CCIE Security Version 5
Advanced Technologies Class

UDP Attacks

What is the UDP attack?

What IOS tools can be used to mitigate it?

UDP Attacks Overview

- UDP is connectionless by design
  - There is no need to establish a handshake before the session is created
  - Because of its nature, it's a powerful and simple attack vector

UDP Attacks Overview

- UDP Flood is the most common attack
  - Attacker sends huge amount of UDP traffic to closed services (UDP ports)
  - The victim has to generate a huge amount of ICMP Port Unreachable messages
  - The victim's resources are exhausted and it's no longer reachable by legit clients

UDP Attack Mitigation

- IOS Mitigation Tools
  - ACL Filtering
  - Rate-limit (CAR – Committed Access Rate)
  - Policing (successor of CAR)
  - Unconditional packet discard via MQC (ACL/NBAR)
  - uRPF
  - Zone-Based Policy Firewall

UDP Attack Mitigation

- Policing Mitigation Implementation Steps
  - Classify the traffic (class-map)
  - Configure the policer (policy-map)
  - Apply the policer at the interface-level (service-policy)
  - Verify its functionality