IPv6 Test Service

Border Gateway Protocol 4+
Over Internet Protocol Version 6
Interoperability Test Suite

Version 3.1

University of New Hampshire
InterOperability Laboratory
IPv6 Test Service
https://www.iol.unh.edu

21 Madbury Road, Suite 100
Durham, NH 03824
Phone: +1-603-862-2804
Fax: +1-603-862-4181

Table of Contents

Acknowledgements

The University of New Hampshire would like to acknowledge the efforts of the following individuals in the development of this test suite:

Timothy Carlin	University of New Hampshire
Chris Brown	University of New Hampshire
Hannah Dukeman	University of New Hampshire
Timothy Winters	QA Café

This document integrated test cases from UNH-IOL Border Gateway Protocol 4+
Over Internet Protocol Version 6 Multi-System Interoperability Test Suite, version 2.3. We also thank the following individuals in the development of this test suite:

Ethan Burns	University of New Hampshire
Eric Barrett	University of New Hampshire
Andrew Gadzik	University of New Hampshire
Sagun Shakya	University of New Hampshire
Fanny Xu	University of New Hampshire

References

[BGP4]	RFC4271 A Border Gateway Protocol 4 (BGP-4). Y. Rekhter, Ed., T. Li, Ed., S. Hares, Ed.. January 2006. (Format: TXT, HTML) (Obsoletes RFC1771) (Updated by RFC6286, RFC6608, RFC6793, RFC7606, RFC7607, RFC7705, RFC8212, RFC8654) (Status: DRAFT STANDARD) (DOI: 10.17487/RFC4271)
[BGP MPE]	RFC4760 Multiprotocol Extensions for BGP-4. T. Bates, R. Chandra, D. Katz, Y. Rekhter. January 2007. (Format: TXT, HTML) (Obsoletes RFC2858) (Updated by RFC7606) (Status: DRAFT STANDARD) (DOI: 10.17487/RFC4760)
[BGP MPE v6]	RFC2545 Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing. P. Marques, F. Dupont. March 1999. (Format: TXT, HTML) (Status: PROPOSED STANDARD) (DOI: 10.17487/RFC2545)
[BGP Cap]	RFC5492 Capabilities Advertisement with BGP-4. J. Scudder, R. Chandra. February 2009. (Format: TXT, HTML) (Obsoletes RFC3392) (Updated by RFC8810) (Status: DRAFT STANDARD) (DOI: 10.17487/RFC5492)
[BGP AS Uniq]	RFC6286 Autonomous-System-Wide Unique BGP Identifier for BGP-4. E. Chen, J. Yuan. June 2011. (Format: TXT, HTML) (Updates RFC4271) (Status: PROPOSED STANDARD) (DOI: 10.17487/RFC6286)
[BGP 4AS]	RFC6793 BGP Support for Four-Octet Autonomous System (AS) Number Space. Q. Vohra, E. Chen. December 2012. (Format: TXT, HTML) (Obsoletes RFC4893) (Updates RFC4271) (Status: PROPOSED STANDARD) (DOI: 10.17487/RFC6793)
[BGP ASMIG]	RFC7705 Autonomous System Migration Mechanisms and Their Effects on the BGP AS_PATH Attribute. W. George, S. Amante. November 2015. (Format: TXT, HTML) (Updates RFC4271) (Status: PROPOSED STANDARD) (DOI: 10.17487/RFC7705)
[BGP EBGP]	RFC8212 Default External BGP (EBGP) Route Propagation Behavior without Policies. J. Mauch, J. Snijders, G. Hankins. July 2017. (Format: TXT, HTML) (Updates RFC4271) (Status: PROPOSED STANDARD) (DOI: 10.17487/RFC8212)
[NIST IPv6 Profile]	"NIST IPv6 Profile", NIST Special Publication (NIST SP) - 500-267Ar1, November 2020. https://doi.org/10.6028/NIST.SP.500-267Ar1
[USGv6-R1]	"USGv6 Profile", NIST Special Publication (NIST SP) - 500-267Br1, November 2020. https://doi.org/10.6028/NIST.SP.500-267Br1

Introduction

Overview

The University of New Hampshire's InterOperability Laboratory (IOL) is an institution designed to improve the interoperability of standards based products by providing an environment where a product can be tested against other implementations of a standard. This suite of tests has been developed to help implementers evaluate the functionality of their BGP based products. This test suite has been designed to test the Interoperability of the device under test with other BGP Capable devices. This test suite focuses on testing configurations of the network that could cause problems when deployed if the device under test does not operate properly with the devices that it is connected to.

The tests do not determine if a product conforms to the BGP standards but they are designed as interoperability tests. These tests provide one method to isolate problems within the BGP capable device that will affect the interoperability performance. Successful completion of all tests contained in this suite does not guarantee that the tested device will operate with other BGP capable devices. However, these tests do provide a reasonable level of confidence that the RUT will function well in most BGP capable environments.

Common Configuration

Topology

- The Router Under Test (RUT) assumes the role of TR1 for all test cases and topologies unless otherwise specified
- No routes are configured unless otherwise specified.
- Connected routes are distributed to BGP unless otherwise specified.
- Host devices may be simulated traffic generators and need not be independent implementations of Hosts.
- Shutdown BGP on all TRs prior to each test part.
- Unless otherwise specified, configure Import and Export Policies as needed for all routes in the topology.
- All tests are conducted in an IPv6-Only environment. Neither the DUT Management, nor the test networks are provisioned with any IPv4 or IPv4 Services.

Group 1: BGP

BGP.IO.1.1: External BGP Peer

Purpose: To verify that a BGP router establishes a connection to a directly connected external peer.

References:
- [BGP4]
- [BGP EBGP]

Test Setup:
Prior to the start of each test part:
- Shutdown BGP on all routers

Procedure:

Part A: External BGP Peer

Step	Action	Expected Result
1.	Shutdown BGP on all TRs.	
2.	TR1 and TR2 are configured as External Peers and BGP is enabled. TR1 and TR3 are configured as External Peers and BGP is enabled. TR1 and TR4 are configured as External Peers and BGP is enabled.	
3.	No Import or Export Policies are configured on any TRs.	
4.	Transmit Traffic from H1 to H2.	Traffic is **not** transmitted to H2.
5.	Transmit Traffic from H1 to H3.	Traffic is **not** transmitted to H3.

6.	Transmit Traffic from H1 to H4.	Traffic is **not** transmitted to H4.

7.	Configure Policies as Below:
	TR1:
	  Import:
	    Link2 from TR2
	    Link3 from TR3
	    Link4 from TR4
	
	TR2:
	  Import:
	    Link1 from TR1
	  Export:
	    Link2 to TR1
	
	TR3:
	  Import:
	    Link1 from TR1
	  Export:
	    Link3 to TR1
	
	TR4:
	  Import:
	    Link1 from TR1
	  Export:
	    Link4 to TR1	

8.	Transmit Traffic from H1 to H2. Transmit Traffic from H2 to H1.	Traffic Route: 1 H1 2 Link1 3 TR1 4 Link5 5 TR2 6 Link2 7 H2 Traffic is **not** transmitted in the return direction from H2 to H1.
9.	Transmit Traffic from H1 to H3. Transmit Traffic from H3 to H1.	Traffic Route: 1 H1 2 Link1 3 TR1 4 Link5 5 TR3 6 Link3 7 H3

		Traffic is **not** transmitted in the return direction from H3 to H1.
10.	Transmit Traffic from H1 to H4. Transmit Traffic from H4 to H1.	Traffic Route: 1 H1 2 Link1 3 TR1 4 Link5 5 TR4 6 Link4 7 H4 Traffic is **not** transmitted in the return direction from H4 to H1.

11.	Configure Policies as Below in addition to those previously configured:
	TR1:
	  Export:
	    Link1 to TR2
	    Link1 to TR3
	    Link1 to TR4	

12.	Transmit Traffic from H1 to H2. Transmit Traffic from H2 to H1.	Traffic Route: 1 H1 2 Link1 3 TR1 4 Link5 5 TR2 6 Link2 7 H2 Traffic is transmitted in both directions between H1 and H2. Traffic transmitted from H2 to H1 should be routed in reverse order.
13.	Transmit Traffic from H1 to H3. Transmit Traffic from H3 to H1.	Traffic Route: 1 H1 2 Link1 3 TR1 4 Link5 5 TR3 6 Link3 7 H3 Traffic is transmitted in both directions between H1 and H3.

		Traffic transmitted from H3 to H1 should be routed in reverse order.
14.	Transmit Traffic from H1 to H4. Transmit Traffic from H4 to H1.	Traffic Route: 1 H1 2 Link1 3 TR1 4 Link5 5 TR4 6 Link4 7 H4 Traffic is transmitted in both directions between H1 and H4. Traffic transmitted from H4 to H1 should be routed in reverse order.

Part B: External BGP Peer Removal and Re-establishment

Step	Action	Expected Result
15.	Shutdown BGP on all Routers.	
16.	TR1 and TR2 are configured as External Peers and BGP is enabled. TR1 and TR3 are configured as External Peers and BGP is enabled. TR1 and TR4 are configured as External Peers and BGP is enabled. TR2 and TR3 are configured as External Peers and BGP is enabled. TR3 and TR4 are configured as External Peers and BGP is enabled.	

17.	Configure a full-mesh of Import and Export Policies. (e.g. TR1 Exports Link1 to all TR1s, and Imports all routes from all TRs. TR2 Exports Link2 to all Routers and Imports all routes from all TRs.)	
18.	Transmit Traffic from H1 to H2.	Traffic Route: 1 H1 2 Link1 3 TR1 4 Link5 5 TR2 6 Link2 7 H2
19.	Transmit Traffic from H1 to H3.	Traffic Route: 1 H1 2 Link1 3 TR1 4 Link5 5 TR3 6 Link3 7 H3
20.	Transmit Traffic from H1 to H4.	Traffic Route: 1 H1 2 Link1 3 TR1 4 Link5 5 TR4 6 Link4 7 H4
21.	Shutdown TR2's interface to Link5.	
22.	Transmit Traffic from H1 to H2.	Traffic Route: 1 H1 2 Link1 3 TR1 4 Link5 5 TR3 6 Link6 7 TR2 8 Link2 9 H2
23.	Enable TR2's interface to Link5. Shutdown TR3's interface to Link5. Shutdown TR4's interface to Link5.	

24.	Transmit Traffic from H1 to H3.	Traffic Route: 1 H1 2 Link1 3 TR1 4 Link5 5 TR2 6 Link6 7 TR3 8 Link3 9 H3
25.	Transmit Traffic from H1 to H4.	Traffic Route: 1 H1 2 Link1 3 TR1 4 Link5 5 TR2 6 Link6 7 TR3 8 Link7 9 TR4 10 Link4 11 H4
26.	Enable TR3's interface to Link5. Enable TR4's interface to Link5.	
27.	Transmit Traffic from H1 to H3.	Traffic Route: 1 H1 2 Link1 3 TR1 4 Link5 5 TR3 8 Link3 9 H3
28.	Transmit Traffic from H1 to H4.	Traffic Route: 1 H1 2 Link1 3 TR1 4 Link5 5 TR4 6 Link4 7 H4

Possible Problems:
- None

BGP.IO.1.2: External Peer Shortest Path Selection

Purpose: To verify that a BGP router establishes a connection to a directly connected external peer and selects the shortest path to the destination.

References:
- [BGP4]

Test Setup:
Prior to the start of each test part:
- Shutdown BGP on all routers
- Configure a full-mesh of Import and Export Policies. (e.g. TR1 Exports Link1 to all peers, and Imports all routes from all peers. TR2 Exports Link2 to all peers and Imports all routes from all peers, etc.)
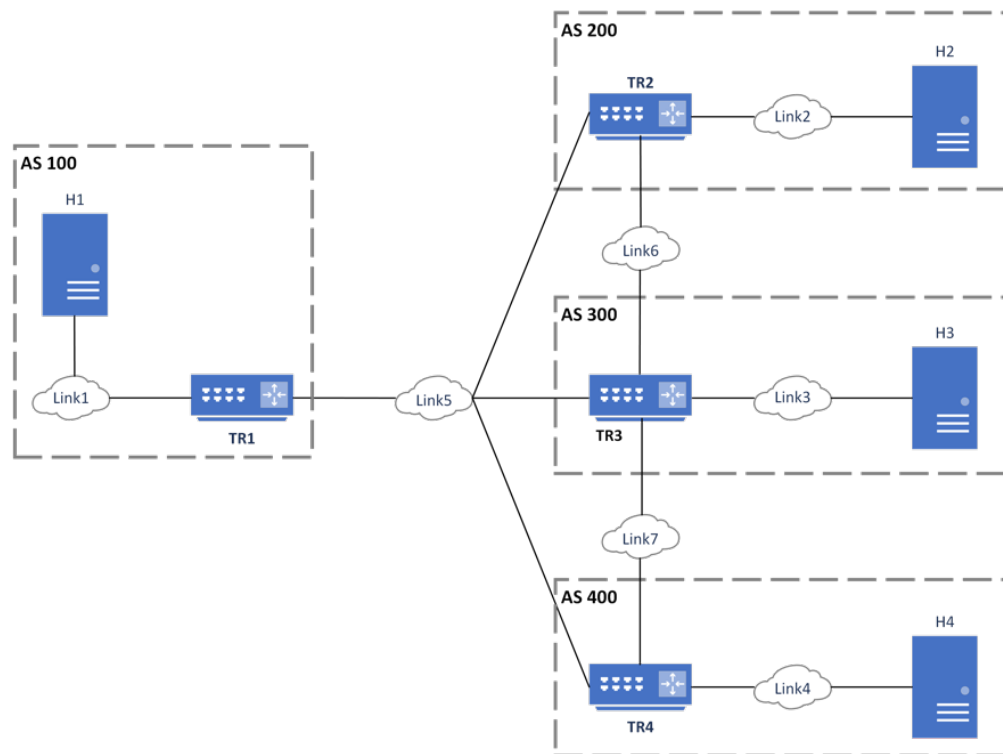
Procedure:

Part A: External BGP Peer Shortest Path

Step	Action	Expected Result
1.	Shutdown BGP on all TRs.	
2.	TR1 and TR2 are configured as External Peers and BGP is enabled. TR1 and TR3 are configured as External Peers and BGP is enabled.	

	TR1 and TR4 are configured as External Peers and BGP is enabled. TR2 and TR3 are configured as External Peers and BGP is enabled. TR3 and TR4 are configured as External Peers and BGP is enabled.	
3.	Transmit Traffic from H1 to H2.	Traffic Route: 1 H1 2 Link1 3 TR1 4 Link5 5 TR2 6 Link2 7 H2
4.	Transmit Traffic from H1 to H3.	Traffic Route: 1 H1 2 Link1 3 TR1 4 Link5 5 TR3 6 Link3 7 H3
5.	Transmit Traffic from H1 to H4.	Traffic Route: 1 H1 2 Link1 3 TR1 4 Link5 5 TR4 4 Link4 5 H4

Part B: Accepting AS PATH Change

Step	Action	Expected Result
6.	Shutdown BGP on all TRs.	
7.	TR1 and TR2 are configured as External Peers and BGP is enabled. TR1 and TR3 are configured as External Peers and BGP is enabled. TR1 and TR4 are configured as External Peers and BGP is enabled. TR2 and TR3 are configured as External Peers and BGP is enabled. TR3 and TR4 are configured as External Peers and BGP is enabled.	

8.	Configure TR2 to prepend its own ASN 3 times on outgoing UPDATES to TR1.	
9.	Configure TR4 to prepend its own ASN 3 times on outgoing UPDATES to TR1.	
10.	Transmit Traffic from H1 to H2.	Traffic Route: 1 H1 2 Link1 3 TR1 4 Link5 5 TR3 6 Link6 7 TR2 8 Link2 9 H2
11.	Transmit Traffic from H1 to H4.	Traffic Route: 1 H1 2 Link1 3 TR1 4 Link5 5 TR3 6 Link7 7 TR4 8 Link4 9 H4
12.	Remove TR2 prepending to TR1.	
13.	Remove TR4 prepending to TR1.	

Part C: Advertising AS PATH Change

Step	Action	Expected Result
14.	Shutdown BGP on all TRs.	
15.	TR1 and TR2 are configured as External Peers and BGP is enabled. TR1 and TR3 are configured as External Peers and BGP is enabled. TR1 and TR4 are configured as External Peers and BGP is enabled. TR2 and TR3 are configured as External Peers and BGP is enabled. TR3 and TR4 are configured as External Peers and BGP is enabled.	
16.	Configure TR1 to prepend its own ASN 4 times on outgoing UPDATES to TR4.	
17.	Configure TR1 to prepend its own ASN 3 times on outgoing UPDATES to TR3.	

18.	Transmit Traffic from H4 to H1.	Traffic Route: 1 H4 2 Link4 3 TR4 4 Link7 5 TR3 6 Link6 7 TR2 8 Link5 9 TR1 10 Link1 11 H1
19.	Transmit Traffic from H3 to H1.	Traffic Route: 1 H3 2 Link3 3 TR3 4 Link6 5 TR2 6 Link5 7 TR1 8 Link1 9 H1
20.	Remove TR1 prepending to TR3 and TR4.	
21.	Configure TR1 to prepend its own ASN 3 times on outgoing UPDATES to TR2.	
22.	Transmit Traffic from H2 to H1.	Traffic Route: 1 H2 2 Link2 3 TR2 4 Link6 5 TR3 6 Link5 7 TR1 8 Link1 9 H1
23.	Remove TR1 prepending to TR2.	

Possible Problems:
- None

BGP.IO.1.3: Internal BGP Peer

Purpose: To verify that a BGP router establishes a connection to a directly connected external peer.

References:
- [BGP4]

Test Setup:
Prior to the start of each test part:
- Shutdown BGP on all routers
- Configure a full-mesh of Import and Export Policies. (e.g. TR1 Exports Link1 to all peers, and Imports all routes from all peers. TR2 Exports Link2 to all peers and Imports all routes from all peers, etc.)

Procedure:
Part A: Internal BGP Peer TR2

Step	Action	Expected Result
1.	Shutdown BGP on all TRs.	
2.	TR1 and TR2 are configured as Internal Peers. TR1 and TR3 are configured as External Peers and BGP is enabled. TR1 and TR4 are configured as External Peers and BGP is enabled. TR3 and TR4 are configured as External Peers and BGP is enabled.	
3.	Transmit Traffic from H2 to H3.	Traffic Route: 1 H2 2 Link2 3 TR2 4 Link6

		5 TR1
		6 Link5
		7 TR3
		8 Link3
		9 H3
4.	Transmit Traffic from H3 to H2.	Traffic Route: 1 H3 2 Link3 3 TR3 4 Link5 5 TR1 6 Link6 7 TR2 8 Link2 9 H2
5.	Transmit Traffic from H2 to H4.	Traffic Route: 1 H2 2 Link2 3 TR2 4 Link6 5 TR1 6 Link5 7 TR4 8 Link4 9 H4
6.	Transmit Traffic from H4 to H2.	Traffic Route: 1 H4 2 Link4 3 TR4 4 Link5 5 TR1 6 Link6 7 TR2 8 Link2 9 H2
7.	Configure TR1 to prepend its own ASN 3 times in UPDATES to TR3.	
8.	Transmit Traffic from H3 to H2.	Traffic Route: 1 H3 2 Link3 3 TR3 4 Link7 5 TR4

		6 Link5
		7 TR1
		8 Link6
		9 TR2
		10 Link2
		11 H2
9.	Remove TR1 prepending to TR3.	
10.	Configure TR1 to prepend its own ASN 3 times in UPDATES to TR4.	
11.	Transmit Traffic from H4 to H2.	Traffic Route:
		1 H4
		2 Link4
		3 TR4
		4 Link7
		5 TR3
		6 Link5
		7 TR1
		8 Link6
		9 TR2
		10 Link2
		11 H2
12.	Remove TR1 prepending to TR4.	

Part B: Internal BGP Peer TR3
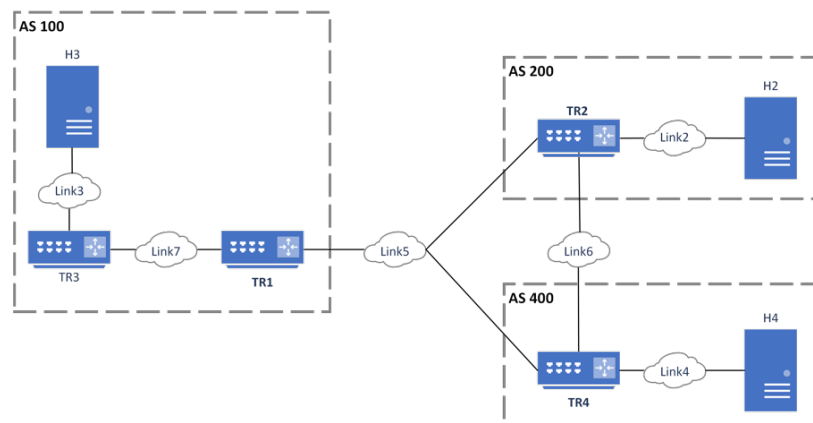
Step	Action	Expected Result
13.	Shutdown BGP on all TRs.	
14.	TR1 and TR3 are configured as Internal Peers. TR1 and TR2 are configured as External Peers and BGP is enabled. TR1 and TR4 are configured as External Peers and BGP is enabled. TR2 and TR4 are configured as External Peers and BGP is enabled.	

15.	Transmit Traffic from H3 to H2.	Traffic Route: 1 H3 2 Link3 3 TR3 4 Link7 5 TR1 6 Link5 7 TR2 8 Link2 9 H2
16.	Transmit Traffic from H2 to H3.	Traffic Route: 1 H2 2 Link2 3 TR2 4 Link5 5 TR1 6 Link7 7 TR3 8 Link3 9 H3
17.	Transmit Traffic from H3 to H4.	Traffic Route: 1 H3 2 Link3 3 TR3 4 Link7 5 TR1 6 Link5 7 TR4 8 Link4 9 H4
18.	Transmit Traffic from H4 to H3.	Traffic Route: 1 H4 2 Link4 3 TR4 4 Link5 5 TR1 6 Link7 7 TR3 8 Link3 9 H3
19.	Configure TR1 to prepend its own ASN 3 times in UPDATES to TR2.	
20.	Transmit Traffic from H2 to H3.	Traffic Route:

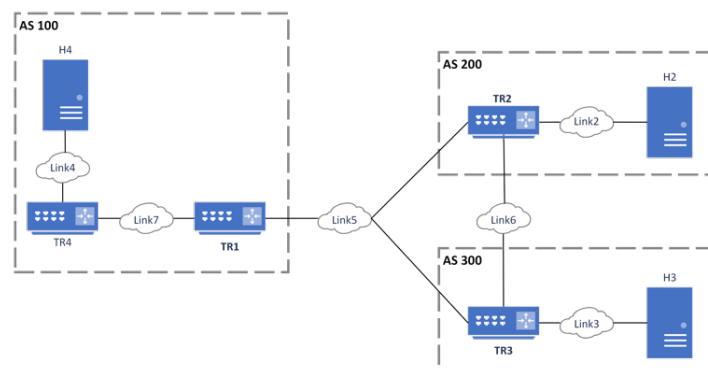| | | 1 H2 |
		2 Link2
		3 TR2
		4 Link6
		5 TR4
		6 Link5
		7 TR1
		8 Link7
		9 TR3
		10 Link3
		11 H3
21.	Remove TR1 prepending to TR2.	
22.	Configure TR1 to prepend its own ASN 3 times in UPDATES to TR4.	
23.	Transmit Traffic from H4 to H3.	Traffic Route: 1 H4 2 Link4 3 TR4 4 Link6 5 TR3 6 Link5 7 TR1 8 Link7 9 TR3 10 Link3 11 H3
24.	Remove TR1 prepending to TR4.	

Part C: Internal BGP Peer TR4

Step	Action	Expected Result
25.	Shutdown BGP on all TRs.	
26.	TR1 and TR4 are configured as Internal Peers. TR1 and TR2 are configured as External Peers and BGP is enabled.	

	TR1 and TR3 are configured as External Peers and BGP is enabled. TR2 and TR3 are configured as External Peers and BGP is enabled.	
27.	Transmit Traffic from H4 to H2.	Traffic Route: 1 H4 2 Link4 3 TR4 4 Link7 5 TR1 6 Link5 7 TR2 8 Link2 9 H2
28.	Transmit Traffic from H2 to H4.	Traffic Route: 1 H2 2 Link2 3 TR2 4 Link5 5 TR1 6 Link7 7 TR4 8 Link4 9 H4
29.	Transmit Traffic from H4 to H3.	Traffic Route: 1 H4 2 Link4 3 TR4 4 Link7 5 TR1 6 Link5 7 TR3 8 Link3 9 H3
30.	Transmit Traffic from H3 to H4.	Traffic Route: 1 H3 2 Link3 3 TR3 4 Link5 5 TR1 6 Link7 7 TR4 8 Link4 9 H4

31.	Configure TR1 to prepend its own ASN 3 times in UPDATES to TR2.	
32.	Transmit Traffic from H2 to H4.	Traffic Route: 1 H2 2 Link2 3 TR2 4 Link6 5 TR3 6 Link5 7 TR1 8 Link7 9 TR4 10 Link4 11 H4
33.	Remove TR1 prepending to TR2.	
34.	Configure TR1 to prepend its own ASN 3 times in UPDATES to TR3.	
35.	Transmit Traffic from H3 to H4.	Traffic Route: 1 H3 2 Link3 3 TR3 4 Link6 5 TR2 6 Link5 7 TR1 8 Link7 9 TR4 10 Link4 11 H4
36.	Remove TR1 prepending to TR3.	

Possible Problems:
- None

BGP.IO.1.4: Transit AS for External BGP Peer

Purpose: To verify that a BGP router establishes a connection to and communicates routes to directly connected external peer as a transit AS.

References:
- [BGP4]

Test Setup:
Prior to the start of each test part:
- Shutdown BGP on all routers
- Configure a full-mesh of Import and Export Policies. (e.g. TR1 Exports Link1 to all peers, and Imports all routes from all peers. TR2 Exports Link2 to all peers and Imports all routes from all peers, etc.)

Procedure:
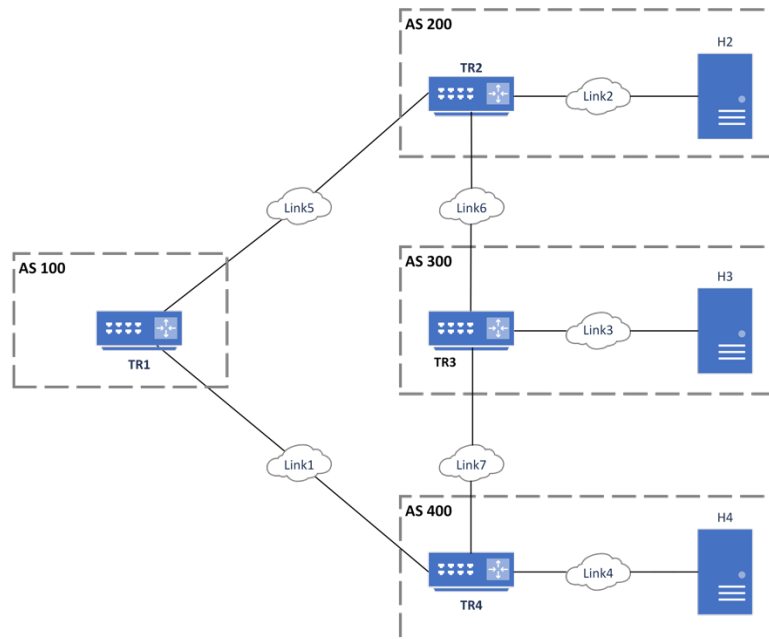
Part A: Transit AS

Step	Action	Expected Result
1.	Shutdown BGP on all TRs.	
2.	TR1 and TR2 are configured as External Peers and BGP is enabled. TR1 and TR4 are configured as External Peers and BGP is enabled. TR2 and TR3 are configured as External Peers and BGP is enabled.	
3.	Transmit Traffic from H2 to H4.	Traffic Route: 1 H2

		2 Link2
		3 TR2
		4 Link5
		5 TR1
		6 Link1
		7 TR4
		8 Link4
		9 H4
4.	Transmit Traffic from H3 to H4.	Traffic Route:
		1 H3
		2 Link3
		3 TR3
		4 Link6
		5 TR2
		6 Link5
		7 TR1
		8 Link1
		9 TR4
		10 Link4
		11 H4

Part B: Transit AS, Shorter AS Path

Step	Action	Expected Result
5.	Shutdown BGP on all TRs.	
6.	TR1 and TR2 are configured as External Peers. TR1 and TR4 are configured as External Peers. TR2 and TR3 are configured as External Peers. TR3 and TR4 are configured as External Peers.	
7.	Configure TR3 to prepend its own ASN 2 times on outgoing UPDATES to TR2.	
8.	Configure TR4 to prepend its own ASN 4 times on outgoing UPDATES to TR3.	
9.	Enable BGP on all TRs.	
10.	Transmit Traffic from H2 to H4.	Traffic Route: 1 H2 2 Link2 3 TR2 4 Link5 5 TR1 6 Link1 7 TR4 8 Link4 9 H4
11.	Transmit Traffic from H3 to H4.	Traffic Route:

		1 H3
		2 Link3
		3 TR3
		4 Link6
		5 TR2
		6 Link5
		7 TR1
		8 Link1
		9 TR4
		10 Link4
		11 H4

Part C: Transit AS, Longer AS Path

Step	Action	Expected Result
12.	Shutdown BGP on all TRs.	
13.	TR1 and TR2 are configured as External Peers. TR1 and TR4 are configured as External Peers. TR2 and TR3 are configured as External Peers. TR3 and TR4 are configured as External Peers.	
14.	Configure TR1 to prepend its own ASN 2 times on outgoing UPDATES to TR2.	
15.	Enable BGP on all TRs.	
16.	Transmit Traffic from H2 to H4.	Traffic Route: 1 H2 2 Link2 3 TR2 4 Link6 5 TR3 6 Link7 7 TR4 8 Link4 9 H4
17.	Shutdown BGP on TR3.	
18.	Transmit Traffic from H2 to H4.	Traffic Route: 1 H2 2 Link2 3 TR2 4 Link5 5 TR1 6 Link1 7 TR4 8 Link4 9 H4

Possible Problems:

- None

Group 2: BGP Negotiation

BGP.IO.2.1: ASN in OPEN Message
Purpose: To verify handling of ASN in OPEN messages.

References:
- [BGP4]
- [BGP ASMIG]

Test Setup:
Prior to the start of each test part:
- Shutdown BGP on all routers
- Configure a full-mesh of Import and Export Policies. (e.g. TR1 Exports Link1 to all peers, and Imports all routes from all peers. TR2 Exports Link2 to all peers and Imports all routes from all peers, etc.)
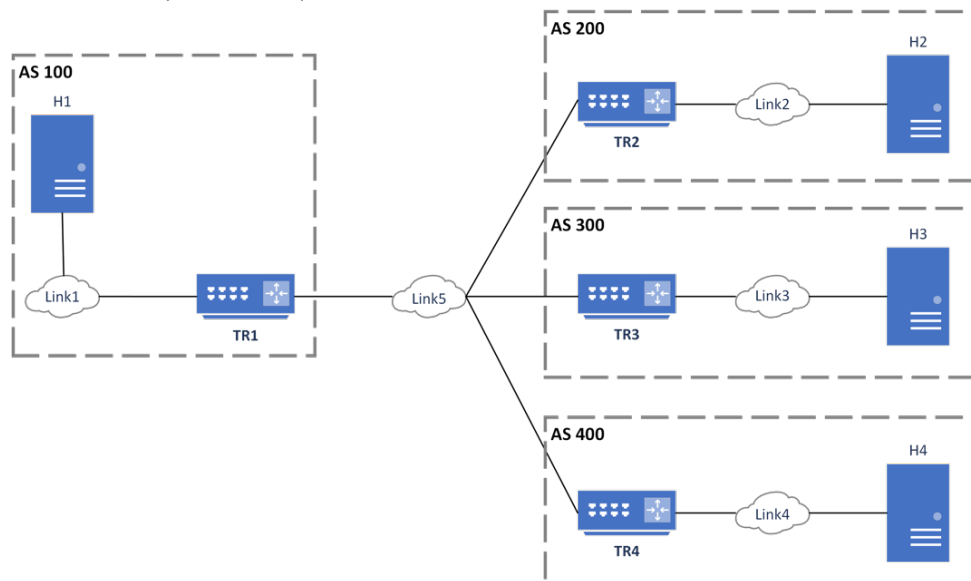
Procedure:

Part A: Mismatched ASN

Step	Action	Expected Result
1.	TR1 and TR2 are configured as External Peers and BGP is enabled. Shutdown BGP on other TRs.	
2.	Transmit Traffic from H1 to H2.	Traffic Route: 1 H1 2 Link1 3 TR1 4 Link5

		5 TR2 6 Link2 7 H2
3.	Shutdown BGP on TR2 and configure ASN as below: TR2 Local ASN: 201 TR1 Remote ASN for TR2: 200	
4.	Enable BGP on TR2.	TR1 sends a NOTIFICATION message with error code OPEN Message Error and error subcode Bad Peer AS
5.	Shutdown BGP on TR2 and configure ASN as below: TR2 Local ASN: 200 TR1 Remote ASN for TR2: 200	
6.	TR1 and TR3 are configured as External Peers and BGP is enabled. Shutdown BGP on other TRs.	
7.	Transmit Traffic from H1 to H3.	Traffic Route: 1 H1 2 Link1 3 TR1 4 Link5 5 TR3 6 Link3 7 H3
8.	Shutdown BGP on TR3 and configure ASN as below: TR3 Local ASN: 301 TR1 Remote ASN for TR3: 300	
9.	Enable BGP on TR3.	TR1 sends a NOTIFICATION message with error code OPEN Message Error and error subcode Bad Peer AS
10.	Shutdown BGP on TR3 and configure ASN as below: TR3 Local ASN: 300 TR1 Remote ASN for TR2: 300	
11.	TR1 and TR4 are configured as External Peers and BGP is enabled. Shutdown BGP on other TRs.	
12.	Transmit Traffic from H1 to H4.	Traffic Route: 1 H1

		2 Link1
		3 TR1
		4 Link5
		5 TR4
		6 Link4
		7 H4
13.	Shutdown BGP on TR4 and configure ASN as below: TR4 Local ASN: 401 TR1 Remote ASN for TR4: 400	
14.	Enable BGP on TR4.	TR1 sends a NOTIFICATION message with error code OPEN Message Error and error subcode Bad Peer AS
15.	Shutdown BGP on TR4 and configure ASN as below: TR4 Local ASN: 400 TR1 Remote ASN for TR2: 400	

Part B: TR1 Migrates ASN

Step	Action	Expected Result
16.	Shutdown BGP on all routers.	
17.	TR1 and TR2 are configured as External Peers and BGP is enabled. TR1 and TR3 are configured as External Peers and BGP is enabled. TR1 and TR4 are configured as External Peers and BGP is enabled.	
18.	Transmit Traffic from H1 to H2.	Traffic Route: 1 H1 2 Link1 3 TR1 4 Link5 5 TR2 6 Link2 7 H2
19.	Transmit Traffic from H1 to H3.	Traffic Route: 1 H1 2 Link1 3 TR1 4 Link5 5 TR3 6 Link3 7 H3

20.	Transmit Traffic from H1 to H4.	Traffic Route: 1 H1 2 Link1 3 TR1 4 Link5 5 TR4 6 Link4 7 H4
21.	Migrate the ASN of TR1. The global ASN of TR1 is configured as 900. Configure the "Local AS" capability of TR1 with AS 100. No changes are made to TR2, TR3, or TR4.	TR1 advertises AS 100 as the "Local AS" in BGP OPEN messages to TR2, TR3, and TR4.
22.	Transmit Traffic from H1 to H2. Transmit Traffic from H2 to H1.	Traffic Route: 1 H1 2 Link1 3 TR1 4 Link5 5 TR2 6 Link2 7 H2 Traffic is transmitted in both directions between H1 and H2. Traffic transmitted from H2 to H1 should be routed in reverse order.
23.	Transmit Traffic from H1 to H3. Transmit Traffic from H3 to H1.	Traffic Route: 1 H1 2 Link1 3 TR1 4 Link5 5 TR3 6 Link3 7 H3 Traffic is transmitted in both directions between H1 and H3. Traffic transmitted from H3 to H1 should be routed in reverse order.
24.	Transmit Traffic from H1 to H4. Transmit Traffic from H4 to H1.	Traffic Route: 1 H1 2 Link1 3 TR1 4 Link5

Step	Action	Expected Result
		5 TR4 6 Link4 7 H4 Traffic is transmitted in both directions between H1 and H4. Traffic transmitted from H4 to H1 should be routed in reverse order.
25.	Shutdown BGP on all routers and configure TR1 back to default ASN of 100 without "Local AS".	

Part C: Peer Migrates ASN

Step	Action	Expected Result
26.	TR1 and TR2 are configured as External Peers and BGP is enabled. TR1 and TR3 are configured as External Peers and BGP is enabled. TR1 and TR4 are configured as External Peers and BGP is enabled.	
27.	Transmit Traffic from H1 to H2. Transmit Traffic from H2 to H1.	Traffic Route: 1 H1 2 Link1 3 TR1 4 Link5 5 TR2 6 Link2 7 H2 Traffic is transmitted in both directions between H1 and H2. Traffic transmitted from H2 to H1 should be routed in reverse order.
28.	Transmit Traffic from H1 to H3. Transmit Traffic from H3 to H1.	Traffic Route: 1 H1 2 Link1 3 TR1 4 Link5 5 TR3 6 Link3 7 H3 Traffic is transmitted in both directions between H1 and H3. Traffic transmitted from H3 to

		H1 should be routed in reverse order.
29.	Transmit Traffic from H1 to H4. Transmit Traffic from H4 to H1.	Traffic Route: 1 H1 2 Link1 3 TR1 4 Link5 5 TR4 6 Link4 7 H4 Traffic is transmitted in both directions between H1 and H4. Traffic transmitted from H4 to H1 should be routed in reverse order.
30.	Migrate the ASN of TR2. The global ASN of TR2 is configured as 220. Configure the "Local AS" capability of TR2 with ASN 200. No changes are made to TR1, TR3, or TR4.	TR2 advertises AS 200 as the "Local AS" in BGP OPEN messages to TR1, TR3, and TR4.
31.	Transmit Traffic from H1 to H2. Transmit Traffic from H2 to H1.	Traffic Route: 1 H1 2 Link1 3 TR1 4 Link5 5 TR2 6 Link2 7 H2 Traffic is transmitted in both directions between H1 and H2. Traffic transmitted from H2 to H1 should be routed in reverse order.
32.	Migrate the ASN of TR3. The global ASN of TR3 is configured as 330. Configure the "Local AS" capability of TR2 with ASN 300. No changes are made to TR1, TR2, or TR4.	TR3 advertises AS 330 as the "Local AS" in BGP OPEN messages to TR1, TR2, and TR4.
33.	Transmit Traffic from H1 to H3. Transmit Traffic from H3 to H1.	Traffic Route: 1 H1 2 Link1 3 TR1 4 Link5

		5 TR3 6 Link3 7 H3 Traffic is transmitted in both directions between H1 and H3. Traffic transmitted from H3 to H1 should be routed in reverse order.
34.	Migrate the ASN of TR4. The global ASN of TR4 is configured as 440. Configure the "Local AS" capability of TR4 with ASN 400. No changes are made to TR1, TR2, or TR3.	TR4 advertises AS 440 as the "Local AS" in BGP OPEN messages to TR1, TR2, and TR3.
35.	Transmit Traffic from H1 to H4. Transmit Traffic from H4 to H1.	Traffic Route: 1 H1 2 Link1 3 TR1 4 Link5 5 TR4 6 Link4 7 H4 Traffic is transmitted in both directions between H1 and H4. Traffic transmitted from H4 to H1 should be routed in reverse order.
36.	Shutdown BGP on all routers and configure all ASN as below without the "Local AS". TR2 Local ASN: 200 TR3 Local ASN: 300 TR4 Local ASN: 400	

Possible Problems:
- None

BGP.IO.2.2: Hold Time Negotiation

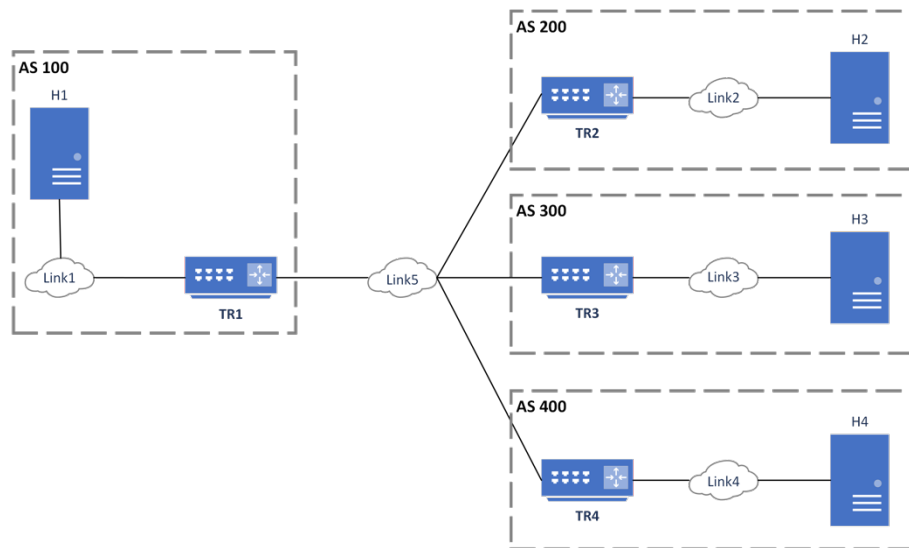**Purpose:** To verify negotiation of the Hold Time.

References:
- [BGP4]

Test Setup:

Prior to the start of each test part:
- Shutdown BGP on all routers
- Configure a full-mesh of Import and Export Policies. (e.g. TR1 Exports Link1 to all peers, and Imports all routes from all peers. TR2 Exports Link2 to all peers and Imports all routes from all peers, etc.)

Procedure:

Part A: Lower Hold Time

Step	Action	Expected Result
1.	Configure Hold Time as below: TR1: 3 Seconds TR2: 6 Seconds TR3: 9 Seconds TR4: 12 Seconds	
2.	TR1 and TR2 are configured as External Peers and BGP is enabled. Shutdown BGP on other TRs.	Observe the actual Hold Time negotiated between TR1 and TR2 is 3 Seconds.
3.	Transmit Traffic from H1 to H2.	Traffic Route: 1 H1 2 Link1 3 TR1

		4 Link5
		5 TR2
		6 Link2
		7 H2
4.	TR1 and TR3 are configured as External Peers and BGP is enabled. Shutdown BGP on other TRs.	Observe the actual Hold Time negotiated between TR1 and TR3 is 3 Seconds.
5.	Transmit Traffic from H1 to H3.	Traffic Route: 1 H1 2 Link1 3 TR1 4 Link5 5 TR3 6 Link3 7 H3
6.	TR1 and TR4 are configured as External Peers and BGP is enabled. Shutdown BGP on other TRs.	Observe the actual Hold Time negotiated between TR1 and TR4 is 3 Seconds.
7.	Transmit Traffic from H1 to H4.	Traffic Route: 1 H1 2 Link1 3 TR1 4 Link5 5 TR4 6 Link4 7 H4
8.	Unconfigure the previously configured Hold Times on all routers.	

Part B: Higher Hold Time

Step	Action	Expected Result
9.	Configure Hold Time as below: TR1: 12 Seconds TR2: 3 Seconds TR3: 6 Seconds TR4: 9 Seconds	
10.	TR1 and TR2 are configured as External Peers and BGP is enabled. Shutdown BGP on other TRs.	Observe the actual Hold Time negotiated between TR1 and TR2 is 3 Seconds.
11.	Transmit Traffic from H1 to H2.	Traffic Route: 1 H1 2 Link1 3 TR1 4 Link5

		5 TR2
		6 Link2
		7 H2
12.	TR1 and TR3 are configured as External Peers and BGP is enabled. Shutdown BGP on other TRs.	Observe the actual Hold Time negotiated between TR1 and TR3 is 6 Seconds.
13.	Transmit Traffic from H1 to H3.	Traffic Route: 1 H1 2 Link1 3 TR1 4 Link5 5 TR3 6 Link3 7 H3
14.	TR1 and TR4 are configured as External Peers and BGP is enabled. Shutdown BGP on other TRs.	Observe the actual Hold Time negotiated between TR1 and TR4 is 9 Seconds.
15.	Transmit Traffic from H1 to H4.	Traffic Route: 1 H1 2 Link1 3 TR1 4 Link5 5 TR4 6 Link4 7 H4

Possible Problems:
- None

Group 3: Extensions

BGP.IO.3.1: Multiprotocol
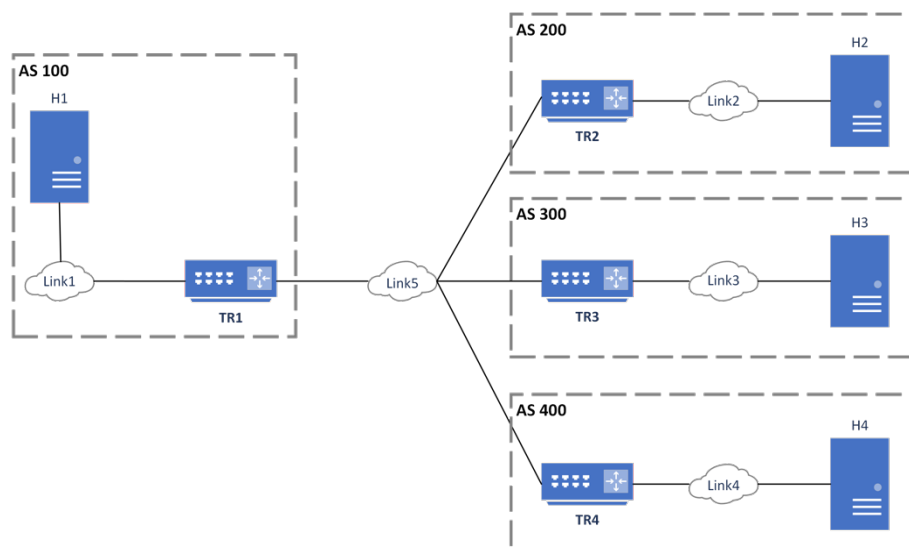**Purpose:** To verify usage of the Multiprotocol extension

References:
- [BGP4]
- [BGP MPE]
- [BGP MPE v6]
- [BGP Cap]

Test Setup:
Prior to the start of each test part:
- Shutdown BGP on all routers
- Configure a full-mesh of Import and Export Policies. (e.g. TR1 Exports Link1 to all peers, and Imports all routes from all peers. TR2 Exports Link2 to all peers and Imports all routes from all peers, etc.)

Procedure:
Part A: Sending MP_REACH_NLRI and MP_UNREACH_NLRI

Step	Action	Expected Result
1.	Configure TR1 **not** to redistribute its Link1 connected route to BGP. TR1 and TR2 are configured as External Peers and BGP is enabled. Shutdown BGP on other TRs.	TR1 transmits the Capabilities Optional Parameter in its OPEN message to announce support for Multiprotocol Extensions. The Capability Code field is 1, the Length field is 4. The AFI

		Field is 2 (IPv6) and the SAFI field is 1 (Unicast).
2.	Configure TR1 to redistribute its Link1 connected route to BGP.	TR1 sends an UPDATE message containing the MP_REACH_NLRI attribute. The attribute lists Link1 in its NLRI, together with the Next Hop to that destination. The UPDATE message includes the ORIGIN and AS_PATH attributes.
3.	Transmit Traffic from H2 to H1.	Traffic Route: 1 H2 2 Link2 3 TR2 4 Link5 5 TR1 6 Link1 7 H1
4.	Configure TR1 **not** to redistribute its Link1 connected route to BGP.	TR1 sends an UPDATE message containing the MP_UNREACH_NLRI attribute. The attribute lists the Link1 unfeasible route.
5.	Transmit Traffic from H2 to H1.	Traffic is not transmitted to H1.
6.	Shutdown BGP on TR1 and TR2.	
7.	Configure TR1 **not** to redistribute its Link1 connected route to BGP. TR1 and TR3 are configured as External Peers and BGP is enabled. Shutdown BGP on other TRs.	TR1 transmits the Capabilities Optional Parameter in its OPEN message to announce support for Multiprotocol Extensions. The Capability Code field is 1, the Length field is 4.
8.	Configure TR1 to redistribute its Link1 connected route to BGP.	TR1 sends an UPDATE message containing the MP_REACH_NLRI attribute. The attribute lists Link1 in its NLRI, together with the Next Hop to that destination. The UPDATE message includes the ORIGIN and AS_PATH attributes.
9.	Transmit Traffic from H3 to H1.	Traffic Route:

		1 H3 2 Link3 3 TR3 4 Link5 5 TR1 6 Link1 7 H1
10.	Configure TR1 **not** to redistribute its Link1 connected route to BGP.	TR1 sends an UPDATE message containing the MP_UNREACH_NLRI attribute. The attribute lists the Link1 unfeasible route.
11.	Transmit Traffic from H3 to H1.	Traffic is not transmitted to H1.
12.	Shutdown BGP on TR1 and TR3.	
13.	Configure TR1 **not** to redistribute its Link1 connected route to BGP. TR1 and TR4 are configured as External Peers and BGP is enabled. Shutdown BGP on other TRs.	TR1 transmits the Capabilities Optional Parameter in its OPEN message to announce support for Multiprotocol Extensions. The Capability Code field is 1, the Length field is 4.
14.	Configure TR1 to redistribute its Link1 connected route to BGP.	TR1 sends an UPDATE message containing the MP_REACH_NLRI attribute. The attribute lists Link1 in its NLRI, together with the Next Hop to that destination. The UPDATE message includes the ORIGIN and AS_PATH attributes.
15.	Transmit Traffic from H4 to H1.	Traffic Route: 1 H4 2 Link4 3 TR4 4 Link5 5 TR1 6 Link1 7 H1
16.	Configure TR1 **not** to redistribute its Link1 connected route to BGP.	TR1 sends an UPDATE message containing the MP_UNREACH_NLRI attribute. The attribute lists the Link1 unfeasible route.

Step	Action	Expected Result
17.	Transmit Traffic from H3 to H1.	Traffic is not transmitted to H1.
18.	Shutdown BGP on TR1 and TR4.	

Part B: Receiving MP_REACH_NLRI and MP_UNREACH_NLRI

Step	Action	Expected Result
19.	Configure TR2 **not** to redistribute its Link2 connected route to BGP. Configure TR3 **not** to redistribute its Link3 connected route to BGP. Configure TR4 **not** to redistribute its Link4 connected route to BGP.	
20.	TR1 and TR2 are configured as External Peers. TR1 and TR3 are configured as External Peers. TR1 and TR4 are configured as External Peers. BGP is enabled on all routers.	All routers transmit the Capabilities Optional Parameter in its OPEN message to announce support for Multiprotocol Extensions. The Capability Code field is 1, the Length field is 4.
21.	Configure TR2 to redistribute its Link2 connected route to BGP.	TR2 sends an UPDATE message containing the MP_REACH_NLRI attribute. The attribute lists Link2 in its NLRI, together with the Next Hop to that destination. The UPDATE message includes the ORIGIN and AS_PATH attributes. TR1 propagates TR2's advertised route to its peers.
22.	Transmit Traffic from H1 to H2.	Traffic Route: 1 H1 2 Link1 3 TR1 4 Link5 5 TR2 6 Link2 7 H2
23.	Configure TR2 **not** to redistribute its Link2 connected route to BGP.	TR2 sends an UPDATE message containing the MP_UNREACH_NLRI attribute. The attribute lists the Link2 unfeasible route. TR1

		propagates TR2's withdrawn route to its peers.
24.	Transmit Traffic from H1 to H2.	Traffic is not transmitted to H2.
25.	Configure TR3 to redistribute its Link3 connected route to BGP.	TR3 sends an UPDATE message containing the MP_REACH_NLRI attribute. The attribute lists Link3 in its NLRI, together with the Next Hop to that destination. The UPDATE message includes the ORIGIN and AS_PATH attributes. TR1 propagates TR3's advertised route to its peers.
26.	Transmit Traffic from H1 to H3.	Traffic Route: 1 H1 2 Link1 3 TR1 4 Link5 5 TR3 6 Link3 7 H3
27.	Configure TR3 **not** to redistribute its Link3 connected route to BGP.	TR3 sends an UPDATE message containing the MP_UNREACH_NLRI attribute. The attribute lists the Link3 unfeasible route. TR1 propagates TR3's withdrawn route to its peers.
28.	Transmit Traffic from H1 to H3.	Traffic is not transmitted to H3.
29.	Configure TR4 to redistribute its Link4 connected route to BGP.	TR4 sends an UPDATE message containing the MP_REACH_NLRI attribute. The attribute lists Link4 in its NLRI, together with the Next Hop to that destination. The UPDATE message includes the ORIGIN and AS_PATH attributes. TR1 propagates TR4's advertised route to its peers.

30.	Transmit Traffic from H1 to H4.	Traffic Route: 1 H1 2 Link1 3 TR1 4 Link5 5 TR4 6 Link4 7 H4
31.	Configure TR4 **not** to redistribute its Link4 connected route to BGP.	TR4 sends an UPDATE message containing the MP_UNREACH_NLRI attribute. The attribute lists the Link4 unfeasible route. TR1 propagates TR4's withdrawn route to its peers.
32.	Transmit Traffic from H1 to H4.	Traffic is not transmitted to H4.

Possible Problems:
- None

BGP.IO.3.2: AS-Wide Unique BGP ID

Purpose: To verify usage of a BGP Identifier which is based on a 4-octet, unsigned, non-zero integer that may not be unique outside of an AS.

References:
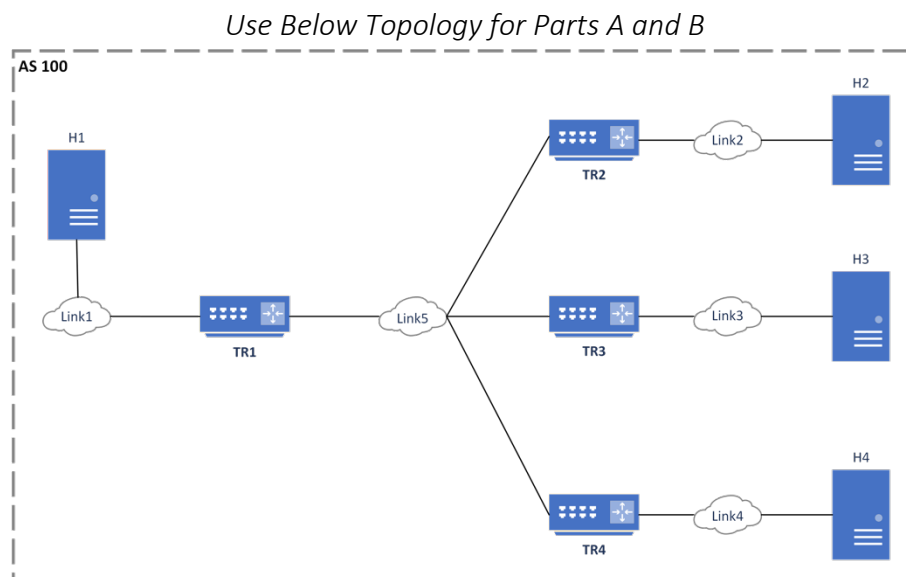- [BGP4]
- [BGP AS Uniq]

Test Setup:

Prior to the start of each test part:
- Shutdown BGP on all routers
- Configure a full-mesh of Import and Export Policies. (e.g. TR1 Exports Link1 to all peers, and Imports all routes from all peers. TR2 Exports Link2 to all peers and Imports all routes from all peers, etc.)

Procedure:

Use Below Topology for Parts A and B

Part A: Internal Peer Unique

Step	Action	Expected Result
1.	Shutdown BGP on all TRs.	
2.	Configure TR1 with a BGP ID of 10.10.10.11. TR1 should not have an IPv4 address configured on any interface.	
3.	Configure TR2 with a BGP ID of 10.10.10.12. TR2 should not have an IPv4 address configured on any interface.	
4.	Configure TR3 with a BGP ID of 10.10.10.13. TR3 should not have an IPv4 address configured on any interface.	

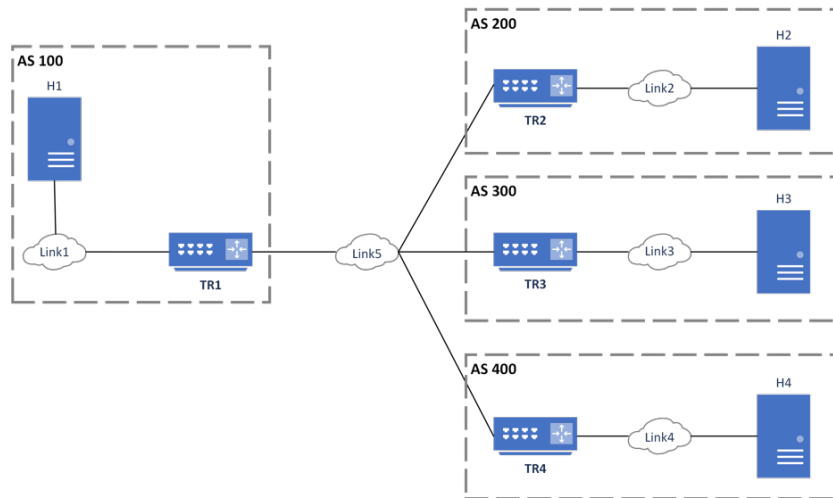|		
5.	Configure TR4 with a BGP ID of 10.10.10.14. TR4 should not have an IPv4 address configured on any interface that matches this BGP ID.	
6.	TR1 and TR2 are configured as Internal Peers. TR1 and TR3 are configured as Internal Peers. TR1 and TR4 are configured as Internal Peers.	
7.	Transmit Traffic from H1 to H2. Transmit Traffic from H2 to H1.	Traffic Route: 1 H1 2 Link1 3 TR1 4 Link5 5 TR2 6 Link2 7 H2 Traffic is transmitted in both directions between H1 and H2. Traffic transmitted from H2 to H1 should be routed in reverse order.
8.	Transmit Traffic from H1 to H3. Transmit Traffic from H3 to H1.	Traffic Route: 1 H1 2 Link1 3 TR1 4 Link5 5 TR3 6 Link3 7 H3 Traffic is transmitted in both directions between H1 and H3. Traffic transmitted from H3 to H1 should be routed in reverse order.
9.	Transmit Traffic from H1 to H4. Transmit Traffic from H4 to H1.	Traffic Route: 1 H1 2 Link1 3 TR1 4 Link5 5 TR4 6 Link4 7 H4 Traffic is transmitted in both directions between H1 and H4. Traffic transmitted from H4 to

		H1 should be routed in reverse order.

Part B: Internal Peer Non-Unique

Step	Action	Expected Result
10.	Shutdown BGP on all TRs.	
11.	Configure TR1 with a BGP ID of 10.10.10.11. TR1 should not have an IPv4 address configured on any interface.	
12.	Configure TR2 with a BGP ID of 10.10.10.11. TR2 should not have an IPv4 address configured on any interface.	
13.	TR1 and TR2 are configured as Internal Peers. Shutdown BGP on other TRs. Enable BGP on TR2 prior to enabling on TR1.	TR1 sends a NOTIFICATION message with error CODE OPEN Message Error and error Subcode set to "Bad BGP Identifier".
14.	Shutdown BGP on TR1 and TR2.	
15.	Configure TR3 with a BGP ID of 10.10.10.11. TR3 should not have an IPv4 address configured on any interface.	
16.	TR1 and TR3 are configured as Internal Peers. Shutdown BGP on other TRs. Enable BGP on TR3 prior to enabling on TR1.	TR1 sends a NOTIFICATION message with error CODE OPEN Message Error and error Subcode set to "Bad BGP Identifier".
17.	Shutdown BGP on TR1 and TR3.	
18.	Configure TR4 with a BGP ID of 10.10.10.11. TR4 should not have an IPv4 address configured on any interface.	
19.	TR1 and TR4 are configured as Internal Peers. Shutdown BGP on other TRs. Enable BGP on TR4 prior to enabling on TR1.	TR1 sends a NOTIFICATION message with error CODE OPEN Message Error and error Subcode set to "Bad BGP Identifier".

Part C: External Peer Unique

Step	Action	Expected Result
20.	Configure TR1 with a BGP ID of 10.10.10.11. TR1 should not have an IPv4 address configured on any interface.	
21.	Configure TR2 with a BGP ID of 10.10.10.12. TR2 should not have an IPv4 address configured on any interface.	
22.	Configure TR3 with a BGP ID of 10.10.10.13. TR3 should not have an IPv4 address configured on any interface.	
23.	Configure TR4 with a BGP ID of 10.10.10.14. TR4 should not have an IPv4 address configured on any interface.	
24.	TR1 and TR2 are configured as External Peers. TR1 and TR3 are configured as External Peers. TR1 and TR4 are configured as External Peers.	
25.	Transmit Traffic from H1 to H2. Transmit Traffic from H2 to H1.	Traffic Route: 1 H1 2 Link1 3 TR1 4 Link5 5 TR2 6 Link2 7 H2 Traffic is transmitted in both directions between H1 and H2. Traffic transmitted from H2 to

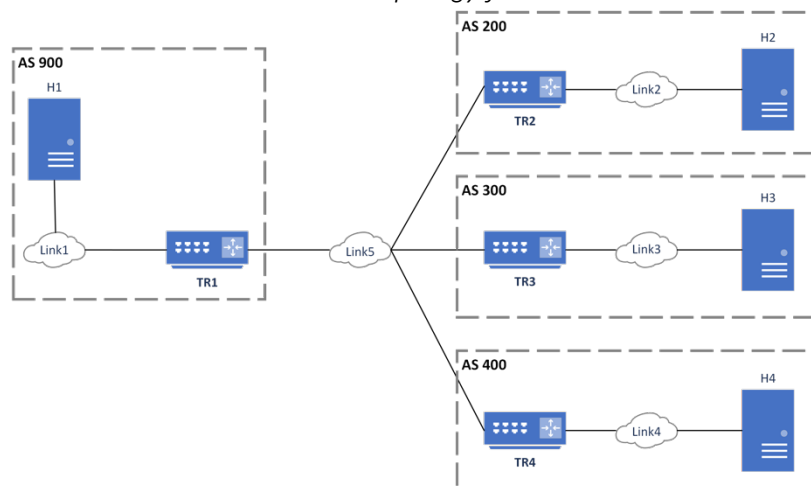| Step	Action	Expected Result
		H1 should be routed in reverse order.
26.	Transmit Traffic from H1 to H3. Transmit Traffic from H3 to H1.	Traffic Route: 1 H1 2 Link1 3 TR1 4 Link5 5 TR3 6 Link3 7 H3 Traffic is transmitted in both directions between H1 and H3. Traffic transmitted from H3 to H1 should be routed in reverse order.
27.	Transmit Traffic from H1 to H4. Transmit Traffic from H4 to H1.	Traffic Route: 1 H1 2 Link1 3 TR1 4 Link5 5 TR4 6 Link4 7 H4 Traffic is transmitted in both directions between H1 and H4. Traffic transmitted from H4 to H1 should be routed in reverse order.

Part D: External Peer Non-Unique – Peer Larger ASN

Step	Action	Expected Result
28.	Configure TR1 with a BGP ID of 10.10.10.11. TR1 should not have an IPv4 address configured on any interface that matches this BGP ID.	
29.	Configure TR2 with a BGP ID of 10.10.10.11. TR2 should not have an IPv4 address configured on any interface that matches this BGP ID.	
30.	TR1 and TR2 are configured as External Peers. Shutdown BGP on other TRs. Enable BGP on TR2 prior to enabling on TR1.	The connection initiated by TR2 should be Preserved.
31.	Shutdown BGP on TR1 and TR2.	

	Configure TR3 with a BGP ID of 10.10.10.11. TR3 should not have an IPv4 address configured on any interface that matches this BGP ID.	
32.		
33.	TR1 and TR3 are configured as External Peers. Shutdown BGP on other TRs. Enable BGP on TR3 prior to enabling on TR1.	The connection initiated by TR3 should be Preserved.
34.	Shutdown BGP on TR1 and TR3.	
35.	Configure TR4 with a BGP ID of 10.10.10.11. TR4 should not have an IPv4 address configured on any interface that matches this BGP ID.	
36. Show c	TR1 and TR4 are configured as External Peers. Shutdown BGP on other TRs. Enable BGP on TR4 prior to enabling on TR1.	The connection initiated by TR4 should be Preserved.

Part E: External Peer Non-Unique – DUT Larger ASN

Use Below Topology for Part E

Step	Action	Expected Result
37.	Configure TR1 with a BGP ID of 10.10.10.11. TR1 should not have an IPv4 address configured on any interface that matches this BGP ID. TR1 is configured with ASN 900.	
38.	Configure TR2 with a BGP ID of 10.10.10.11. TR2 should not have an IPv4 address configured on any interface that matches this BGP ID.	
39.	TR1 and TR2 are configured as External Peers. Shutdown BGP on other TRs.	The connection initiated by TR1 should be Preserved.

	Enable BGP on TR2 prior to enabling on TR1.	
40.	Shutdown BGP on TR1 and TR2.	
41.	Configure TR3 with a BGP ID of 10.10.10.11. TR3 should not have an IPv4 address configured on any interface that matches this BGP ID.	
42.	TR1 and TR3 are configured as External Peers. Shutdown BGP on other TRs. Enable BGP on TR3 prior to enabling on TR1.	The connection initiated by TR1 should be Preserved.
43.	Shutdown BGP on TR1 and TR3.	
44.	Configure TR4 with a BGP ID of 10.10.10.11. TR4 should not have an IPv4 address configured on any interface that matches this BGP ID.	
45.	TR1 and TR4 are configured as External Peers. Shutdown BGP on other TRs. Enable BGP on TR4 prior to enabling on TR1.	The connection initiated by TR1 should be Preserved.

Possible Problems:
- None

BGP.IO.3.3: 4-Octet AS

Purpose: To verify the usage of 4-Octet ASN.
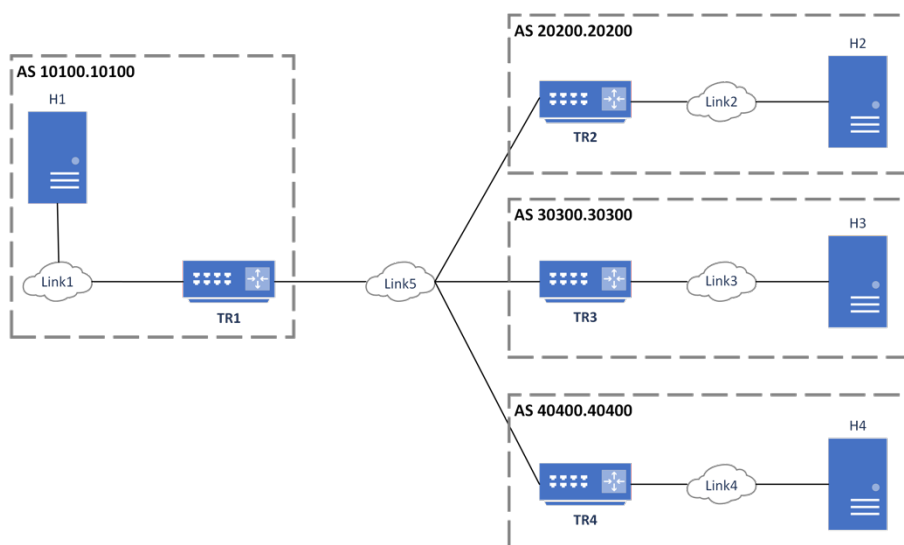
References:
- [BGP4]
- [BGP 4AS]

Test Setup:

Prior to the start of each test part:
- Shutdown BGP on all routers
- Configure a full-mesh of Import and Export Policies. (e.g. TR1 Exports Link1 to all peers, and Imports all routes from all peers. TR2 Exports Link2 to all peers and Imports all routes from all peers, etc.)
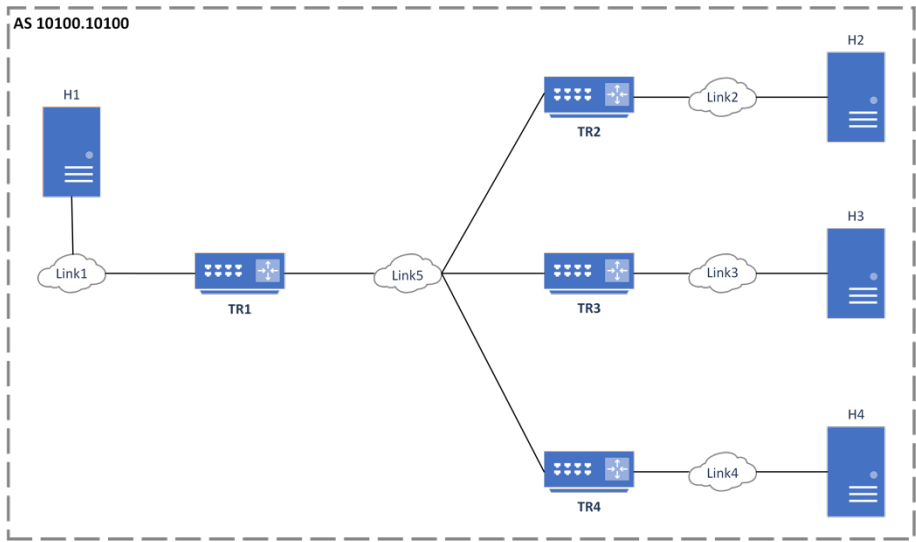
Procedure:

Part A: External Peer 4-Octet AS Capability

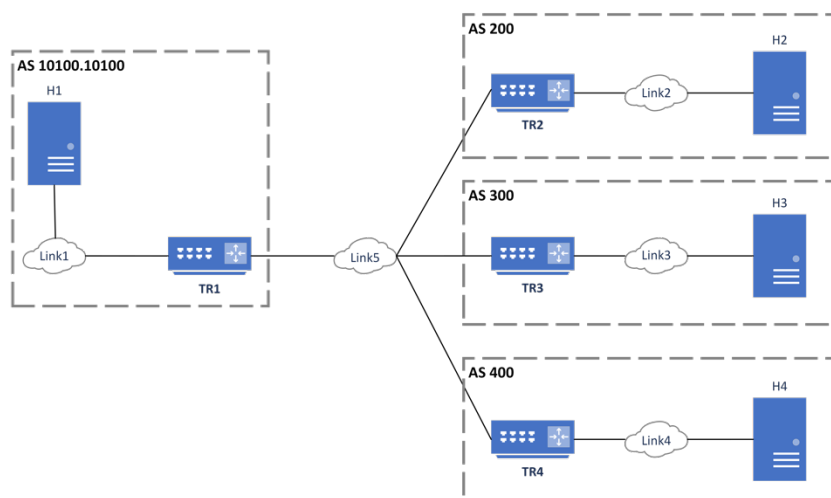| Step	Action	Expected Result
1.	All TRs are configured to support 4-Octet AS and are configured with the specified 4-Octet AS.	
2.	TR1 and TR2 are configured as External Peers and BGP is enabled. TR1 and TR3 are configured as External Peers and BGP is enabled. TR1 and TR4 are configured as External Peers and BGP is enabled.	TR1 advertises to each peer (TR2, TR3, TR4) that it supports four-octet AS number Extensions. The capability code is 65 ("support for four-octet AS number capability").

		The Capability Length field is 4. The AS number of TR1 is carried in the Capability Value field.

Part B: Internal Peer 4-Octet AS Capability

Step	Action	Expected Result
3.	All TRs are configured to support 4-Octet AS and are configured with the specified 4-Octet AS.	
4.	TR1 and TR2 are configured as Internal Peers and BGP is enabled. TR1 and TR3 are configured as Internal Peers and BGP is enabled. TR1 and TR4 are configured as Internal Peers and BGP is enabled.	TR1 advertises to each peer (TR2, TR3, TR4) that it supports four-octet AS number Extensions. The capability code is 65 ("support for four-octet AS number capability"). The Capability Length field is 4. The AS number is carried in the Capability Value field.

Part C: External Peers 2-octet AS

Step	Action	Expected Result
5.	TR1 is configured to support 4-Octet AS and is configured with the specified AS. TR2, TR3, and TR4 are configured with the specified 2-octet AS.	
6.	TR1 and TR2 are configured as External Peers and BGP is enabled. TR1 and TR3 are configured as External Peers and BGP is enabled. TR1 and TR4 are configured as External Peers and BGP is enabled.	
7.	Transmit Traffic from H1 to H2. Transmit Traffic from H2 to H1.	Traffic Route: 1 H1 2 Link1 3 TR1 4 Link5 5 TR2 6 Link2 7 H2 Traffic is transmitted in both directions between H1 and H2. Traffic transmitted from H2 to H1 should be routed in reverse order.
8.	Transmit Traffic from H1 to H3. Transmit Traffic from H3 to H1.	Traffic Route: 1 H1 2 Link1 3 TR1

		4 Link5
		5 TR3
		6 Link3
		7 H3
		Traffic is transmitted in both directions between H1 and H3. Traffic transmitted from H3 to H1 should be routed in reverse order.
9.	Transmit Traffic from H1 to H4. Transmit Traffic from H4 to H1.	Traffic Route: 1 H1 2 Link1 3 TR1 4 Link5 5 TR4 6 Link4 7 H4 Traffic is transmitted in both directions between H1 and H4. Traffic transmitted from H4 to H1 should be routed in reverse order.

Possible Problems:
- None

Modification Record

Version	Date	Editor	Modification
3.1	January 2023	Hannah Dukeman	• Removed 3.4
3.0	November 2021	Timothy Carlin	• Incorporated new RFCs • Updates to procedure format • Updates to Network Topology
2.3	July 23, 2014		• Added Network labels
2.2	February 24, 2014		• Changed incorrect step 26 in test 1.1D from TN4 to TN2. • Changed typo in step 82 on test 1.2F from TR1 to TR3. • Changed observable results in test 1.3E • Specified re-enabling peers on tests 1.1B, 1.2B, and 1.3B • Specified to disable prepending on tests 1.1E, 1.2E, 1.3D, and 1.3E.Added updated IOL logo
2.1	June 22, 2010		• Added a third interoperability partner to test case 1.1 and 1.2. • Traceroutes only needed to test transit and non-transit. Removed extraneous traceroutes. • Added test cases to 1.2 for non-transit test cases. • Changed focus of 1.3 to External and Internal BGP Peers. • Changed focus of 1.4 to Internal BGP Peers.
2.0	March 2, 2006		• Re-worded test procedures. • Re-numbered test 2.1 and test 2.2 to test 1.3 and test 1.4 respectively • Changed the RUT to be in AS 1 in test 1.2 and test 1.4
1.1	June 17, 2005		• Re-worded test procedures. • Re-ordered observable results. • Changed TR3 to be TR2 in step 6 of test 2.2
1.0	March 14, 2005		• Removed TR5 from Test 2.1, and 2.2

			• Added updated pictures to the Test Suite. • Changed the names of the Test Routers and Test Nodes in all tests.
0.2	June 10, 2004		• Tests 2.1 and 2.2, added configuration on the RUT to include setting next-hop to self for internal peers.
0.1	August 7, 2003		• Initial Version