IPSec

IPv6

To overcome limitation of IPv4

- Small space address (2**32)
- No support for mobility
- No security
- Survivability thus best effort as philosophy

IPv4 packet

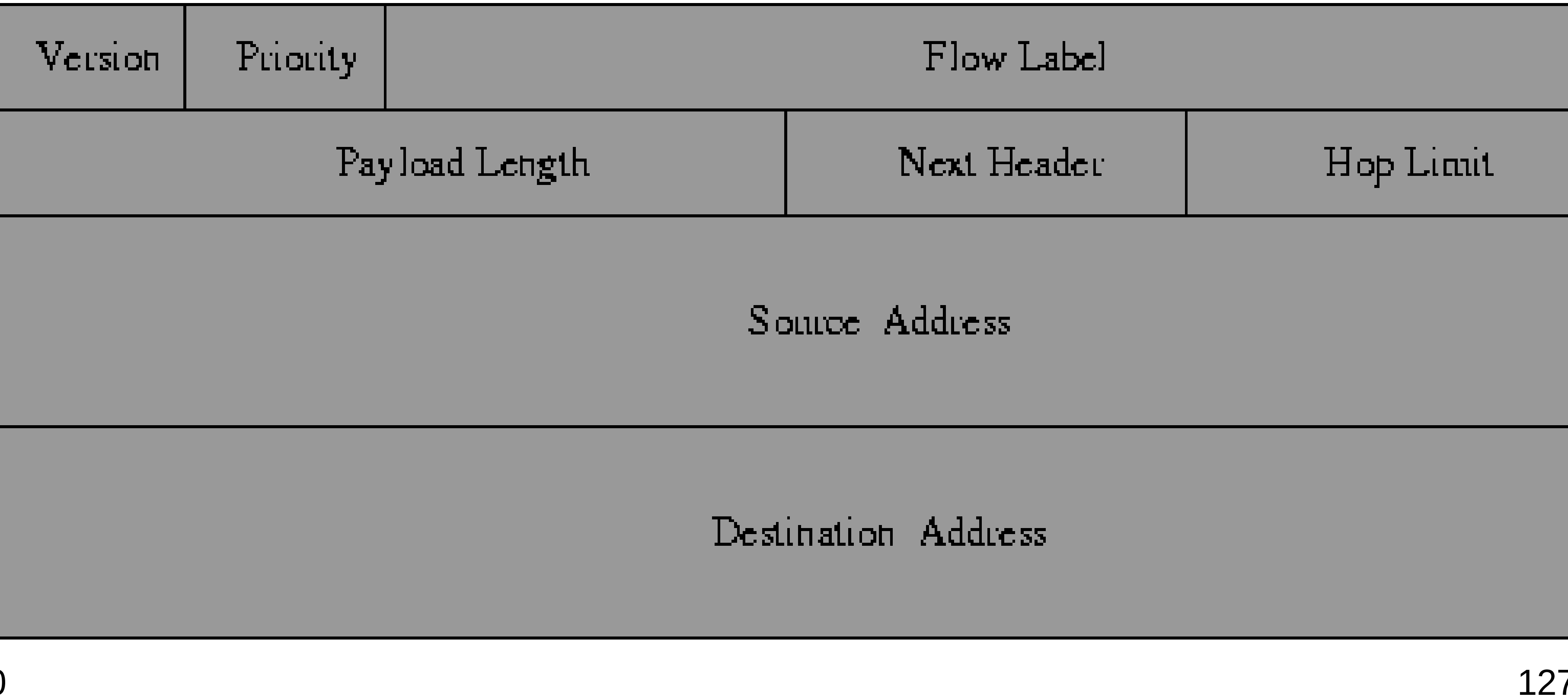
0
1
8
31
Classe A
0
net id
host id
0
2
16
31
Classe B
1 0
net id
host id
0
2
24
31
Classe C
1 1
net id
host id

IPv6

IPv6

– Huge space address (2**128)
– Support for mobility
– Security (IPsec)
– Quality of service
– Backward compatibility
– Efficiency

IPv6 packet


Version
Priority
Flow Label
Payload Length
Next Header
Hop Limit
Source Address
Destination Address
0
127

IPv6

- Security in design phase and not retro fitted as in IPv4:
  - Authentication and connectionless integrity (AH)
  - Confidentiality + Traffic control + Autentication (ESP)
  - IKE key exchange
- Security mechanisms and cryptographic algorithms independency
- We are at network level so used for VPN

IPSec security services

- Security services offered by IPv6:

- *Data Origin Authentication* verifies that each datagram was originated by the claimed sender

- *Data integrity* verifies that the contents of the datagram were not changed in transit, either deliberately or due to random errors

- *Data confidentiality* conceals the cleartext of a message, typically by using encryption

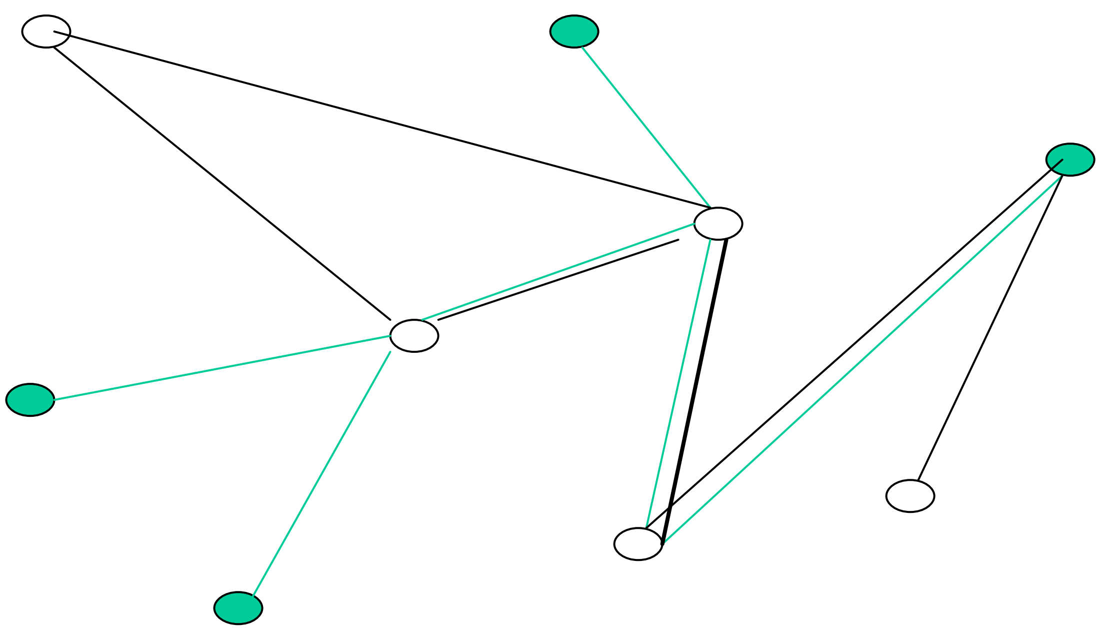
IPSec security services (2)

- *Replay protection* assures that an attacker can not intercept a datagram and play it back at some later time

- *Automated management of cryptographic keys and security associations* assures he possibility of automatic configuration $\rightarrow$ Scalability

VPN: Virtual Private Network

- A private (logical) network build on top of a public and shared physical network



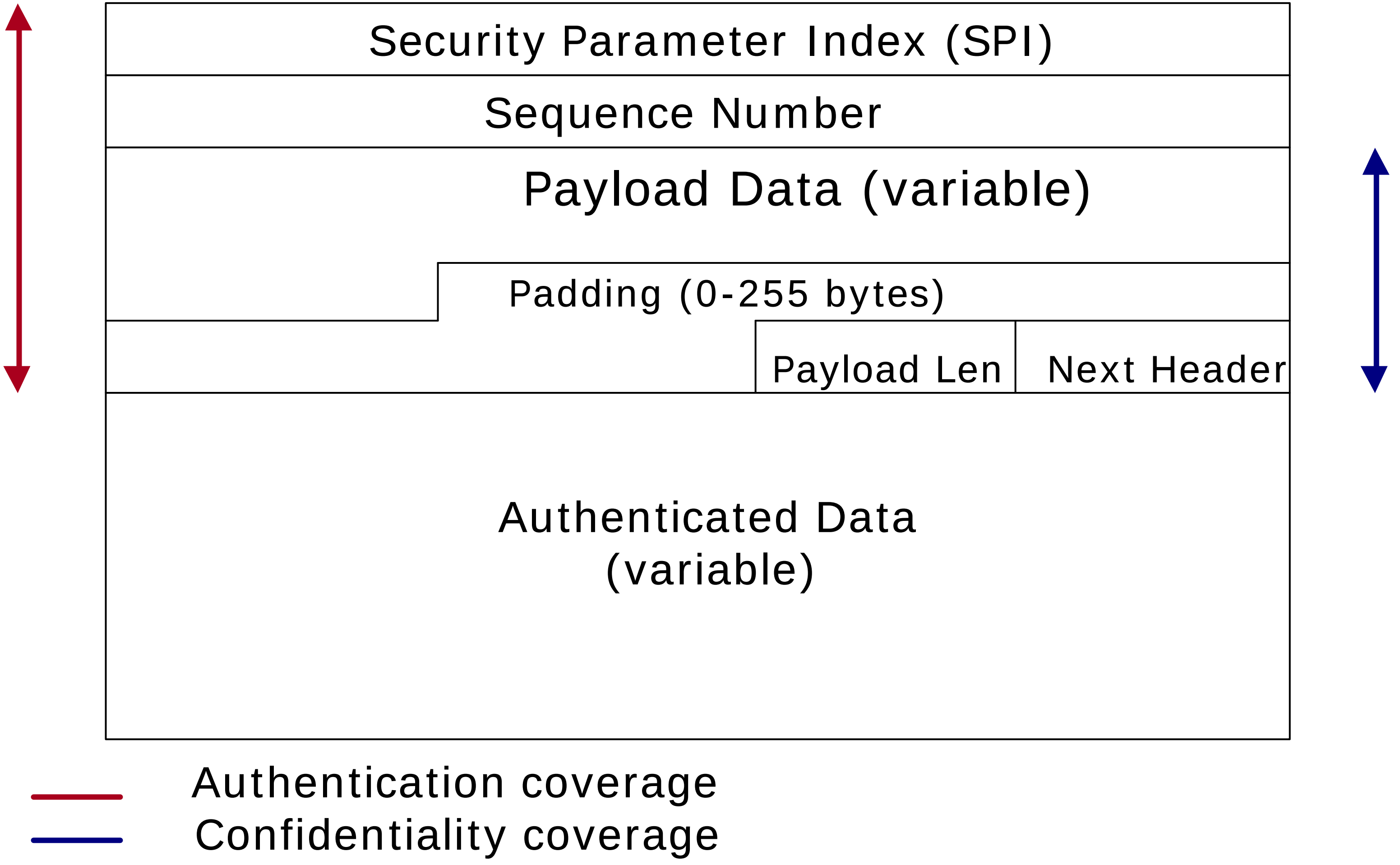
Virtual Private Networks

- **Branch Office Interconnection:** a VPN that enables communications between physically separated intranets that are members of a single corporate network
- **Inter-company Connections:** a VPN that enables secure communications between intranets of different companies, using the public Internet as a backbone
- **Remote Access:** a VPN that enables secure communications between a remote host and its home corporate network

AH: Authentication Header

Next Header	Payload Len	Reserved
Security Parameter Index (SPI)		
Sequence Number Field		
Authenticated Data (variable)		

ESP: Encapsulation Security Payload



IKE: Internet Key Exchange

– ISAKMP provides a framework for authentication and key exchange but does not define them.

– Oakley describes a series of key exchanges-- called "modes"-- and details the services provided by each (e.g. perfect forward secrecy for keys, identity protection, and authentication).

– IKE: Instantiation of ISAKMP/Oakley (promoted by Cisco)

IKE

- Set parameters for Security Association (SA)
- Scalability
- Several security levels and modes
  - Shared key
  - Digital Certificates
  - Crypto algorithms independency
- Additional security features (i.e. PFS, anticlogging)

Transport vs Tunnel mode

IPv6 specifies two modes:

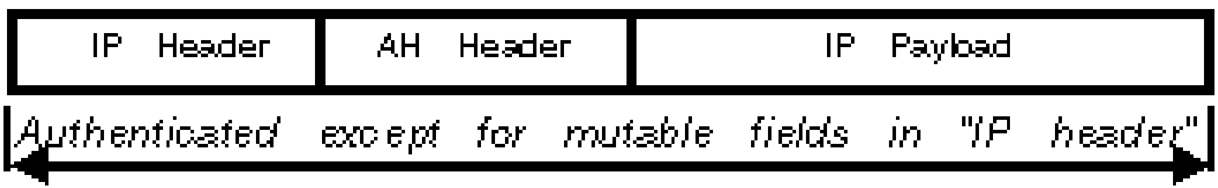
- Tunnel Mode for gw-to-gw and host-to-gw connections

- Transfer mode for host-to-host connections

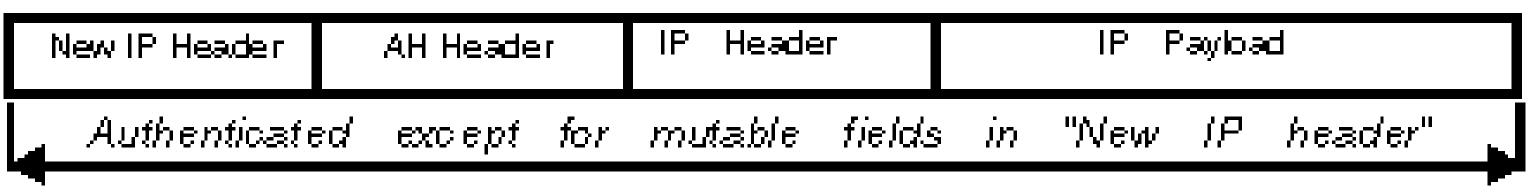
AH

Original Datagram:

Original Datagram Protected by AH-Transport Mode:



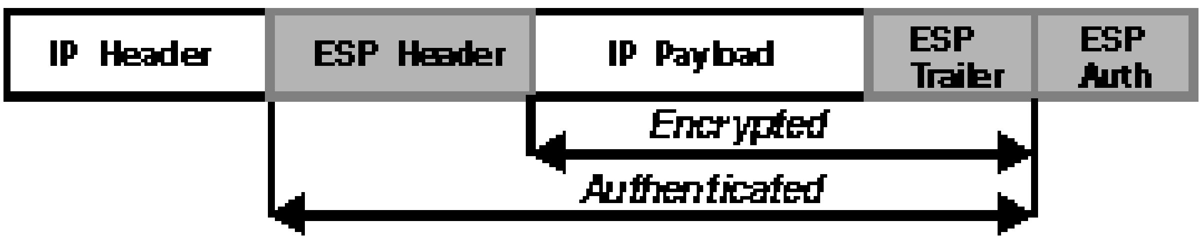
Original Datagram Protected by AH-tunnel Mode:



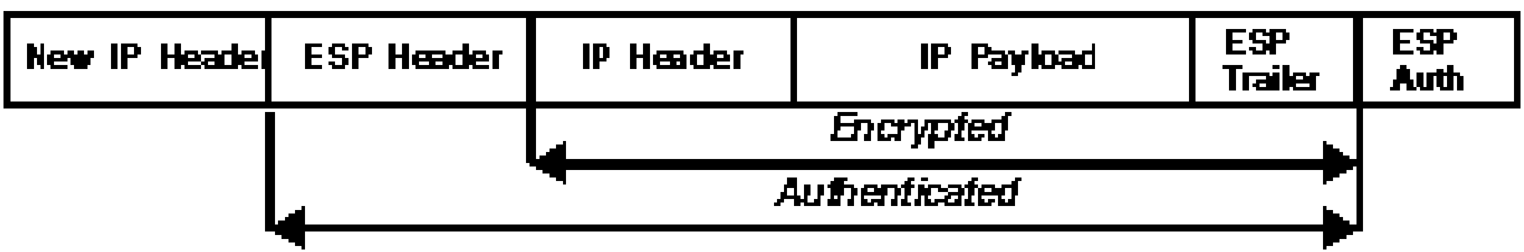
ESP

Original Datagram:

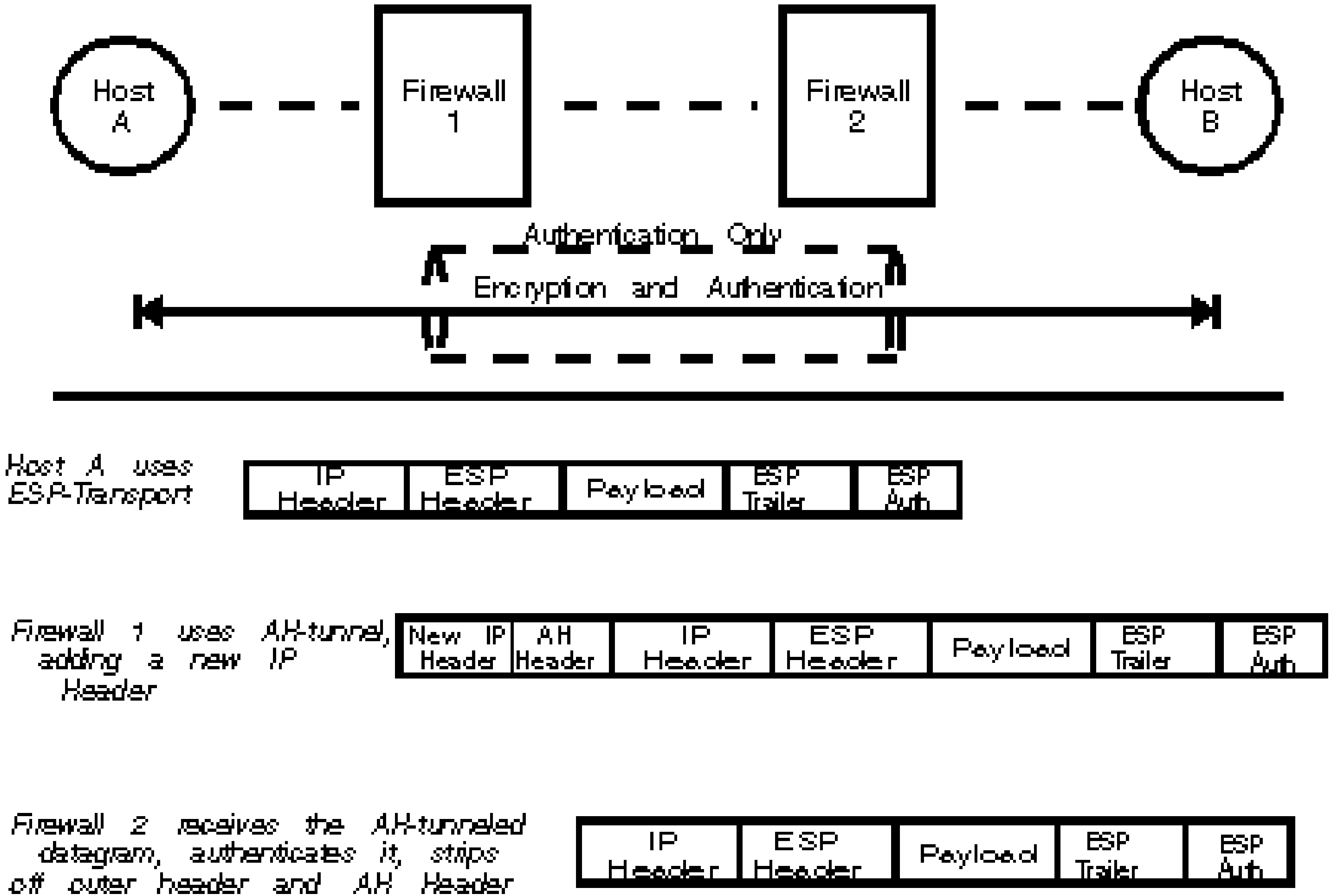
Original Datagram Protected by ESP-Transport Mode:



Original Datagram Protected by ESP-tunnel:



Example


Host A
Firewall 1
Firewall 2
Host B
Authentication Only
Encryption and Authentication
Host A uses ESP-Transport
IP Header
ESP Header
Payload
ESP Trailer
ESP Auth
Firewall 1 uses AH-tunnel, adding a new IP Header
New IP Header
AH Header
IP Header
ESP Header
Payload
ESP Trailer
ESP Auth
Firewall 2 receives the AH-tunneled datagram, authenticates it, strips off outer header and AH Header
IP Header
ESP Header
Payload
ESP Trailer
ESP Auth

IPSec limitations

- Problems with NAT
- Network security
- Replay attacks
- Legacy
- Slow deployment of IPv6

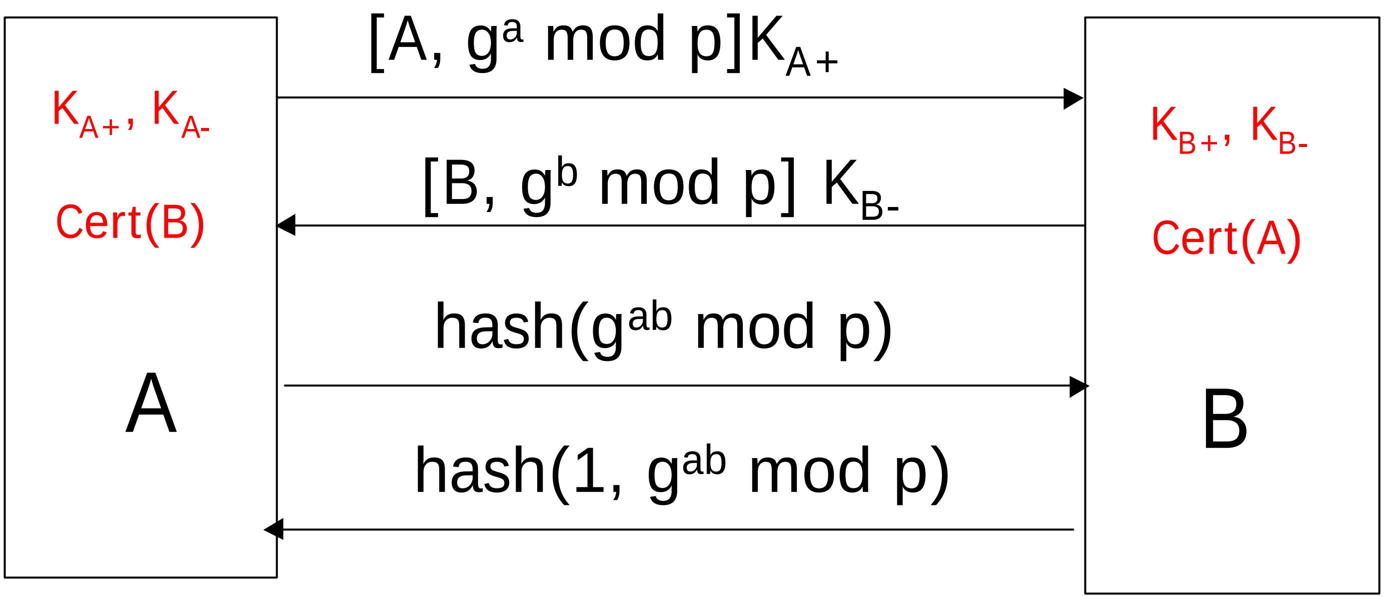
Perfect Forward Secrecy

- PFS if the attacker record past ciphertext than get the long term-secret at time T_1 but he cannot decrypt ciphertext generated before time T_1

- PFS secure the past against future attack

- Generation of temporary session key not derivable from long-term information

PFS: example



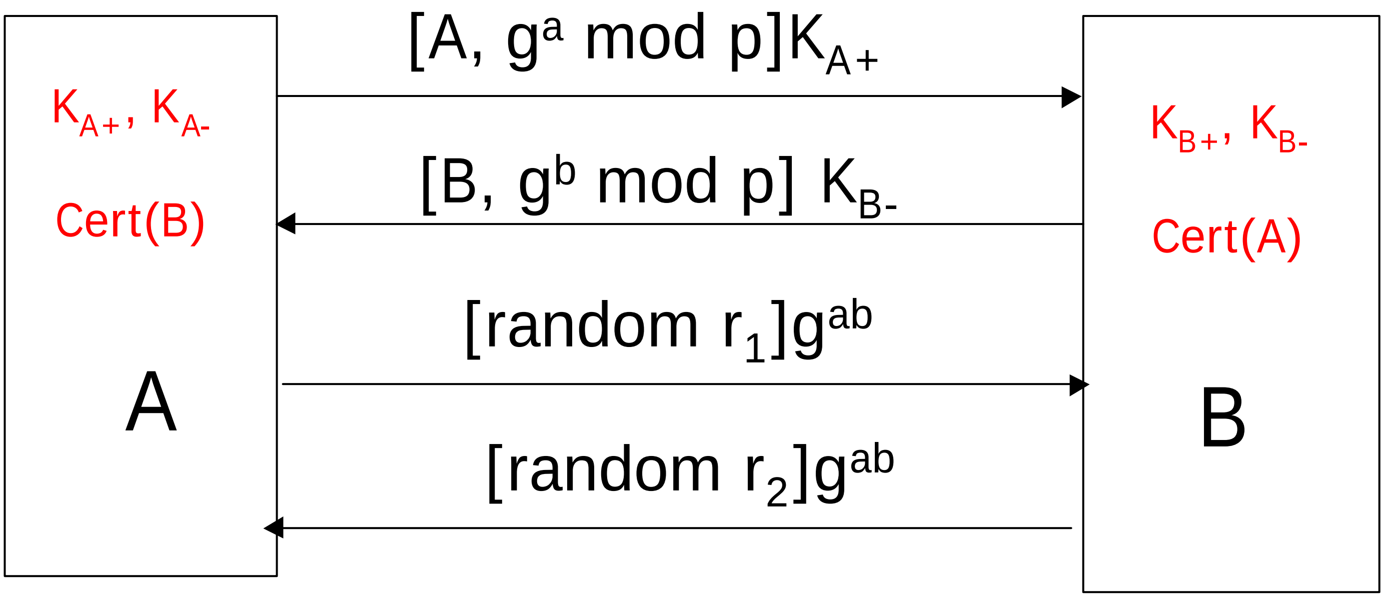
K_{A+}, K_{A-}
Cert(B)
A
$[A, g^a \bmod p]K_{A+}$
$[B, g^b \bmod p]\ K_{B-}$
$hash(g^{ab} \bmod p)$
$hash(1, g^{ab} \bmod p)$
K_{B+}, K_{B-}
Cert(A)
B

Secret key generation

- When two parties share secret key is good practice if both contribute to the generation
  - to prevent poorly chosen secret
  - to prevent possible impersonation consequent to break-ins

Secret key generation

- Example



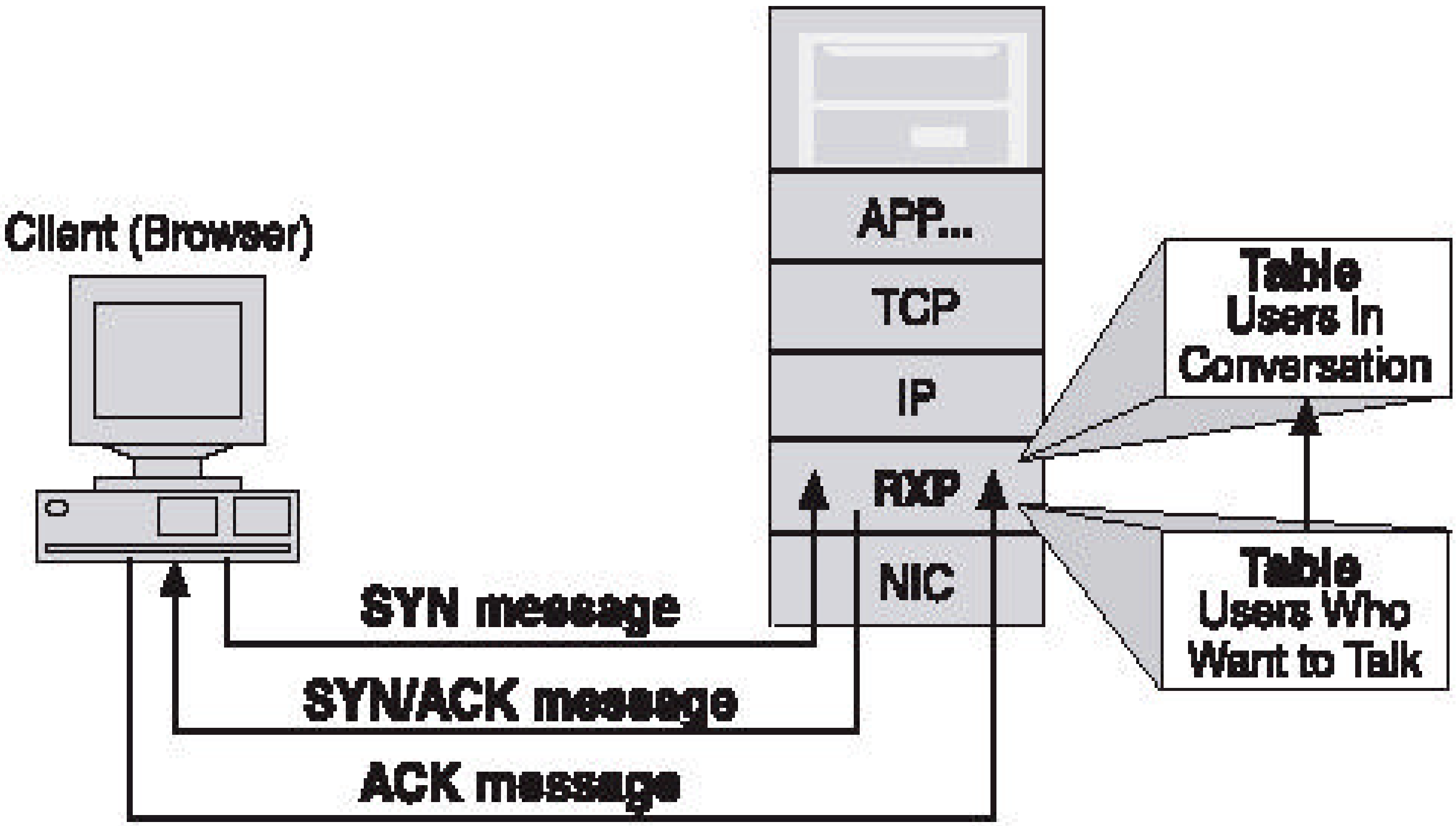
Shared key $k = r_1 \mid r_2$

Denial of Service

- DoS affects the availability property by maliciously denying access to resources/services

- DoS is one of the most common and effective attacks. It’s difficult to prevent and even more difficult to solve

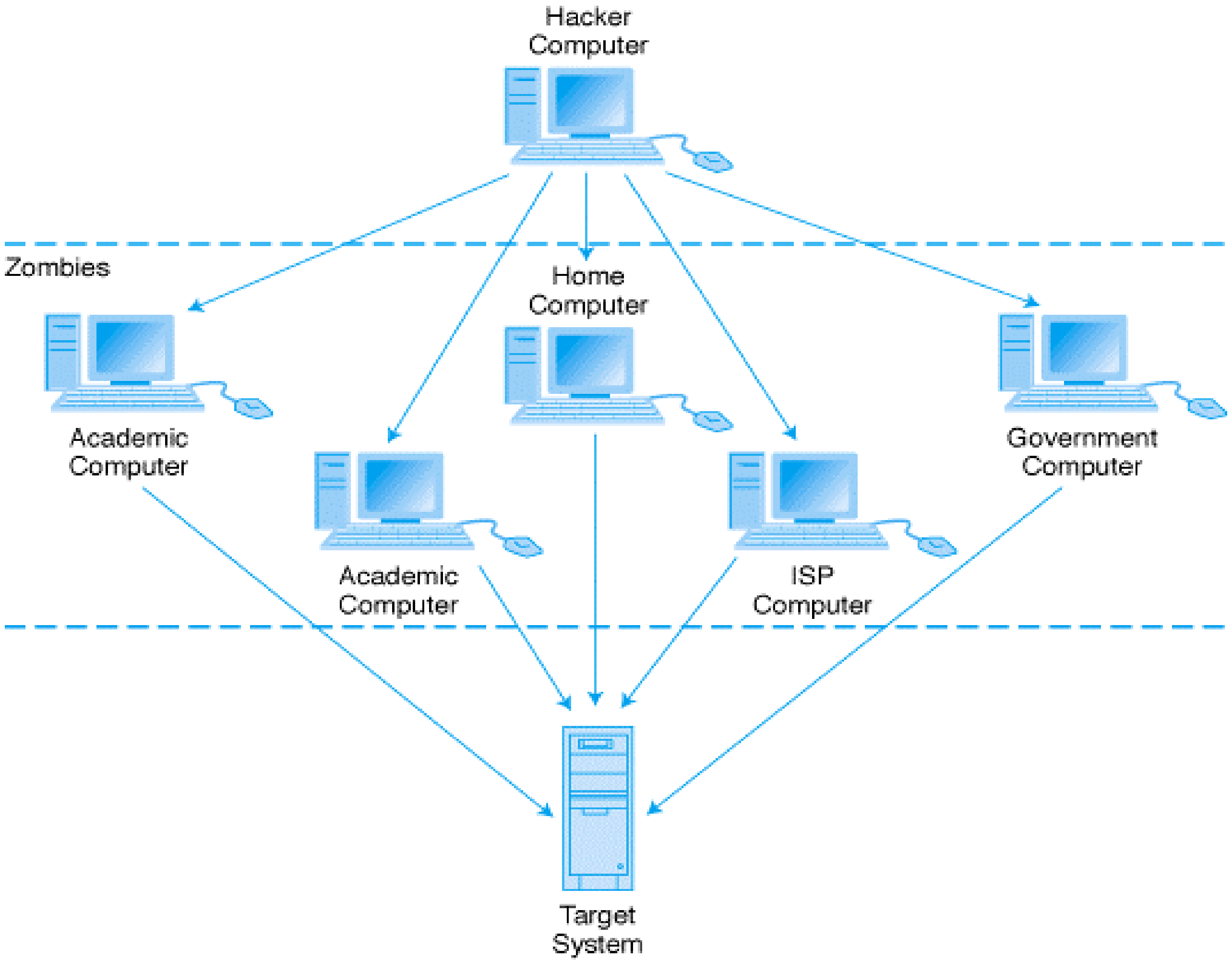
DoS: Sync flood



3-way Handshake

Distributed DoS

- Situation is even worse with DDoS

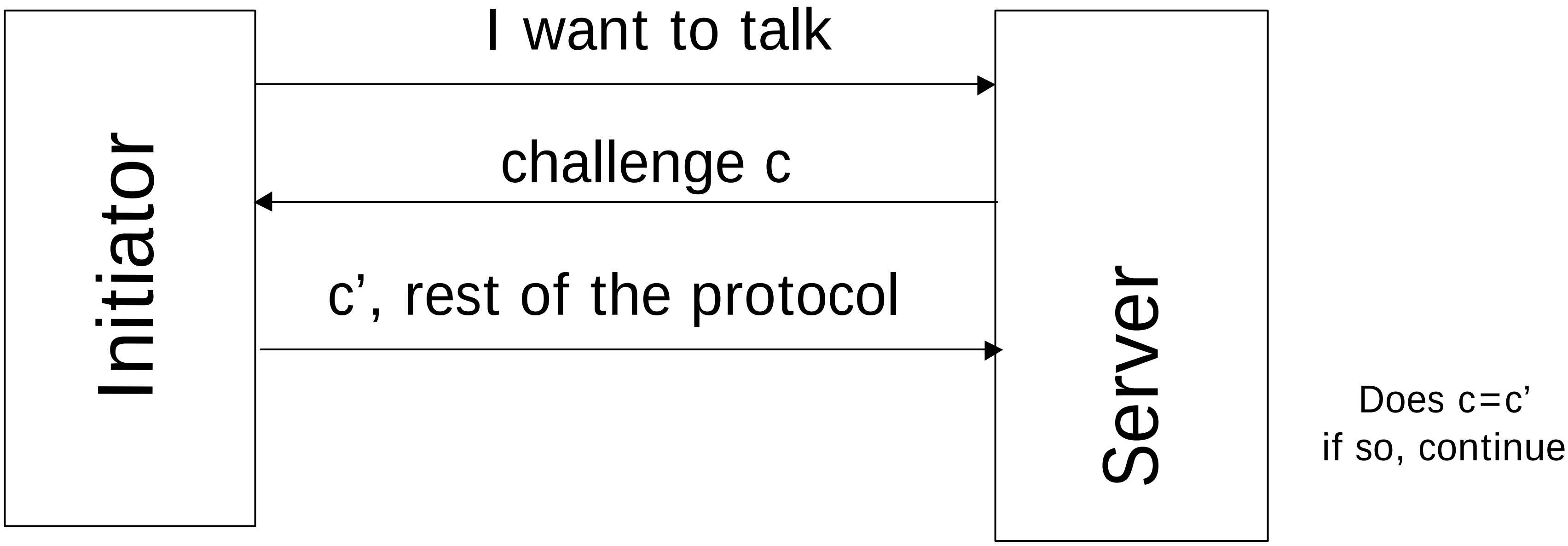


Denial of Service: prevention

- Reverse Path Filtering (deny invalid IPs)
- Allow only good traffic into your network (ingress filtering)
- Allow only good traffic out of your network (egress filtering)
- Stop directed broadcast traffic (to avoid being an amplifier)

....problem...all solutions limit functionalities

Denial of Service: solutions



c=hash(IP addr, secret) → stateless cookie

Denial of Service: solutions

- Puzzles: relies on the asymmetry of computation. Low for server high for client (initiator). This should discourage mounting DoS attacks.
- example

What is the hash of word x?

- Still powerful clients can mount DoS
- Not very effective with DDoS

Denial of Service: solutions

- So called Turing tests

Existing Yahoo! users

ID

password

Word you see below

The answer cannot be processed automatically but human intervention is needed