Session 8: Panel- Experience with Firewalls and IPsec

Moderator:	Stephen Kent - BBN Technologies
Panelists:	Naganand Doraswamy- Bay Networks
	Cheryl Madson - Cisco Systems
	Dan McDonald - Sun Microsystems

Why Internet Layer Security?

- Security is independent of network technology, i.e., protection across different WANs and LANs
- Endpoint selection flexibility, i.e., individual host or whole LAN/CAN environment
- Security Services
  - confidentiality (limited traffic flow confidentiality)
  - data origin authentication
  - peer entity authentication
  - partial sequence integrity (anti-replay)
  - access control (via key management)
- Well suited to centralized device management and to automated key management

IPsec Applications

- Secure communication via the public Internet
  - intranets
  - extranets
  - mobile users
- Alternatives
  - real (not virtual) private networks
  - 800 dialup access (for mobile users)
  - authentication-only firewall traversal
  - Mad magazine approach (“What, me worry?)

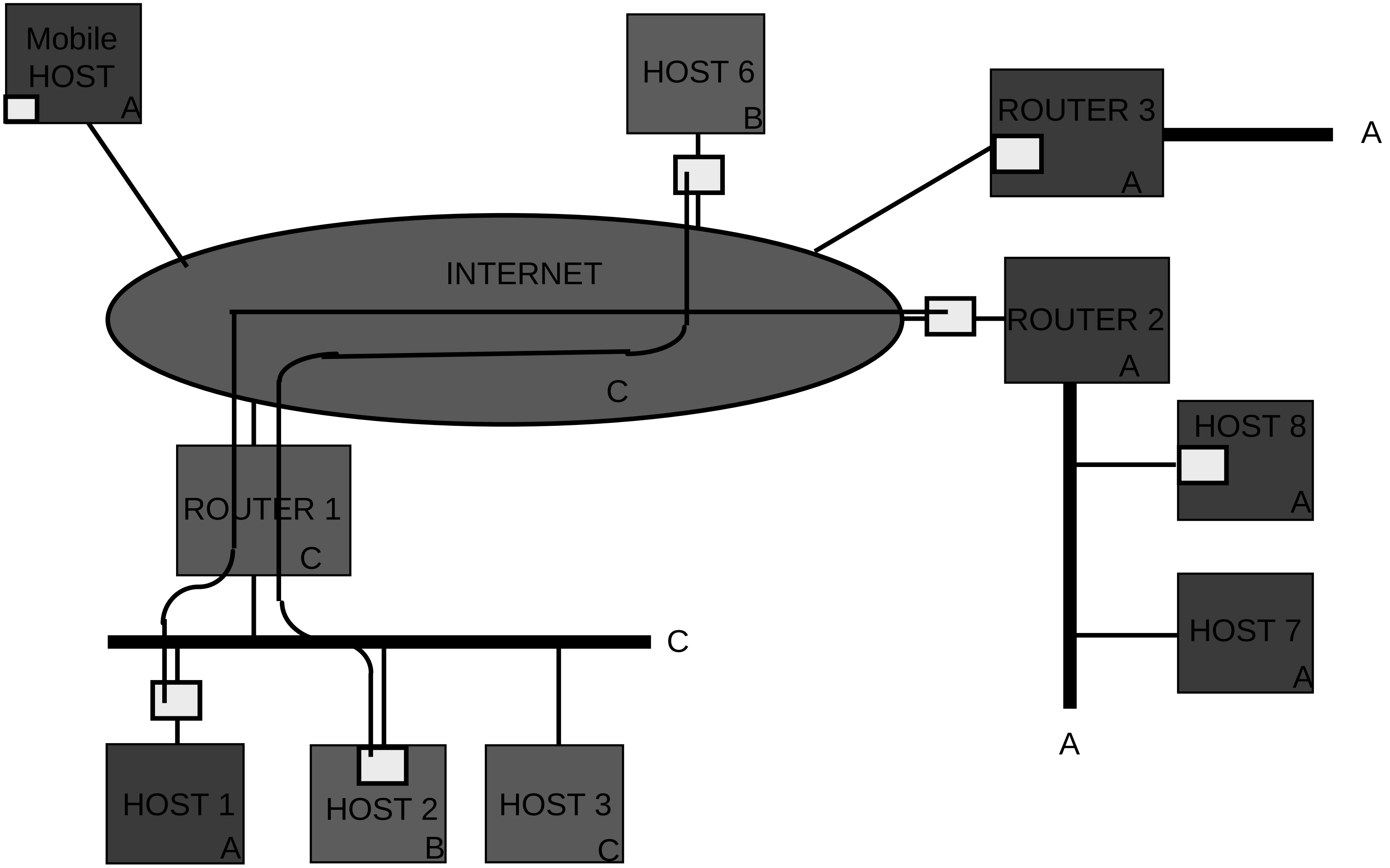
Why Not Internet Layer Security?

- Dependent on use of IP
  - but tunneling over IP accommodates a lot of other protocols
- Additional per-packet and per security association (SA) overhead
  - header overhead, crypto symch, SA establishment
- Implementations in routers/firewalls are complex
  - tunnel management, fast per-packet lookup, ...
- Host implementations often involve kernel mods
  - “bump in the stack” is an option, but has its own problems

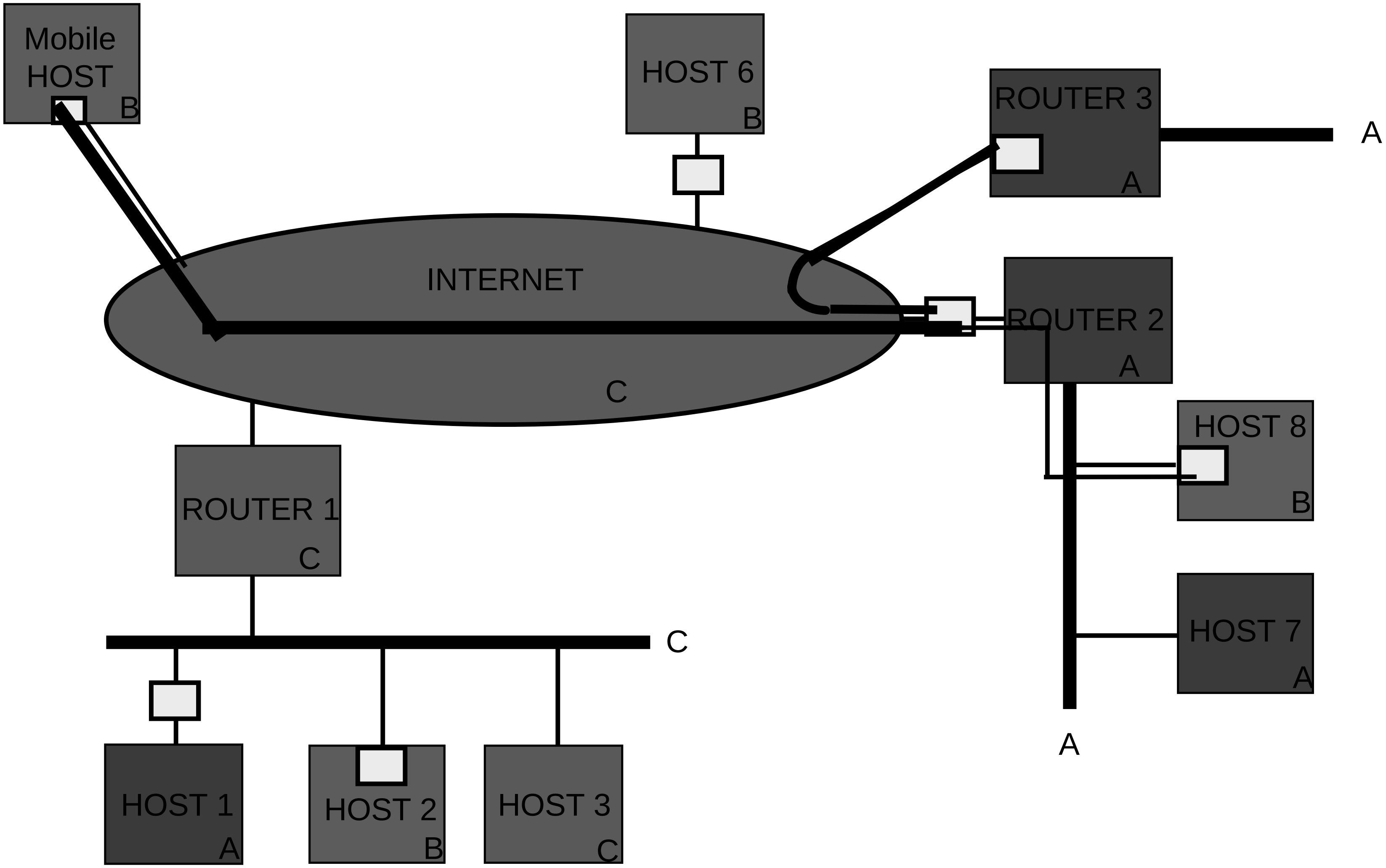
IPsec

- Adopted as Proposed Standards by the IETF (7/95), but radically revised, reissued in 2Q98?
- Authentication Header (AH) for (whole datagram) integrity and authenticity, optional anti-replay
- Encapsulating Security Payload (ESP) for mix-and-match confidentiality, authentication & integrity, and anti-replay
- Can encapsulate IP, ICMP, TCP, UDP, ...
- Separate security association negotiation protocols tied to key management, e.g., ISAKMP/Oakley & SKIP
- Algorithm independence,

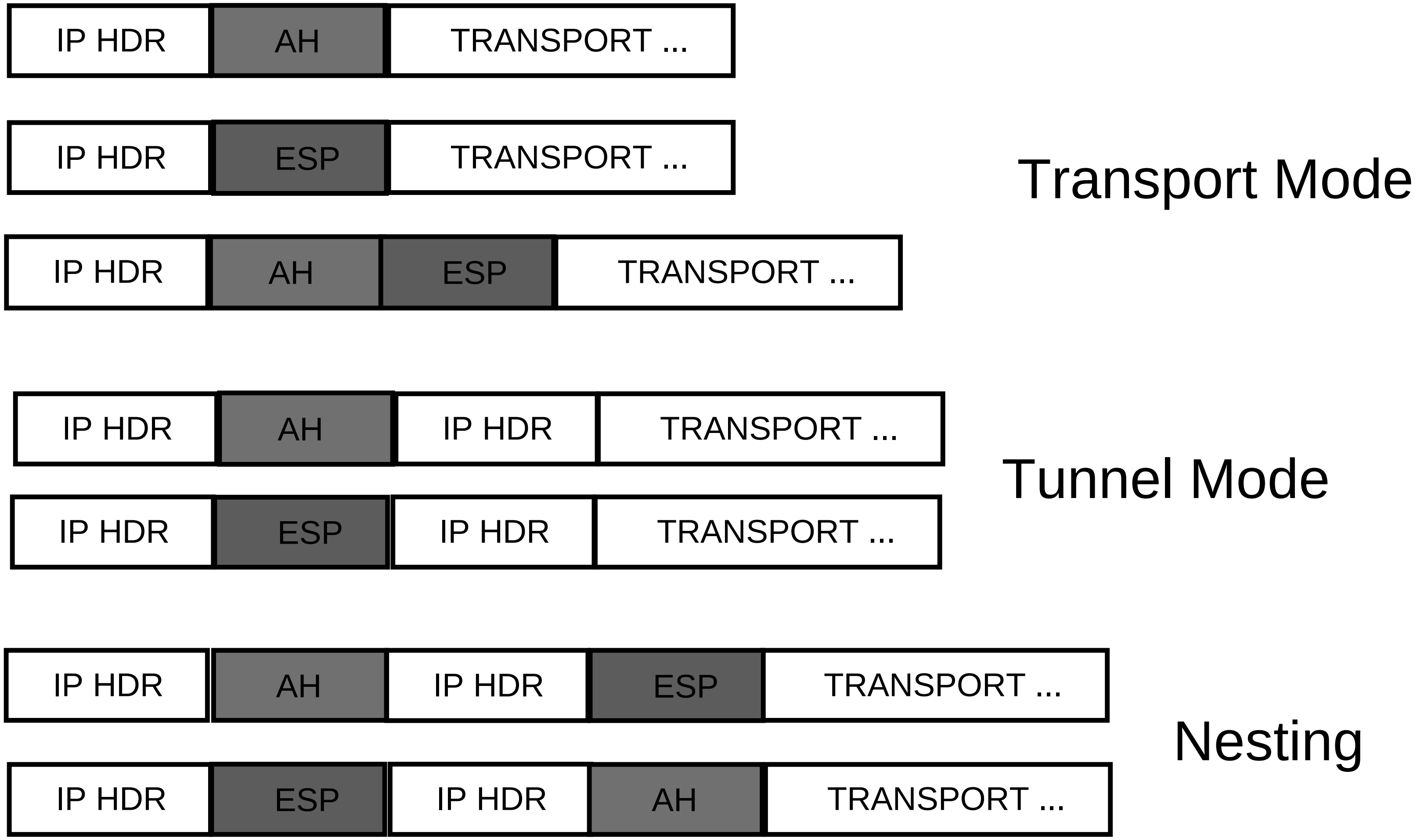
IPsec Path Examples



More IPsec Path Examples



AH and ESP Layering Options



IP HDR | AH | TRANSPORT ...

IP HDR | ESP | TRANSPORT ...

IP HDR | AH | ESP | TRANSPORT ...

Transport Mode

IP HDR | AH | IP HDR | TRANSPORT ...

IP HDR | ESP | IP HDR | TRANSPORT ...

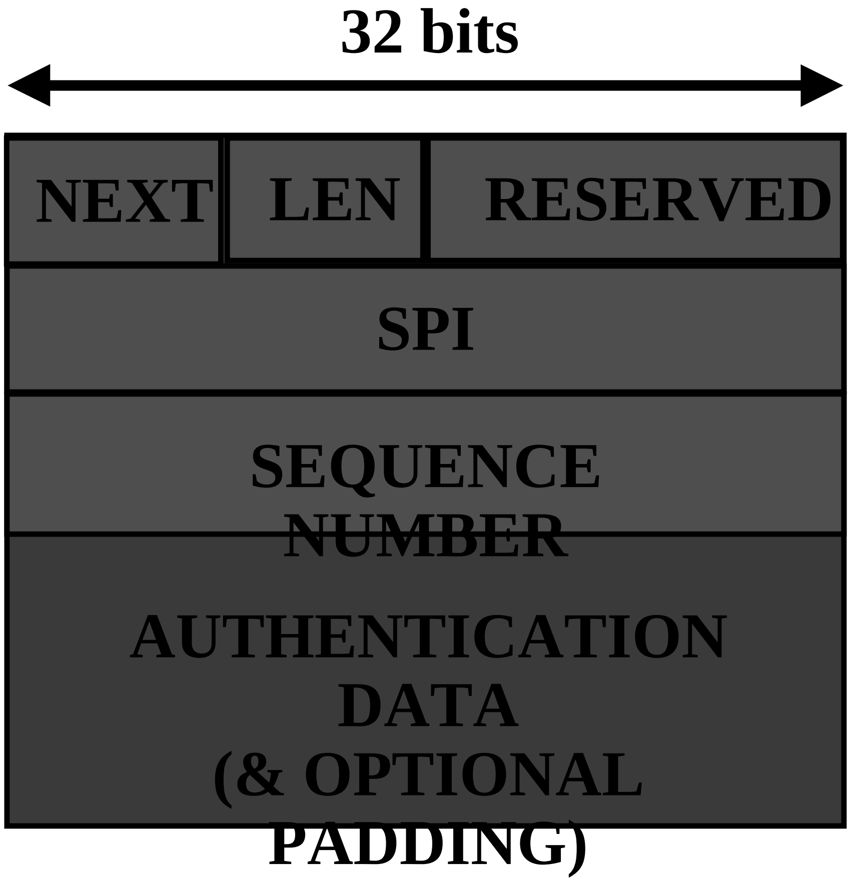
Tunnel Mode

IP HDR | AH | IP HDR | ESP | TRANSPORT ...

IP HDR | ESP | IP HDR | AH | TRANSPORT ...

Nesting

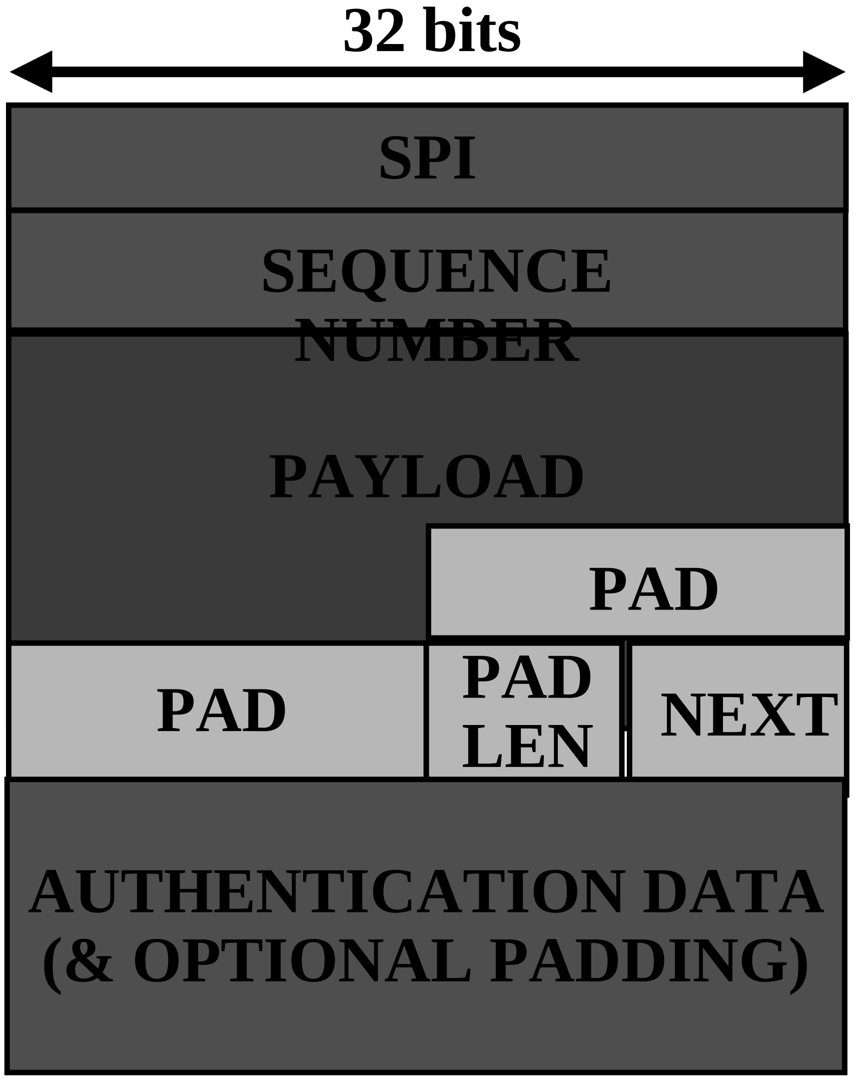
AH Format



32 bits

NEXT	LEN	RESERVED
SPI		
SEQUENCE NUMBER		
AUTHENTICATION DATA (& OPTIONAL PADDING)		

ESP Format


32 bits
SPI
SEQUENCE NUMBER
PAYLOAD
PAD
PAD
PAD LEN
NEXT
AUTHENTICATION DATA (& OPTIONAL PADDING)

AH & ESP Default Algorithms

- HMAC with MD5 or SHA-1 for integrity and authenticity
- DES-CBC for confidentiality
- Anti-replay sequence nuber receive window size:
  - recommended size is 64
  - minimum of 32 required
  - larger sizes optional, in multiples of 32
- NULL encryption and NULL authentication options for ESP to support mix and match functionality