IPv6 Security Considerations Per Device Type

**Host**
- IPSec (if needed)
- RH0 [RFC5095]
- Overlapping Frags [RFC5722]
- Atomic Fragments [RFC6946]
- NDP Fragmentation [RFC6980]
- Header chain [RFC7112]
- Stable IIDs [RFC8064][RFC7217][RFC7136]

**Switch**
- IPv6 ACLs
- RA-Guard [RFC6105]
- DHCPv6 guard
- IPv6 snooping
- IPv6 source/prefix guard
- IPv6 destination guard
- MLD snooping [RFC4541]
- DHCPv6-Shield [RFC7610]

**Router**
- Ingress Filtering and RPF
- DHCPv6 Relay [RFC8213]
- OSPFv3 Auth. [RFC4552]
- or / and [RFC7166]
- IS-IS [RFC5310]
- or, less preferred, [RFC5304]
- MBGP
- TCP-AO [RFC5925]
- Obsoleted MD5 Signature Option [RFC2385]

**Security Equipment**
- Header chain [RFC7112]
- Support EHs Inspection
- Encapsulated Traffic Inspection

**CPE**
- Router
- Security Equipment
- DHCPv6 Server Privacy Issues

**Disable if not used:** LLMNR, mDNS, DNS-SD, IPv6 DNS Autodiscovery, transition mechanisms
IPv6 Security Considerations On Your Network

Control Plane Security

- BGP
- IGP
- NDP
- MLD
- NDP
- DHCPv6
- MLD

IPv6 Internet

P2P links

Router

Forwarding Plane Security

- Firewall
- Switch
- FHS

* All Name resolution related protocols

Version: 20190206