IPv6 Address Autoconfiguration
IPv6 Authentication and Privacy
IPv6 Neighbor Discovery
IPv6 Routing

Allison Mankin
ISI

mankin@isi.edu

IPv6 Address Autoconfiguration

- the problem
  - system bootstrap (‘plug and play’)
  - address renumbering
- goals
  - deal with a range of environments
    - ‘dentist office’ to large enterprise
  - deal with range of administrative desires
    - rigid control to trusting

Autoconfiguration Types

- stateless
  - no specific record of address to node mapping saved
  - if deterministic process used there is no need
  - requires a unique-to-the-subnet ‘cookie’
  - topologically significant prefix combined with cookie
- statefull
  - record kept of address mapping
  - requires at least a unique-to-the-subnet ‘cookie’
  - does not require that cookie be part of address

IPv6 Address Autoconfiguration Types

- stateless address autoconfiguration

  prefix identifying subnet concatenated with IEEE 48 bit address from LAN controller

- Dynamic Host Configuration Protocol for IPv6

  DHCPng

  can use address from stateless autoconfiguration or create its own

  can provide additional network specific information

  can have administrative controls on address generation

  e.g., don't generate addresses for unregistered nodes

  can register node in DNS

Stateless Autoconfiguration Process

- router sends periodic advertisement
  - host can also send a Router Solicitation to speed up process
- advertisement may include prefix information
  - one or more address prefixes with length to identify subnet
  - bit to indicate if host may use prefix information to create its own address(es)
- if bit is on the host may concatenate IEEE address and prefix(s) to form address(es)
- if bit is off the host must use DHCPng to get addresses

Address Renumbering

- want to be able to migrate net to new addresses
  - when change provider
  - when change network architecture
- IPv6 supports multiple addresses per interface
- two procedures
  - 1/ have router add a new prefix to advertisement and advertise that old prefix is no longer valid
  - 2/ when DHCPng address lease runs out return a new address for node to use
- requires DNS update
- existing conversations can continue
  - no new ones with old address

IPv6 Security

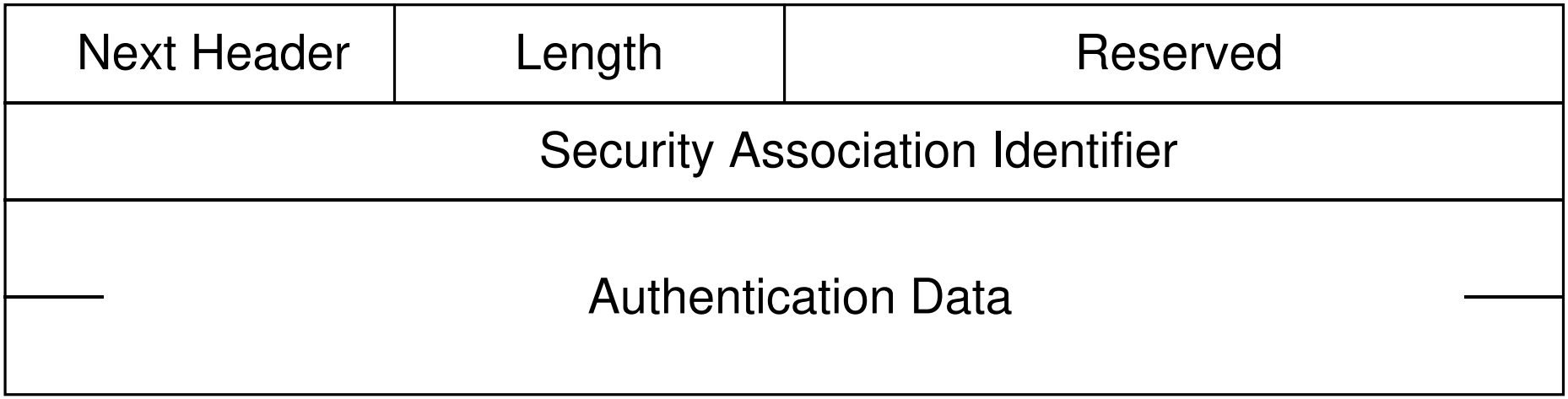
- there is a recognition that the Internet needs strong security
- the goal is to provide strong protection as a matter of course throughout the Internet

Authentication and Privacy

- IPv6 requires support for authentication and privacy
  - not required to use them
  - support in implementation required by standard
- key management needed but outside of IPv6 scope
- security association formed between two hosts, applications, or users
  - normally one in each direction
- security association identified with a 32 bit SAID
  - used in combination with destination address to uniquely identify security association

IPv6 Authentication Header

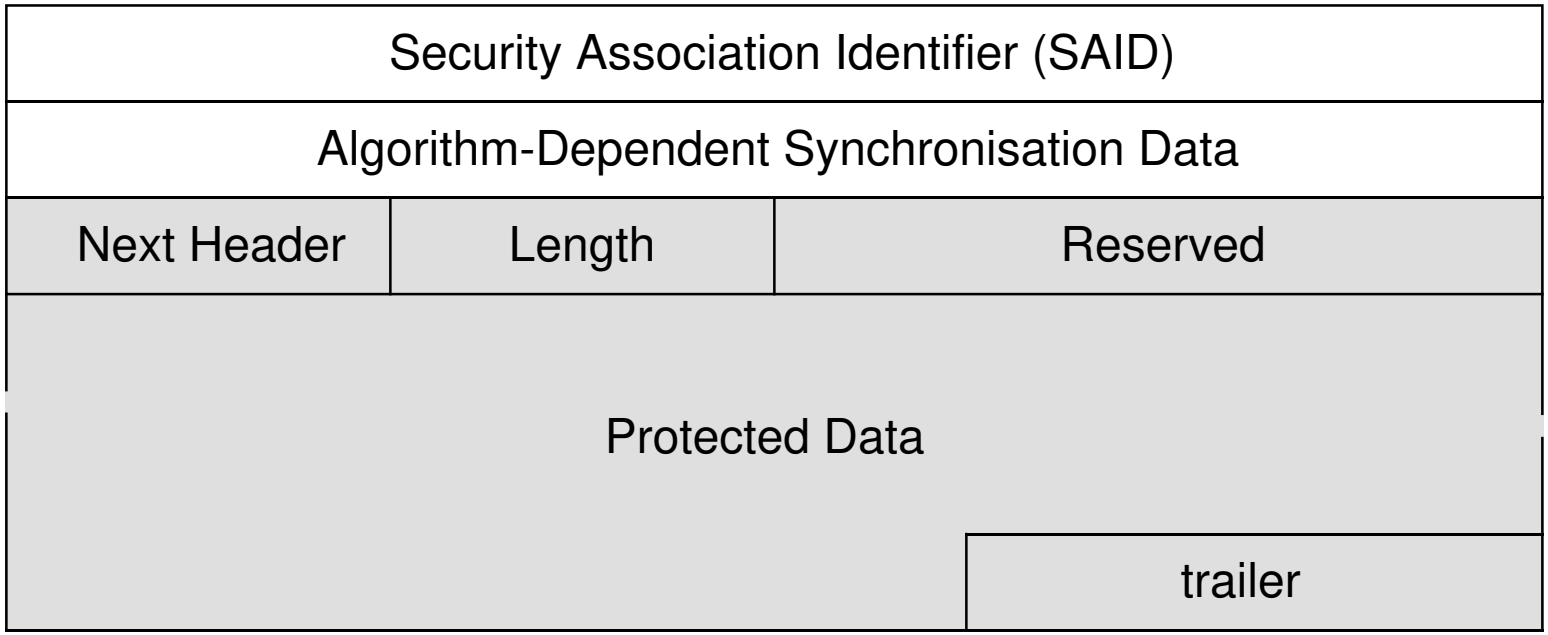
- contains encrypted digest of packet contents
  - all of packet including header, other than fields that change during packet forwarding
- support for keyed MD5 required
  - other digests optional
- can limit spoofing type attacks



IPv6 Security Protocol

- provides for confidentiality via encryption
- some legal issues
- can encrypt part or all of a datagram
- must be last unencrypted field in datagram
- can support encrypted tunnels through IPv6 Internet

IPv6 Security Protocol Format



Neighbor Discovery

- three functions
  - find a router
  - find destination node
  - set subnet-wide parameters
- routers
  - periodically send ‘I-am-here’ advertisments
  - indicates router’s address, may include other information
- nodes
  - send ‘where-are-you’ solicitation for router or other node
  - target returns a ‘general advertisment’ with MAC information

Neighbor Discovery Overview

- node hears about router from periodic advertisement
  - also can send solicitation to reduce start-up latency
- if router advertisement(s) do not include prefixes
  - node sends all packets to routers, may get redirect back
- if router advertisement(s) do include prefixes
  - node can figure out if destination is on same subnet and send solicitation directly to destination node if yes
- if no router advertisements heard
  - node assumes all destinations are on local subnet

Router I-Am-Here Advertisment

- contain:
  - router's IPv6 address
  - information lifetime
- may contain
  - hop limit
  - MTU value
  - indication of mobility support
  - address prefix(es)
  - notice of address prefix change(s)

Routing

- hierarchical addresses used in IPv6
- 1st version ‘provider based’ hierarchy
- working on geographic or interconnect-point based
- address assignment a concern from the start
- easy renumbering may be important in maintaining efficient use of routing table space

Routing Paradigm

- longest-match routing will be used
- also source routing
- existing routing protocols will be modified for IPv6
  - RIPv2
  - OSPF
  - IS-IS
  - IDRP