Information Model for DDoS Open Threat Signaling (DOTS)

draft-reddy-dots-info-model-00

July 2015

IETF 93

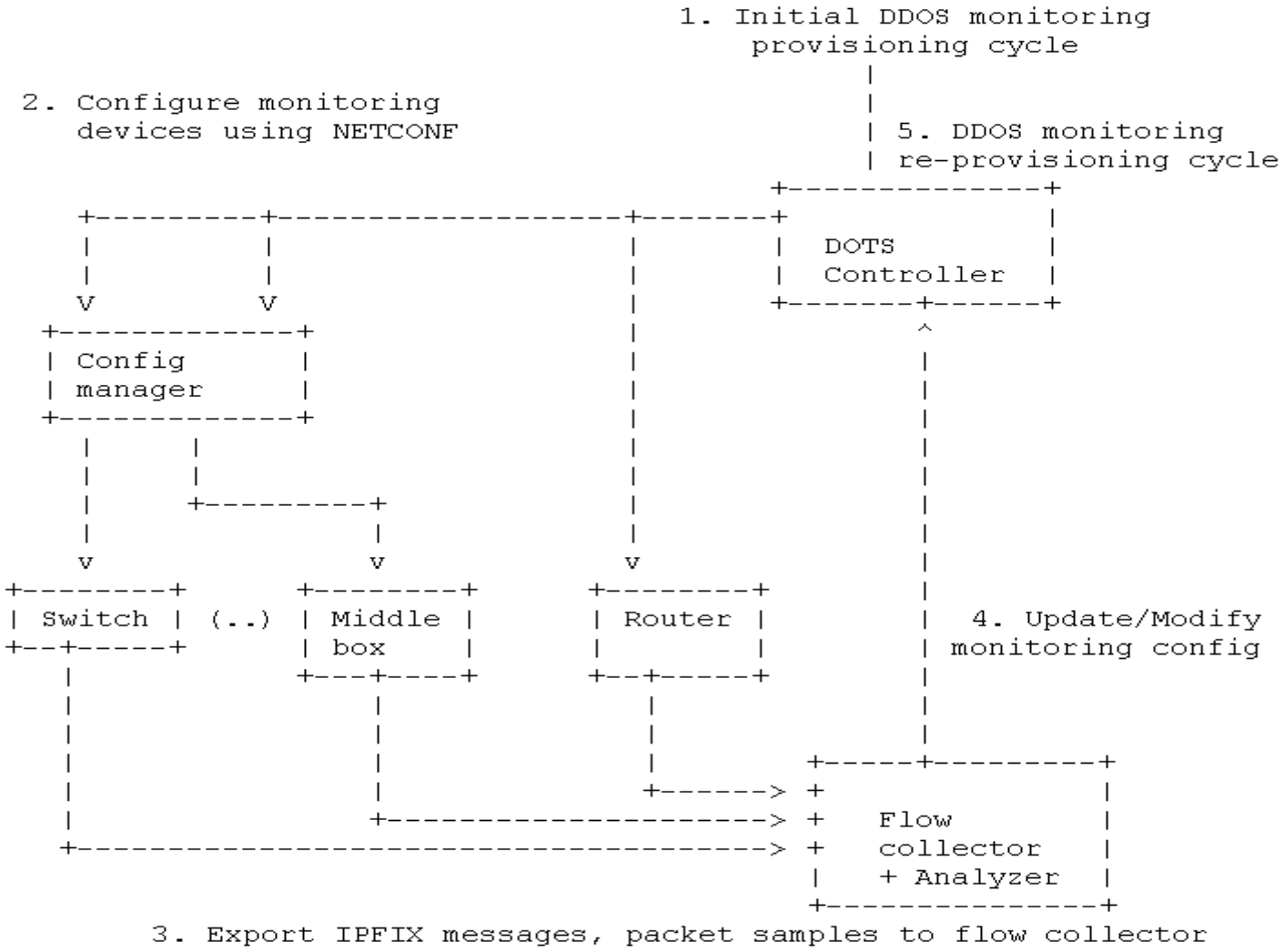
Authors: T. Reddy, P. Patil, M. Geller, D. Wing, S. Rao and M. Boucadair

Presenter : Tirumaleswar Reddy

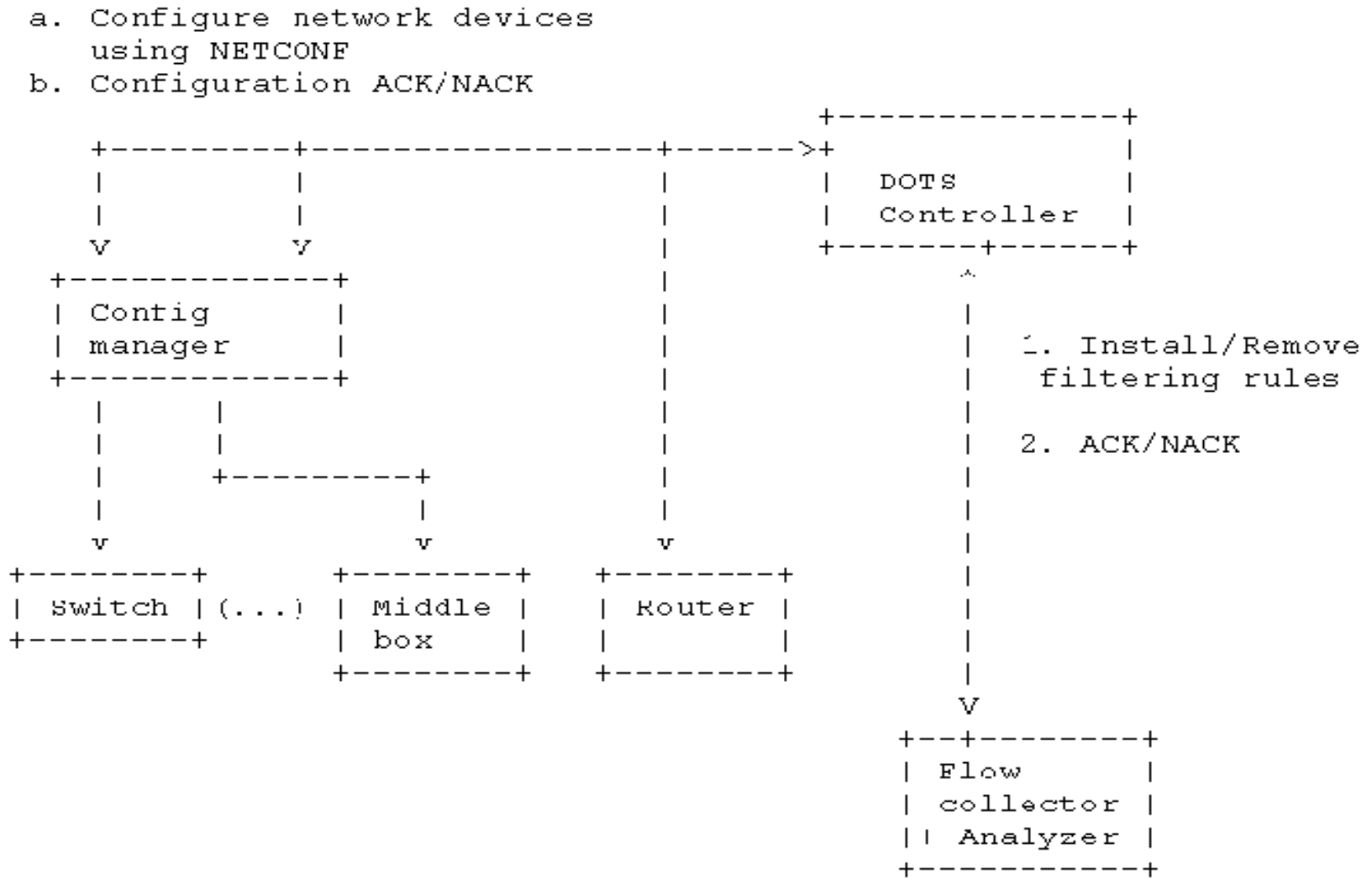
Overview

- Discusses the need and the mechanisms to dynamically update configuration of network monitoring devices to help identify DDOS attacks.
- Programming network devices to take appropriate action on the suspect traffic.

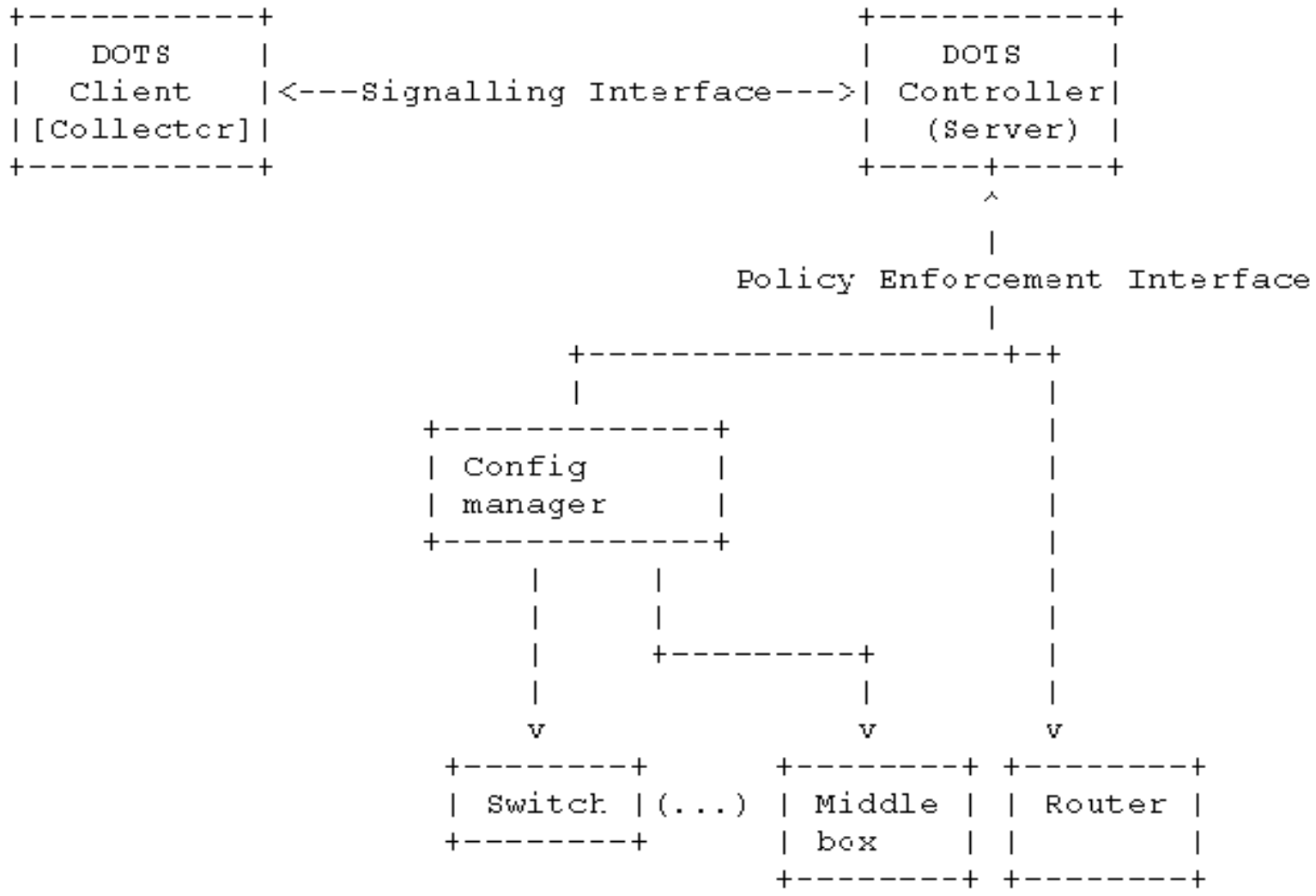
Configuration Cycle for IPFIX



Configuration Cycle for Attack Mitigation



Signaling Interface & Policy Enforcement Interface



Questions ?