**Objective:** Improving BGP plane resilience by protocol configuration and extension.

**BGP and Rationales**
- **Border Gateway Protocol (BGP)**
  - De facto standard of inter-domain routing
  - Controlling the distribution of global routes
  - The largest man-made distributed system
    - 10,000 Autonomous Systems and 100,000 BGP routers
- **BGP infrastructure** has to be improved in **evolutionary, scalable** and **deployable** ways.

**BGP Session Reliability**
- **Two failure causes**
  1. Service-stop
     - BGP router nonresponse
     - IGP routing disruption
  2. Severe network congestion
     - Traffic engineering failures (TCP saturation)
     - Warm attacks (UDP saturation)

**Service-stop**
- Impact of the time interval of the service stop on BGP session failure probability

**Severe network congestion**
- Impact of the packet drop probability on BGP session lifetime

**IBGP Network Resilience**

**Resilience analysis**
- Cause-based reliability analysis
  - Based on IBGP overlay network model.
  - Consider typical failure scenarios in IP networks
- Two metrics for IBGP resilience:
  - IBGP failure probability
  - Probability of IBGP session failures.
- Expected connectivity loss
  - Average number of IBGP router pairs which have no valid IBGP signaling path.

**IBGP RR Network Configuration**
- IBGP route reflection network configuration
  - How to cluster IBGP routers?
  - How many redundant reflectors needed?
  - How to place reflectors?
- Using redundant elements does not necessarily increase IBGP resilience.

**Optimizing IBGP RR Networks**
- Appropriate route reflection design makes IBGP more robust.
  - Minimizing expected connectivity loss
  - Minimizing IBGP failure probability
- In general, the optimization problem is NP hard. In some special settings, there are efficient solutions.

**Conclusion:** BGP resilience can be improved in a deployable way by configuring Internal BGP networks and TCP appropriately.