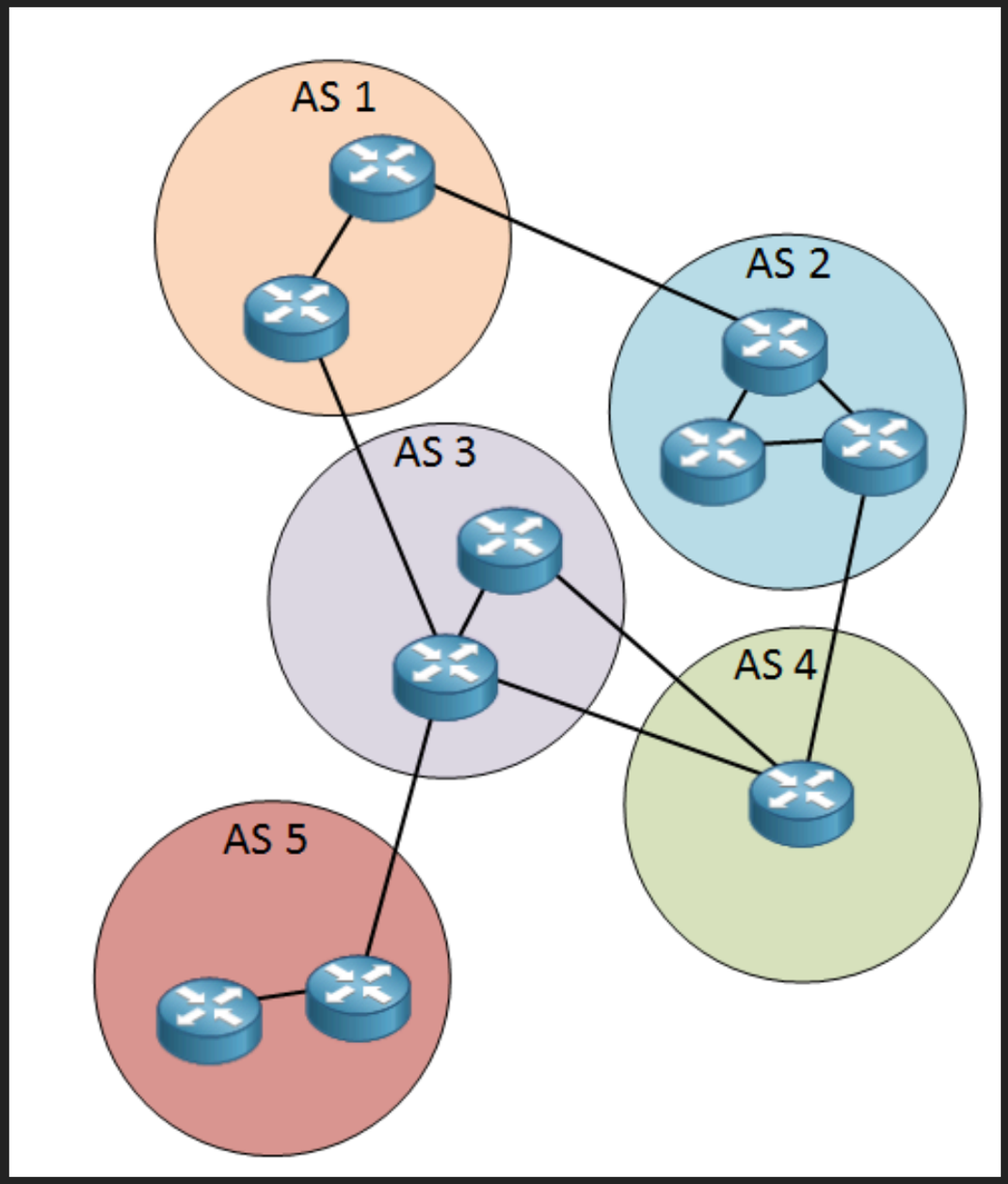
# BGP HIJACKING WITH LOKI

MIKE HAM

# BGP REFRESHER

- BGP makes the internet work
- Traffic between two ISPs will traverse the BGP protocol
- Path Vector routing
- Some security mechanisms built in, by and large still an attackable surface
- Many high-profile cases of BGP attacks show relevance



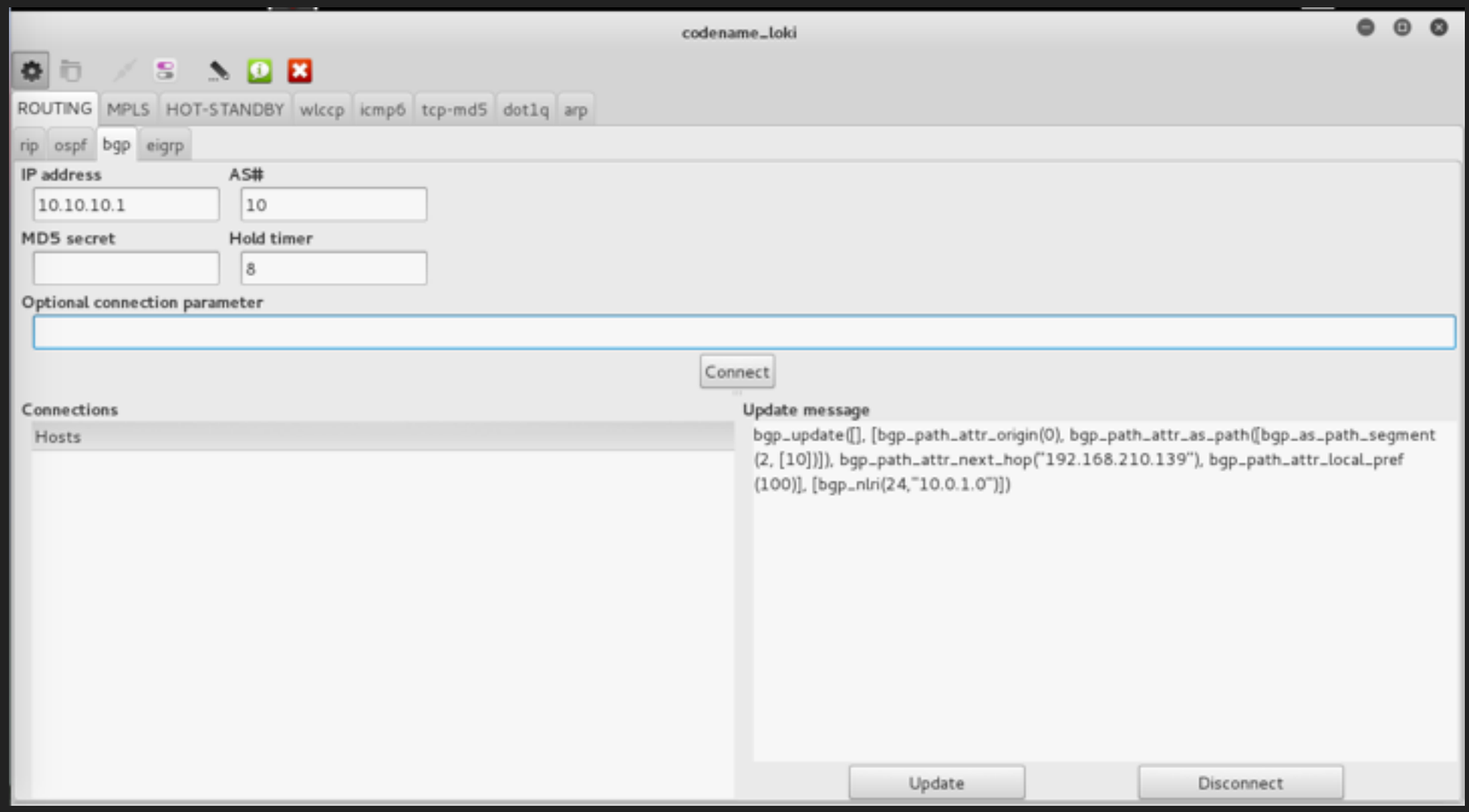
# SUB PREFIX HIJACKING

- AS advertises a shorter prefix to a network than the true owner of the subnet
- Flaw/feature in BGP dictates that a more specific prefix should be trusted over the larger prefixes
- ASN1000 legitimately owns 138.247.80.0/24
- ASN1337 lies and says they own 138.247.80.0/25 which is a smaller portion of the 138.247.80.0/24 block
- Traffic for 138.247.80.1-127 gets routed to ASN1337

# BGP HIJACKING WITH LOKI

# LOKI

- Python based tool
- Built in support for many different layer 3 attacks



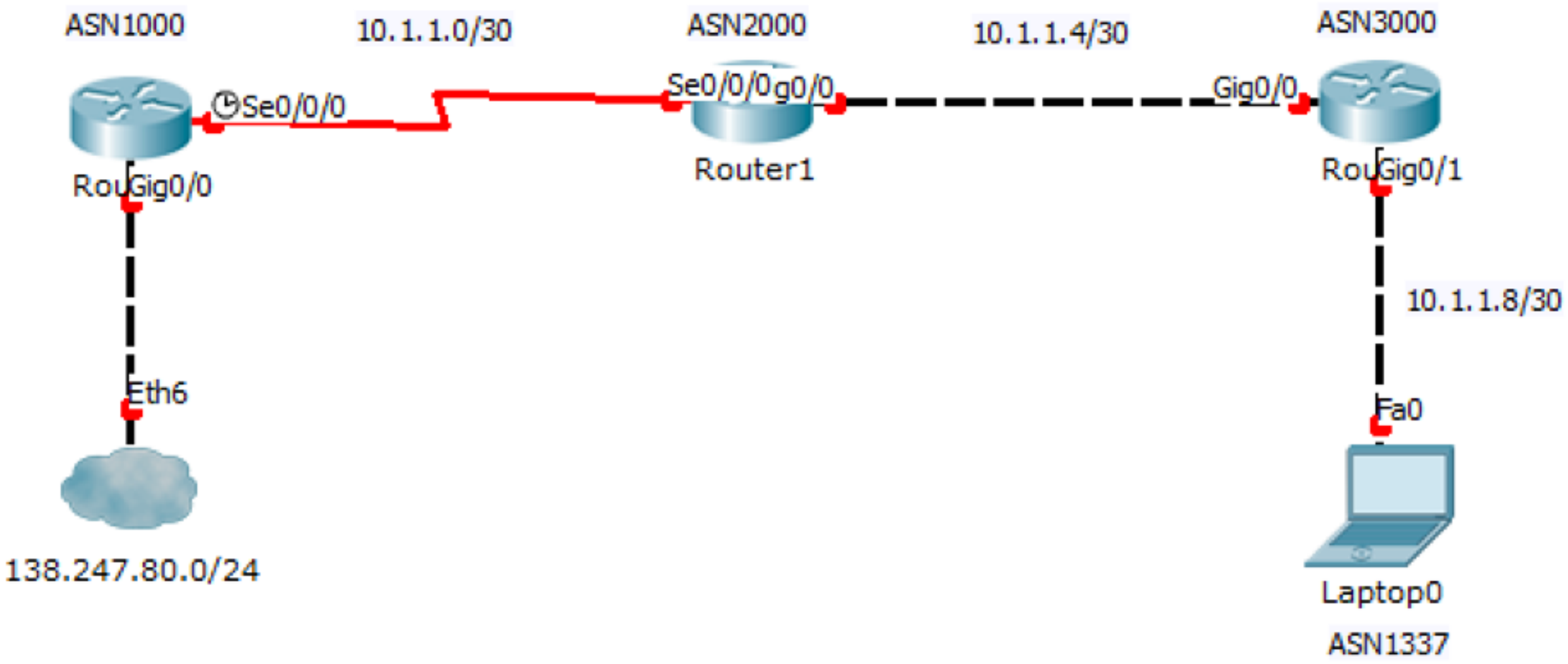
# INSTALLATION

- Does not come installed on Kali, need to download some packages on your own then you can get it to go
  - loki_0.2.7-1_amd64.deb
  - pylibpcap_0.6.2-1_amd64.deb
  - python-dpkt_1.6+svn54-1_all.deb
  - libssl0.9.8_0.9.8o-7_amd64.deb
  - python-dumbnet_1.12-3.1_amd64.deb
  - python-central_0.6.17ubuntu2_all.deb

# DEFENSES

- BGP Neighbor Authentication with MD5
- BGP Time To Live Security Check
- Configuring Maximum Prefixes
- Filtering BGP Prefixes with Prefix Lists
- Filtering BGP Prefixes with Autonomous System Path Access Lists
- AS Path Length Limiting
- Infrastructure ACLs
- Control Plane Policing

# NETWORK DIAGRAM



# DEMO.