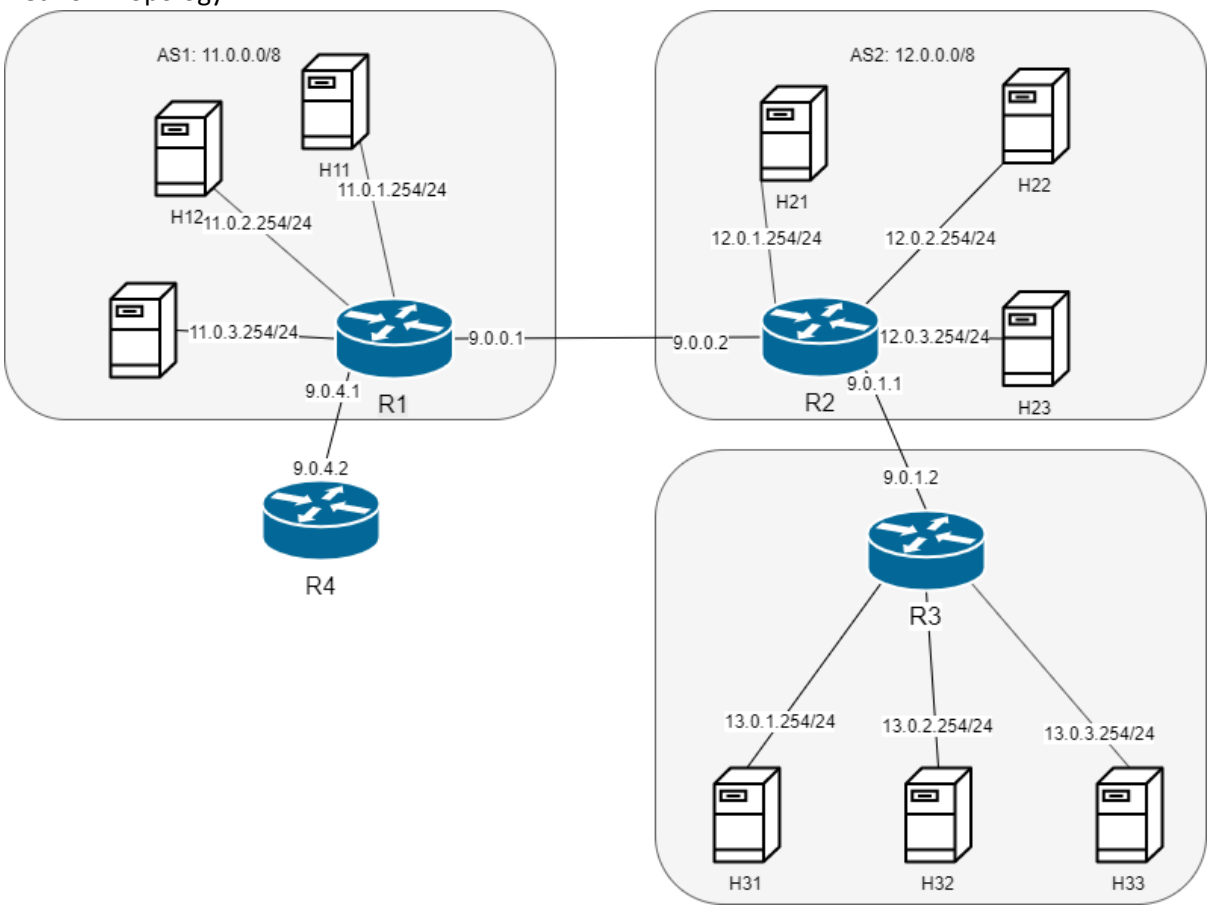
Lee Gui An (1002651)
50.012 Networks
Lab 5: BGP/SDN

Part 1: Getting Started

Network Topology:



AS1: R1				
SRC INTERFACE	DEST INTERFACE	IP	AS	MASK
R1	H11	11.0.1.254/24	1	11.0.0.0/8
R1	H12	11.0.2.254/24		
R1	H13	11.0.3.254/24		
R1	R2	9.0.0.1	-	-
R1	R4	9.0.4.1	-	-
AS2: R2				
SRC INTERFACE	DEST INTERFACE	IP	AS	MASK
R2	H21	12.0.1.254/24	2	12.0.0.0/8
R2	H22	12.0.2.254/24		
R2	H23	12.0.3.254/24		
R2	R1	9.0.0.2	-	-
R2	R3	9.0.1.1	-	-
AS3: R3				
SRC INTERFACE	DEST INTERFACE	IP	AS	MASK
R3	H31	13.0.1.254/24	3	13.0.0.0/8
R3	H32	13.0.2.254/24		
R3	H33	13.0.3.254/24		
R3	R2	9.0.1.2	-	-

Lee Gui An (1002651)
50.012 Networks
Lab 5: BGP/SDN

AS4: R4				
SRC INTERFACE	DEST INTERFACE	IP	AS	MASK
R4	R1	9.0.4.2	-	-

Part 2: BGP Re-establishment

When we initially reset the BGP tables, there is a NOTIFICATION message to all other routers that the routing table has been reset. Then, BGP re-establishment starts with an OPEN message from the router to another router, followed by an OPEN message reply from the other. These OPEN messages contain information about which AS the router belongs to, and what capabilities this router has for routing purposes. This is then followed by UPDATE messages to and from each router which outline the routing paths that are in each router. AS2 has 2 UPDATE messages, carrying the advertising for its own AS, and AS3.

Part 3: Reaching 13.0.1.1 from AS1

Initially, it was impossible to reach 13.0.1.1 (aka h31) from AS1. This was because the routing information was not being propagated through AS2 to reach AS1 – this was fixed by increasing the value of ebgp-nexthop at both AS3 and AS2 such that the advertised address space would have a TTL high enough to reach AS1. (in this case, 3).

Part 4: Attack on BGP

What happened was that when we started advertising our rogue network AS4's BGP in the same address space as AS3, the BGP protocol called for an update to the routing table in R1, since it had a better (shorter) address to the advertised address space (13.0.0.0/24). This caused R1 to re-route all requests to AS4 instead of AS3, causing it to connect to our attacker's network.