



FRONTIER COMMUNICATIONS CUSTOMER BGP ROUTING POLICY AND CONFIGURATION GUIDE

DISTRIBUTION DATE

1.0 INTRODUCTION	1
2.0 GENERAL	1
3.0 CUSTOMER BGP REQUIREMENTS	2
4.0 CUSTOMER BGP CONFIGURATION GUIDE	2
4.1 COMMUNITY-BASED SIGNALING	3
4.2 FCA BGP COMMUNITIES ON ADVERTISED ROUTES.....	6
5.0 FRONTIER ROUTING POLICY	8
5.1 FRONTIER BGP INGRESS POLICY	8
5.2 FRONTIER BGP EGRESS POLICY	9
6.0 SUPPORT AND MAINTENANCE	11

1.0 Introduction

Before being approved for BGP routing, customers must review the policies outlined below. These policies have been implemented to ensure top-rate network performance and reduce the possibility of routing problems while still allowing customers to control routing behavior to the fullest extent possible.

Frontier Communications of America (FCA) reserves the right to add, delete, or modify any of the policies contained herein at any time, without notice. Please find the most recent revision of this document at: http://ipadmin.frontier.com/bgp_policy.pdf

Question or comments regarding this policy should be forwarded to bgp@frontiernet.net. Responses will be processed within two business days.

2.0 General

All customers wishing to run BGP with FCA must submit a BGP routing application. FCA will process the application within 2 business days of submission. The online application can be found at: http://ipadmin.frontier.com/bgp_procedures_new.html

FCA employ best-known practices to establish, maintain, and troubleshoot BGP sessions with all BGP4 compliant router vendors. However, FCA makes no warranty that it can establish and maintain a BGP session with any customer provided equipment due to vendor incompatibility.

FCA is not responsible for customer equipment configurations and problems arising from customer equipment mis-configurations. It is recommended that all customers deploying BGP be skilled in configuring and troubleshooting the protocol.

If any of the above filter policies cited in this document are violated and not corrected in a timely manner after customer notification, FCA may administratively shutdown the BGP session until the issue is remedied. Customers continually leaking the above mentioned routes will be converted from BGP to static routing

3.0 Customer BGP Requirements

In order to use BGP to exchange routing information with FCA, customers must meet certain requirements:

Customers must be multi-homed to run BGP, either multi-homed to FCA's network only, or multi-homed with FCA and one or more other providers.

Customers must have a registered public AS number. The only exception is for customers who are multi-homed to FCA only and have requested a private-AS.

Customers must have Ethernet Internet Access (EIA) service from FCA. FCA will not run BGP with a customer over a DSL line, regardless of line rate.

4.0 Customer BGP Configuration Guide

Once approved for BGP, the customer has various BGP configuration options and features they may deploy or configure. Some of these require coordination with FCA and others do not.

FCA dynamically exchanges routes with customers using BGP only. FCA will use BGP version 4.

Customer BGP peering sessions to FCA may optionally support MD5 authentication. FCA reserves the right to require a customer to use a MD5 authentication key for BGP sessions.

Customer BGP peering sessions are typically implemented to the interface address. However, upon an approved request, FCA will support multi-hop peering for load balancing across multiple interfaces. When configuring multi-hop BGP, customers must provide their own IP address for their Loopback Interface for which the BGP session will be established. When applying for BGP peering please indicate the desire to use EBGP-Multihop in the comments field. FCA will use EBGP-Multihop when a customer requests BGP peering and the customer does not connect directly to a router which we support BGP customers on.

FCA optionally supports BFD (bidirectional forwarding detection) on a BGP session with the following settings:

- Transmit interval equal to or greater than 250 ms.
- Multiplier set to three.
- Cannot be on an aggregate (lacp or etherchannel) interface.

4.1 Community-based Signaling

FCA standard BGP sessions are configured to accept routes with BGP community-based signaling (similar to that described in RFC 1998.) Customers can specify a special treatment of a prefix based on pre-defined communities attached to each prefix by the customer. Customers can send communities to adjust FCA local preference, modify export behavior and perform selective AS-path prepending. Customers can use various combinations of these communities to control their inbound traffic flows.

FCA strips any unrecognized BGP communities received from the customer and does not propagate any BGP communities to non-customers, originated by FCA or otherwise.

4.1.1 Local Preference Manipulation

FCA's Backbone Local Preference Policy uses the following values:

FCA Local Preference	Route Origin
65	FCA Transit Peers
75-85	FCA Bi-lateral Peers

100	FCA BGP Customers (default)
100	FCA Internal and static routed customers

Customers may send the following communities to modify BGP local preference given to networks announced to FCA:

IPv4 Community	FCA Local Preference	Effect on FCA Route Preference
5650:60	60	<i>Last Resort</i> -- Only use this route when alternate providers no longer have this route.
5650:70	70	<i>Backup #2</i> – Prefer this route over FCA Transit Peers, but not over Bilateral Peers or routes from other FCA customer sessions.
5650:90	90	<i>Backup #1</i> – Prefer this route over FCA transit and bilateral peers, but not over other routes from other FCA customer sessions.
5650:110	110	<i>Preferred</i> – This route is preferred over all others

IPv6 Community	FCA Local Preference	Effect on FCA Route Preference
5650:6060	60	<i>Last Resort</i> -- Only use this route when alternate providers no longer have this route.
5650:6070	70	<i>Backup #2</i> – Prefer this route over FCA Transit Peers, but not over Bilateral Peers or routes from other FCA customer sessions.
5650:6090	90	<i>Backup #1</i> – Prefer this route over FCA transit and bilateral peers, but not over other routes from other FCA customer sessions.
5650:6110	110	<i>Preferred</i> – This route is preferred over all others

IPv4 Community	Export Behavior
5650:640	Do not export to any BGP Peers or Customers (similar to well known community 'No Export')
5650:666	Do not export to any BGP peers, but do export to FCA BGP customers
5650:200	Prefix remains announced to all BGP peers and customers, however the next-hop is rewritten to a local discard route within the core. This community is often referred to as a blackhole community and is used primarily for mitigating DDOS attacks from the customer side.

4.1.2 Export Manipulation / Blackhole

Customers may send the following communities to modify FCA default export behavior, which is to export all announced routes (assuming they have passed FCA filters) to all BGP peers including customers:

IPv6 Community	Export Behavior
5650:6640	Do not export to any BGP Peers or Customers (similar to well known community 'No Export')
5650:6666	Do not export to any BGP peers, but do export to FCA BGP customers
5650:6200	Prefix remains announced to all BGP peers and customers, however the next-hop is rewritten to a local discard route within the core. This community is often referred to as a blackhole community and is used primarily for mitigating DDOS attacks from the customer side.

4.1.3 Selective Prepend Manipulation

Selective prepends allow the customer to have FCA perform AS-path prepending to the Internet on the customer's behalf. This allows increased control over inbound traffic flows more than simple AS-path prepending performed by the customer. With traditional AS-path prepending, the padded AS-path is seen identically by all FCA peers. With selective as-path prepending, FCA allows customers to have FCA prepend only to certain interesting peers. FCA current routing policy permits this feature with approximately 20 of its peers (large and/or high traffic networks). Selective AS-path prepending also supplies a mechanism to allow customers to prevent export to these peers individually.

Because publicly providing a community/peer cross-reference table would violate peering contracts FCA has with certain of its peers, customers are asked to privately request the Selective Prepend Supplement document via e-mail to bgp@frontiernet.net. Customers will be expected to provide a valid FCA circuit ID as well as peering IP address and AS number if possible. Once the request is received, the Selective Prepend Supplement will promptly be forwarded to the requestor.

4.2 FCA BGP Communities on Advertised Routes

FCA sends communities with routes to customers by default. Customers may match on these communities and apply various internal policies to manipulate outbound traffic flows. The communities listed in this section describe those communities that FCA attaches to routes.

4.2.1 Region Marking

FCA uses BGP communities to mark what region a particular route is learned. The region numbers coincide with FCA's IBGP regions. Customers that have multiple diverse connections to FCA may use these region communities to match and apply an internal policy to ensure that the optimal path is used. FCA region origination communities are as follows:

IPv4 Community	Region of Origin
5650:501	Announced from a router in Region 1 (North West)
5650:502	Announced from a router in Region 2 (South West)
5650:503	Announced from a router in Region 3 (North Central)
5650:504	Announced from a router in Region 4 (South Central)
5650:505	Announced from a router in Region 5 (North East)
5650:506	Announced from a router in Region 6 (South East)

IPv6 Community	Region of Origin
5650:6501	Announced from a router in Region 1 (North West)
5650:6502	Announced from a router in Region 2 (South West)
5650:6503	Announced from a router in Region 3 (North Central)
5650:6504	Announced from a router in Region 4 (South Central)
5650:6505	Announced from a router in Region 5 (North East)
5650:6506	Announced from a router in Region 6 (South East)

4.2.2 Prefix Origin Marking

Additionally FCA uses BGP communities to mark which type of network a particular announcement was learned. These communities are additive to the Region marking communities, in other words, any network announced by FCA should have at minimum both a Region marking community and a Network marking community. Network origination marking communities are as follows:

IPv4 Community	Network of Origin
5650:900	Route originated from FCA core (FCA aggregate CIDR blocks)
5650:920	Static routed customers of FCA using non-FCA IP space
5650:930	Route learned from an FCA bilateral peer
5650:950	Route learned from an FCA full peer
5650:960	Route learned from a directly connected DIA/EIA customer
5650:970	Static routed customer but the static route will not be exported outside 5650
5650:980	Connected route redistributed from a public exchange point from which FCA peers
5650:990	Route learned from an FCA BGP customer

IPv6 Community	Network of Origin
5650:6900	IPv6 Route originated from FCA core (FCA aggregate CIDR blocks)
5650:6920	IPv6 Static routed customers of FCA using non-FCA IP Space
5650:6930	IPv6 Route learned from an FCA bilateral peer
5650:6950	IPv6 Route learned from an FCA full peer
5650:6960	IPv6 Route learned from a directly connected DIA/EIA customer
5650:6970	IPv6 Static routed customer but the static route will not be exported outside 5650
5650:6980	IPv6 Connected route redistributed from a public exchange point from which FCA peers
5650:6990	IPv6 Route learned from an FCA BGP customer

5.0 Frontier Routing Policy

5.1 Frontier BGP Ingress Policy

All prefixes announced to FCA must be accompanied by proper netblock registration which must be obtainable through WHOIS services provided by a Regional Internet Registry or RWHOIS. This registration must reflect clear association or affiliation with the AS intending to make the announcement. As an alternative, LOA can be provided by the organization with the delegation authority of the netblock in question.

FCA filters ingress on AS-path and prefix. As such, outbound network announcements should be filtered by applying explicit prefix and AS-path filters, not exclusive (i.e. AS-filters should list your AS and AS paths you would like to announce and deny all others instead of denying just the AS's of external peers you may have). For details on how to submit, view, and update your current AS-path and prefix filters, please see below.

FCA will accept network announcements originated only from the customer AS and AS's for which the customer is intentionally providing transit. FCA will not accept leaking of full Internet routes.

FCA prefix filters for public AS customers are built such that any prefix filter entry up to /24 for IPv4 and prefix up to /48 for IPv6 is allowed by default. FCA feels it is the role of the Autonomous System

administrator to responsibly aggregate. All network announcements whose prefix length is greater than /24 for IPv4 or greater /48 for IPv6 will not be accepted by FCA nor propagated to its peers.

FCA prefix filters for private AS customers are built such that network announcements with prefix length up to /30 are accepted. Contiguous networks between /24 and /30 must be aggregated to the highest CIDR boundary and will be enforced with exact prefix filter entries.

All customers are encouraged to aggregate their contiguous network announcements to the highest CIDR boundary.

FCA will not accept default routes or illegal RFC address space to include RFC 1918 and LINK- LOCAL addresses.

FCA as-path filters are configured by default to allow unlimited as-path prepends as well as unlimited as-path prepends for any AS's the customer has allowed transit.

FCA does not policy route or alter any of its BGP configurations, including filter policies or communities, for any individual customer. This ensures the FCA network is maintained in a robust fashion and reduces mean-time-to-repair for BGP related trouble.

FCA has deployed route dampening. FCA maintains a reasonable route dampening policy based on RIPE-229. FCA may apply dampening to customer's network announcements in cases of heavy update/withdrawal activity. This policy is standard across all aggregation routers and is non-negotiable. In case of dampening, customers may contact FCA to have their dampened routes cleared by issuing a trouble-ticket with the FCA's NOC. This does not include external paths outside the FCA network.

Values used in FCA's Aggregation Routers for route dampening:

- Penalty for route flap: 1000 for withdrawn or readvertised route; 500 for path attribute change
- Max Suppress Duration: 30 minutes
- Half-Life Decay: 10 minutes
- Reuse value: 3000
- Suppress: 6000

5.2 Frontier BGP Egress Policy

FCA offers several types of route announcements for the customer to choose. The characteristics for each announcement type are described below. Customers are asked to choose which type of announcement they desire when filling out the BGP routing application. The customer may request a different announcement type at any time after the session is established by following the procedures listed below.

- **Default Route Only.** FCA sends only a default route to the customer (0.0.0.0/0). This is different than a static default that the customer may set themselves in that this default route learned via BGP inherits all of the dynamic characteristics that BGP provides. Choosing this option is useful when low memory use is a priority on the customer router. Note that choosing only a default route may lead suboptimal routing and packet delivery.
- **Partial Routes.** FCA sends to the customer FCA (AS5650) routes and FCA EBGP customer routes. At present, they number approximately 1600. This option is useful when memory constraints on the customer router are important however the customer still wants the ability to make semi-informed routing decisions. Obtaining partial routes without a default is usually not useful because it may limit reachability to the entire Internet. For this reason, obtaining only partial routes is not very common and is normally recommended the customer receive partial plus default routes.
- **Partial plus Default Routes.** FCA sends to the customer FCA (AS5650) routes and FCA EBGP customer routes as well as a default route. This option is useful when memory constraints on the customer router are important however the customer still wants the ability to make semi-informed routing decisions based on FCA announced networks. Obtaining the default route in addition to the partial route ensures reachability to other networks not specifically advertised with partial routes.
- **Full Routes.** FCA sends the customer full Internet routes which make up explicit network announcements to every destination on the Internet. At present, full Internet routes number approximately 537,490. Obtaining full Internet routes is useful for customers where memory utilization is not an issue on their router as full Internet routes often requires over 1 Gig of memory. Obtaining full Internet routes allows for fully-informed routing decisions and optimal packet delivery.
- **Full plus Default Routes.** FCA sends the customer full Internet routes as well as a default route. Obtaining full Internet routes is useful for customers where memory utilization is not an issue on their router. In addition, they receive a default route, which allows routing of packets where an explicit route does not exist. Some customers prefer this because it may offer a safety net of sorts. This may not always work however because it may simply result in moving the lack of reachability from the customer's network to FCA's network. For this reason, choosing full routes plus a default is not very common.

6.0 Support and Maintenance

Please be aware that if the customer does not use a Public Route Registry, like RADB, FCA will create a proxy object for the customer. Any changes to that object will need to be requested from the Frontier NOC, as shown below.

Requests for the following should be made via e-mail to noc@frontiernet.net:

- Changes to inbound filters

Please indicate the specifics of the AS-path or prefix filter change.

- Snapshots of existing filters

Indicate that you would simply like a snapshot of presently configured filters.

- Changes to announcement type

Indicate the new announcement type you desire.

In your requests, please include the following information:

- Company Name
- FCA Circuit Identification Number
- Technical Contact Name and Phone Number
- Preferred E-mail address
- AS Number
- Interface connected IP address or Peering IP address (if different)

Response time for any of the requests above will be processed in two business days. Any questions regarding previously submitted changes should be directed to bgp@frontiernet.net.