ip access-list	Disabled
debug ip bgp	
debug ip icmp	Disabled
debug ip igmp	Disabled
debug ip mfm	Disabled
debug ip mrtm	Disabled
debug ip ospf	Disabled
debug ip packet	Disabled
debug ip pim	Disabled
debug ip policy	Disabled
debug ip redistribute	Disabled
debug ip rip	Disabled
debug ip rip database	
debug ip rip events	Disabled
debug ip rip trigger	Disabled

Table A-4 Debug Commands

Command	Default
debug ip tcp transactions	Disabled
debug ip udp	Disabled
debug ipsec ike	Disabled
debug ipsec ipsec	Disabled
debug ipsec sadb	Disabled
debug ipsec spd	Disabled
debug packet-cable	Disabled
debug ppp fsm	Disabled
debug ppp packet	Disabled
debug radius	
debug snmp	Disabled
debug sntp	
debug specmgr	
debug ssh	
debug tacacs	
debug tacacs events	
debug task monitor	Task Monitor is disabled **delay-interval** = 20 seconds for the SRM, 5 seconds for all other modules **mem-switchover** = do both (switch-over, then reboot and switch-over) **registers** = no display **suspend-task** = no **switchover-reboot** = yes **threshold-interval** = 180 seconds **threshold-mem-low = 16000000 bytes, 0 = off** **threshold-percent = 99 percent** **idle-trigger** = 10 percent **num-times** = 1
show debugging	
undebug all	

Table A-5 Access List Commands

Command	Default
access-class in	
access-list (standard)	
access-list (extended)	
ip access-group	
ip access-list	
show access-lists	All access lists are displayed.

Table A-6 Routing Policy Commands

Command	Default
default-information originate	Disabled
default-metric	A built-in automatic metric translation for each routing protocol
ip local policy route-map	
ip policy route-map	No policy routing
match as-path	
match community	
match ip address	
match ip next-hop	
match ip route-source	
match metric	
match route-type external	
match route-type internal	
match tag	
route-map	
set as-path prepend	

Table A-6 Routing Policy Commands

Command	Default
set automatic-tag	
set comm-list	
set community	
set default interface null0	Disabled
set interface null0	Disabled
set ip default next-hop	
set ip diff-serv	0
set ip next-hop	Disabled
set ip qos queue	
set local-preference	
set metric	Metric value dynamically learned or a default value
set metric-type	Disabled
set origin	
set tag	If not specified, tag is forwarded to the new destination protocol.
set weight	
show ip redistribute	
show ip traffic	
show route-map	

Table A-7 RIP Commands

Command	Default
auto-summary	Disabled
clear ip rip statistics	
default-information originate	Disabled
default-metric	Automatic metric translations given for each routing protocol

Table A-7 RIP Commands

Command	Default
distance	120
distribute-list in	Disabled
distribute-list out	Disabled
ip rip authentication key	
ip rip host routes	Disabled
ip rip message-digest key	Disabled
ip rip receive version	0 (RIP version 1 and 2)
ip rip send version	2 (RIP version 2 only)
ip split-horizon	Enabled
maximum-paths	
network	
offset-list	Disabled
output-delay	0
passive-interface	
redistribute	Disabled
router rip	
show ip rip database	
source-port 520	Disabled
timers basic	**update** = 30 seconds **invalid** = 180 seconds **flush** = 300 seconds
version	RIP receives version 1 and 2, but sends only version 1

Table A-8 OSPF Commands

Command	Default
area authentication	No authentication
area default-cost	

Table A-8 OSPF Commands

Command	Default
area nssa	No NSSA area is defined.
area range	
area stub	
area virtual-link	**hello-interval** = 10 seconds **retransmit-interval** = 5 seconds **transmit-delay** = 1 second **dead-interval** = 40 seconds
auto-cost reference-bandwidth	10 Mbps
auto-virtual-link	Disabled
clear ip ospf	
default-information originate	Disabled
default-metric	
distance	120
distance ospf	**intra-area distance** = 110 **inter-area distance** = 110 **external distance** = 110
distribute-list	Disabled
ip ospf authentication-key	
ip ospf cost	
ip ospf database-filter all out	Disabled
ip ospf dead-interval	40 seconds
ip ospf hello-interval	10 seconds
ip ospf message-digest-key	Disabled
ip ospf network	Dependant upon the network type
ip ospf priority	1
ip ospf retransmit-interval	5 seconds
ip ospf transmit-delay	1 second
maximum-paths	
network area	Disabled
passive-interface	

Table A-8 OSPF Commands

Command	Default
redistribute	Disabled
rfc1583-compatible	Disabled
router ospf	
show ip ospf	
show ip ospf database	
show ip ospf interface	
show ip ospf memory	
show ip ospf neighbor	
show ip ospf network	
show ip ospf virtual-links	
summary-address	All redistributed routes advertised separately
timers spf	**SPF delay** = 5 seconds **SPF hold time** = 10 seconds

Table A-9 IGMP Commands

Command	Default
clear ip igmp counters	
ip igmp access-group	Any group allowed on interface
ip igmp query-interval	125 seconds
ip igmp query-max-response-time	10 seconds
ip igmp querier-timeout	Query value x 2
ip igmp static-group	Disabled
ip igmp version	Version 2
ip igmp version1-querier	Disabled
show ip igmp interface	
show ip igmp groups	
show ip igmp statistics	

Table A-10 IP Multicast Commands

Command	Default
ip mroute	
ip mroute static distance	
ip mroute unicast distance	
ip multicast-routing	Disabled
show ip rpf	
clear ip multicast fwd-cache	
clear ip multicast proto-cache	
mtrace	Group address or group hostname = 224.2.0.1
show ip multicast cache-summary	
show ip multicast fwd-cache	
show ip multicast interface	
show ip multicast oi-fwd-cache	
show ip multicast no-oi-fwd-cache	
show ip multicast proto-cache	

Table A-11 CMTS Commands

Command	Default
arp timeout	60 minutes
band	
cable cmts type	Domestic
cable deny ip	
cable dhcp-giaddr primary	The giaddr for cable modems is the primary IP address on the cable interface. The giaddr for Hosts is the first secondary IP address on the cable interface.

Table A-11 CMTS Commands

Command	Default
cable downstream carrier-only	Modulation to the RF carrier is disabled.
cable downstream description	
cable downstream frequency	555000000 Hz
cable downstream interleave-depth	The command default is 8 for North American DOCSIS.
cable downstream modulation	64 QAM
cable downstream power-level	550 dBmV
cable downstream schedule	
cable downstream shutdown	The downstream port on the cable interface is disabled or "shut down" by default.
cable downstream trap-enable-if	Disabled
cable downstream trap-enable-rdn	Disabled
cable flap-list aging	1440 minutes
cable flap-list insertion-time	60 seconds
cable flap-list miss-threshold	6
cable flap-list percentage threshold	10 percent
cable flap-list power-adjust threshold	2 dBmV
cable flap-list size	256 cable modems
cable flap-list trap-enable	Enabled
cable helper-address	
cable host authorization range	
cable insert-interval	The default insertion interval is 20 hundredths of a second.
cable intercept	None
cable modem qos dsa	None
cable modem qos dsc	
cable modem qos dsd	None
cable modem max-hosts	
cable modem max-hosts-all	
cable modem-aging-timer	Disabled

Table A-11 CMTS Commands

Command	Default
cable modem ucc	
cable modulation-profile	
cable multi-ds-override	Disabled
cable privacy cert	Trust is set to "untrusted" Certificate validity checking is enabled
cable privacy auth life-time	604800 seconds (7 days)
cable privacy cm-auth life-time	604800 seconds (7 days)
cable privacy cm-auth reset	profile 1
cable privacy cm-tek life-time	43200 seconds
cable privacy cm-tek reset	
cable privacy mcast access	
cable privacy tek life-time	43200 seconds
cable qos-profile	
cable shared-secret	Null string
cable spectrum-group	
cable sync-interval	
cable ucd-interval	1000 milliseconds
cable upstream channel-width	
cable upstream concatenation	Enabled
cable upstream data-backoff	
cable upstream description	
cable upstream force-frag	The force fragmentation feature is set to 0 for no forced fragmentation of large data grants.
cable upstream frequency	None
cable upstream invited-range-interval	10000 milliseconds
cable upstream map-interval	4000 microseconds
cable upstream max-calls	The default maximum number of calls is 0.

Table A-11 CMTS Commands

Command	Default
cable upstream minislot-size	Channel Width / Minislot Size 3200000 Hz 4 ticks 1600000 Hz 8 ticks 800000 Hz 16 ticks 400000 Hz 32 ticks 200000 Hz 64 ticks
cable upstream modem-ranging-delay	250 microseconds
cable upstream modulation-profile	modulation profile 1
cable upstream physical-delay	The fixed physical delay is 400 microseconds.
cable upstream power-level	0 dB
cable upstream power-level default	0 dB
cable upstream pre-equalization	
cable upstream range-backoff	start 0, end 4
cable upstream range-forced-continue	
cable upstream range-power-override	
cable upstream rate-limit	Disabled
cable upstream spectrum-group	
cable upstream shutdown	Each upstream port is disabled.
cable upstream trap-enable-cmts	Disabled
cable upstream trap-enable-if	Disabled
cable upstream trap-enable-rdn	Disabled
cable utilization-interval	0 = disabled
clear cable flap-list	
clear cable modem offline	
clear cable modem	
clear cable qos svc-flow statistics	
clear cable ucc-stats	
clear counters cable	
collect interval	
collect resolution	200000 Hz

Table A-11 CMTS Commands

Command	Default
dhcp leasequery authorization on	
dhcp throttle on	Disabled
dhcp throttle window	One DHCP Request packet every 5000 milliseconds (five seconds)
fft display	
fft setup	**sample** = 2048 **window** = rectangular
fft start	
fft store	
guard-band	North America = 0 Hz Europe = 0 Hz
hop action band	Upstream band priority = 128
hop action channel-width	Upstream band priority = 128
hop action frequency	Upstream band priority = 128
hop action modulation-profile	Modulation profiles = 1 or 2 Upstream band priority = 128
hop action power-level	Upstream band priority = 128
hop action roll-back	Disabled
hop period	300 seconds
hop threshold flap	Disabled
interface cable	
ip address	
ip dhcp relay information option	DHCP option-82 disabled
load-balancing static	Disabled
ping docsis	
show cable downstream	
show cable flap-list	
show cable insert-interval	
show cable modem	
show cable modem cpe	

Table A-11 CMTS Commands

Command	Default
show cable modem detail	
show cable modem hosts	
show cable modem mac	
show cable modem maintenance	
show cable modem offline	
show cable modem phy	
show cable modem registered	
show cable modem stats	
show cable modem summary	
show cable modem summary total	
show cable modem svc-flow-id	
show cable modem time-registered	
show cable modem timing-offset	
show cable modem unregistered	
show cable modulation-profile	
show cable privacy auth	
show cable privacy cm-auth	
show cable privacy cmts	
show cable privacy tek	
show cable qos profile	
show cable qos svc-flow classifier	
show cable qos svc-flow dynamic-stat	
show cable qos svc-flow log	
show cable qos svc-flow param-set	
show cable qos svc-flow phs	
show cable qos svc-flow statistics	
show cable qos svc-flow summary	
show cable qos svc-flow upstream-stat	
show cable spectrum-group	

Table A-11 CMTS Commands

Command	Default
show cable spectrum-group load-balance summary	
show cable sync-interval	
show cable ucd-interval	
show cable ucc-stats	
show cable upstream	
show interfaces cable	
show interfaces cable configuration	
show interfaces cable downstream	
show interfaces cable intercept	None
show interfaces cable service-class	
show interfaces cable stats	
show interfaces cable upstream	
show stats cmts	
show stats summary error	
time band	
time delete	

Table A-12 BGP Commands

Command	Default
aggregate-address	Disabled
auto-summary	Enabled
bgp always-compare-med	
bgp confederation identifier	
bgp confederation peers	

Table A-12 BGP Commands

Command	Default
bgp dampening	**half life** = 15 minutes **route reuse** = 750 **route suppression** = 2000 **maximum suppression time** = 4 times the half-life
bgp default local-preference	
bgp permit	Disabled
bgp router-id	
clear ip bgp	Disabled
clear ip bgp dampening	
clear ip bgp flap-statistics	
default-information originate	Disabled
default-metric	
distance bgp	**external distance** = 20 **internal distance** = 200 **local distance** = 200
distribute-list in	Disabled
distribute-list out	Disabled
ip as-path access-list	
ip community-list	
match as-path	
match community	
maximum-paths	
neighbor advertisement-interval	30 seconds for external peers 5 seconds for internal peers
neighbor default-originate	
neighbor description	
neighbor distribute-list	
neighbor ebgp-multihop	
neighbor filter-list	Disabled

Table A-12 BGP Commands

Command	Default
neighbor maximum-prefix	Disabled Threshold default, 75%
neighbor next-hop-self	Disabled
neighbor password	Disabled
neighbor peer-group (assigning members)	
neighbor peer-group (creating)	
neighbor remote-as	
neighbor remove-private-as	No removal
neighbor route-map	
neighbor route-reflector-client	
neighbor send-community	
neighbor shutdown	
neighbor soft-reconfiguration inbound	No storage
neighbor timers	**keepalive** = 60 seconds **hold time** = 180 seconds
neighbor update-source loopback	Best local address
neighbor weight	**learned routes** = 0 **routes sourced by local router** = 32768
network	
redistribute	Disabled
router bgp	
route-map	
set as-path prepend	
set comm-list	
set community	
set local-preference	
set metric-type	Disabled
set origin	
set tag	If not specified, tag is forwarded to the new destination protocol.

Table A-12 BGP Commands

Command	Default
set ip next-hop	Disabled
set weight	
show ip bgp	
show ip bgp cidr-only	
show ip bgp community	
show ip bgp community-list	
show ip bgp dampened-paths	
show ip bgp flap-statistics	
show ip bgp memory	
show ip bgp neighbors	
show ip bgp paths	
show ip bgp peer-group	
show ip bgp regexp	
show ip bgp summary	
show ip as-path-access-list	
show ip community-list	
synchronization	
timers bgp	**keepalive** = 60 seconds **holdtime** = 180 seconds

Table A-13 PIM Commands

Command	Default
ip pim border	
ip pim bsr-candidate	30 bits
ip pim bsr-candidate ip-address	Hash mask length = 30 bits
ip pim dr-priority	The default DR priority for the BSR is 1, which means that the BSR is the DR.

Table A-13 PIM Commands

Command	Default
ip pim message-interval	60 seconds
ip pim query-interval	30 seconds
ip pim rp-candidate	
ip pim rp-candidate group-list	
ip pim rp-candidate interval	60 seconds
ip pim rp-candidate ip-address	
ip pim rp-candidate priority	0
ip pim spt-threshold lasthop	1024 kbps
ip pim spt-threshold rp	0
network	
pim accept-rp	Disabled
pim register-checksum	Complete IP packet length
pim rp-address	No PIM rendezvous points are preconfigured.
pim unicast-route-lookup	
router pim	
show ip pim	

Table A-14 Service Class Commands

Command	Default
activity-timeout	0 seconds
admission-timeout	200 seconds
admitted-bw-threshold	0
allow-share	Disabled for every service class.
cable service-class	

Table A-14 Service Class Commands

Command	Default
cap	BE-UP = 0 BE-DOWN = 0 UGS = 100 UGS-AD = 80 RTPS = 5 NRTPS = 5
clear cable srvclass-stats	
grant-interval	UGS = 10000 UGS-AD = 10000
grant-jitter	UGS = 2000 UGS-AD = 2000
grant-size	UGS = 152 UGS-AD = 152
grants-per-interval	1
mab	1
max-burst	BE-DOWN = 1522 BE-UP = 1522 RTPS = 1522 NRTPS = 1522
max-concat-burst	0 (no limit)
max-latency	0 microseconds
max-rate	0 bps
min-pkt-size	128 bytes
min-rate	0 bps
name	
poll-interval	UGS-AD = 10000 RTPS = 50000 NRTPS = 50000
poll-jitter	UGS-AD = 5000 RTPS = 25000

Table A-14 Service Class Commands

Command	Default
req-trans-policy	BE-UP = 0 UGS = 0x7f UGS-AD = 0x7f RTPS = 0x1f NRTPS = 0
restricted admission disabled	
schedpriority	1
show cable service-class	
show cable srvclass-stats	
tos-overwrite	**TOS AND mask** BE-UP = 0xff UGS = 0xff UGS-AD = 0xff RTPS = 0xff NRTPS = 0xff **TOS OR mask** BE-UP = 0 UGS = 0 UGS-AD = 0 RTPS = 0 NRTPS = 0
trafpriority	0

Table A-15 Secure Shell Server Commands

Command	Default
show ssh config	
show ssh hostkey-fingerprint	
show users	
ssh ciphers	
ssh enable	
ssh-keygen2	bits = 1024 hostkeyfile = **nvram:** *hostkey* type = **dsa**
ssh load-host-key-files	hostkey = *hostkey*.pub
ssh logout session-id	

Table A-15 Secure Shell Server Commands

Command	Default
ssh message-authentication	any
ssh password-authentication radius	
ssh password-guesses	3
ssh port	22
ssh session-limit	8 simultaneous SSH sessions
ssh timeout	5 minutes

Table A-16 PacketCable Commands

Command	Default
cable dynamic-service authorization-mode	
cable dynamic-service active-timeout	0 (timer is disabled)
clear configuration	
clear counters ipsec	
clear packet-cable cops	
clear packet-cable gate	
clear packet-cable statistics	
cmts-ip	Any CMTS IP address
dqos client-timer	3000 milliseconds
dqos cms-ip	Any CMS IP address
dqos cops-trap-enable	Disabled
dqos emergency-trap-enable	Disabled
dqos pepid	"Motorola CMTS"
dqos res-req-trap-enable	Disabled
dqos shutdown	Disabled
dqos t0/t1-timer	**t0-timer** = 30 **t1-timer** = 250
em element-number	0

Table A-16 PacketCable Commands

Command	Default
em event-disable-mask	0x00000000
em event-priority	128
em flag-override	Disabled
em max-batch-events	6
em max-batch-time	10 seconds
em qos-descriptor-disable	Enabled
em retry-count	3
em retry-interval	2 seconds
em rks	
em shutdown	Enabled
em udp-port	1813
es	Enabled
ike client-addr	
ike phase1	Lifetime = 28800 Lifesize = 0
ike phase2	Lifetime = 28800 Lifesize = 0
ike retries	3
ike timeout	10 seconds
ipsec	
ipsec shutdown	Disabled
packet-cable	
show ipsec	
show packet-cable configuration	
show packet-cable cops	
show packet-cable gate	
show packet-cable statistics	
spd policy	
spd preshared-key	

Table A-17 VLAN Tagging Commands

Command	Default
bridge cable modem	
bridge mode trunk	
clear bridge vlan counters	
encapsulation dot1q	
show bridge vlan	

Index

D

E

F

G

H

I

L

M

N

O

P

R

S

T

U

V

Visit our website at:
www.motorola.com

526363-001-00
Rev. B
2/06

MGBI