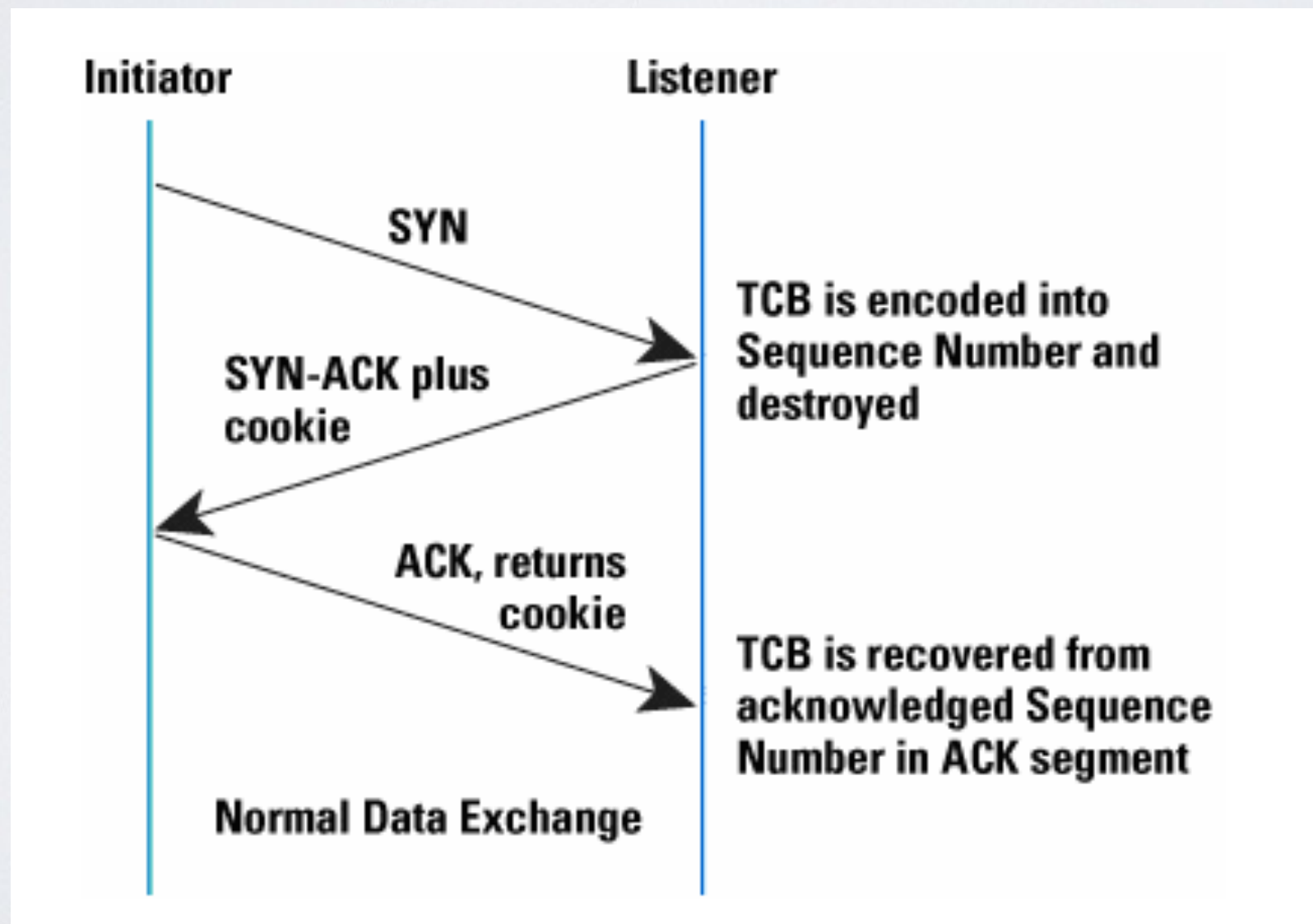


# Preventing TCP-syn flooding

**TCP-syn cookie** prevents from maintaining a queue of half-opened TCP connections



# Preventing Transport Layer DOS and DDOS attacks in general

## **Network Ingress Filtering** (a.k.a BCP 38)

*Best Current Practice* to limit the impact of DOS and DDOS

1. Deny packets with spoofed addresses from leaving the router
  2. Ensure that traffic is traceable to its correct source network
- ➡ Implemented by ISPs (Internet Service Providers)