b

backup

To back up an ASA configuration, certificates, keys, and images, use the **backup** command in privileged EXEC mode.

backup [**/noconfirm**] [**context** *ctx-name*] [**interface** *name*] [**passphrase** *value*] [**location** *path*]

Syntax Description

/noconfirm	Specifies not to prompt for the **location** and **cert-passphrase** parameters. Allows you to bypass warning and error messages to continue the backup.
context *ctx-name*	In multiple context mode from the system execution space, enter the **context** keyword to backup the specified context. Each context must be backed up individually; that is, re-enter the **backup** command for each file.
interface *name*	(Optional) Specifies the interface name through which the backup will be copied. If you do not specify the interface, the ASA checks the management-only routing table; if there are no matches, it then checks the data routing table.
location *path*	The backup **location** can be a local disk or a remote URL. If you do not provide a location, the following default names are used: • Single mode—disk0:*hostname* .backup.*timestamp* .tar.gz • Multiple mode—disk0:*hostname* .context-*ctx-name* .backup.*timestamp* .tar.gz
passphrase *value*	During the backup of VPN certificates and preshared keys, a secret key identified by the **cert-passphrase** keyword is required to encode the certificates. You must provide a passphrase to be used for encoding and decoding the certificates in PKCS12 format. The backup only includes RSA key pairs tied to the certificates and excludes any standalone certificates.

Command Default

If you do not provide a location, the following default names are used:

- Single mode—disk0:*hostname* .backup.*timestamp* .tar.gz
- Multiple mode—disk0:*hostname* .context-*ctx-name* .backup.*timestamp* .tar.gz

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
9.3(2)	This command was added.
9.5(1)	The **interface** *name* argument was added.

Usage Guidelines

See the following guidelines:

- You should have at least 300 MB of disk space available at the backup location before you start a backup.
- If you make any configuration changes during or after a backup, those changes will not be included in the backup. If you change a configuration after making the backup, then perform a restore, this configuration change will be overwritten. As a result, the ASA might behave differently.
- You can start only one backup at a time.
- You can only restore a configuration to the same ASA version as when you performed the original backup. You cannot use the restore tool to migrate a configuration from one ASA version to another. If a configuration migration is required, the ASA automatically upgrades the resident startup configuration when it loads the new ASA OS.
- If you use clustering, you can only back up the startup-configuration, running-configuration, and identity certificates. You must create and restore a backup separately for each unit.
- If you use failover, you must create and restore a backup separately for the active and standby units.
- If you set a master passphrase for the ASA, then you need that master passphrase to restore the backup configuration that you create with this procedure. If you do not know the master passphrase for the ASA, see the CLI configuration guide to learn how to reset it before continuing with the backup.
- If you import PKCS12 data (with the **crypto ca trustpoint** command) and the trustpoint uses RSA keys, the imported key pair is assigned the same name as the trustpoint. Because of this limitation, if you specify a different name for the trustpoint and its key pair after you have restored an ASDM configuration, the startup configuration will be the same as the original configuration, but the running configuration will include a different key pair name. This means that if you use different names for the key pair and trustpoint, you cannot restore the original configuration. To work around this issue, make sure that you use the same name for the trustpoint and its key pair.
- If you do not specify the interface, the ASA checks the management-only routing table; if there are no matches, it then checks the data routing table. Note that if you have a default route through a management-only interface, all **backup** traffic will match that route and never check the data routing table. In this scenario, always specify the interface if you need to back up through a data interface.
- You cannot back up using the CLI and restore using ASDM, or vice versa.
- When backup location command is issued, ensure to use double slash ‘//’ for the directory path. For example,

```
ciscoasa# backup location disk0://sample-backup
```

- Each backup file includes the following content:
    - Running-configuration
    - Startup-configuration

- All security images

Cisco Secure Desktop and Host Scan images

Cisco Secure Desktop and Host Scan settings

AnyConnect (SVC) client images and profiles

AnyConnect (SVC) customizations and transforms

- • Identity certificates (includes RSA key pairs tied to identity certificates; excludes standalone keys)
    - VPN pre-shared keys
    - SSL VPN configurations
    - Application Profile Custom Framework (APCF)
    - Bookmarks
    - Customizations
    - Dynamic Access Policy (DAP)
    - Plug-ins
    - Pre-fill scripts for connection profiles
    - Proxy Auto-config
    - Translation table
    - Web content
    - Version information

Examples

The following example shows how to create a backup:

```
ciscoasa# backup location disk0://sample-backup
Backup location [disk0://sample-backup]?
Begin backup...
Backing up [ASA version] ... Done!
Backing up [Running Config] ... Done!
Backing up [Startup Config]  ... Done!
Enter a passphrase to encrypt identity certificates. The default is cisco. You will be
required to enter the same passphrase while doing a restore: cisco
Backing up [Identity Certificates] ... Done!
IMPORTANT: This device uses master passphrase encryption. If this backup file is used to
restore to a device with a different master passphrase, you will need to provide the current
 master passphrase during restore.
Backing up [VPN Pre-shared keys] ... Done!
Backing up [SSL VPN Configurations: Application Profile Custom Framework] ... Done!
Backing up [SSL VPN Configurations: Bookmarks]... Done!
Backing up [SSL VPN Configurations: Customization] ... Done!
Backing up [SSL VPN Configurations: Dynamic Access Policy] ... Done!
Backing up [SSL VPN Configurations: Plug-in] ... Done!
Backing up [SSL VPN Configurations: Pre-fill scripts for Connection Profile] ... Done!
Backing up [SSL VPN Configurations: Proxy auto-config] ... Done!
Backing up [SSL VPN Configurations: Translation table] ... Done!
Backing up [SSL VPN Configurations: Web Content] ... Done!
Backing up [Anyconnect(SVC) client images and profiles] ... Done!
Backing up [Anyconnect(SVC) customizations and transforms] ... Done!
Backing up [Cisco Secure Desktop and Host Scan images] ... Done!
Backing up [UC-IME tickets] ... Done!
Compressing the backup directory ... Done!
Copying Backup ... Done!
Cleaning up ... Done!
Backup finished!
```

Related Commands

Command	Description
restore	Restores an ASA configuration, keys, certificates, and images from a backup file.

backup interface

For models with a built-in switch, such as the ASA 5505, use the **backup interface** command in interface configuration mode to identify a VLAN interface as a backup interface, for example, to an ISP. To restore normal operation, use the **no** form of this command.

backup interface vlan *number*
backup interface vlan *number*

Syntax Description

vlan *number*	Specifies the VLAN ID of the backup interface.

Command Default

By default, the **backup interface** command is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.
7.2(2)	The Security Plus license no longer limits the number of VLAN interfaces to 3 for normal traffic, 1 for a backup interface, and 1 for failover; you can now configure up to 20 interfaces without any other limitations. Therefore ,the **backup interface** command is not required to enable more than 3 interfaces.

Usage Guidelines

This command can be entered in the interface configuration mode for a VLAN interface only. This command blocks all through traffic on the identified backup interface unless the default route through the primary interface goes down.

When you configure Easy VPN with the **backup interface** command, if the backup interface becomes the primary, then the ASA moves the VPN rules to the new primary interface. See the **show interface** command to view the state of the backup interface.

Be sure to configure default routes on both the primary and backup interfaces so that the backup interface can be used when the primary fails. For example, you can configure two default routes: one for the primary interface with a lower administrative distance, and one for the backup interface with a higher distance. See the **dhcp client route distance** command to override the administrative distance for default routes acquired from a DHCP server. To configure dual ISP support, see the **sla monitor** and **track rtr** commands for more information.

You cannot configure a backup interface when the **management-only** command is already configured on the interface.

Examples

The following example configures four VLAN interfaces. The backup-isp interface only allows through traffic when the primary interface is down. The **route** commands create default routes for the primary and backup interfaces, with the backup route at a lower administrative distance.

```
ciscoasa(config)# interface vlan 100
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config-if)# backup interface vlan 400
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface vlan 200
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 10.2.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface vlan 300
ciscoasa(config-if)# nameif dmz
ciscoasa(config-if)# security-level 50
ciscoasa(config-if)# ip address 10.3.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface vlan 400
ciscoasa(config-if)# nameif backup-isp
ciscoasa(config-if)# security-level 50
ciscoasa(config-if)# ip address 10.1.2.1 255.255.255.0
ciscoasa(config-if)# no shutdown
ciscoasa(config)# interface ethernet 0/0
ciscoasa(config-if)# switchport access vlan 100
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet 0/1
ciscoasa(config-if)# switchport access vlan 200
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet 0/2
ciscoasa(config-if)# switchport access vlan 300
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet 0/3
ciscoasa(config-if)# switchport access vlan 400
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# route outside 0 0 10.1.1.2 1
ciscoasa(config)# route backup-isp 0 0 10.1.2.2 2
```

Related Commands

Command	Description
forward interface	Restricts an interface from initiating traffic to another interface.
interface vlan	Creates a VLAN interface and enters interface configuration mode.
dhcp client route distance	Overrides the administrative distance for default routes acquired from a DHCP server.
sla monitor	Creates an SLA monitoring operation for static route tracking.
track rtr	Tracks the state of an SLA monitoring operation.

backup-package auto

To configure automatic backup and restore operations on a Cisco ISA 3000, use the **backup-package auto** command in privileged EXEC mode. To disable automatic backup or restore, use the **no** form of this command.

backup-package { **backup** | **restore** } **auto**
no backup-package { **backup** | **restore** } **auto**

Syntax Description

backup	Indicates that you are configuring automatic backup.
restore	Indicates that you are configuring automatic restore.

Command Default

The default backup and restore modes are manual.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.7(1)	This command was added.

Usage Guidelines

The backup and restore modes are independent and you can configure them separately.

Use the **backup-package location** command to specify the backup and restore configuration parameters for automatic backup and restore operations.

Examples

The following example shows the use of the **backup-package** command to set automatic back-up:

```
ciscoasa# backup-package backup auto
```

Related Commands

Command	Description
show backup-package summary	Displays a summary of back-up and restore package parameters.

backup-package location

To configure the backup and restore locations to be used in subsequent backup and restore operations on a Cisco ISA 3000, use the **backup-package location** command in privileged EXEC mode. To reset the backup or restore location to the default value, use the **no** form of this command.

backup-package { **backup** | **restore** } [**interface** *name*] **location disk** *n* **:** [**passphrase** *string*
no backup-package { **backup restore** } **location**

Syntax Description

backup	Indicates that you are defining backup parameters.
interface *name*	(Optional) The name of the interface to be used for backup or restore communications.
location disk*n***:**	The storage-media location where the back-up package information is stored.
passphrase *string*	(Optional) The passphrase to be used for encrypting the backup information, or retrieving the backed-up information.
restore	Indicates that you are defining restore parameters.

Command Default

The default **location** is **disk3:**, which contains an SD card.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.7(1)	This command was added.

Usage Guidelines

The backup and restore operations are independent and can be configured separately.

Generally, configuring **backup-package** information is a one-time operation to let you subsequently manually back up and restore the device configuration without having to provide additional parameters.

Examples

The following example shows the use of the **backup-package location** command to set the backup parameters, with “cisco” as the encryption passphrase:

```
ciscoasa# backup-package backup location disk3: passphrase cisco
```

Related Commands

Command	Description
show backup-package status	Displays package information for either backup or restore.
show backup-package summary	Displays a summary of backup and restore package parameters.

backup-servers

To configure backup servers, use the **backup-servers** command in group-policy configuration mode. To remove a backup server, use the **no** form of this command.

backup-servers { *server1 server2....server10* | **clear-client-config | keep-client-config** }
no backup-servers { *server1 server2....server10* | **clear-client-config | keep-client-config** }

Syntax Description

clear-client-config	Specifies that the client uses no backup servers. The ASA pushes a null server list.
keep-client-config	Specifies that the ASA sends no backup server information to the client. The client uses its own backup server list, if configured.
server1 server 2 .... server10	Provides a space delimited, priority-ordered list of servers for the VPN client to use when the primary ASA is unavailable. Identifies servers by IP address or hostname. The list can be 500 characters long, but can contain only 10 entries.

Command Default

Backup servers do not exist until you configure them, either on the client or on the primary ASA.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Group-policy configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

To remove the backup-servers attribute from the running configuration, use the **no** form of this command without arguments. This enables inheritance of a value for backup servers from another group policy.

IPsec backup servers let a VPN client connect to the central site when the primary ASA is unavailable. When you configure backup servers, the ASA pushes the server list to the client as the IPsec tunnel is established.

Configure backup servers either on the client or on the primary ASA. If you configure backup servers on the ASA, it pushes the backup server policy to the clients in the group, replacing the backup server list on the client if one is configured.

Note If you are using hostnames, it is wise to have backup DNS and WINS servers on a separate network from that of the primary DNS and WINS servers. Otherwise, if clients behind a hardware client obtain DNS and WINS information from the hardware client via DHCP, the connection to the primary server is lost, and the backup servers have different DNS and WINS information, clients cannot be updated until the DHCP lease expires. In addition, if you use hostnames and the DNS server is unavailable, significant delays can occur.

Examples

The following example shows how to configure backup servers with IP addresses 10.10.10.1 and 192.168.10.14, for the group policy named "FirstGroup":

```
ciscoasa
(config)#
 group-policy FirstGroup attributes
ciscoasa
(config-group-policy)#
 backup-servers 10.10.10.1 192.168.10.14
```

banner (global)

To configure the ASDM, session, login, or message-of-the-day banner, use the banner command in global configuration mode. To remove all lines from the banner keyword specified (**exec**, **login**, or **motd**), use the **no** form of this command.

banner { **asdm** | **exec** | **login** | **motd** *text* }
no banner { **asdm** | **exec** | **login** | **motd** [*text*] }

Syntax Description

asdm	Configures the system to display a banner after you successfully log in to ASDM. The user is prompted to either continue to complete login, or to disconnect. This option lets you require users to accept the terms of a written policy before connecting.
exec	Configures the system to display a banner before displaying the enable prompt.
login	Configures the system to display a banner before the password login prompt when accessing the ASA using Telnet or a serial console.
motd	Configures the system to display a message-of-the-day banner when you first connect.
text	Line of message text to display.

Command Default

The default is no banner.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.2(4)/8.0(3)	The **asdm** keyword was added.
9.0(1)	The **banner login** command supports serial console connections.

Usage Guidelines

The banner command configures a banner to display for the keyword specified. The *text* string consists of all characters following the first white space (space) until the end of the line (carriage return or line feed [LF]). Spaces in the text are preserved. However, you cannot enter tabs through the CLI.

Subsequent *text* entries are added to the end of an existing banner unless the banner is cleared first.

Note The tokens $(domain) and $(hostname) are replaced with the hostname and domain name of the ASA. When you enter a $(system) token in a context configuration, the context uses the configured in the system configuration.

Multiple lines in a banner are handled by entering a new banner command for each line that you want to add. Each line is then appended to the end of the existing banner.

Note The maximum length of the authorization prompt for banners is 235 characters or 31 words, whichever limitation is reached first.

When accessing the ASA through Telnet or SSH, the session closes if there is not enough system memory available to process the banner messages or if a TCP write error occurs. Only the **exec** and **motd** s support access to the ASA through SSH. The login banner does not support SSHv1 clients or SSH clients that do not pass the username as part of the initial connection.

To replace a banner, use the no banner command before adding the new lines.

Use the no banner { exec | login | motd } command to remove all the lines for the banner keyword specified.

The no banner command does not selectively delete text strings, so any *text* that you enter at the end of the no banner command is ignored.

Examples

The following example shows how to configure the **asdm**, **exec**, **login**, and **motd** banners:

```
ciscoasa(config)#  banner asdm You successfully logged in to ASDM
ciscoasa(config)#  banner motd Think on These Things
ciscoasa(config)#  banner exec Enter your password carefully
ciscoasa(config)#  banner login Enter your password to log in
ciscoasa(config)# show running-config banner
asdm:
You successfully logged in to ASDM
exec:
Enter your password carefully
login:
Enter your password to log in
motd:
Think on These Things
```

The following example shows how to add a second line to the **motd** banner:

```
ciscoasa(config)# banner motd and Enjoy Today
ciscoasa(config)# show running-config banner motd
Think on These Things and Enjoy Today
```

Related Commands

Command	Description
clear configure	Removes all banners.
show running-config	Displays all banners.

banner (group-policy)

To display a banner or welcome text on remote clients when they connect, use the **banner** command in group-policy configuration mode. To delete a banner, use the **no** form of this command.

banner { **value** *_string* | **none** }
no banner

Note If you configure multiple banners under a VPN group policy, and you delete any one of the banners, all banners are deleted.

Syntax Description

none	Sets a banner with a null value, thereby disallowing a banner. Prevents inheriting a banner from a default or specified group policy.
value *banner_string*	Constitutes the banner text. Maximum string size is 4000 characters for post-login banners. Use the "\n" sequence to insert a carriage return. The recommended configuration is around 80 to 100 characters per line since clients and browser wrap it up around that limit for display per line.

Command Default

There is no default banner.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Group-policy configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.
9.5(1)	Increased the post-login banner length value to 4000.

Usage Guidelines

The banner is locally configured on the ASA, and the user must click either Accept or Disconnect to the post-login banner.

Note The behavior on older architectures, such as IKEv1 and Secure Client version 3.0, is supported without error.

To prevent inheriting a banner, use the **banner none** command.

The IPsec VPN client supports full HTML for the banner. However, the clientless portal and the Secure Client support partial HTML. To ensure the banner displays correctly to remote users, follow these guidelines:

- For IPsec client users, use the /n tag.
- For Secure Client, use the <BR> tag.
- For clientless users, use the <BR> tag.

Examples

The following example shows how to create a banner for the group policy named “FirstGroup”:

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# banner
value Welcome to Cisco Systems
7.0.
```

base-url

(Optional) Configures the base URL of the Clientless VPN. This URL is used in SAML metadata, which is provided to third-party IdPs, so that IdPs can redirect endpoint users back to the ASA.

(Optional) From version 9.17.1, this command configures the base URL of the SAML service provider for VPN authentication. This URL is used in SAML metadata, which is provided to third-party IdPs, so that IdPs can redirect endpoint users back to the ASA.

To disable this feature, use the **no** form of this command

base-url { **value _ string** }
no base-url

Syntax Description

base-url	URL of the Clientless VPN

Command Default

None.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Parameters configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.5(2)	This command was added.

Usage Guidelines

- When base-url is configured, it is the base URL of AssertionConsumerService and SingleLogoutService, and is displayed in **show saml metadata**.
- When base-url is not configured, the base URL is created from the ASA's hostname and domain-name. For example, **https://ssl-vpn.cisco.com** is the base URL in **show saml metadata** when hostname is "ssl-vpn" and domain-name is "cisco.com".
- When neither base-url or hostname and domain-name are configured, **show saml metadata** displays an error.

Examples

The following example sets up a base-url:

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# saml idp myIdp
ciscoasa(config-webvpn-saml-idp)# base url https://ClientlessVPN.com
```

Related Commands

Command	Description
signature	Enable or disable signature in SAML request. By default, the signature is disabled.
timeout	Configures the SAML IdP timeout.
trustpoint	Configures the trustpoint in saml-idp sub-mode.
url	Configures the SAML IdP URL.

basic-mapping-rule

To configure the basic mapping rule in a Mapping Address and Port (MAP) domain, use the **basic-mapping-rule** command in MAP domain configuration mode. Use the **no** form of this command to delete the basic mapping rule.

basic-mapping-rule
no basic-mapping-rule

Command Default

No defaults.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
MAP domain configuration mode	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.13(1)	This command was introduced.

Usage Guidelines

The customer edge (CE) device uses the basic mapping rule to determine its dedicated IPv4 addressing or shared address and port set assignment. The CE device first translates the system's IPv4 address to an IPv4 address and port within the pool's prefix and port range (using NAT44), then MAP translates the new IPv4 address to an IPv6 address within the pool defined by the rule's IPv6 prefix. The packet is then ready to be transmitted over the service provider's IPv6-only network to a border relay (BR) device.

When you enter the **basic-mapping-rule** command, you enter MAP domain basic mapping rule configuration mode, where you can configure the IPv4, IPv6, and port properties of the rule.

Examples

The following example creates a MAP-T domain named 1 and configures the translation rules for the domain.

```
ciscoasa(config)# map-domain 1

ciscoasa(config-map-domain)# default-mapping-rule 2001:DB8:CAFE:CAFE::/64

ciscoasa(config-map-domain)# basic-mapping-rule

ciscoasa(config-map-domain-bmr)# ipv4-prefix 192.168.3.0 255.255.255.0

ciscoasa(config-map-domain-bmr)# ipv6-prefix 2001:cafe:cafe:1::/64

ciscoasa(config-map-domain-bmr)# start-port 1024
ciscoasa(config-map-domain-bmr)# share-ratio 16
```

Related Commands

Commands	Description
basic-mapping-rule	Configures the basic mapping rule for a MAP domain.
default-mapping-rule	Configures the default mapping rule for a MAP domain.
ipv4-prefix	Configures the IPv4 prefix for the basic mapping rule in a MAP domain.
ipv6-prefix	Configures the IPv6 prefix for the basic mapping rule in a MAP domain.
map-domain	Configures a Mapping Address and Port (MAP) domain.
share-ratio	Configures the number of ports in the basic mapping rule in a MAP domain.
show map-domain	Displays information about Mapping Address and Port (MAP) domains.
start-port	Configures the starting port for the basic mapping rule in a MAP domain.

basic-security

To define an action when the Security (SEC) option occurs in a packet header with IP Options inspection, use the **basic-security** command in parameters configuration mode. To disable this feature, use the **no** form of this command.

basic-security action { **allow** | **clear** }
no basic-security action { **allow** | **clear** }

Syntax Description

allow	Allow packets containing the Security IP option.
clear	Remove the Security option from packet headers and then allow the packets.

Command Default

By default, IP Options inspection drops packets containing the Security IP option.

You can change the default using the **default** command in the IP Options inspection policy map.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Parameters configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.5(1)	This command was added.

Usage Guidelines

This command can be configured in an IP Options inspection policy map.

You can configure IP Options inspection to control which IP packets with specific IP options are allowed through the ASA. You can allow a packet to pass without change or clear the specified IP options and then allow the packet to pass.

Examples

The following example shows how to set up an action for IP Options inspection in a policy map:

```
ciscoasa(config)# policy-map type inspect ip-options ip-options_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# basic-security action allow
ciscoasa(config-pmap-p)# router-alert action allow
```

Related Commands

Command	Description
class	Identifies a class map name in the policy map.

Command	Description
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

bfd echo

To enable BFD echo mode on the interface, use the bfd **echo** command in interface configuration mode. To disable BFD echo mode, use the **no** form of this command.

bfd echo
no bfd echo

Syntax Description

This command has not arguments or keywords.

Command Default

BFD echo mode is disabled by default for BFD IPv4 sessions.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.6(2)	This command was added.

Usage Guidelines

Echo mode is enabled by default, but not supported in BFD IPv6 sessions. Entering the **no bfd echo** command without any keywords turns off the sending of echo packets and signifies that the ASA is unwilling to forward echo packets received from BFD neighbor routers.

When echo mode is enabled, the minimum echo transmit interval and required minimum transmit interval values are taken from the **bfd interval milliseconds min_rx milliseconds** parameters, respectively.

Before using BFD echo mode, you must disable the sending of Internet Control Message Protocol (ICMP) redirect messages by entering the **no ip redirects** command to avoid high CPU utilization.

Examples

The following example associates a BFD template with a BFD map.

```
(config)# interface gigabitethernet 0/0
(config-if)# bfd echo
```

Related Commands

Command	Description
authentication	Configures authentication in a BFD template for single-hop and multi-hop sessions.
bfd interval	Configures the baseline BFD parameters on the interface.

Command	Description
bfd map	Configures a BFD map that associates addresses with multi-hop templates.
bfd slow-timers	Configures the BFD slow timers value.
bfd template	Binds a single-hop BFD template to an interface.
bfd-template single-hop | multi-hop	Configures the BFD template and enters BFD configuration mode.
clear bfd counters	Clears the BFD counters.
echo	Configures echo in the BFD single-hop template.
neighbor	Configures BFD support for BGP so that BGP is registered to receive forwarding path detection failure messages from BFD.
show bfd drops	Displays the numbered of dropped packets in BFD.
show bfd map	Displays the configured BFD maps.
show bfd neighbors	Displays a line-by-line listing of existing BFD adjacencies.
show bfd summary	Displays summary information for BFD.

bfd interval

To configure the baseline BFD parameters on the interface, use the bfd command in interface configuration mode. To remove the baseline BFD session parameters, use the **no** form of this command.

bfd interval *milliseconds* **min_rx** *milliseconds* **multiplier** *multiplier-value*
no bfd interval *milliseconds* **min_rx** *milliseconds* **multiplier** *multiplier-value*

Syntax Description

interval	Specifies the rate at which BFD control packets are sent to BFD peers. The range is 50 to 999 milliseconds.
min_rx	Specifies the rate at which BFD control packets are expected to be received from BFD peers. The range is 50 to 999 milliseconds.
multiplier	Specifies the rate at which BFD control packets must be missed from a BFD peer before BFD declares that the peer is unavailable and the Layer 3 BFD peer is informed of the failure. The range is 3 to 50.
milliseconds	The value in milliseconds.
multiplier-value	The value of the multiplier.

Command Default

This command has no default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.6(2)	This command was added.

Examples

The following example associates a BFD template with a BFD map.

```
(config)# interface gigabitethernet 0/0
(config-if)# bfd interval 50 min_rx 50 multiplier 3
```

Related Commands

Command	Description
authentication	Configures authentication in a BFD template for single-hop and multi-hop sessions.
bfd echo	Enables BFD echo mode on the interface,
bfd map	Configures a BFD map that associates addresses with multi-hop templates.
bfd slow-timers	Configures the BFD slow timers value.
bfd template	Binds a single-hop BFD template to an interface.
bfd-template single-hop | multi-hop	Configures the BFD template and enters BFD configuration mode.
clear bfd counters	Clears the BFD counters.
echo	Configures echo in the BFD single-hop template.
neighbor	Configures BFD support for BGP so that BGP is registered to receive forwarding path detection failure messages from BFD.
show bfd drops	Displays the numbered of dropped packets in BFD.
show bfd map	Displays the configured BFD maps.
show bfd neighbors	Displays a line-by-line listing of existing BFD adjacencies.
show bfd summary	Displays summary information for BFD.

bfd map

To configure a BFD map that associates addresses with multi-hop templates, use the bfd map command in global configuration mode. To delete a BFD map, use the **no** form of this command.

bfd map { **ipv4** | **ipv6** } *destination/cdir source/cdir template-name*
no bfd map

Syntax Description

ipv4	Configures an IPv4 address.
ipv6	Configures an IPv6 address.
destination/cdir	The destination prefix/length.
source/cdir	The source prefix/length.
template-name	Name of the BFD template associated with the BFD map.

Command Default

This command has no default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.6(2)	This command was added.

Examples

The following example associates a BFD template with a BFD map.

```
ciscoasa(config)# bfd map ipv4 10.11.11.0/24 10.36.42.5/32 multihop-template1
```

Related Commands

Command	Description
authentication	Configures authentication in a BFD template for single-hop and multi-hop sessions.
bfd echo	Enables BFD echo mode on the interface,
bfd interval	Configures the baseline BFD parameters on the interface.

Command	Description
bfd slow-timers	Configures the BFD slow timers value.
bfd template	Binds a single-hop BFD template to an interface.
bfd-template single-hop | multi-hop	Configures the BFD template and enters BFD configuration mode.
clear bfd counters	Clears the BFD counters.
echo	Configures echo in the BFD single-hop template.
neighbor	Configures BFD support for BGP so that BGP is registered to receive forwarding path detection failure messages from BFD.
show bfd drops	Displays the numbered of dropped packets in BFD.
show bfd map	Displays the configured BFD maps.
show bfd neighbors	Displays a line-by-line listing of existing BFD adjacencies.
show bfd summary	Displays summary information for BFD.

bfd slow-timers

To configure the BFD slow timers value, use the bfd slow-timers command in global configuration mode.

bgp slow-timers [*milliseconds*]

Syntax Description

milliseconds	(Optional) The BFD slow timers value in milliseconds. The range is 1000 to 30,000. The default is 1000.

Command Default

The default value of the BFD slow timer is 1000 milliseconds.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.6(2)	This command was added.

Examples

The following example configures BFD slow timers for 14,000 milliseconds.

```
ciscoasa(config)# bfd slow-timers 14000
```

Related Commands

Command	Description
authentication	Configures authentication in a BFD template for single-hop and multi-hop sessions.
bfd echo	Enables BFD echo mode on the interface,
bfd interval	Configures the baseline BFD parameters on the interface.
bfd map	Configures a BFD map that associates addresses with multi-hop templates.
bfd template	Binds a single-hop BFD template to an interface.
bfd-template single-hop | multi-hop	Configures the BFD template and enters BFD configuration mode.
clear bfd counters	Clears the BFD counters.

Command	Description
echo	Configures echo in the BFD single-hop template.
neighbor	Configures BFD support for BGP so that BGP is registered to receive forwarding path detection failure messages from BFD.
show bfd drops	Displays the numbered of dropped packets in BFD.
show bfd map	Displays the configured BFD maps.
show bfd neighbors	Displays a line-by-line listing of existing BFD adjacencies.
show bfd summary	Displays summary information for BFD.

bfd-template

To configure the BFD template and enter BFD configuration mode, use the bfd-template command in global configuration mode. To disable a BFD template, use the **no** form of this command.

bfd-template [**single-hop** | **multi-hop**] *template-name*
no bfd-template [**single-hop** | **multi-hop**] *template-name*

Syntax Description

single-hop	Specifies a single-hop BFD template.
multi-hop	Specifies a multi-hop BFD template.
template-name	Name of the BFD template.

Command Default

This command has no default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.6(2)	This command was added.

Usage Guidelines

Use this command to create a BFD template and enter BFD configuration mode. You can also specify a set of BFD interval values in the template. BFD interval values specified as part of the BFD template are not specific to a single interface.

Examples

The following example configures a single-hop BFD template.

```
ciscoasa(config)# bfd single-hop node1
ciscoasa(config-bfd)# interval min-tx 100 min-rx 100 mulitplier 3
```

The following example configures multi-hop BFD template.

```
ciscoasa(config)# bfd multi-hop mh-template
ciscoasa(config-bfd)# interval min-tx 100 min-rx 100 mulitplier 3
```

Related Commands

Command	Description
authentication	Configures authentication in a BFD template for single-hop and multi-hop sessions.
bfd echo	Enables BFD echo mode on the interface,
bfd interval	Configures the baseline BFD parameters on the interface.
bfd map	Configures a BFD map that associates addresses with multi-hop templates.
bfd slow-timers	Configures the BFD slow timers value.
bfd template	Binds a single-hop BFD template to an interface.
clear bfd counters	Clears the BFD counters.
echo	Configures echo in the BFD single-hop template.
neighbor	Configures BFD support for BGP so that BGP is registered to receive forwarding path detection failure messages from BFD.
show bfd drops	Displays the numbered of dropped packets in BFD.
show bfd map	Displays the configured BFD maps.
show bfd neighbors	Displays a line-by-line listing of existing BFD adjacencies.
show bfd summary	Displays summary information for BFD.

bgp aggregate-timer

To set the interval at which BGP routes will be aggregated or to disable timer-based route aggregation, use the bgp aggregate-timer command in address family configuration mode. To restore the default value, use the no form of this command.

bgp aggregate-timer *seconds*
no bgp aggregate-timer

Syntax Description

seconds	The interval (in seconds) at which the system will aggregate BGP routes. Valid values are in the range from 6 to 60 or else 0 (zero). The default value is 30. A value of 0 (zero) disables timer-based aggregation and starts aggregation immediately.

Command Default

The default value of the bgp aggregate timer is 30 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Address-family configuration, Address-family IPv6 sub mode	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.2(1)	This command was added.
9.3(2)	This command was modified to be supported in address-family IPv6 sub mode.

Usage Guidelines

Use this command to change the default interval at which BGP routes are aggregated.

In very large configurations, even if the aggregate-address summary-only command is configured, more specific routes are advertised and later withdrawn. To avoid this behavior, configure the bgp aggregate-timer to 0 (zero), and the system will immediately check for aggregate routes and suppress specific routes.

Examples

The following example configures BGP route aggregation at 20-second intervals:

```
ciscoasa(config)# router bgp 50
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# bgp aggregate-timer 20
```

The following example starts BGP route aggregation immediately:

```
ciscoasa(config)# router bgp 50
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# aggregate-address 10.0.0.0 255.0.0.0 summary-only
ciscoasa(config-router-af)# bgp aggregate-timer 20
```

Related Commands

Command	Description
address-family ipv4	Enters the address family configuration mode to configure a routing session using standard IP Version 4 (IPv4) address prefixes.
aggregate-address	Creates an aggregate entry in a Border Gateway Protocol (BGP) database.

bgp always-compare-med

To enable the comparison of the Multi Exit Discriminator (MED) for paths from neighbors in different autonomous systems, use the bgp always-compare-med command in router configuration mode. To disallow the comparison, use the no form of this command.

bgp always-compare-med
no bgp always-compare-med

Syntax Description

This command has no arguments or keywords.

Command Default

ASA routing software does not compare the MED for paths from neighbors in different autonomous systems if this command is not enabled or if the no form of this command is entered.

The MED is compared only if the autonomous system path for the compared routes is identical.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router configuration	• Yes	—	• Yes	• Yes	• Yes

Command History

Release	Modification
9.2(1)	This command was added.

Usage Guidelines

The MED, as stated in RFC 1771, is an optional non-transitive attribute that is a four octet non-negative integer. The value of this attribute may be used by the BGP best path selection process to discriminate among multiple exit points to a neighboring autonomous system.

The MED is one of the parameters that is considered when selecting the best path among many alternative paths. The path with a lower MED is preferred over a path with a higher MED. During the best-path selection process, MED comparison is done only among paths from the same autonomous system. The bgp always-compare-med command is used to change this behavior by enforcing MED comparison between all paths, regardless of the autonomous system from which the paths are received.

The bgp deterministic-med command can be configured to enforce deterministic comparison of the MED value between all paths received from within the same autonomous system.

Examples

In the following example, the local BGP routing process is configured to compare the MED from alternative paths, regardless of the autonomous system from which the paths are received:

```
ciscoasa(config)# router bgp 5000
ciscoasa(config-router)# bgp always-compare-med
```

Related Commands

Command	Description
bgp deterministic-med	Enforces the deterministic comparison of the Multi Exit Discriminator (MED) value between all paths received from within the same autonomous system.

bgp asnotation dot

To change the default display and regular expression match format of Border Gateway Protocol (BGP) 4-byte autonomous system numbers from asplain (decimal values) to dot notation, use the bgp asnotation dot command in router configuration mode. To reset the default 4-byte autonomous system number display and regular expression match format to asplain, use the no form of this command.

bgp asnotation dot
no bgp asnotation dot

Syntax Description

This command has no arguments or keywords.

Command Default

BGP autonomous system numbers are displayed using asplain (decimal value) format in screen output, and the default format for matching 4-byte autonomous system numbers in regular expressions is asplain.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router configuration	• Yes	—	• Yes	• Yes	• Yes

Command History

Release	Modification
9.2(1)	This command was added.

Usage Guidelines

Prior to January 2009, BGP autonomous system numbers that were allocated to companies were 2-octet numbers in the range from 1 to 65535 as described in RFC 4271, A Border Gateway Protocol 4 (BGP-4).

Due to increased demand for autonomous system numbers, the Internet Assigned Number Authority (IANA) will start in January 2009 to allocate four-octet autonomous system numbers in the range from 65536 to 4294967295. RFC 5396, Textual Representation of Autonomous System (AS) Numbers, documents three methods of representing autonomous system numbers. Cisco has implemented the following two methods:

- Asplain—Decimal value notation where both 2-byte and 4-byte autonomous system numbers are represented by their decimal value. For example, 65526 is a 2-byte autonomous system number and 234567 is a 4-byte autonomous system number.
- Asdot—Autonomous system dot notation where 2-byte autonomous system numbers are represented by their decimal value and 4-byte autonomous system numbers are represented by a dot notation. For example, 65526 is a 2-byte autonomous system number and 1.169031 is a 4-byte autonomous system number (this is dot notation for the 234567 decimal numbers).

Cisco implementation of 4-byte autonomous system numbers uses asplain as the default display format for autonomous system numbers, but you can configure 4-byte autonomous system numbers in both the asplain and asdot format. In addition, the default format for matching 4-byte autonomous system numbers in regular expressions is asplain, so you must ensure that any regular expressions to match 4-byte autonomous system numbers are written in the asplain format. If you want to change the default show command output to display 4-byte autonomous system numbers in the asdot format, use the bgp asnotation dot command under router configuration mode. When the asdot format is enabled as the default, any regular expressions to match 4-byte autonomous system numbers must be written using the asdot format, or the regular expression match will fail. Tables below show that although you can configure 4-byte autonomous system numbers in either asplain or asdot format, only one format is used to display show command output and control 4-byte autonomous system number matching for regular expressions, and the default is asplain format.

To display 4-byte autonomous system numbers in show command output and to control matching for regular expressions in the asdot format, you must configure the bgp asnotation dot command. After enabling the bgp asnotation dot command, a hard reset must be initiated for all BGP sessions by entering the clearbgp * command.

Table 1: Default Asplain 4-byte Autonomous System Number Format

Format	Configuration Format	Show Command Output and Regular Expression Match Format
asplain	2-byte: 1 to 65534-byte: 65536 to 4294967295	2-byte: 1 to 65534-byte: 65536 to 4294967295
asdot	2-byte: 1 to 65534-byte: 1.0 to 65535.65535	2-byte: 1 to 65534-byte: 65536 to 4294967295

Table 2: Asdot 4-Byte Autonomous System Number Format

Format	Configuration Format	Show Command Output and Regular Expression Match Format
asplain	2-byte: 1 to 655354-byte: 65536 to 4294967295	2-byte: 1 to 655354-byte: 1.0 to 65535.65535
asdot	2-byte: 1 to 655354-byte: 1.0 to 65535.65535	2-byte: 1 to 655354-byte: 1.0 to 65535.65535

Examples

The following output from the show bgp summary command shows the default asplain format of the 4-byte autonomous system numbers. Note the asplain format of the 4-byte autonomous system numbers, 65536 and 65550.

```
ciscoasa(config-router)# show bgp summary
BGP router identifier 172.17.1.99, local AS number 65538
BGP table version is 1, main routing table version 1

 Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  Statd
 192.168.1.2     4       65536       7       7        1    0    0 00:03:04      0
 192.168.3.2     4       65550       4       4        1    0    0 00:00:15      0
```

The following configuration is performed to change the default output format to the asdot notation format:

```
ciscoasa# configure terminal
ciscoasa(config)# router bgp 65538
ciscoasa(config-router)# bgp asnotation dot
```

After the configuration is performed, the output is converted to asdot notation format as shown in the following output from the show bgp summary command. Note the asdot format of the 4-byte autonomous system numbers, 1.0 and 1.14 (these are the asdot conversions of the 65536 and 65550 autonomous system numbers).

```
ciscoasa(config-router)# show bgp summary
BGP router identifier 172.17.1.99, local AS number 1.2
BGP table version is 1, main routing table version 1
Neighbor        V          AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  Statd
192.168.1.2     4         1.0       9       9        1    0    0 00:04:13     0
192.168.3.2     4        1.14       6       6        1    0    0 00:01:24     0
```

After the bgp asnotation dot command is configured, the regular expression match format for 4-byte autonomous system paths is changed to asdot notation format. Although a 4-byte autonomous system number can be configured in a regular expression using either asplain format or asdot format, only 4-byte autonomous system numbers configured using the current default format are matched. In the first example, the show bgp regexp command is configured with a 4-byte autonomous system number in asplain format. The match fails because the default format is currently asdot format and there is no output. In the second example using asdot format, the match passes and the information about the 4-byte autonomous system path is shown using the asdot notation.

```
ciscoasa(config-router)# show bgp regexp ^65536$
ciscoasa(config-router)# show bgp regexp ^1\.0$
BGP table version is 2, local router ID is 172.17.1.99
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
Network          Next Hop            Metric LocPrf Weight Path
*> 10.1.1.0/24      192.168.1.2              0             0 1.0 i
```

Note The asdot notation uses a period, which is a special character in Cisco regular expressions. To remove the special meaning, use a backslash before the period.

Related Commands

Command	Description
show bgp summary	Displays the status of all Border Gateway Protocol (BGP) connections.
show bgp regexp	Displays routes matching the autonomous system path regular expression.

bgp bestpath compare-routerid

To configure a Border Gateway Protocol (BGP) routing process to compare identical routes received from different external peers during the best path selection process and to select the route with the lowest router ID as the best path, use the bgp bestpath compare-routerid command in router configuration mode.

To return the BGP routing process to the default operation, use the no form of this command.

bgp bestpath compare-routerid
no bgp bestpath compare-routerid

Syntax Description

This command has no arguments or keywords.

Command Default

The behavior of this command is disabled by default; BGP selects the route that was received first when two routes with identical attributes are received.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router configuration	• Yes	—	• Yes	• Yes	• Yes

Command History

Release	Modification
9.2(1)	This command was added.

Usage Guidelines

The bgp bestpath compare-routerid command is used to configure a BGP routing process to use the router ID as the tie breaker for best path selection when two identical routes are received from two different peers (all the attributes are the same except for the router ID). When this command is enabled, the lowest router ID will be selected as the best path when all other attributes are equal.

Examples

In the following example, the BGP routing process is configured to compare and use the router ID as a tie breaker for best path selection when identical paths are received from different peers:

```
ciscoasa(config)# router bgp 5000
ciscoasa(config-router)# bgp bestpath compare-routerid
```

bgp bestpath med missing-as-worst

To configure a Border Gateway Protocol (BGP) routing process to assign a value of infinity to routes that are missing the Multi Exit Discriminator (MED) attribute (making the path without a MED value the least desirable path), use the bgp bestpath med missing-as-worst command in router configuration mode. To return the router to the default behavior (assign a value of 0 to the missing MED), use the no form of this command.

bgp bestpath med missing-as-worst
no bgp bestpath med missing-as-worst
bgp bestpath med missing-as-worst

Syntax Description

This command has no arguments or keywords.

Command Default

ASA software assigns a value of 0 to routes that are missing the MED attribute, causing the route with the missing MED attribute to be considered the best path.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router configuration	• Yes	—	• Yes	• Yes	• Yes

Command History

Release	Modification
9.2(1)	This command was added.

Examples

In the following example, the BGP router process is configured to consider a route with a missing MED attribute as having a value of infinity (4294967294), making this path the least desirable path:

```
ciscoasa(config)# router bgp 5000
ciscoasa(config-router)# bgp bestpath med missing-as-worst
```

bgp-community new-format

To configure BGP to display communities in the format AA:NN (autonomous system:community number/4-byte number), use the bgp-community new-format command in global configuration mode. To configure BGP to display communities as a 32-bit number, use the no form of this command.

bgp-community new-format
no bgp-community new-format

Syntax Description

This command has no arguments or keywords.

Command Default

BGP communities (also when entered in the AA:NN format) are displayed as a 32-bit numbers if this command is not enabled or if the no form is entered.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.2(1)	This command was added.

Usage Guidelines

The bgp-community new-format command is used to configure the local router to display BGP communities in the AA:NN format to conform with RFC-1997.

This command only affects the format in which BGP communities are displayed; it does not affect the community or community exchange. However, expanded IP community lists that match locally configured regular expressions may need to be updated to match on the AA:NN format instead of the 32-bit number.

RFC 1997, BGP Communities Attribute, specifies that a BGP community is made up of two parts that are each 2 bytes long. The first part is the autonomous system number and the second part is a 2-byte number defined by the network operator.

Examples

In the following example, a router that uses the 32-bit number community format is upgraded to use the AA:NN format:

```
ciscoasa(config)# bgp-community new-format
ciscoasa(config-router)# no bgp transport path-mtu-discovery
```

The following sample output shows how BGP community numbers are displayed when the bgp-community new-format command is enabled:

```
ciscoasa(router)# show bgp 10.0.0.0
BGP routing table entry for 10.0.0.0/8, version 4
Paths: (2 available, best #2, table Default-IP-Routing-Table)
Advertised to non peer-group peers:
10.0.33.35
35
10.0.33.35 from 10.0.33.35 (192.168.3.3)
Origin incomplete, metric 10, localpref 100, valid, external
Community: 1:1
Local
0.0.0.0 from 0.0.0.0 (10.0.33.34)
Origin incomplete, metric 0, localpref 100, weight 32768, valid, sourced, best
```

bgp default local-preference

To change the default local preference value, use the bgp default local-preference command in router configuration mode. To return the local preference value to the default setting, use the no form of this command.

bgp default local-preference *number*
no bgp default local-preference *number*

Syntax Description

number	Local preference value from 0 to 4294967295.

Command Default

ASA software applies a local preference value of 100 if this command is not enabled or if the no form of this command is entered.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router configuration	• Yes	—	• Yes	• Yes	• Yes

Command History

Release	Modification
9.2(1)	This command was added.

Usage Guidelines

The local preference attribute is a discretionary attribute that is used to apply the degree of preference to a route during the BGP best path selection process. This attribute is exchanged only between iBGP peers and is used to determine local policy. The route with the highest local preference is preferred.

Examples

In the following example, the local preference value is set to 200:

```
ciscoasa(config)# router bgp 5000
ciscoasa(config-router)# bgp default local-preference 200
```

bgp deterministic-med

To enforce the deterministic comparison of the Multi Exit Discriminator (MED) value between all paths received from within the same autonomous system use the bgp deterministic-med command in router configuration mode. To disable the required MED comparison, use the no form of this command.

bgp deterministic-med
no bgp deterministic-med

Syntax Description

This command has no arguments or keywords.

Command Default

ASA software does not enforce the deterministic comparison of the MED variable between all paths received from the same autonomous system.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router configuration	• Yes	—	• Yes	• Yes	• Yes

Command History

Release	Modification
9.2(1)	This command was added.

Usage Guidelines

The bgp always-compare-med command is used to enable the comparison of the Multi Exit Discriminator (MED) for paths from neighbors in different autonomous systems. After the bgp always-compare-med command is configured, all paths for the same prefix that are received from different neighbors, which are in the same autonomous system, will be grouped together and sorted by the ascending MED value (received-only paths are ignored and not grouped or sorted).

The best path selection algorithm will then pick the best paths using the existing rules; the comparison is made on a per neighbor autonomous system basis and then global basis. The grouping and sorting of paths occurs immediately after this command is entered. For correct results, all routers in the local autonomous system must have this command enabled (or disabled).

Examples

In the following example, BGP is configured to compare the MED during path selection for routes advertised by the same sub autonomous system within a confederation:

```
ciscoasa(config)# router bgp 50000
ciscoasa(config-router)# bgp deterministic-med
```

The following example show bgp command output shows how route selection is affected by the configuration of the bgp deterministic-med command. The order in which routes are received affects how routes are selected for best path selection when the bgp deterministic-med command is not enabled. The following sample output from the show bgp command shows three paths that are received for the same prefix (10.100.0.0), and the bgp deterministic-med command is not enabled:

```
ciscoasa(router)# show bgp 10.100.0.0
BGP routing table entry for 10.100.0.0/16, version 40
Paths: (3 available, best #3, advertised over IBGP, EBGP)
109
   192.168.43.10 from 192.168.43.10 (192.168.43.1)
     Origin IGP, metric 0, localpref 100, valid, internal
 2051
   192.168.43.22 from 192.168.43.22 (192.168.43.2)
     Origin IGP, metric 20, localpref 100, valid, internal
 2051
   192.168.43.3 from 192.168.43.3 (10.4.1.1)
     Origin IGP, metric 30, valid, external, best
```

If the bgp deterministic-med feature is not enabled on the router, the route selection can be affected by the order in which the routes are received. Consider the following scenario in which a router received three paths for the same prefix:

The clear bgp * command is entered to clear all routes in the local routing table.

```
ciscoasa(router)# clear bgp *
```

The show bgp command is issued again after the routing table has been repopulated. Note that the order of the paths changed after clearing the BGP session. The results of the selection algorithm also changed because the order in which the paths were received was different for the second session.

```
ciscoasa(router)# show bgp 10.100.0.0


BGP routing table entry for 10.100.0.0/16, version 2
Paths: (3 available, best #3, advertised over EBGP)
 109 192.168.43.10 from 192.168.43.10 (192.168.43.1)
     Origin IGP, metric 0, localpref 100, valid, internal
 2051
   192.168.43.3 from 192.168.43.3 (10.4.1.1)
     Origin IGP, metric 30, valid, external
 2051
   192.168.43.22 from 192.168.43.22 (192.168.43.2)
     Origin IGP, metric 20, localpref 100, valid, internal, best
```

If the bgp deterministic-med command is enabled, then the result of the selection algorithm will always be the same, regardless of the order in which the paths are received by the local router. The following output is always generated when the bgp deterministic-med command is entered on the local router in this scenario:

```
ciscoasa(router)# show bgp 10.100.0.0
BGP routing table entry for 10.100.0.0/16, version 15
Paths: (3 available, best #1, advertised over EBGP)
 109
   192.168.43.10 from 192.168.43.10 (192.168.43.1)
     Origin IGP, metric 0, localpref 100, valid, internal, best 3
   192.168.43.22 from 192.168.43.22 (192.168.43.2)
      Origin IGP, metric 20, localpref 100, valid, internal 3
   192.168.43.3 from 192.168.43.3 (10.4.1.1)
     Origin IGP, metric 30, valid, external
```

Related Commands

Command	Description
bgp always compare-med	Enables the comparison of the Multi Exit Discriminator (MED) for paths from neighbors in different autonomous systems.
clear bgp	Resets BGP connections using hard or soft reconfigurations.
show bgp	Displays entries in the Border Gateway Protocol (BGP) routing table.

bgp enforce-first-as

To configures an ASA to deny an update received from an external BGP (eBGP) peer that does not list its autonomous system number at the beginning of the AS_PATH in the incoming update, use the bgp enforce-first-as command in router configuration mode. To disable this behavior, use the no form of this command.

bgp enforce-first-as
no bgp enforce-first-as

Syntax Description

This command has no arguments or keywords.

Command Default

The behavior of this command is enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router configuration	• Yes	—	• Yes	• Yes	• Yes

Command History

Release	Modification
9.2(1)	This command was added.

Usage Guidelines

The bgp enforce-first-as command is used to deny incoming updates received from eBGP peers that do not list their autonomous system number as the first segment in the AS_PATH attribute. Enabling this command prevents a misconfigured or unauthorized peer from misdirecting traffic (spoofing the local router) by advertising a route as if it was sourced from another autonomous system.

Examples

In the following example, all incoming updates from eBGP peers are examined to ensure that the first autonomous system number in the AS_PATH is the local AS number of the transmitting peer. In the following example, updates from the 10.100.0.1 peer will be discarded if the first AS number is not 65001:

```
ciscoasa(config)# router bgp 50000
ciscoasa(config-router)# bgp enforce-first-as
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# neighbor 10.100.0.1 remote-as 65001
```

Related Commands

Command	Description
address-family ipv4	Enter address-family configuration mode.
neighbor remote-as	Add an entry to the BGP or the multiprotocol BGP routing table.

bgp fast-external-fallover

To configure a Border Gateway Protocol (BGP) routing process to immediately reset external BGP peering sessions if the link used to reach these peers goes down, use the bgp fast-external-fallover command in router configuration mode. To disable BGP fast external fallover, use the no form of this command.

bgp fast-external-fallover
no bgp fast-external-fallover

Syntax Description

This command has no arguments or keywords.

Command Default

BGP fast external fallover is enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router configuration	• Yes	—	• Yes	• Yes	• Yes

Command History

Release	Modification
9.2(1)	This command was added.

Usage Guidelines

The bgp fast-external-fallover command is used to disable or enable fast external fallover for BGP peering sessions with directly connected external peers. The session is immediately reset if link goes down. Only directly connected peering sessions are supported. If BGP fast external fallover is disabled, the BGP routing process will wait until the default hold timer expires (3 keepalives) to reset the peering session. BGP fast external fallover can also be configured on a per-interface basis using the ip bgp fast-external-fallover interface configuration command.

Examples

In the following example, the BGP fast external fallover feature is disabled. If the link through which this session is carried flaps, the connection will not be reset.

```
ciscoasa(config)# router bgp 50000
ciscoasa(config-router)# no bgp fast-external-fallover
```

Related Commands

Command	Description
ip bgp fast-external-fallover	Configure per-interface fast external fallover.

bgp graceful-restart

To configure a Border Gateway Protocol (BGP) routing process for graceful restart in a non-stop forwarding configuration, use the **bgp graceful-restart** command in router configuration mode. To disable BGP graceful restart, use the **no** form of this command.

bgp graceful-restart [**restart-time** *seconds* | **stalepath-time** *seconds*]
no bgp graceful-restart [**restart-time** *seconds* | **stalepath-time seconds**]

Syntax Description

restart-time *seconds*	The maximum time period (in seconds) that the system will wait for a graceful-restart-capable neighbor to return to normal operation after a restart event occurs. The default is 120 seconds. Values are from 1 to 3600 seconds.
stalepath-time *seconds*	The maximum time period (in seconds) that the system will hold stale paths for a restarting peer. All stale paths are deleted after this timer expires. The default value is 360 seconds. Values are from 1 to 3600 seconds.

Command Default

BGP graceful restart is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router configuration	• Yes	—	• Yes	—	• Yes

Command History

Release	Modification
9.3(1)	This command was added.
9.19(1)	This command was extended to support graceful restart for IPv6 address family.

Usage Guidelines

Use this command to enable graceful restart for non-stop forwarding. With graceful restart, the system can advertise the ability to maintain the forwarding state for an address group during restart. Use the **neighbor ha-mode graceful-restart** command to configure restart capability for each BGP neighbor router.

Examples

The following example shows how to enable graceful restart globally using the default timers.

```
ciscoasa(config)# router bgp 50000
ciscoasa(config-router)# bgp graceful-restart
```

Related Commands

Command	Description
neighbor ha-mode graceful-restart	Configure the Border Gateway Protocol (BGP) graceful restart capability for a BGP neighbor

bgp inject-map

To configure conditional route injection to inject more specific routes into a Border Gateway Protocol (BGP) routing table, use the bgp inject-map command in address family configuration mode. To disable a conditional route injection configuration, use the no form of this command.

bgp inject-map *inject-map exist-map* **exist-map** [**copy-attributes**]
no bgp inject-map *inject-map exist-map* **exist-map**

Syntax Description

inject-map	Name of the route map that specifies the prefixes to inject into the local BGP routing table.
exist-map exist-map	Specifies the name of the route map containing the prefixes that the BGP speaker will track.
copy-attributes	(Optional) Configures the injected route to inherit attributes of the aggregate route.

Command Default

No specific routes are injected into a BGP routing table.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Address-family configuration, Address-family IPv6 sub mode	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.2(1)	This command was added.
9.3(2)	This command was modified to be supported in address-family IPv6 sub mode.

Usage Guidelines

The bgp inject-map command is used to configure conditional route injection. Conditional route injection allows you to originate a more specific prefix into a BGP routing table without a corresponding match. Two route maps (exist-map and inject-map) are configured in global configuration mode and then specified with the bgp inject-map command in address family configuration mode.

The exist-map argument specifies a route map that defines the prefix that the BGP speaker will track. This route map must contain a match ip address prefix-list command statement to specify the aggregate prefix and a match ip route-source prefix-list command statement to specify the route source.

The inject-map argument defines the prefixes that will be created and installed into the routing table. Injected prefixes are installed in the local BGP RIB. A valid parent route must exist; Only prefixes that are equal to or more specific than the aggregate route (existing prefix) can be injected.

The optional copy-attributes keyword is used to optionally configure the injected prefix to inherit the same attributes as the aggregate route. If this keyword is not entered, the injected prefix will use the default attributes for locally originated routes.

Examples

In the following example, conditional route injection is configured. Injected prefixes will inherit the attributes of the aggregate (parent) route.

```
ciscoasa(config)# ip prefix-list ROUTE permit 10.1.1.0/24
ciscoasa(config)# ip prefix-list ROUTE_SOURCE permit 10.2.1.1/32
ciscoasa(config)# ip prefix-list ORIGINATED_ROUTES permit 10.1.1.0/25
ciscoasa(config)# ip prefix-list ORIGINATED_ROUTES permit 10.1.1.128/25
ciscoasa(config)# route-map LEARNED_PATH permit 10
ciscoasa(config-route-map)# match ip address prefix-list ROUTE
ciscoasa(config-route-map)# match ip route-source prefix-list ROUTE_SOURCE
ciscoasa(config-route-map)# exit
ciscoasa(config)# route-map ORIGINATE permit 10
ciscoasa(config-route-map)# set ip address prefix-list ORIGINATED_ROUTES
ciscoasa(config-route-map)# set community 14616:555 additive
ciscoasa(config-route-map)# exit
ciscoasa(config)# router bgp 50000
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# bgp inject-map ORIGINATE exist-map LEARNED_PATH copy-attributes
```

Related Commands

Command	Description
ip prefix-list	Creates a prefix-list or adds a prefix-list entry.
set community	Sets the BGP communities attributes.
address-family ipv4	Enters the address-family configuration mode.

bgp log-neighbor-changes

To enable logging of BGP neighbor resets, use the bgp log-neighbor-changes command in router configuration mode. To disable the logging of changes in BGP neighbor adjacencies, use theno form of this command.

bgp log-neighbor-changes
no bgp log-neighbor-changes

Syntax Description

This command has no arguments or keywords.

Command Default

Logging of BGP neighbor is enabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router configuration	• Yes	—	• Yes	• Yes	• Yes

Command History

Release	Modification
9.2(1)	This command was added.

Usage Guidelines

The bgp log-neighbor-changes command enables logging of BGP neighbor status changes (up or down) and resets for troubleshooting network connectivity problems and measuring network stability. Unexpected neighbor resets might indicate high error rates or high packet loss in the network and should be investigated.

Using the bgp log-neighbor-changes command to enable status change message logging does not cause a substantial performance impact, unlike, for example, enabling per BGP update debugging.

The neighbor status change messages are not tracked if the bgp log-neighbor-changes command is not enabled, except for the reset reason, which is always available as output of the show bgp neighbors command.

The eigrp log-neighbor-changes command enables logging of Enhanced Interior Gateway Routing Protocol (EIGRP) neighbor adjacencies, but messages for BGP neighbors are logged only if they are specifically enabled with the bgp log-neighbor-changes command.

Use the show logging command to display the log for the BGP neighbor changes.

Examples

The following example logs neighbor changes for BGP in router configuration mode.

```
ciscoasa(config)# bgp router 40000
ciscoasa(config-router)# bgp log-neighbor-changes
```

Related Commands

Command	Description
show BGP neighbors	Displays information about BGP connection to neighbors.

bgp maxas-limit

To configure Border Gateway Protocol (BGP) to discard routes that has a number of autonomous system numbers in AS-path that exceed the specified value, use the bgp maxas-limit command in router configuration mode. To return the router to default operation, use the no form of this command.

bgp max-as limit *number*
no bgp max-as limit

Syntax Description

number	Maximum number of autonomous system numbers in the AS-path attribute of the BGP Update message, ranging from 1 to 254. In addition to setting the limit on the number of autonomous system numbers within the AS-path segment, the command limits the number of AS-path segments to ten. The behavior to allow ten AS-path segments is built into the bgp maxas-limit command.

Command Default

No routes are discarded.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router configuration	• Yes	—	• Yes	• Yes	• Yes

Command History

Release	Modification
9.2(1)	This command was added.

Usage Guidelines

The bgp maxas-limit command is used to limit the number of autonomous system numbers in the AS-path attribute that are permitted in inbound routes. If a route is received with an AS-path segment that exceeds the configured limit, the BGP routing process will discard the route.

Examples

This example sets a maximum number of autonomous systems numbers in the AS-path attribute to 30.

```
ciscoasa(config)# router bgp 4000
ciscoasa(config)# bgp maxas-limit 30
```

bgp nexthop

To configure Border Gateway Protocol (BGP) next-hop address tracking, use the bgp nexthop command in address family or router configuration mode. To disable BGP next-hop address tracking, use the no form of this command.

bgp nexthop { **trigger** { **delay** *seconds* | **enable** } | **route-map** *map-name* }
no bgp nexthop { **trigger** { **delay** *seconds* | **enable** } | **route-map** *map-name* }

Syntax Description

trigger	Specifies the use of BGP next-hop address tracking. Use this keyword with the delay keyword to change the next-hop tracking delay. Use this keyword with the enable keyword to enable next-hop address tracking.
delay	Changes the delay interval between checks on updated next-hop routes installed in the routing table.
seconds	Number of seconds specified for the delay. Valid values are from 0 to 100. Default is 5.
enable	Enables BGP next-hop address tracking.
route-map	Specifies the use of a route map that is applied to the route in the routing table that is assigned as the next-hop route for BGP prefixes.
map-name	Name of a route map.

Command Default

BGP next-hop address tracking is enabled by default for IPv4.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Address-family configuration Address-family IPv6 sub mode	• Yes	—	• Yes	—	• Yes

Command History

Release	Modification
9.2(1)	This command was added.
9.3(2)	This command was modified to be supported in address-family IPv6 sub mode.

Usage Guidelines

BGP next-hop address tracking is event driven. BGP prefixes are automatically tracked as peering sessions are established. Next-hop changes are rapidly reported to BGP as they are updated in the routing information base (RIB). This optimization improves overall BGP convergence by reducing the response time to next-hop changes for routes installed in the RIB. When a best-path calculation is run in between BGP scanner cycles, only the changes are processed and tracked.

Note BGP next-hop address tracking improves BGP response time significantly. However, unstable Interior Gateway Protocol (IGP) peers can introduce instability to BGP. We recommend that you aggressively dampen unstable IGP peering sessions to mitigate the possible impact to BGP.

- BGP next-hop address tracking is not supported under the IPv6 address family.

Use the trigger keyword with the delay keyword and seconds argument to change the delay interval between routing table walks for BGP next-hop address tracking. You can increase the performance of BGP next-hop address tracking by tuning the delay interval between full routing table walks to match the tuning parameters for the IGP. The default delay interval is 5 seconds, which is an optimal value for a fast-tuned IGP. In the case of an IGP that converges more slowly, you can change the delay interval to 20 seconds or more, depending on the IGP convergence time.

Use the trigger keyword with the enable keyword to enable BGP next-hop address tracking. BGP next-hop address tracking is enabled by default.

Use the route-map keyword and map-name argument to allow a route map to be used. The route map is used during the BGP best-path calculation and is applied to the route in the routing table that covers the Next_Hop attribute for BGP prefixes. If the next-hop route fails the route-map evaluation, the next-hop route is marked as unreachable. This command is per address family, so different route maps can be applied for next-hop routes in different address families.

Note Only the match ip address command is supported in the route map. No set commands or other match commands are supported.

Examples

The following example shows how to change the delay interval between routing table walks for BGP next-hop address tracking to occur every 20 seconds under an IPv4 address family session.

```
ciscoasa(config)# router bgp 50000
ciscoasa(config-router)# address-family ipv4 unicast
ciscoasa(config-router-af)# bgp nexthop trigger delay 20
```

The following example shows how to disable next-hop address tracking for the IPv4 address family:

```
ciscoasa(config)# router bgp 50000
ciscoasa(config-router)# address-family ipv4 unicast
ciscoasa(config-router-af)# no bgp nexthop trigger enable
```

The following example shows how to configure a route map that permits a route to be considered as a next-hop route only if the address mask length is more than 25. This configuration will avoid any prefix aggregates being considered as a next-hop route.

```
ciscoasa(config)# router bgp 45000
ciscoasa(config-router)# address-family ipv4 unicast
ciscoasa(config-router-af)# bgp nexthop route-map CHECK-NEXTHOP
ciscoasa(config-router-af)# exit-address-family
ciscoasa(config-router)# exit
ciscoasa(config)# ip prefix-list FILTER25 seq 5 permit 0.0.0.0/0 ge 25
ciscoasa(config)# route-map CHECK-NEXTHOP permit 10
ciscoasa(config)# match ip address prefix-list FILTER25
```

bgp redistribute-internal

To configure iBGP redistribution into an interior gateway protocol (IGP), such as EIGRP or OSPF, use the bgp redistribute-internal command in address family configuration mode. To return the router to default behavior and stop iBGP redistribution into IGPs, use the no form of this command.

bgp redistribute-internal
no bgp redistribute-internal

Syntax Description

This command has no arguments or keywords.

Command Default

IBGP routes are redistributed into IGPs.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Address-family configuration Address-family IPv6 sub mode	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.2(1)	This command was added.
9.3(2)	This command was modified to be supported in address-family IPv6 sub mode.

Usage Guidelines

The bgp redistribute-internal command is used to configure iBGP redistribution into an IGP. The clear bgp command must be entered to reset BGP connections after this command is configured.

When redistributing BGP into any IGP, be sure to use IP prefix-list and route-map statements to limit the number of prefixes that are redistributed.

Caution Exercise caution when redistributing iBGP into an IGP. Use IP prefix-list and route-map statements to limit the number of prefixes that are redistributed. Redistributing an unfiltered BGP routing table into an IGP can have a detrimental effect on normal IGP network operation.

Examples

In the following example, BGP to OSPF route redistribution is enabled:

```
ciscoasa(config)# router ospf 300
ciscoasa(config-router)# redistribute bgp 200
ciscoasa(config-router)# exit
ciscoasa(config)# router bgp 200
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# bgp redistribute-internal
```

bgp router-id

To configure a fixed router ID for the local Border Gateway Protocol (BGP) routing process, use the bgp router-id command in address family router configuration mode. To remove the fixed router ID from the running configuration file and restore the default router ID selection, use the no form of this command.

bgp router-id *ip-address*
no bgp router-id

Syntax Description

ip-address	Router identifier in the form of an IP address.

Command Default

When this command is not enabled, the router ID is set to the highest IP address on a physical interface.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Address-family configuration Router configuration mode	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.2(1)	This command was added.
9.3(2)	This command was modified.

Usage Guidelines

The bgp router-id command is used to configure a fixed router ID for the local BGP routing process. The router ID is entered in IP address format. Any valid IP address can be used, even an address that is not locally configured on the router.Peering sessions are automatically reset when the router ID is changed. Separate router ID per context is possible.

Examples

The following example shows how to configure the local router with a fixed BGP router ID of 192.168.254.254

```
ciscoasa(config)# router bgp 5000
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# bgp router-id 19.168.254.254
```

bgp scan-time

To configure scanning intervals of Border Gateway Protocol (BGP) routers for next hop validation use the bgp scan-time command in address family configuration mode. To return the scanning interval of a router to its default scanning interval of 60 seconds, use the no form of this command.

bgp scan-time *scanner-interval*
no bgp scan-time *scanner-interval*

Syntax Description

scanner-interval	The scanning interval of BGP routing information. Valid values are from 15 to 60 seconds. The default is 60 seconds

Command Default

The default scanning interval is 60 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Address family configuration	• Yes	—	• Yes	• Yes	• Yes

Command History

Release	Modification
9.2(1)	This command was added.

Usage Guidelines

Entering the no form of this command does not disable scanning, but removes it from the output of the show running-config command.

While bgp nexthop address tracking (NHT) is enabled for an address family, the bgp scan-time command will not be accepted in that address family and will remain at the default value of 60 seconds. NHT must be disabled before the bgp scan-time command will be accepted in either router mode or address family mode.

Examples

In the following router configuration example, the scanning interval for next hop validation of IPv4 unicast routes for BGP routing tables is set to 20 seconds:

```
ciscoasa(config)# router bgp 100
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# no synchronization
ciscoasa(config-router-af)# bgp scan-time 20
```

Related Commands

Command	Description
show running-config	Displays the configuration that is currently displayed on the ASA.
bgp nexthop	Configures BGP next-hop address tracking.

bgp suppress-inactive

To suppress the advertisement of routes that are not installed in the routing information base (RIB), use the bgp suppress-inactive command in address family or router configuration mode.

bgp suppress-inactive
no bgp suppress-inactive

Syntax Description

This command has no arguments or keywords.

Command Default

No routes are suppressed.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Address family configuration Address family IPv6 sub-mode	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.2(1)	This command was added.
9.3(2)	This command was modified to be supported in address-family IPv6 sub mode.

Usage Guidelines

The bgp suppress-inactive command is used to prevent routes that are not installed in the RIB (inactive routes) from being advertised to peers. If this feature is not enabled or if the no form of this command is used, Border Gateway Protocol (BGP) will advertise inactive routes.

Note BGP marks routes that are not installed into the RIB with a RIB-failure flag. This flag will also appear in the output of the show bgp command; for example, Rib-Failure (17). This flag does not indicate an error or problem with the route or the RIB, and the route may still be advertised depending on the configuration of this command. Enter the show bgp rib-failure command to see more information about the inactive route.

Examples

In the following example, the BGP routing process is configured to not advertise routes that are not installed in the RIB:

```
ciscoasa(config)# router bgp 5000
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# bgp suppress-inactive
```

Related Commands

Command	Description
show bgp	Displays entries in the BGP routing table.
show bgp rib-failure	Displays BGP routes that failed to install in the Routing Information Base (RIB) table.

bgp transport

To enable TCP transport session parameters globally for all Border Gateway Protocol (BGP) sessions, use the bgp transport command in router configuration mode. To disable TCP transport session parameters globally for all BGP sessions, use the no form of this command.

bgp transport path-mtu-discovery
no bgp transport path-mtu-discovery

Syntax Description

path-mtu-discovery	Enables transport path maximum transmission unit (MTU) discovery.

Command Default

TCP path MTU discovery is enabled by default for all BGP sessions.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router configuration	• Yes	—	• Yes	• Yes	• Yes

Command History

Release	Modification
9.2(1)	This command was added.

Usage Guidelines

This command is enabled by default because it is used to allow BGP sessions to take advantage of larger MTU links, which can be very important for internal BGP (iBGP) sessions. Use the show bgp neighbors command to ensure that TCP path MTU discovery is enabled.

Examples

The following example shows how to disable TCP path MTU discovery for all BGP sessions:

```
ciscoasa(config)# router bgp 4500
ciscoasa(config-router)# no bgp transport path-mtu-discovery
```

The following example shows how to enable TCP path MTU discovery for all BGP sessions:

```
iscoasa(config)# router bgp 4500
ciscoasa(config-router)# bgp transport path-mtu-discovery
```

Related Commands

Command	Description
show bgp neighbors	Displays information about BGP connections to neighbors.

blocks

To allocate additional memory to block diagnostics (displayed by the **show blocks** command), use the **blocks** command in privileged EXEC mode. To set the value back to the default, use the **no** form of this command.

blocks queue history enable [*memory_size*]
no blocks queue history enable [*memory_size*]

Syntax Description

memory_sizes	(Optional) Sets the memory size for block diagnostics in bytes, instead of applying the dynamic value. If this value is greater than free memory, an error message appears and the value is not accepted. If this value is greater than 50% of free memory, a warning message appears, but the value is accepted.

Command Default

The default memory assigned to track block diagnostics is 2136 bytes.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

To view the currently allocated memory, enter the **show blocks queue history** command.

If you reload the ASA, the memory allocation returns to the default.

The amount of memory allocated will be at most 150 KB, but never more than 50% of free memory. Optionally, you can specify the memory size manually.

Examples

The following example increases the memory size for block diagnostics:

```
ciscoasa# blocks queue history enable
```

The following example increases the memory size to 3000 bytes:

```
ciscoasa# blocks queue history enable 3000
```

The following example attempts to increase the memory size to 3000 bytes, but the value is more than the available free memory:

```
ciscoasa# blocks queue history enable 3000
ERROR: memory size exceeds current free memory
```

The following example increases the memory size to 3000 bytes, but the value is more than 50% of the free memory:

```
ciscoasa# blocks queue history enable 3000
WARNING: memory size exceeds 50% of current free memory
```

Related Commands

Command	Description
clear blocks	Clears the system buffer statistics.
show blocks	Shows the system buffer usage.

boot

To specify which image the system uses at the next reload and which configuration file the system uses at startup, use the **boot** command in global configuration mode. To restore the default value, use the **no** form of this command.

boot { **config** | **system** } *url*
no boot { **config** | **system** } *url*

Syntax Description

config	Specifies which configuration file to use when the system is loaded.
system	Specifies which image file to use when the system is loaded.
url	Sets the location of the image or configuration. In multiple context mode, all remote URLs must be accessible from the admin context. See the following URL syntax: • **disk0:/**[*path/*]*filename* For the ASA, this URL indicates the internal Flash memory. You can also use **flash** instead of **disk0**; they are aliased. • **disk1:/**[*path/*]*filename* For the ASA, this URL indicates the external Flash memory card. This option is not available for the ASA Services Module. • **flash:/**[*path/*]*filename* This URL indicates the internal Flash memory. • **tftp://**[*user*[**:***password*]**@**]*server*[:*port*]/[*path/*]*filename*[**;int=***interface_name*] Specify the interface name if you want to override the route to the server address. This option is available for the **boot system** command for the ASA 5500 series only; the **boot config** command requires the startup configuration to be on the flash memory. Only one **boot system tftp:** command can be configured, and it must be the first one configured.

Command Default

- ASA image:
  - Firepower 1000, and 2100 in Appliance mode—Boots the previously-running boot image.
  - Other Physical ASAs—Boots the first application image that it finds in internal flash memory.
  - ASA Virtual—Boots the image in the read-only boot:/ partition that was created when you first deployed.
  - Firepower 4100/9300 chassis—The Secure Firewall eXtensible Operating System (FXOS) determines which ASA image to boot. You cannot use this procedure to set the ASA image.
  - Firepower 2100 in Platform mode—The FXOS system determines which ASA/FXOS package to boot. You cannot use this procedure to set the ASA image.

- Startup configuration—By default, the ASA boots from a startup configuration that is a hidden file.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.0(1)	This command was added.
9.13(1)	This command added Firepower 1000 and 2100 in Appliance mode support.

Usage Guidelines

If you have more than one ASA or ASDM image, you should specify the image that you want to boot. If you do not set the image, the default boot image is used, and that image may not be the one intended. For the startup configuration, you can optionally specify a configuration file.

See the following model guidelines:

- Firepower 4100/9300 chassis—ASA upgrades are managed by FXOS; you cannot upgrade the ASA within the ASA operating system, so do not use this command for the ASA image. You can upgrade ASA and FXOS separately from each other, and they are listed separately in the FXOS directory listing. The ASA package always includes ASDM.
- Firepower 2100 in Platform mode—The ASA, ASDM, and FXOS images are bundled together into a single package. Package updates are managed by FXOS; you cannot upgrade the ASA within the ASA operating system, so do not use this command for the ASA image. You cannot upgrade ASA and FXOS separately from each other; they are always bundled together.
- Firepower 1000 and 2100 in Appliance mode—The ASA, ASDM, and FXOS images are bundled together into a single package. Package updates are managed by ASA using this command. Although these platforms use the ASA to identify the image to boot, the underlying mechanism is different from legacy ASAs.
- ASA Virtual—The initial deployment ASA virtual package puts the ASA image in the read-only boot:/ partition. When you upgrade the ASA virtual, you specify a different image in flash memory. Note that if you later clear your configuration (**clear configure all**), then the ASA virtual will revert to loading the original deployment image. The initial deployment ASA virtual package also includes an ASDM image that it places in flash memory. You can upgrade the ASDM image separately.

When you save the **boot config** command to the startup configuration using the **write memory** command, you also save the settings to the CONFIG_FILE environment variable, which the ASA uses to determine the startup configuration to boot when it restarts.

If you want to use a startup configuration file at the new location that is different from the current running configuration, then be sure to copy the startup configuration file to the new location after you save the running configuration. Otherwise, the running configuration will overwrite the new startup configuration when you save it.

Tip The ASDM image file is specified by the asdm image command.

boot system for the Firepower 1000 and 2100 in Appliance Mode

You can only enter a single **boot system** command. If you upgrade to a new image, then you must enter **no boot system** to remove the previous image you set.

Note that you may not have a **boot system** command present in your configuration; for example, if you installed the image from ROMMON, have a new device, or you removed the command manually.

The **boot system** command performs an action when you enter it: the system validates and unpacks the image and copies it to the boot location (an internal location on disk0 managed by FXOS). The new image will load when you reload the ASA. If you change your mind prior to reloading, you can enter the **no boot system** command to delete the new image from the boot location, so the current image continues to run. You can even delete the original image file from the ASA flash memory after you enter this command, and the ASA will boot correctly from the boot location.

Unlike other models, this command in the startup configuration does not affect the booting image, and is essentially cosmetic. The last-loaded boot image will always run upon reload. If you do not save the configuration after you enter this command, then when you reload, the old command will be present in your configuration, even though the new image was booted. Be sure to save the configuration so that the configuration remains in sync.

You can only load images with the original filename from the Cisco download site. If you change the filename, it will not load. You can also reimage to the Secure Firewall Threat Defense (formerly Firepower Threat Defense) by loading an threat defense image. In this case, you are prompted to reload immediately.

boot system for Other Models

You can enter up to four **boot system** command entries to specify different images to boot from in order; the ASA boots the first image it finds successfully. When you enter the **boot system** command, it adds an entry at the bottom of the list. To reorder the boot entries, you must remove all entries using the **clear configure boot system** command, and re-enter them in the order you desire. Only one **boot system tftp** command can be configured, and it must be the first one configured.

When you save the **boot system** command to the startup configuration using the **write memory** command, you also save the settings to the BOOT environment variable, which the ASA uses to determine the startup image to boot when it restarts.

Examples

The following example specifies that at startup the ASA should load a configuration file called configuration.txt:

```
ciscoasa(config)# boot config disk0:/configuration.txt
```

Related Commands

Command	Description
asdm image	Specifies the ASDM software image.
show bootvar	Displays boot file and configuration environment variables.

border style

To customize the border of the WebVPN Home page that is displayed to authenticated WebVPN users, use the **border style** command in customization configuration mode. To remove the command from the configuration and cause the value to be inherited, use the **no** form of this command.

border style *value*
no border style *value*

Syntax Description

value	Specifies the Cascading Style Sheet (CSS) parameters to use. The maximum number of characters allowed is 256.

Command Default

The default style of the border is background-color:#669999;color:white.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Customization configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.1(1)	This command was added.

Usage Guidelines

The **style** option is expressed as any valid Cascading Style Sheet (CSS) parameters. Describing these parameters is beyond the scope of this document. For more information about CSS parameters, consult CSS specifications at the World Wide Web Consortium (W3C) website at www.w3.org. Appendix F of the CSS 2.1 Specification contains a convenient list of CSS parameters, and is available at www.w3.org/TR/CSS21/propidx.html.

Here are some tips for making the most common changes to the WebVPN pages—the page colors:

- You can use a comma-separated RGB value, an HTML color value, or the name of the color if recognized in HTML.
- RGB format is 0,0,0, a range of decimal numbers from 0 to 255 for each color (red, green, blue); the comma-separated entry indicates the level of intensity of each color to combine with the others.
- HTML format is #000000, six digits in hexadecimal format; the first and second represent red, the third and fourth green, and the fifth and sixth represent blue.

Note To easily customize the WebVPN pages, we recommend that you use ASDM, which has convenient features for configuring style elements, including color swatches and preview capabilities.

Examples

The following example customizes the background color of the border to the RGB color #66FFFF, a shade of green:

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# border style background-color:66FFFF
```

Related Commands

Command	Description
application-access	Customizes the Application Access box of the WebVPN Home page.
browse-networks	Customizes the Browse Networks box of the WebVPN Home page.
web-bookmarks	Customizes the Web Bookmarks title or links on the WebVPN Home page.
file-bookmarks	Customizes the File Bookmarks title or links on the WebVPN Home page.

breakout

To break out 10GB ports from a 40GB or higher interface, use the **breakout** command in global configuration mode. To rejoin the interfaces, use the **no** form of the command.

breakout *slot port*
no breakout *slot port*

Syntax Description

slot *port*	Specifies the interface slot and port that you want to break out. For example, to break out the Ethernet2/1 40GB interface, you would specify **2** for the slot and 1 for the port

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.18(1)	This command was added.

Usage Guidelines

Breakout ports can be used just like any other physical Ethernet port, including being added to EtherChannels.

If an interface is already in use in your configuration, you will have to manually remove any configuration related to interfaces that will no longer be present.

You must use a supported breakout cable. See the hardware installation guide for more information.

For clustering or failover, make sure the cluster/failover link is not using the parent interface (for breaking out) or the child interface (for rejoining); you cannot make changes to the interface if it is in use for the cluster/failover link.

For clustering or failover, enter this command on the control node/active unit; the module state is replicated to the other nodes.

For rejoining, you must rejoin all child ports for the interface.

Examples

The following example breaks out the Ethernet2/1 40GB interface. The resulting child interfaces will be identified as Ethernet2/1/1, Ethernet2/1/2, Ethernet2/1/3, and Ethernet2/1/4.

```
ciscoasa(config)# breakout 2 1
```

The following example rejoins the Ethernet2/1 40GB interface.

```
ciscoasa(config)# no breakout 2 1
```

Related Commands

Command	Description
interface	Configures an interface.

bridge-group

To assign an interface to a bridge group, use the **bridge-group** command in interface configuration mode. To unassign an interface, use the **no** form of this command. Bridge groups connect the same network on its interfaces.

bridge-group *number*
no bridge-group *number*

Syntax Description

number	Specifies an integer between 1 and 100. For 9.3(1) and later, the range is increased to between 1 and 250.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.4(1)	This command was added.
9.3(1)	The number range was increased to between 1 and 250 to support 250 BVIs.
9.6(2)	The maximum interfaces per bridge group was increased from 4 to 64.
9.7(1)	Support for routed mode was added.

Usage Guidelines

For 9.2 and earlier, You can configure up to 8 bridge groups in single mode or per context in multiple mode; for 9.3(1) and later, you can configure up to 250 bridge groups. Each bridge group can include up to 64 interfaces (4 interfaces for 9.6(1) and earlier). You cannot assign the same interface to more than one bridge group. Note that you must use at least 1 bridge group; data interfaces must belong to a bridge group.

Note Although you can configure multiple bridge groups on the ASA 5505, the restriction of 2 data interfaces in transparent mode on the ASA 5505 means you can only effectively use 1 bridge group.

Assign a management IP address to the bridge group using the **interface bvi** command and then the **ip address** command.

Each bridge group connects to a separate network. Bridge group traffic is isolated from other bridge groups; traffic is not routed to another bridge group within the ASA, and traffic must exit the ASA before it is routed by an external router back to another bridge group in the ASA.

You might want to use more than one bridge group if you do not want the overhead of security contexts, or want to maximize your use of security contexts. Although the bridging functions are separate for each bridge group, many other functions are shared between all bridge groups. For example, all bridge groups share a syslog server or AAA server configuration. For complete security policy separation, use security contexts with one bridge group in each context.

Examples

The following example assigns GigabitEthernet 1/1 to bridge group 1:

```
ciscoasa(config)# interface gigabitethernet 1/1
ciscoasa(config-if)# bridge-group 1
```

Related Commands

Command	Description
interface	Configures an interface.
interface bvi	Enters the interface configuration mode for a bridge group so you can set the management IP address.
ip address	Sets the management IP address for a bridge group.
nameif	Sets the interface name.
security-level	Sets the interface security level.

browse-networks

To customize the Browse Networks box of the WebVPN Home page that is displayed to authenticated WebVPN users, use the **browse-networks** command in webvpn customization configuration mode. To remove the command from the configuration and cause the value to be inherited, use the **no** form of this command.

browse-networks { **title** | **message** | **dropdown** } { **text** | **style** } *value*
no browse-networks [{ **title** | **message** | **dropdown** } { **text** | **style** } *value*]

Syntax Description

dropdown	Specifies a change to the drop-down list.
message	Specifies youa change to the message displayed under the title.
style	Specifies a change to the style.
text	Specifies a change to the text.
title	Specifies a change to the title.
value	Indicates the actual text to display. The maximum number of characters allowed is 256. This value applies to Cascading Style Sheet (CSS) parameters also.

Command Default

The default title text is “Browse Networks”.

The default title style is:

background-color:#99CCCC;color:black;font-weight:bold;text-transform:uppercase

The default message text is “Enter Network Path”.

The default message style is:

background-color:#99CCCC;color:maroon;font-size:smaller.

The default dropdown text is “File Folder Bookmarks”.

The default dropdown style is:

border:1px solid black;font-weight:bold;color:black;font-size:80%.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Webvpn customization configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.1(1)	This command was added.

Usage Guidelines

The **style** option is expressed as any valid Cascading Style Sheet (CSS) parameters. Describing these parameters is beyond the scope of this document. For more information about CSS parameters, consult CSS specifications at the World Wide Web Consortium (W3C) website at www.w3.org. Appendix F of the CSS 2.1 Specification contains a convenient list of CSS parameters, and is available at www.w3.org/TR/CSS21/propidx.html.

Here are some tips for making the most common changes to the WebVPN pages—the page colors:

- You can use a comma-separated RGB value, an HTML color value, or the name of the color if recognized in HTML.
- RGB format is 0,0,0, a range of decimal numbers from 0 to 255 for each color (red, green, blue); the comma separated entry indicates the level of intensity of each color to combine with the others.
- HTML format is #000000, six digits in hexadecimal format; the first and second represent red, the third and fourth green, and the fifth and sixth represent blue.

Note To easily customize the WebVPN pages, we recommend that you use ASDM, which has convenient features for configuring style elements, including color swatches and preview capabilities.

Examples

The following example changes the title to “Browse Corporate Networks”, and the text within the style to blue:

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# browse-networks title text Browse Corporate Networks
ciscoasa(config-webvpn-custom)# browse-networks title style color:blue
```

Related Commands

Command	Description
application-access	Customizes the Application Access box of the WebVPN Home page.
file-bookmarks	Customizes the File Bookmarks title or links on the WebVPN Home page.
web-applications	Customizes the Web Application box of the WebVPN Home page.
web-bookmarks	Customizes the Web Bookmarks title or links on the WebVPN Home page.