Troubleshoot routing and BGP

This guide helps you diagnose and resolve common routing and BGP issues with Cloudflare WAN. These issues can affect traffic delivery, cause unexpected latency, or result in connectivity loss.

Quick diagnostic checklist

If you are experiencing routing or BGP issues, check these items first:

1. **BGP session state**: Verify session is **Established**, not stuck in **Connect** or **Active**.
2. **Firewall rules**: Ensure TCP port `179` is permitted bidirectionally between your router and Cloudflare.
3. **Tunnel or CNI health**: Check that underlying connectivity is healthy. Degraded tunnels affect route priority.
4. **Static route conflicts**: Static routes take precedence over BGP routes at equal priority.

Resolve common issues

BGP session not establishing

This section covers BGP peering sessions (beta) between your network and Cloudflare, established over CNI or tunnels.

Symptoms

- BGP session never reaches **Established** state
- No routes being advertised or received
- Router logs show repeated connection attempts

BGP session states

State	Meaning	Action
Established	Session up, exchanging routes	Normal operation
Active	Attempting to initiate connection	Check firewall rules, verify neighbor IP
Connect	TCP connection in progress	Check port `179` access, verify peering IP
Idle	Session down, no connection attempts	Check configuration, verify BGP is enabled

Solution

1. Verify your firewall permits TCP port `179` bidirectionally between your router and the Cloudflare peering address.
2. Confirm the neighbor IP matches the Cloudflare-provided peering address exactly.
3. Verify your ASN configuration matches the dashboard settings. Only eBGP is supported, so your ASN must differ from the Cloudflare account ASN.
4. If using MD5 authentication, verify the password matches on both sides.

Unexpected traffic routing or latency

Symptoms

- Traffic from specific regions routed through distant data centers
- Higher than expected latency for regional users
- Traffic not using the closest tunnel or CNI

Causes

- Tunnel health degradation causing route deprioritization
- Regional route scoping misconfiguration
- BGP route priorities not set as expected
- Static routes overriding BGP routes

Solution

1. **Check tunnel health**: Degraded tunnels have 500,000 added to their route priority. Down tunnels have 1,000,000 added. Traffic shifts to healthier paths, which may be in different regions. Refer to Troubleshoot tunnel health for diagnostic steps.
2. **Review route priorities**: Lower priority values indicate higher preference. Verify your routes have the expected priority configuration.
   - Default BGP route priority: `100`
   - Static routes at priority `100` take precedence over BGP routes at `100`
3. **Check regional scoping**: If you use region-scoped routes, ensure all regions have route coverage. Traffic arriving at a region without a matching route is dropped.
4. **Use Network Analytics**: Review traffic patterns to identify where traffic is landing and which paths it follows. Refer to Network Analytics for usage instructions.

CNI link failures

Symptoms

- CNI shows down in dashboard
- BGP session over CNI drops
- Traffic fails over to tunnels or alternate CNIs

CNI issue layers

CNI issues can occur at multiple layers:

Issue type	Impact	What to check
Physical link down	All traffic over that CNI affected	Light levels, cross-connect status
BGP session down	Dynamic routes withdrawn	BGP neighbor state on your router
Prefixes withdrawn	Specific routes unavailable	BGP advertised and received routes

A healthy physical link can still have BGP issues. A healthy BGP session can exist while specific prefixes are withdrawn.

Solution

Check physical layer (your side):

1. Verify the interface is administratively up on your router.
2. Check optical light levels (Tx/Rx dBm). Abnormal readings indicate fiber or transceiver issues.
3. If light levels are low or absent on your receive side, contact your data center to verify cross-connect status.

Check BGP session:

1. Verify BGP neighbor state on your router shows **Established**.
2. Check for MD5 authentication mismatches if authentication is configured.
3. Review BGP logs for error messages indicating why the session may have dropped.

Check for maintenance:

1. Review Cloudflare Status ↗ for scheduled maintenance affecting your CNI location.
2. Some maintenance events may temporarily affect CNI connectivity even when marked as non-disruptive.

Refer to Network Interconnect for CNI configuration and setup information.

Static and BGP route conflicts

Symptoms

- BGP routes not being used despite being learned
- Traffic not following expected BGP path
- Route changes not taking effect as expected

Cause

Cloudflare prefers static routes when static and BGP routes share the same prefix and priority. This ensures manually configured routes take precedence unless explicitly deprioritized.

Solution

Adjust route priorities based on your preference:

- **To prefer BGP routes**: Set static route priority to a higher number (for example, `150` or `200`). Higher numbers indicate lower preference.
- **To prefer static routes**: Keep static route priority at or below `100`. BGP routes default to priority `100`.

Route type	Prefix	Priority	Selected
Static	`10.0.0.0/24`	`100`	Yes (static wins ties)
BGP	`10.0.0.0/24`	`100`	No

To make the BGP route preferred in this example, change the static route priority to `150` or higher, or remove the static route entirely.

Refer to Route prioritization for detailed information on how priorities work.

CNI, tunnel, and BGP health

Understanding the relationship between these components helps diagnose routing issues:

Component	What it monitors	Impact when unhealthy
CNI health	Physical or virtual interconnect link status	BGP session may drop. All traffic over that CNI is affected.
Tunnel health	Logical GRE or IPsec tunnel through health check probes	Route priority penalized. Traffic steers to healthier tunnels.
BGP session	Control plane connectivity for dynamic routing	Dynamic routes withdrawn. Static routes remain unaffected.

A healthy CNI can have an unhealthy tunnel if health check probes are blocked or misconfigured. BGP routes can be withdrawn even when the underlying physical link is operational.

Gather information for support

If you have worked through this guide and still experience routing issues, gather the following information before contacting Cloudflare support.

Required information

1. **Account ID** and affected prefix(es), tunnel name(s), or CNI identifier(s)
2. **Timestamps** (in UTC) when the issue occurred
3. **BGP configuration details:**
    - Your ASN and Cloudflare peering ASN
    - Neighbor IP addresses
    - Sanitized router configuration (remove passwords and keys)
4. **Current state information:**
    - BGP session state from your router
    - Dashboard screenshots showing prefix, route, or tunnel status

Helpful diagnostic data

- **Router logs**: BGP neighbor logs covering the incident timeframe
- **Traceroute results**: From affected source networks to your prefix
- **For CNI issues**: Optical light level readings from your equipment

Router diagnostic commands

Collect output from these commands (syntax varies by vendor):

```sh
# Show BGP neighbor status
show bgp neighbors

# Show BGP summary
show bgp ipv4 unicast summary

# Show specific prefix in BGP table
show bgp ipv4 unicast <YOUR_PREFIX>

# Show interface status (for CNI)
show interface <YOUR_INTERFACE_NAME>

# Show received and advertised routes
show bgp ipv4 unicast neighbors <YOUR_NEIGHBOR_IP> routes
show bgp ipv4 unicast neighbors <YOUR_NEIGHBOR_IP> advertised-routes
```

Resources

- Traffic steering: Route prioritization, BGP communities, and ECMP behavior
- Configure routes: Static route configuration
- Network Interconnect: CNI setup and BGP peering
- Troubleshoot tunnel health: Tunnel-specific diagnostic steps
- Network Analytics: Traffic analysis and monitoring
- Cloudflare Status ↗: Maintenance and incident notifications