BGP

This chapter describes how to configure the ASA to route data, perform authentication, and redistribute routing information using the Border Gateway Protocol (BGP).

This chapter includes the following sections:

Information About BGP

BGP is an inter autonomous system routing protocol. An autonomous system is a network or group of networks under a common administration and with common routing policies. BGP is used to exchange routing information for the Internet and is the protocol used between Internet service providers (ISP). This section includes the following topics:

When to Use BGP

Customer networks, such as universities and corporations, usually employ an Interior Gateway Protocol (IGP) such as OSPF for the exchange of routing information within their networks. Customers connect to ISPs, and ISPs use BGP to exchange customer and ISP routes. When BGP is used between autonomous systems (AS), the protocol is referred to as External BGP (EBGP). If a service provider is using BGP to exchange routes within an AS, then the protocol is referred to as Interior BGP (IBGP).

Routing Table Changes

BGP neighbors exchange full routing information when the TCP connection between neighbors is first established. When changes to the routing table are detected, the BGP routers send to their neighbors only those routes that have changed. BGP routers do not send periodic routing updates, and BGP routing updates advertise only the optimal path to a destination network.

Routes learned via BGP have properties that are used to determine the best route to a destination, when multiple paths exist to a particular destination. These properties are referred to as BGP attributes and are used in the route selection process:

- Weight -- This is a Cisco-defined attribute that is local to a router. The weight attribute is not advertised to neighboring routers. If the router learns about more than one route to the same destination, the route with the highest weight is preferred.
- Local preference -- The local preference attribute is used to select an exit point from the local AS. Unlike the weight attribute, the local preference attribute is propagated throughout the local AS. If there are multiple exit points from the AS, the exit point with the highest local preference attribute is used as an exit point for a specific route.
- Multi-exit discriminator -- The multi-exit discriminator (MED) or metric attribute is used as a suggestion to an external AS regarding the preferred route into the AS that is advertising the metric. It is referred to as a suggestion because the external AS that is receiving the MEDs may also be using other BGP attributes for route selection. The route with the lower MED metric is preferred.
- Origin -- The origin attribute indicates how BGP learned about a particular route. The origin attribute can have one of three possible values and is used in route selection.
  - IGP- The route is interior to the originating AS. This value is set when the network router configuration command is used to inject the route into BGP.
  - EGP-The route is learned via the Exterior Border Gateway Protocol (EBGP).
  - Incomplete- The origin of the route is unknown or learned in some other way. An origin of incomplete occurs when a route is redistributed into BGP.
- AS_path -- When a route advertisement passes through an autonomous system, the AS number is added to an ordered list of AS numbers that the route advertisement has traversed. Only the route with the shortest AS_path list is installed in the IP routing table.
- Next hop -- The EBGP next-hop attribute is the IP address that is used to reach the advertising router. For EBGP peers, the next-hop address is the IP address of the connection between the peers. For IBGP, the EBGP next-hop address is carried into the local AS.
- Community -- The community attribute provides a way of grouping destinations, called communities, to which routing decisions (such as acceptance, preference, and redistribution) can be applied. Route maps are used to set the community attribute. The predefined community attributes are as follows:
  - no-export- Do not advertise this route to EBGP peers.
  - no-advertise- Do not advertise this route to any peer.
  - internet- Advertise this route to the Internet community; all routers in the network belong to it.

BGP Path Selection

BGP may receive multiple advertisements for the same route from different sources. BGP selects only one path as the best path. When this path is selected, BGP puts the selected path in the IP routing table and propagates the path to its neighbors. BGP uses the following criteria, in the order presented, to select a path for a destination:

- If the path specifies a next hop that is inaccessible, drop the update.
- Prefer the path with the largest weight.
- If the weights are the same, prefer the path with the largest local preference.
- If the local preferences are the same, prefer the path that was originated by BGP running on this router.
- If no route was originated, prefer the route that has the shortest AS_path.
- If all paths have the same AS_path length, prefer the path with the lowest origin type (where IGP is lower than EGP, and EGP is lower than incomplete).
- If the origin codes are the same, prefer the path with the lowest MED attribute.
- If the paths have the same MED, prefer the external path over the internal path.
- If the paths are still the same, prefer the path through the closest IGP neighbor.
- If both paths are external, prefer the path that was received first (the oldest one).
- Prefer the path with the lowest IP address, as specified by the BGP router ID.
- If the originator or router ID is the same for multiple paths, prefer the path with the minimum cluster list length.
- Prefer the path that comes from the lowest neighbor address.

Licensing Requirements for BGP

Model	License Requirement
ASAv	Standard or Premium License.
All other models	Base License.

Guidelines and Limitations

This section includes the guidelines and limitations for this feature.

Context Mode Guidelines

Supported in single and multiple context mode.

Firewall Mode Guidelines

Does not support transparent firewall mode. BGP is supported only in router mode.

Failover Guidelines

Supports Stateful Failover in single and multiple context mode.

Note When you delete and reapply the BGP configuration in the user context allow a delay of 60 seconds, to enable the slave/ standby ASA unit to sync.

Clustering Guidelines

Does not support clustering.

IPv6 Guidelines

Does not support IPv6.

Graceful Restart Guidelines

Does not support graceful restart.

Configuring BGP

This section describes how to enable the BGP process on your system. After you have enabled BGP, see the following topics to learn how to customize the BGP process on your system.

Task List to Configure a BGP Process

Step 1 In ASDM, choose **Configuration > Device Setup > Routing > BGP**.

Step 2 Enable the BGP routing process by checking the **Enable BGP routing** check box on the General tab. See Enabling BGP, page 28-5.

Step 3 Define the configuration related to the best path selection process for BGP routing on the BGP > Best Path tab. See Defining the Best Path for a BGP Routing Process, page 28-6.

Step 4 Configure the Policy Lists for BGP routing on the BGP > Policy Lists tab. See Configuring Policy Lists, page 28-6.

Step 5 Configure the AS Path Filters for BGP routing on the BGP > AS Path Filters tab. See Configuring AS Path Filters, page 28-8.

Step 6 Configure Community Rules for BGP routing on the BGP > Community Rules tab. See Configuring Community Rules, page 28-8.

Step 7 Configure IPv4 Address Family Settings on the BGP > IPv4 Family tab. See Configuring IPv4 Address Family Settings, page 28-9.

Enabling BGP

This section describes the steps required to enable BGP routing, establish a BGP routing process and configure general BGP parameters.

Step 1 For single-mode, in ASDM, choose **Configuration > Device Setup > Routing > BGP > General**.

Note For multi-mode, in ASDM choose **Configuration > Context Management > BGP**. After enabling BGP, switch to a security context and enable BGP by choosing **Configuration > Device Setup > Routing > BGP > General**.

The General pane appears.

Step 2 Check the **Enable BGP Routing** check box.

Step 3 In the AS Number field, enter the autonomous system (AS) number for the BGP process. The AS number internally includes multiple autonomous numbers. The AS number can be from 1 to 4294967295 or from 1.0 to XX.YY.

Step 4 (Optional) Check the **Limit the number of AS numbers in the AS_PATH attribute of received routes** check box to restrict the number of AS numbers in AS_PATH attribute to a specific number. Valid values are from 1 to 254.

Step 5 (Optional) Check the **Log neighbor changes** check box to enable logging of BGP neighbor changes (up or down) and resets. This helps in troubleshooting network connectivity problems and measuring network stability.

Step 6 (Optional) Check the **Use TCP path MTU discovery** check box to use the Path MTU Discovery technique to determine the maximum transmission unit (MTU) size on the network path between two IP hosts. This avoids IP fragmentation.

Step 7 (Optional) Check the **Enable fast external failover** check box to reset the external BGP session immediately upon link failure.

Step 8 (Optional) Check the **Enforce that first AS is peer's AS for EBGP routes** check box to discard incoming updates received from external BGP peers that do not list their AS number as the first segment in the AS_PATH attribute. This prevents a mis-configured or unauthorized peer from misdirecting traffic by advertising a route as if it was sourced from another autonomous system.

Step 9 (Optional) Check the **Use dot notation for AS numbers** check box to split the full binary 4-byte AS number into two words of 16 bits each, separated by a dot. AS numbers from 0-65553 are represented as decimal numbers and AS numbers larger than 65535 are represented using the dot notation.

Step 10 Specify the timer information in the Neighbor timers area:

- Enter the time interval for which the BGP neighbor remains active after not sending a keepalive message in the Keepalive interval field. At the end of this keepalive interval, the BGP peer is declared dead, if no messages are sent. The default value is 60 seconds.
- Enter the time interval for which the BGP neighbor remains active while a BGP connection is being initiated and configured in the Hold Time field.The default values is 180 seconds.

- (Optional) Enter the minimum time interval for which the he BGP neighbor remains active while a BGP connection is being initiated and configured in the Min. Hold Time field. Specify a value from 0 to 65535.

Step 11 Click **OK**.

Step 12 Click **Apply**.

Defining the Best Path for a BGP Routing Process

This section describes the steps required to configure the BGP best path. For more information on the best path, see BGP Path Selection, page 28-3.

Step 1 In ASDM, choose **Configuration > Device Setup > Routing > BGP > Best Path**.

The Best Path configuration pane appears.

Step 2 In the Default Local Preference field, specify a value between 0 and 4294967295. The default value is 100. Higher values indicate higher preference. This preference is sent to all routers and access servers in the local autonomous system.

Step 3 Check the **Allow comparing MED from different neighbors** check box to allow the comparison of Multi Exit Discriminator (MED) for paths from neighbors in different autonomous systems.

Step 4 Check the **Compare router-id for identical EBGP paths** check box to compare similar paths received from external BGP peers during the best path selection process and switch the best path to the route with the lowest router ID.

Step 5 Check the **Pick the best MED path among paths advertised from the neighboring AS** check box to enable MED comparison among paths learned from confederation peers.add a new network entry. The comparison between MEDs is made only if no external autonomous systems are there in the path.

Step 6 Check the **Treat missing MED as the least preferred one** check box to consider the missing MED attribute as having a value of infinity, making this path the least desirable; therefore, a path with a missing MED is least preferred.

Step 7 Click **OK**.

Step 8 Click **Apply**.

Configuring Policy Lists

When a policy list is referenced within a route map, all of the match statements within the policy list are evaluated and processed. Two or more policy lists can be configured with a route map. A policy list can also coexist with any other preexisting match and set statements that are configured within the same route map but outside of the policy list. This section describes the steps required to configure policy lists.

Step 1 In ASDM, choose **Configuration > Device Setup > Routing > BGP > Policy Lists**.

Step 2 Click **Add**.

The Add Policy List dialog box appears. From this dialog box, you can add a policy list name, its redistribution access (that is, permit or deny), match interfaces, specify IP addresses, match the AS path, match community names list, match metrices, and match tag numbers.

Step 3 Enter a name for the policy list.

Step 4 Click the **Permit** or **Deny** radio button to indicate the redistribution access.

Step 5 Check the **Match Interfaces** check box to distribute routes that have their next hop out of one of the interfaces specified.

- Enter the interface name in the Interface field, or click the ellipses to display the Browse Interface dialog box.
- Choose one or more interfaces, click **Interface**, then click **OK**.

Step 6 In the Specify IP area, configure the following:

- Check the **Match Address** check box to redistribute any routes that have a destination network number address that is permitted by a standard access list or prefix list, and performs policy routing on packets.
  - Specify an access list / prefix list or click the ellipses to display the Browse Access List dialog box.
  - Choose one or more access lists, click **Access List**, then click **OK**.
- Check the **Match Next Hop** check box to redistribute any routes that have a next hop router address passed by one of the access lists or prefix lists specified.
  - Specify an access list/ prefix list or click the ellipses to display the Browse Access List dialog box.
  - Choose one or more access lists, click **Access List**, then click **OK**.
- Check the **Match Route Source** check box to redistribute routes that have been advertised by routers and access servers at the address specified by the access lists or prefix list.
  - Specify an access list / prefix list or click the ellipses to display the Browse Access List dialog box.
  - Choose one or more access lists, click **Access List**, then click **OK**.

Step 7 Check the **Match AS Path** check box to match a BGP autonomous system path.

- Specify an AS path filter or click the ellipses to display the Browse AS Path Filter dialog box.
- Choose one or more AS Path Filters, click **AS Path Filter**, then click **OK**.

Step 8 Check the **Match Community Names List** check box to match a BGP community.

- Specify a community rule or click the ellipses to display the Browse Community Rules dialog box.
- Choose one or more community rules, click **Community Rules**, then click **OK**.
- Check the **Match the specified community exactly** check box to match a specific BGP community.

Step 9 Check the **Match Metrices** check box to redistribute routes with the metric specified. If you specify more than one metric, the routes can be matched with either metric.

Step 10 Check the **Match Tag Numbers** check box to redistribute routes in the routing table that match the specified tags. If you specify more than one tag number, routes can be matched with either metric.

Step 11 Click **OK**.

Step 12 Click **Apply**.

Configuring AS Path Filters

An AS path filter allows you to filter the routing update message by using access lists and look at the individual prefixes within an update message. If a prefix within the update message matches the filter criteria then that individual prefix is filtered out or accepted depending on what action the filter entry has been configured to carry out. This section describes the steps required to configure AS path filters.

Note The **as-path access-lists** are not the same as the regular firewall ACLs.

Step 1 In ASDM, choose **Configuration > Device Setup > Routing > BGP > AS Path Filters**.

Step 2 Click **Add**.

The Add Filters dialog box appears. From this dialog box, you can add a filter name, its redistribution access (that is, permit or deny), and regular expression.

Step 3 Enter a name for the AS Path Filter. Specify a value between 1 and 500.

Step 4 Click the **Permit** or **Deny** radio button to indicate the redistribution access.

Step 5 Specify the regular expression. Click **Build** to build regular expression.

Step 6 Click **Test** to test if a regular expression matches a string of your choice.

Step 7 Click **OK**.

Step 8 Click **Apply**.

Configuring Community Rules

A community is a group of destinations that share some common attribute. You can use community lists to create groups of communities to use in a match clause of a route map. Just like an access list, a series of community lists can be created. Statements are checked until a match is found. As soon as one statement is satisfied, the test is concluded. This section describes the steps required to configure community rules.

Step 1 In ASDM, choose **Configuration > Device Setup > Routing > BGP > Community Rules**.

Step 2 Click **Add**.

The Add Community Rule dialog box appears. From this dialog box, you can add a rule name, rule type, its redistribution access (that is, permit or deny) and specific communities.

Step 3 Enter a name for the community rule.

Step 4 Click **Standard** or **Expanded** radio button to indicate the community rule type.

Step 5 Click **Permit** or **Deny** radio button to indicate the redistribution access.

Step 6 Do one of the following:

- Specify a community number in the Communities field. Valid values are from 1 to 4294967200.
- For an expanded community list, specify the regular expression. Click **Build** to build regular expression.

- Check the **Internet** (well-known community) check box to specify the Internet community. Routes with this community are advertised to all peers (internal and external).
- Check the **Do not advertise to any peers** (well-known community) check box to specify the no-advertise community. Routes with this community are not advertised to any peer (internal or external).
- Check the **Do not export to next AS** (well-known community) check box to specify the no-export community. Routes with this community are advertised to only peers in the same autonomous system or to only other sub-autonomous systems within a confederation. These routes are not advertised to external peers

Step 7 Click **OK**.

Step 8 Click **Apply**.

Configuring IPv4 Address Family Settings

The IPv4 settings for BGP can be set up from the IPv4 family option within the BGP configuration setup. The IPv4 family section includes subsections for General settings, Aggregate address settings, Filtering settings and Neighbor settings. Each of these subsections enable you to customize parameters specific to the IPv4 family.

This section describes how to customize the BGP IPv4 family settings and includes the following topics:

Configuring IPv4 Family General Settings

This section describes the steps required to configure the general IPv4 settings.

Step 1 In ASDM, choose **Configuration > Device Setup > Routing > BGP > IPv4 Family**.

Step 2 Click **General**.

The general IPv4 family BGP parameters configuration pane is displayed.

Step 3 Choose a value for the router ID from the Router ID drop-down list. Choose IP address and specify a router identifier in the form of an IP address. Alternately, choose Automatic.

Step 4 Specify external, internal and local distances in the Administrative Distances area.

Step 5 Choose a route map name from the Learned Routes Map drop-down list. Click **Manage** to add and configure route maps.

Step 6 (Optional) Check the **Generate Default Route** check box to configure a BGP routing process to distribute a default route (network 0.0.0.0).

Step 7 (Optional) Check the **Summarize subnet routes into network-level routes** check box to configure automatic summarization of subnet routes into network-level routes.

Step 8 (Optional) Check the **Advertise inactive routes** check box to advertise routes that are not installed in the routing information base (RIB).

Step 9 (Optional) Check the **Redistribute iBGP into an IGP** check box to configure iBGP redistribution into an interior gateway protocol (IGP), such as IS-IS or OSPF.

Step 10 (Optional) Enter a scanning interval (in seconds) for BGP routers for next-hop validation in the Scanning Interval field. Valid values are from 5 to 60 seconds.

Step 11 (Optional) Check the **Enable address tracking** check box to enable BGP next hop address tracking. Specify the delay interval between checks on updated next-hop routes installed in the routing table in the **Delay Interval** field.

Step 12 (Optional) Specify the maximum number of parallel internal Border Gateway Protocol (iBGP) routes that can be installed in a routing table in the Number of paths field and check the **iBGP multipaths** check box.

Step 13 Click **Apply**.

Configuring IPv4 Family Aggregate Address Settings

This section describes the steps required to define the aggregation of specific routes into one route.

Step 1 In ASDM, choose **Configuration > Device Setup > Routing > BGP > IPv4 Family**.

Step 2 Click **Aggregate Address**.

The Aggregate Address parameters configuration pane is displayed.

Step 3 Click **Add**.

The Add Aggregate Address pane is displayed.

Step 4 Specify a network object in the Network field.

Step 5 Check the **Generate autonomous system set path information** check box to generate autonomous system set path information.

Step 6 Check the **Filters all more- specific routes from the updates** check box to filter all more-specific routes from updates.

Step 7 Choose a route-map from the Attribute Map drop-down list. Click **Manage** to add or configure a route map.

Step 8 Choose a route-map from the Advertise Map drop-down list. Click **Manage** to add or configure a route.

Step 9 Choose a route-map from the Suppress Map drop-down list. Click **Manage** to add or configure a route.

Step 10 Click **OK**.

Step 11 Specify a value for the aggregate timer (in seconds) in the Aggregate Timer field. Valid values are 0 or any value between 6 and 60.

Step 12 Click **Apply**.

Configuring IPv4 Family Filtering Settings

This section describes the steps required to filter routes or networks received in incoming BGP updates.

Step 1 In ASDM, choose **Configuration > Device Setup > Routing > BGP > IPv4 Family**.

Step 2 Click **Filtering**.

The Define filters for BGP updates pane is displayed.

Step 3 Click **Add**.

The Add Filter pane is displayed.

Step 4 Choose a direction from the Direction drop-down list. The direction will specify if the filter should be applied to inbound updates or outbound updates.

Step 5 Choose an access list from the Access List drop-down list. Click **Manage** to add a new ACL.

Step 6 Choose a protocol from the Protocol drop-down list. This is applicable only if the outbound direction is selected.

Step 7 Choose a process ID for the protocol specified from the Process ID drop-down list.

Step 8 Click **OK**.

Step 9 Click **Apply**.

Configuring IPv4 Family BGP Neighbor Settings

This section describes the steps required to define BGP neighbors and neighbor settings.

Note You cannot add neighbors that support graceful restart, because ASA 9.2.1 does not support graceful restart.

Step 1 In ASDM, choose **Configuration > Device Setup > Routing > BGP > IPv4 Family**.

Step 2 Click **Neighbor**.

The Define BGP neighbors pane is displayed.

Step 3 Click **Add**.

The Add BGP Neighbor pane is displayed.

Step 4 Click **General** in the left pane.

Step 5 Enter a BGP neighbor IP address in the IP Address field. This IP address is added to the BGP neighbor table.

Step 6 Enter the autonomous system to which the BGP neighbor belongs in the Remote AS field.

Step 7 (Optional) Enter a description for the BGP neighbor in the Description field.

Step 8 (Optional) Check the **Shutdown neighbor administratively** check box to disable a neighbor or peer group.

Step 9 (Optional) Check the **Enable address family** check box to enable communication with the BGP neighbor.

Step 10 Click **Filtering** in the left pane.

Step 11 (Optional) Choose the appropriate incoming or outgoing access control list in the Filter routes using an access list area, to distribute BGP neighbor information. Click **Manage** to add an ACL and ACEs as required.

Step 12 (Optional) Choose the appropriate incoming or outgoing route maps in the Filter routes using a route map area, to apply a route map to incoming or outgoing routes. Click **Manage** to configure a route map.

Step 13 (Optional) Choose the appropriate incoming or outgoing prefix list in the Filter routes using a prefix list area, to distribute BGP neighbor information. Click **Manage** to configure prefix lists.

Step 14 (Optional) Choose the appropriate incoming or outgoing AS path filter in the Filter routes using AS path filter area, to distribute BGP neighbor information. Click **Manage** to configure AS path filters.

Step 15 (Optional) Check the **Limit the number of prefixes allowed from the neighbor** check box to control the number of prefixes that can be received from a neighbor.

- Enter the maximum number of prefixes allowed from a specific neighbor in the Maximum prefixes field.
- Enter the percentage (of maximum) at which the router starts to generate a warning message in the Threshold level field. Valid values are integers between 1 to 100. The default value is 75.
- (Optional) Check the **Control prefixes received from a peer** check box to specify additional controls for the prefixes received from a peer. Do one of the following:
  - Click **Terminate peering when prefix limit is exceeded** to stop the BGP neighbor when the prefix limit is reached. Specify the interval after which the BGP neighbor will restart in the Restart interval field.
  - Click **Give only warning message when prefix limit is exceeded** to generate a log message when the maximum prefix limit is exceeded. Here, the BGP neighbor will not be terminated.

Step 16 Click **Routes** in the left pane.

Step 17 Enter the minimum interval (in seconds) between the sending of BGP routing updates in the Advertisement Interval field.

Step 18 (Optional) Check the **Generate Default route** check box to allow the local router to send the default route 0.0.0.0 to a neighbor to use as a default route.

- Choose the route map that allows the route 0.0.0.0 to be injected conditionally from the Route map drop-down list. Click **Manage** to add and configure a route map.

Step 19 (Optional) Check the **Remove private autonomous system (AS) numbers from outbound routing updates** check box to exclude the private AS numbers from being advertised on outbound routes.

Step 20 Click **Timers** in the left pane.

Step 21 (Optional) Check the **Set timers for the BGP peer** check box to set the keepalive frequency, hold time and minimum hold time.

- Enter the frequency (in seconds) with which the ASA sends keepalive messages to the neighbor. in the Keepalive frequency field. Valid values are between 0 and 65535. The default value is 60 seconds.
- Enter the interval (in seconds) after not receiving a keepalive message that the ASA declares a peer dead, in the Hold time field. The default value is 180 seconds.

- (Optional) Enter the minimum interval (in seconds) after not receiving a keepalive message that the ASA declares a peer dead, in the Min Hold time field.

Step 22 Click **Advanced** in the left pane.

Step 23 (Optional) Check the **Enable Authentication** check box to enable MD5 authentication on a TCP connection between two BGP peers.

- Choose an encryption type from the Encryption Type drop-down list.
- Enter a password in the Password field. Reenter the password in the Confirm Password field.

Note The password is case-sensitive and can be up to 25 characters long, when the s**ervice password-encryption** command is enabled and up to 81 characters long, when the **service password-encryption** command is not enabled. The first character cannot be a number. The string can contain any alphanumeric characters, including spaces.You cannot specify a password in the format number-space-anything. The space after the number can cause authentication to fail.

Step 24 (Optional) Check the **Send Community Attribute to this neighbor** check box.

Step 25 (Optional) Check the **Use ASA as next hop for neighbor** check box to configure the router as the next-hop for a BGP speaking neighbor or peer group.

Step 26 Do one of the following:

- Click **Allow connections with neighbor that is not directly connected** to accept and attempt BGP connections to external peers residing on networks that are not directly connected.
  - (Optional) Enter the time-to-live in the TTL hops field. Valid values are between 1 and 255.
  - (Optional) Check the **Disable connection verification** check box to disable connection verification to establish an eBGP peering session with a single-hop peer that uses a loopback interface.
- Click **Limit number of TTL hops to neighbor** to enable you to secure a BGP peering session.
  - Enter the maximum number of hops that separate eBGP peers in the TTL hops field. Valid values are between 1 and 254.

Step 27 (Optional) Enter a weight for the BGP neighbor connection in the Weight field.

Step 28 Choose the BGP version that the ASA will accept from the BGP version drop-down list.

Note The version can be set to 2 to force the software to use only Version 2 with the specified neighbor. The default is to use Version 4 and dynamically negotiate down to Version 2 if requested.

Step 29 (Optional) Check the **TCP Path MTU Discovery** check box to enable a TCP transport session for a BGP session.

Step 30 Choose the TCP connection mode from the TCP transport mode drop-down list.

Step 31 Click **Migration** in the left pane

Step 32 (Optional) Check the **Customize the AS number for routes received from the neighbor** check box to customize the AS_PATH attribute for routes received from an eBGP neighbor.

- Enter the local autonomous system number in the Local AS Number field. Valid values are between 1 and 65535.

- (Optional) Check the **Do not prepend local AS number for routes received from neighbor** check box. The local AS number will not be prepended to any routes received from eBGP peer.
- (Optional) Check the **Replace real AS number with local AS number in routes received from neighbor** check box. The AS number from the local routing process is not prepended.
- (Optional) Check the **Accept either real AS number or local AS number in routes received from neighbor** check box.

Step 33 Click **OK**.

Step 34 Click **Apply**.

Configuring IPv4 Network Settings

This section describes the steps required to define the networks to be advertised by the BGP routing process.

Step 1 In ASDM, choose **Configuration > Device Setup > Routing > BGP > IPv4 Family**.

Step 2 Click **Networks**.

The Define networks to be advertised by the BGP routing process configuration pane appears.

Step 3 Click **Add**.

The Add Network pane is displayed.

Step 4 Specify the network that BGP will advertise in the Address field.

Step 5 (Optional) Choose a network or subnetwork mask from the Netmask drop-down list.

Step 6 Choose a route map that should be examined to filter the networks to be advertised from the Route Map drop-down list. Click **Manage** to configure or add a route map.

Step 7 Click **OK**.

Step 8 Click **Apply**.

Configuring Redistribution Settings

This section describes the steps required to define the conditions for redistributing routes from another routing domain into BGP.

Step 1 In ASDM, choose **Configuration > Device Setup > Routing > BGP > IPv4 Family**.

Step 2 Click **Redistribution**.

The Redistribution pane is displayed.

Step 3 Click **Add**.

The Add Redistribution pane is displayed.

Step 4 Choose the protocol from which you want to redistribute routes into the BGP domain from the Source Protocol drop-down list.

Step 5 Choose a process ID for the source protocol from the Process ID drop-down list.

Step 6 (Optional) Enter a metric for the redistributed route in the Metric field.

Step 7 Choose a route map that should be examined to filter the networks to be redistributed from the Route Map drop-down list. Click **Manage** to configure or add a route map.

Step 8 Check one or more of the Internal, External and NSSA External Match check boxes to redistribute routes from an OSPF network.

Note This step is only applicable for redistribution from OSPF networks.

Step 9 Click **OK**.

Step 10 Click **Apply**.

Configuring Route Injection Settings

This section describes the steps required to define the routes to be conditionally injected into the BGP routing table.

Step 1 In ASDM, choose **Configuration > Device Setup > Routing > BGP > IPv4 Family**.

Step 2 Click **Route Injection**.

The Route Injection pane is displayed.

Step 3 Click **Add**.

The Add Conditionally injected route pane is displayed.

Step 4 Choose the route map that specifies the prefixes to inject into the local BGP routing table from the Inject Map drop-down list.

Step 5 Choose the route map containing the prefixes that the BGP speaker will track from the Exist Map drop-down list.

Step 6 Check the **Injected routes will inherit the attributes of the aggregate route** check box to configure the injected route to inherit attributes of the aggregate route.

Step 7 Click **OK**.

Step 8 Click **Apply**.

Monitoring BGP

You can use the following commands to monitor the BGP routing process. For examples and descriptions of the command output, see the command reference. Additionally, you can disable the logging of neighbor change messages and neighbor warning messages.

To monitor or disable various BGP routing statistics, perform the following steps:

To monitor BGP neighbors, perform the following steps:

Step 1 In ASDM choose **Monitoring > Routing > BGP Neighbors**.

Each row represents one BGP neighbor. For each neighbor, the list includes the IP address, the AS number, the router ID, the state (active, idle and so on) and the uptime.

Step 2 Click the BGP neighbor that you want to monitor.

Step 3 To refresh the current list of neighbors, click **Refresh**.

To monitor or disable various BGP routes, perform the following steps:

Step 1 In ASDM choose **Monitoring > Routing > BGP Routes**.

Each row represents one BGP route. For each route, the list includes the status code, IP address, the next hop address, the route metric, the local preference values, the weight and the path.

Step 2 Click the BGP route that you want to monitor.

Step 3 To refresh the current list of routes, click **Refresh**.

Feature History for BGP

Table 28-1 lists each feature change and the platform release in which it was implemented. ASDM is backward-compatible with multiple platform releases, so the specific ASDM release in which support was added is not listed.

Table 28-1 Feature History for BGP

Feature Name	Platform Releases	Feature Information
BGP Support	9.2(1)	Support was added for routing data, performing authentication, and redistributing and monitoring routing information using the Border Gateway Protocol. We introduced the following ASDM screens: Configuration > Device Setup > Routing > BGP Monitoring > Routing > BGP Neighbors, Monitoring > Routing > BGP Routes We modified the following ASDM screens: Configuration > Device Setup > Routing > Static Routes> Add > Add Static Route Configuration > Device Setup > Routing > Route Maps> Add > Add Route Map