BGP Simulator User Manual

Table of Contents

Introduction

The BGP Simulator with Trust-Based Security is a C++ based discrete-event simulator designed to model the Border Gateway Protocol (BGP-4). Unlike standard simulators, this tool integrates a dynamic trust and reputation system to test how routing decisions could be shielded against malicious activities, such as prefix hijacking.

Features

- Complete Finate State Machine in BGP-4 (OPEN, UPDATE, KEEPALIVE, NOTIFICATION)
- Voting system where routers build trust tables and calculate scores for their peers based on interactions and peer recommendations
- Attack simulation allows users to simulate a prefix hijack and observe its effects on routing decisions, as well as withdraw the falsely announced route
- Users can manipulate the network in real time by shutdown/startup and policy commands

System Architecture and Trust Logic

Standard BGP relies heavily on trust between peers, making it vulnerable to route hijacking. This simulator enhances the protocol by adding a Trust Score to the decision-making process. The simulator needs further development to make effective routing decisions based on trust score alone.

Routers adjust trust scores based on the validity of updates received from a peer. Routers exchange trust information. A router can influence its neighbor's opinion of a third router. The standard BGP decision process (Local Pref, AS Path, etc.) is augmented. If a peer's trust score drops below a specific threshold, their route advertisements may be deprioritized or ignored.

This is a discrete-event simulator. Time does not move automatically. The user advances time using the tick command. This allows for precise observation of state changes and message propagation step-by-step.

Installation And Setup

Prerequisites

- Operating System: Linux, macOS, or Windows (with MinGW/WSL)
- Compiler: A C++ compiler supporting the C++17 standard (e.g., g++)

Compilation

1. Open your terminal
2. Clone the GitHub repository
3. Navigate to the project source directory
4. Run the compilation command

```
g++ -std=c++17 -Wall -o bgp_sim simulator.cpp
```

Configuration Guide

To run a simulation, you must define the network topology in a .conf file. The project directory includes a predefined topology, but the user can freely modify routers, prefixes and links.

Topology File Structue

Modify the file named topology.conf before running the simulator. This file defines the Routers, Autonomous Systems (AS), and the physical links between them.

Command Line Interface (CLI) Reference

Once the simulator is running (./bgp_sim -c topology.conf), use the following commands at the BGP-Sim> prompt.

Command	**Description**
show ip bgp <router_id>	Displays the Routing Information Base (RIB) for the specified router.
show peers <router_id>	Shows the status (Idle, Connect, Established) of all BGP neighbors.
show trust <router_id>	Displays the calculated trust scores the router holds for its peers.

Command	**Description**
tick [n]	Advances the simulation clock by *n* steps (default is 1). Essential for processing queued messages.
shutdown <router_id>	Simulates a router failure/shutdown, closing BGP sessions.
startup <router_id>	Restores a previously shut down router.
neighbor <id> <ip> remote-as <as>	Manually configures a new BGP peer connection.
neighbor <r_id> <p_ip> route-reflector-client	Configure peer as route reflector client.

Command	**Description**
announce <r_id> <p/l>	Forces a router to announce a prefix. Used for normal traffic or to simulate **Prefix Hijacking**.
withdraw <r_id> <p/l>	Withdraws a previously announced route.
policy <r_id> [in|out] deny <p/l>	Applies a filter to drop specific prefixes inbound or outbound.

Tutorials

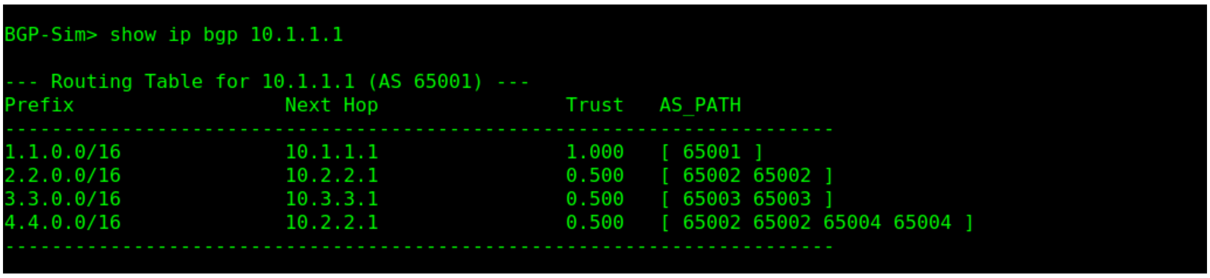
Inspect The BGP Routing Table

First, we need to verify that the router has learned paths to other networks. The simulator modifies the standard routing table by adding a Trust column, which indicates the reputation score of the neighbor advertising the route.

Run the following command:

```
show ip bgp <router_id>
```

In the image below, note that the router has learned prefixes 2.2.0.0/16 through 4.4.0.0/16. The Trust column shows a score (e.g., 0.500) for the next hop, which influences the best-path selection.



```
BGP-Sim> show ip bgp 10.1.1.1

--- Routing Table for 10.1.1.1 (AS 65001) ---
Prefix                  Next Hop                Trust   AS_PATH
----------------------------------------------------------------------
1.1.0.0/16              10.1.1.1                1.000   [ 65001 ]
2.2.0.0/16              10.2.2.1                0.500   [ 65002 65002 ]
3.3.0.0/16              10.3.3.1                0.500   [ 65003 65003 ]
4.4.0.0/16              10.2.2.1                0.500   [ 65002 65002 65004 65004 ]
----------------------------------------------------------------------
```

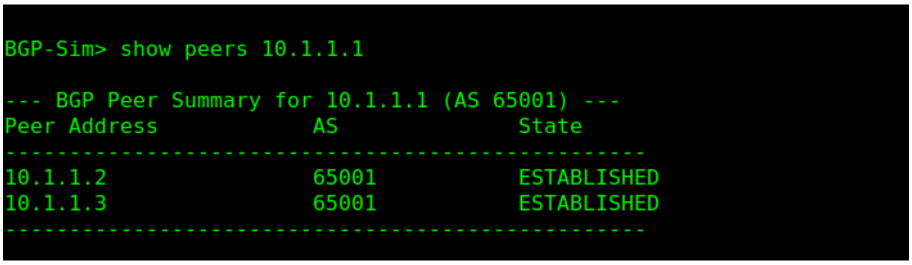
Verify Peer Connectivity

If the routing table is empty or missing prefixes, you must check if the BGP sessions are active. This command displays the neighbor adjacency state.

Run the following command:

```
show peers <router_id>
```

Look for the State column. As shown below, neighbors 10.1.1.2 and 10.1.1.3 are in the ESTABLISHED state, meaning the BGP session is fully operational and exchanging updates.



```
BGP-Sim> show peers 10.1.1.1

--- BGP Peer Summary for 10.1.1.1 (AS 65001) ---
Peer Address            AS              State
--------------------------------------------------
10.1.1.2                65001           ESTABLISHED
10.1.1.3                65001           ESTABLISHED
--------------------------------------------------
```

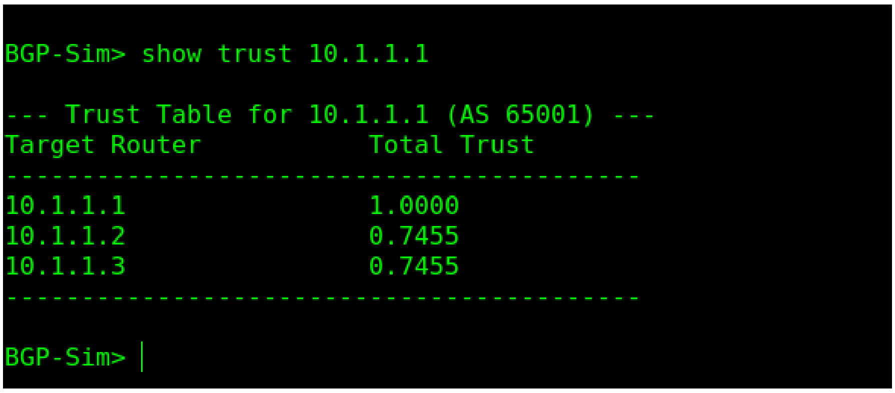
Audit Trust Scores

The core feature of this simulator is the dynamic reputation system. You can view the raw trust values a router has assigned to its peers based on their past behavior and voting consensus.

Run the following command:

```
show trust <router_id>
```

The Total Trust score represents the aggregated reputation of a neighbor. In the example below, Router 10.1.1.2 has a calculated trust score of 0.7455. If this score drops below the configured threshold, Router 10.1.1.1 may stop accepting routes from it.



```
BGP-Sim> show trust 10.1.1.1

--- Trust Table for 10.1.1.1 (AS 65001) ---
Target Router           Total Trust
------------------------------------------
10.1.1.1                1.0000
10.1.1.2                0.7455
10.1.1.3                0.7455
------------------------------------------

BGP-Sim> |
```

Establish Connections and Use “Tick”

In this discrete-event simulator, network changes do not happen in real-time. You must manually advance the simulation clock using the tick command. This allows you to observe the step-by-step handshake process of BGP.

The example below demonstrates how to configure a new link between Router 10.1.1.1 and Router 10.4.4.1, and how to use tick to force convergence.

First, configure the neighbor on Router 1 only:

```
neighbor 10.1.1.1 10.4.4.1 remote-as 65004
```

When you run tick 5, observe the output in the screenshot. Router 1 sends an OPEN message, but Router 4 rejects it (Ignoring) because it has not yet been configured to recognize Router 1 as a peer.

Next, configure the corresponding peer on Router 4:

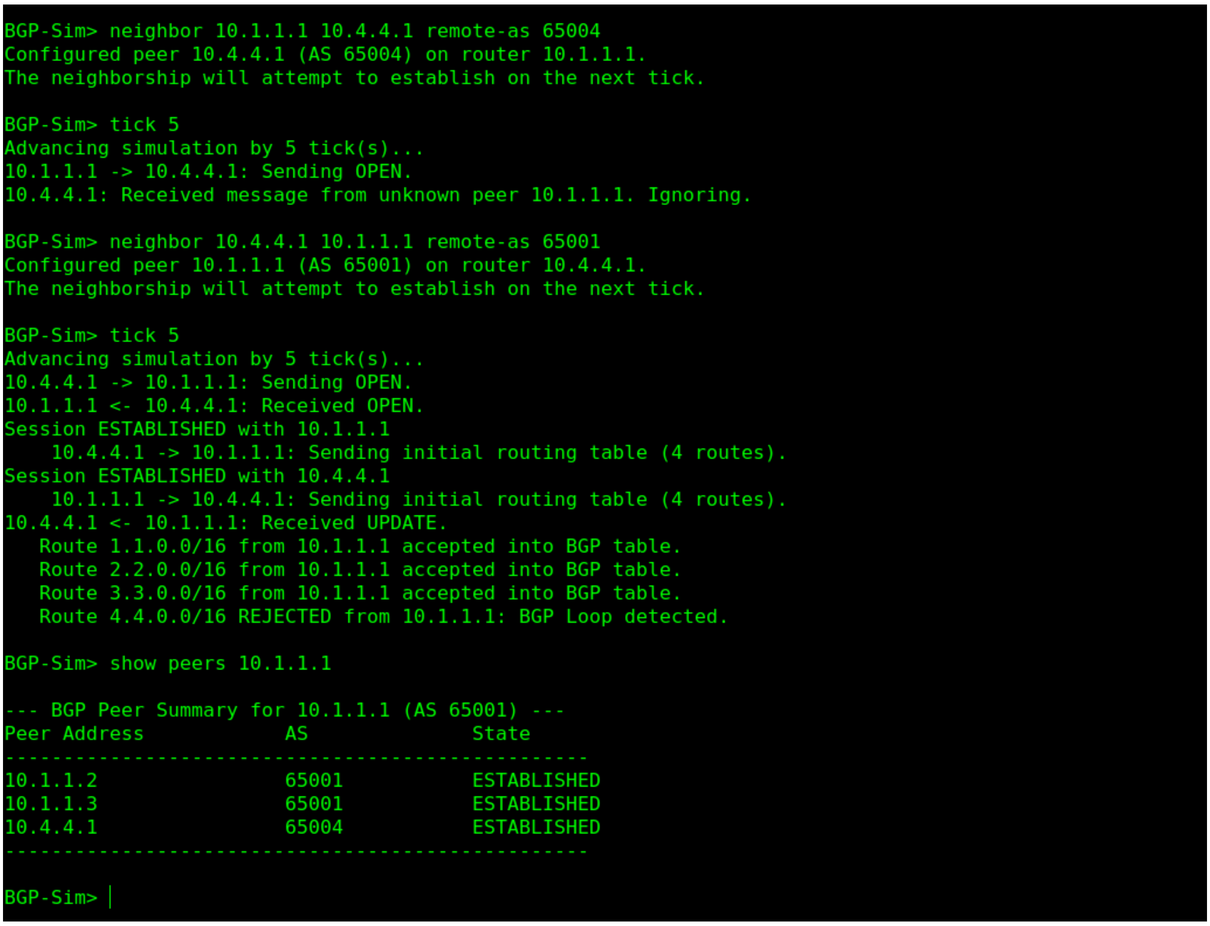
```
neighbor 10.4.4.1 10.1.1.1 remote-as 65001
```

Now that both sides are configured, run the time command again:

```
tick 5
```

Finally, checking the status confirms the new link is up.

```
show peers 10.1.1.1
```



```
BGP-Sim> neighbor 10.1.1.1 10.4.4.1 remote-as 65004
Configured peer 10.4.4.1 (AS 65004) on router 10.1.1.1.
The neighborship will attempt to establish on the next tick.

BGP-Sim> tick 5
Advancing simulation by 5 tick(s)...
10.1.1.1 -> 10.4.4.1: Sending OPEN.
10.4.4.1: Received message from unknown peer 10.1.1.1. Ignoring.

BGP-Sim> neighbor 10.4.4.1 10.1.1.1 remote-as 65001
Configured peer 10.1.1.1 (AS 65001) on router 10.4.4.1.
The neighborship will attempt to establish on the next tick.

BGP-Sim> tick 5
Advancing simulation by 5 tick(s)...
10.4.4.1 -> 10.1.1.1: Sending OPEN.
10.1.1.1 <- 10.4.4.1: Received OPEN.
Session ESTABLISHED with 10.1.1.1
    10.4.4.1 -> 10.1.1.1: Sending initial routing table (4 routes).
Session ESTABLISHED with 10.4.4.1
    10.1.1.1 -> 10.4.4.1: Sending initial routing table (4 routes).
10.4.4.1 <- 10.1.1.1: Received UPDATE.
   Route 1.1.0.0/16 from 10.1.1.1 accepted into BGP table.
   Route 2.2.0.0/16 from 10.1.1.1 accepted into BGP table.
   Route 3.3.0.0/16 from 10.1.1.1 accepted into BGP table.
   Route 4.4.0.0/16 REJECTED from 10.1.1.1: BGP Loop detected.

BGP-Sim> show peers 10.1.1.1

--- BGP Peer Summary for 10.1.1.1 (AS 65001) ---
Peer Address            AS              State
--------------------------------------------------
10.1.1.2                65001           ESTABLISHED
10.1.1.3                65001           ESTABLISHED
10.4.4.1                65004           ESTABLISHED
--------------------------------------------------

BGP-Sim> |
```

Applying Inbound and Outbound Policies

The simulator allows you to apply inbound and outbound policies to control traffic flow. This is useful for traffic engineering or blocking malicious prefixes manually.

In this example, filter out the prefix 4.4.0.0/16 from Router 10.2.2.1.

First, we check the routing table to confirm the route currently exists.

```
show ip bgp 10.2.2.1
```

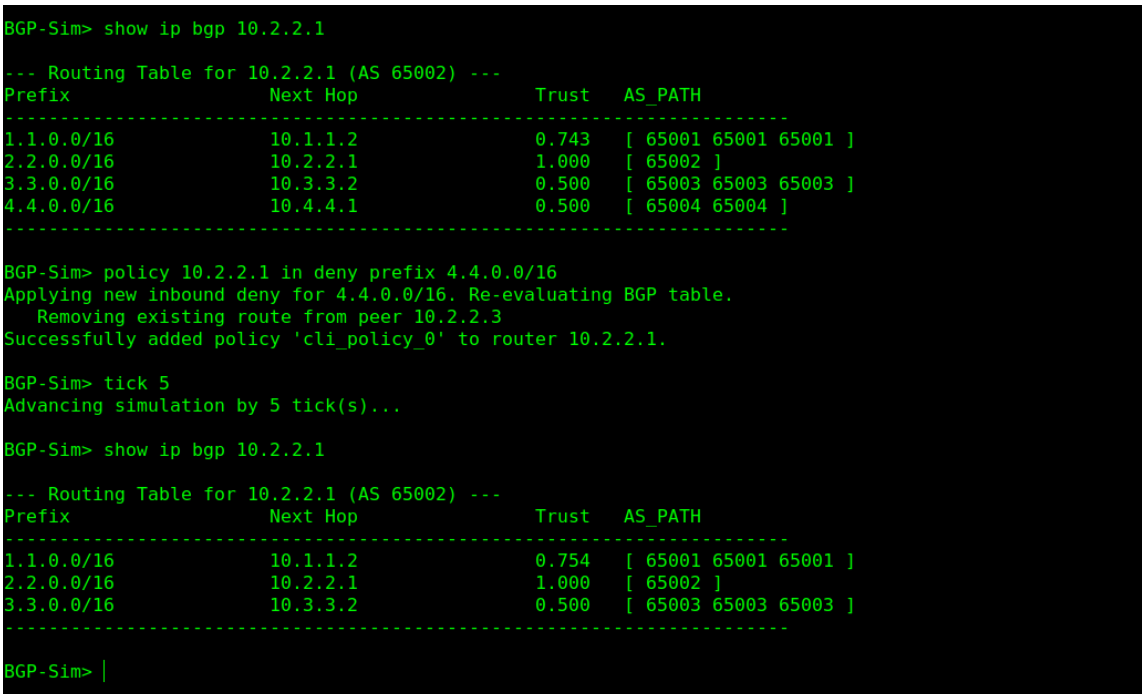
The table lists 4.4.0.0/16 with a next hop of 10.4.4.1. The table lists 4.4.0.0/16 via a next hop of 10.4.4.1.

Apply an inbound policy to deny this specific prefix. This forces the router to drop any advertisements for this network from its neighbors.

```
policy <router_id> <direction> <action> prefix <network/mask>

policy 10.2.2.1 in deny prefix 4.4.0.0/16
```

Observe the immediate log output: "Removing existing route from peer" The simulator instantly re-evaluates the BGP table when a policy is committed. Verify

Verify the after state with the show ip bgp command.



```
BGP-Sim> show ip bgp 10.2.2.1

--- Routing Table for 10.2.2.1 (AS 65002) ---
Prefix                  Next Hop                Trust   AS_PATH
-----------------------------------------------------------------------
1.1.0.0/16              10.1.1.2                0.743   [ 65001 65001 65001 ]
2.2.0.0/16              10.2.2.1                1.000   [ 65002 ]
3.3.0.0/16              10.3.3.2                0.500   [ 65003 65003 65003 ]
4.4.0.0/16              10.4.4.1                0.500   [ 65004 65004 ]
-----------------------------------------------------------------------

BGP-Sim> policy 10.2.2.1 in deny prefix 4.4.0.0/16
Applying new inbound deny for 4.4.0.0/16. Re-evaluating BGP table.
   Removing existing route from peer 10.2.2.3
Successfully added policy 'cli_policy_0' to router 10.2.2.1.

BGP-Sim> tick 5
Advancing simulation by 5 tick(s)...

BGP-Sim> show ip bgp 10.2.2.1

--- Routing Table for 10.2.2.1 (AS 65002) ---
Prefix                  Next Hop                Trust   AS_PATH
-----------------------------------------------------------------------
1.1.0.0/16              10.1.1.2                0.754   [ 65001 65001 65001 ]
2.2.0.0/16              10.2.2.1                1.000   [ 65002 ]
3.3.0.0/16              10.3.3.2                0.500   [ 65003 65003 65003 ]
-----------------------------------------------------------------------

BGP-Sim> |
```

Shutdown and Startup

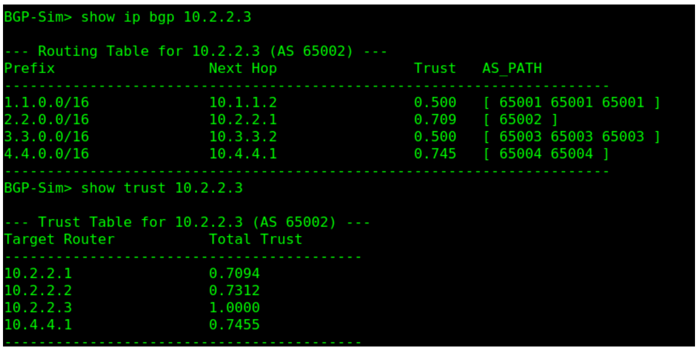
To simulate a power outage or hardware crash, use the shutdown command.

```
shutdown 10.4.4.1

 tick 5
```

As soon as the simulation clock advances, the neighbor 10.2.2.3 detects the failure.

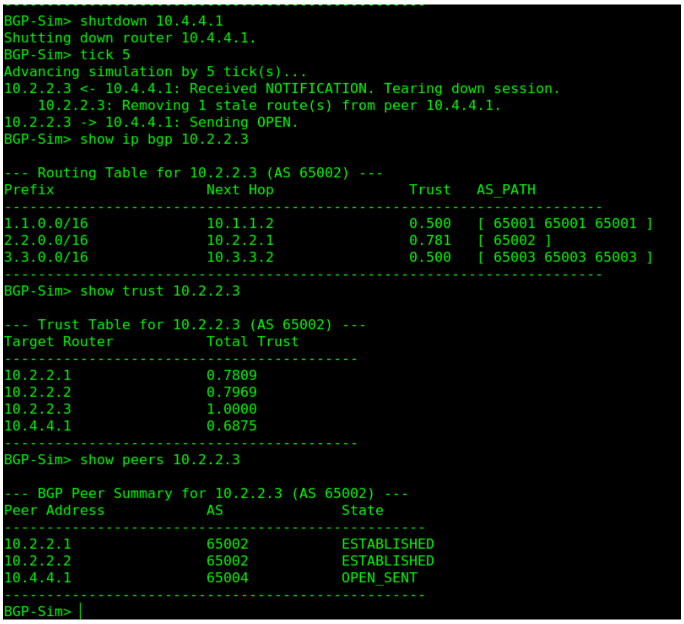
Running show ip bgp 10.2.2.3 confirms that the prefix 4.4.0.0/16 has been immediately removed from the routing table to prevent black-holing traffic.

Initial state:



```
BGP-Sim> show ip bgp 10.2.2.3

--- Routing Table for 10.2.2.3 (AS 65002) ---
Prefix                  Next Hop                Trust   AS_PATH
-----------------------------------------------------------------------
1.1.0.0/16              10.1.1.2                0.500   [ 65001 65001 65001 ]
2.2.0.0/16              10.2.2.1                0.709   [ 65002 ]
3.3.0.0/16              10.3.3.2                0.500   [ 65003 65003 65003 ]
4.4.0.0/16              10.4.4.1                0.745   [ 65004 65004 ]
-----------------------------------------------------------------------
BGP-Sim> show trust 10.2.2.3

--- Trust Table for 10.2.2.3 (AS 65002) ---
Target Router           Total Trust
------------------------------------------
10.2.2.1                0.7094
10.2.2.2                0.7312
10.2.2.3                1.0000
10.4.4.1                0.7455
------------------------------------------
```

After shutdown and time advancement:



```
--------------------------------------------------
BGP-Sim> shutdown 10.4.4.1
Shutting down router 10.4.4.1.
BGP-Sim> tick 5
Advancing simulation by 5 tick(s)...
10.2.2.3 <- 10.4.4.1: Received NOTIFICATION. Tearing down session.
    10.2.2.3: Removing 1 stale route(s) from peer 10.4.4.1.
10.2.2.3 -> 10.4.4.1: Sending OPEN.
BGP-Sim> show ip bgp 10.2.2.3

--- Routing Table for 10.2.2.3 (AS 65002) ---
Prefix                  Next Hop                Trust   AS_PATH
-----------------------------------------------------------------------
1.1.0.0/16              10.1.1.2                0.500   [ 65001 65001 65001 ]
2.2.0.0/16              10.2.2.1                0.781   [ 65002 ]
3.3.0.0/16              10.3.3.2                0.500   [ 65003 65003 65003 ]
-----------------------------------------------------------------------
BGP-Sim> show trust 10.2.2.3

--- Trust Table for 10.2.2.3 (AS 65002) ---
Target Router           Total Trust
------------------------------------------
10.2.2.1                0.7809
10.2.2.2                0.7969
10.2.2.3                1.0000
10.4.4.1                0.6875
------------------------------------------
BGP-Sim> show peers 10.2.2.3

--- BGP Peer Summary for 10.2.2.3 (AS 65002) ---
Peer Address            AS              State
--------------------------------------------------
10.2.2.1                65002           ESTABLISHED
10.2.2.2                65002           ESTABLISHED
10.4.4.1                65004           OPEN_SENT
--------------------------------------------------
BGP-Sim> |
```

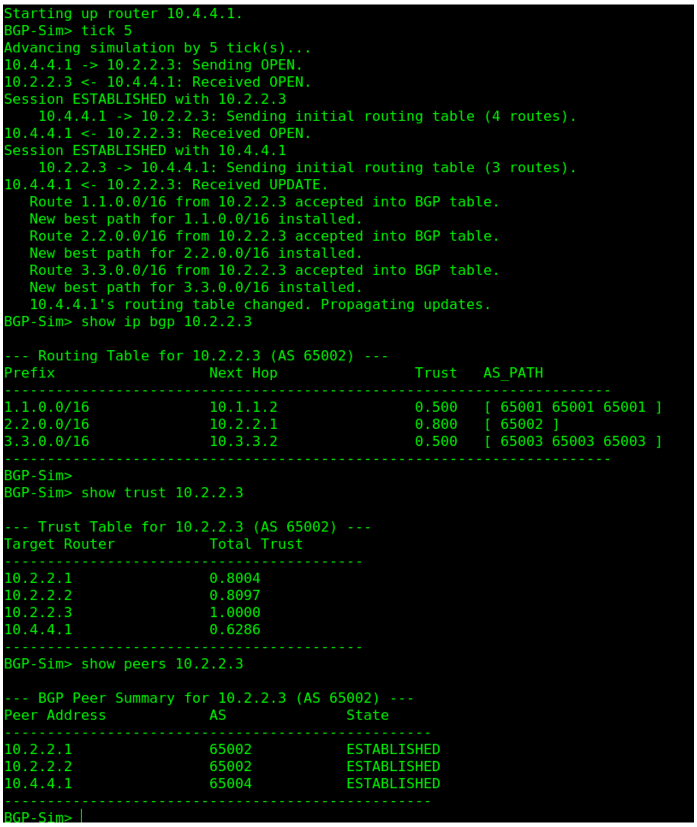
To power on the router, write this command:

```
startup 10.4.4.1
```

Advance time again:

```
tick 5
```

The routers automatically re-initiate the TCP handshake and BGP OPEN exchange. As shown in the image below, the route 4.4.0.0/16 is successfully restored in the table for Router 10.2.2.3.

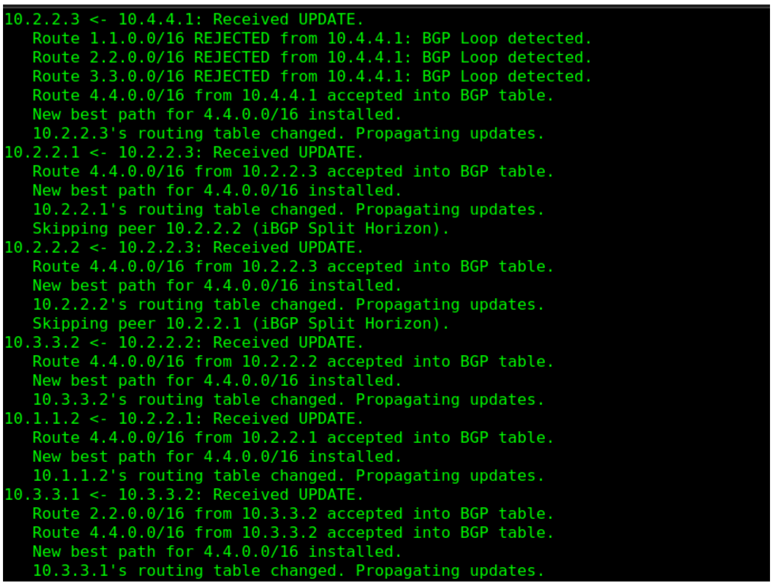


```
Starting up router 10.4.4.1.
BGP-Sim> tick 5
Advancing simulation by 5 tick(s)...
10.4.4.1 -> 10.2.2.3: Sending OPEN.
10.2.2.3 <- 10.4.4.1: Received OPEN.
Session ESTABLISHED with 10.2.2.3
    10.4.4.1 -> 10.2.2.3: Sending initial routing table (4 routes).
10.4.4.1 <- 10.2.2.3: Received OPEN.
Session ESTABLISHED with 10.4.4.1
    10.2.2.3 -> 10.4.4.1: Sending initial routing table (3 routes).
10.4.4.1 <- 10.2.2.3: Received UPDATE.
   Route 1.1.0.0/16 from 10.2.2.3 accepted into BGP table.
   New best path for 1.1.0.0/16 installed.
   Route 2.2.0.0/16 from 10.2.2.3 accepted into BGP table.
   New best path for 2.2.0.0/16 installed.
   Route 3.3.0.0/16 from 10.2.2.3 accepted into BGP table.
   New best path for 3.3.0.0/16 installed.
   10.4.4.1's routing table changed. Propagating updates.
BGP-Sim> show ip bgp 10.2.2.3

--- Routing Table for 10.2.2.3 (AS 65002) ---
Prefix                  Next Hop                Trust   AS_PATH
-----------------------------------------------------------------------
1.1.0.0/16              10.1.1.2                0.500   [ 65001 65001 65001 ]
2.2.0.0/16              10.2.2.1                0.800   [ 65002 ]
3.3.0.0/16              10.3.3.2                0.500   [ 65003 65003 65003 ]
-----------------------------------------------------------------------
BGP-Sim>
BGP-Sim> show trust 10.2.2.3

--- Trust Table for 10.2.2.3 (AS 65002) ---
Target Router           Total Trust
------------------------------------------
10.2.2.1                0.8004
10.2.2.2                0.8097
10.2.2.3                1.0000
10.4.4.1                0.6286
------------------------------------------
BGP-Sim> show peers 10.2.2.3

--- BGP Peer Summary for 10.2.2.3 (AS 65002) ---
Peer Address            AS              State
--------------------------------------------------
10.2.2.1                65002           ESTABLISHED
10.2.2.2                65002           ESTABLISHED
10.4.4.1                65004           ESTABLISHED
--------------------------------------------------
BGP-Sim> |
```

Original routes from 10.4.4.1 must be re-sent manually.

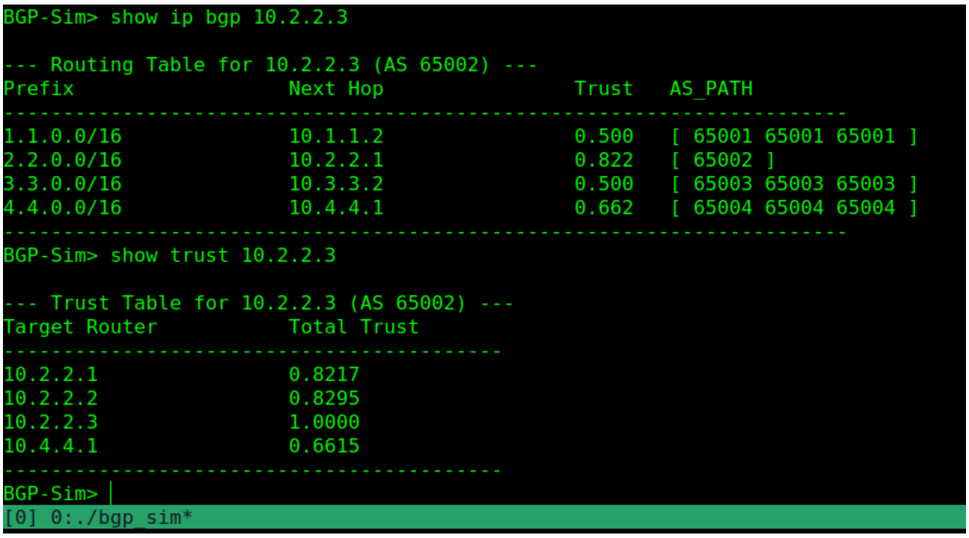
```
resend-routes 10.4.4.1
```

You will see a detailed log message for each router that received updates from the router that resent its routes. New best paths are installed.



```
10.2.2.3 <- 10.4.4.1: Received UPDATE.
   Route 1.1.0.0/16 REJECTED from 10.4.4.1: BGP Loop detected.
   Route 2.2.0.0/16 REJECTED from 10.4.4.1: BGP Loop detected.
   Route 3.3.0.0/16 REJECTED from 10.4.4.1: BGP Loop detected.
   Route 4.4.0.0/16 from 10.4.4.1 accepted into BGP table.
   New best path for 4.4.0.0/16 installed.
   10.2.2.3's routing table changed. Propagating updates.
10.2.2.1 <- 10.2.2.3: Received UPDATE.
   Route 4.4.0.0/16 from 10.2.2.3 accepted into BGP table.
   New best path for 4.4.0.0/16 installed.
   10.2.2.1's routing table changed. Propagating updates.
   Skipping peer 10.2.2.2 (iBGP Split Horizon).
10.2.2.2 <- 10.2.2.3: Received UPDATE.
   Route 4.4.0.0/16 from 10.2.2.3 accepted into BGP table.
   New best path for 4.4.0.0/16 installed.
   10.2.2.2's routing table changed. Propagating updates.
   Skipping peer 10.2.2.1 (iBGP Split Horizon).
10.3.3.2 <- 10.2.2.2: Received UPDATE.
   Route 4.4.0.0/16 from 10.2.2.2 accepted into BGP table.
   New best path for 4.4.0.0/16 installed.
   10.3.3.2's routing table changed. Propagating updates.
10.1.1.2 <- 10.2.2.1: Received UPDATE.
   Route 4.4.0.0/16 from 10.2.2.1 accepted into BGP table.
   New best path for 4.4.0.0/16 installed.
   10.1.1.2's routing table changed. Propagating updates.
10.3.3.1 <- 10.3.3.2: Received UPDATE.
   Route 2.2.0.0/16 from 10.3.3.2 accepted into BGP table.
   Route 4.4.0.0/16 from 10.3.3.2 accepted into BGP table.
   New best path for 4.4.0.0/16 installed.
   10.3.3.1's routing table changed. Propagating updates.
```

Verify the previously shut down router re-appears in the BGP routing table with the show ip bgp command. You may observe that the trust score of the shut down router has decreased since trust scores are affected by the number of successful interactions.



```
BGP-Sim> show ip bgp 10.2.2.3

--- Routing Table for 10.2.2.3 (AS 65002) ---
Prefix                  Next Hop                Trust   AS_PATH
-----------------------------------------------------------------------
1.1.0.0/16              10.1.1.2                0.500   [ 65001 65001 65001 ]
2.2.0.0/16              10.2.2.1                0.822   [ 65002 ]
3.3.0.0/16              10.3.3.2                0.500   [ 65003 65003 65003 ]
4.4.0.0/16              10.4.4.1                0.662   [ 65004 65004 65004 ]
-----------------------------------------------------------------------
BGP-Sim> show trust 10.2.2.3

--- Trust Table for 10.2.2.3 (AS 65002) ---
Target Router           Total Trust
------------------------------------------
10.2.2.1                0.8217
10.2.2.2                0.8295
10.2.2.3                1.0000
10.4.4.1                0.6615
------------------------------------------
BGP-Sim> |
[0] 0:./bgp_sim*
```

Announce and Withdraw

The announce and withdraw commands are used to simulate a full attack and remediation cycle, demonstrating how a malicious router can inject false routing information and how the network recovers when that information is removed.

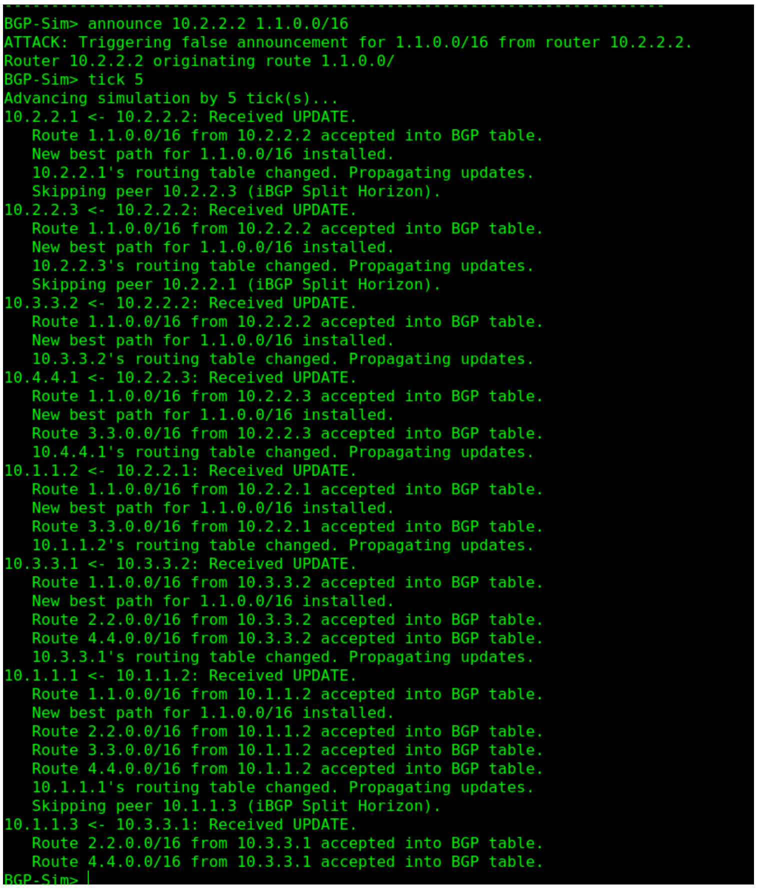
The "attacker" router 10.2.2.2 (AS 65002) was commanded to falsely announce the prefix 1.1.0.0/16. This prefix rightfully belongs to AS 65001, making this a classic BGP hijack attempt.

Syntax: announce <router_id> <prefix/length>

Use this command to simulate an attack where Router 10.2.2.2 attempts to hijack traffic meant for the 1.1.0.0/16 network.

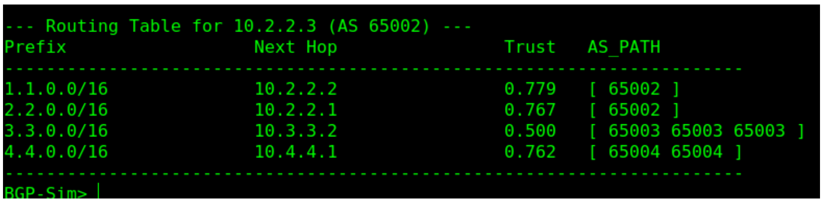
```
announce 10.2.2.2 1.1.0.0/16

tick 5
```

The simulator will log an ATTACK trigger. After advancing the simulation (using tick), you will see UPDATE messages propagating to neighboring routers. Peers will evaluate the new route. If the hijacked path is shorter or preferred by policy, peers will install it and begin routing traffic to the attacker.



```
--------------------------------------------------------------------------
BGP-Sim> announce 10.2.2.2 1.1.0.0/16
ATTACK: Triggering false announcement for 1.1.0.0/16 from router 10.2.2.2.
Router 10.2.2.2 originating route 1.1.0.0/
BGP-Sim> tick 5
Advancing simulation by 5 tick(s)...
10.2.2.1 <- 10.2.2.2: Received UPDATE.
   Route 1.1.0.0/16 from 10.2.2.2 accepted into BGP table.
   New best path for 1.1.0.0/16 installed.
   10.2.2.1's routing table changed. Propagating updates.
   Skipping peer 10.2.2.3 (iBGP Split Horizon).
10.2.2.3 <- 10.2.2.2: Received UPDATE.
   Route 1.1.0.0/16 from 10.2.2.2 accepted into BGP table.
   New best path for 1.1.0.0/16 installed.
   10.2.2.3's routing table changed. Propagating updates.
   Skipping peer 10.2.2.1 (iBGP Split Horizon).
10.3.3.2 <- 10.2.2.2: Received UPDATE.
   Route 1.1.0.0/16 from 10.2.2.2 accepted into BGP table.
   New best path for 1.1.0.0/16 installed.
   10.3.3.2's routing table changed. Propagating updates.
10.4.4.1 <- 10.2.2.3: Received UPDATE.
   Route 1.1.0.0/16 from 10.2.2.3 accepted into BGP table.
   New best path for 1.1.0.0/16 installed.
   Route 3.3.0.0/16 from 10.2.2.3 accepted into BGP table.
   10.4.4.1's routing table changed. Propagating updates.
10.1.1.2 <- 10.2.2.1: Received UPDATE.
   Route 1.1.0.0/16 from 10.2.2.1 accepted into BGP table.
   New best path for 1.1.0.0/16 installed.
   Route 3.3.0.0/16 from 10.2.2.1 accepted into BGP table.
   10.1.1.2's routing table changed. Propagating updates.
10.3.3.1 <- 10.3.3.2: Received UPDATE.
   Route 1.1.0.0/16 from 10.3.3.2 accepted into BGP table.
   New best path for 1.1.0.0/16 installed.
   Route 2.2.0.0/16 from 10.3.3.2 accepted into BGP table.
   Route 4.4.0.0/16 from 10.3.3.2 accepted into BGP table.
   10.3.3.1's routing table changed. Propagating updates.
10.1.1.1 <- 10.1.1.2: Received UPDATE.
   Route 1.1.0.0/16 from 10.1.1.2 accepted into BGP table.
   New best path for 1.1.0.0/16 installed.
   Route 2.2.0.0/16 from 10.1.1.2 accepted into BGP table.
   Route 3.3.0.0/16 from 10.1.1.2 accepted into BGP table.
   Route 4.4.0.0/16 from 10.1.1.2 accepted into BGP table.
   10.1.1.1's routing table changed. Propagating updates.
   Skipping peer 10.1.1.3 (iBGP Split Horizon).
10.1.1.3 <- 10.3.3.1: Received UPDATE.
   Route 2.2.0.0/16 from 10.3.3.1 accepted into BGP table.
   Route 4.4.0.0/16 from 10.3.3.1 accepted into BGP table.
BGP-Sim> |
```

After the hijack, the BGP routing table look as follows:



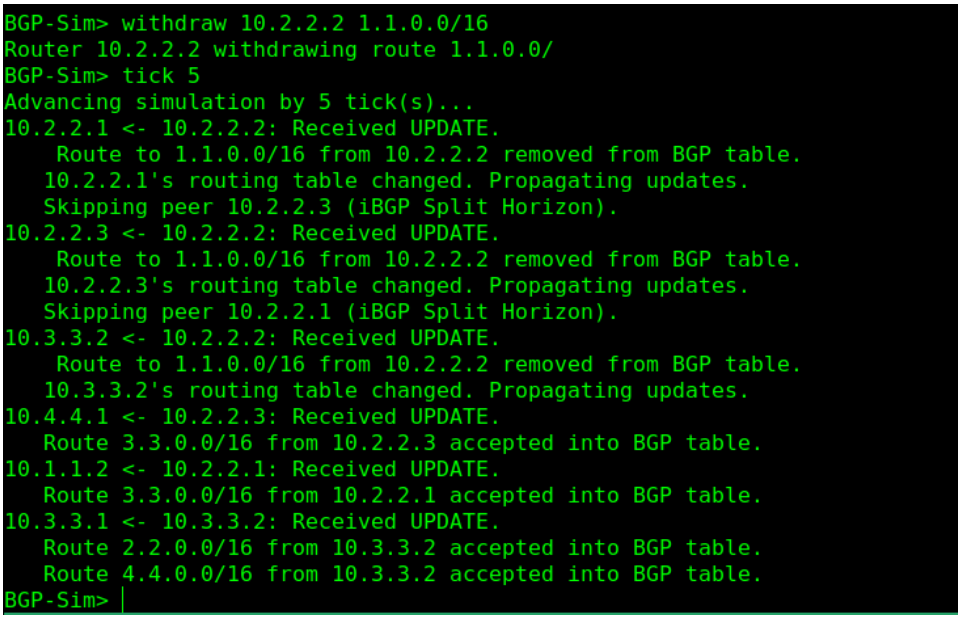
```
--- Routing Table for 10.2.2.3 (AS 65002) ---
Prefix              Next Hop            Trust   AS_PATH
-----------------------------------------------------------------------
1.1.0.0/16          10.2.2.2            0.779   [ 65002 ]
2.2.0.0/16          10.2.2.1            0.767   [ 65002 ]
3.3.0.0/16          10.3.3.2            0.500   [ 65003 65003 65003 ]
4.4.0.0/16          10.4.4.1            0.762   [ 65004 65004 ]
-----------------------------------------------------------------------
BGP-Sim> |
```

The withdraw command instructs a router to send a BGP WITHDRAW message for a specific prefix. This simulates the cessation of an attack, the correction of a configuration error, or a link failure. It forces the network to re-converge.

withdraw <router_id> <prefix/length>

```
withdraw 10.2.2.2 1.1.0.0/16

tick 5
```

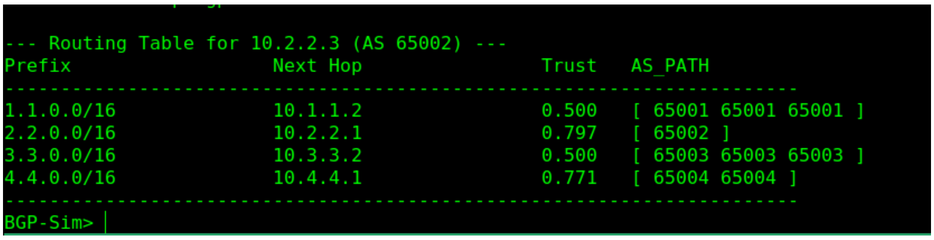
The target router sends updates to all established peers indicating the route is no longer available. Neighbors immediately remove the route from their BGP tables. Routers will automatically search their tables for alternative paths. If a legitimate route exists (the original owner of the prefix), the routers will promote that path to the routing table, restoring normal connectivity.



```
BGP-Sim> withdraw 10.2.2.2 1.1.0.0/16
Router 10.2.2.2 withdrawing route 1.1.0.0/
BGP-Sim> tick 5
Advancing simulation by 5 tick(s)...
10.2.2.1 <- 10.2.2.2: Received UPDATE.
    Route to 1.1.0.0/16 from 10.2.2.2 removed from BGP table.
   10.2.2.1's routing table changed. Propagating updates.
   Skipping peer 10.2.2.3 (iBGP Split Horizon).
10.2.2.3 <- 10.2.2.2: Received UPDATE.
    Route to 1.1.0.0/16 from 10.2.2.2 removed from BGP table.
   10.2.2.3's routing table changed. Propagating updates.
   Skipping peer 10.2.2.1 (iBGP Split Horizon).
10.3.3.2 <- 10.2.2.2: Received UPDATE.
    Route to 1.1.0.0/16 from 10.2.2.2 removed from BGP table.
   10.3.3.2's routing table changed. Propagating updates.
10.4.4.1 <- 10.2.2.3: Received UPDATE.
   Route 3.3.0.0/16 from 10.2.2.3 accepted into BGP table.
10.1.1.2 <- 10.2.2.1: Received UPDATE.
   Route 3.3.0.0/16 from 10.2.2.1 accepted into BGP table.
10.3.3.1 <- 10.3.3.2: Received UPDATE.
   Route 2.2.0.0/16 from 10.3.3.2 accepted into BGP table.
   Route 4.4.0.0/16 from 10.3.3.2 accepted into BGP table.
BGP-Sim>
```

After performing an announce or withdraw, always verify the network state using the show ip bgp command.

```
show ip bgp 10.2.2.3
```



```
--- Routing Table for 10.2.2.3 (AS 65002) ---
Prefix                  Next Hop                Trust   AS_PATH
------------------------------------------------------------------------
1.1.0.0/16              10.1.1.2                0.500   [ 65001 65001 65001 ]
2.2.0.0/16              10.2.2.1                0.797   [ 65002 ]
3.3.0.0/16              10.3.3.2                0.500   [ 65003 65003 65003 ]
4.4.0.0/16              10.4.4.1                0.771   [ 65004 65004 ]
------------------------------------------------------------------------
BGP-Sim>
```