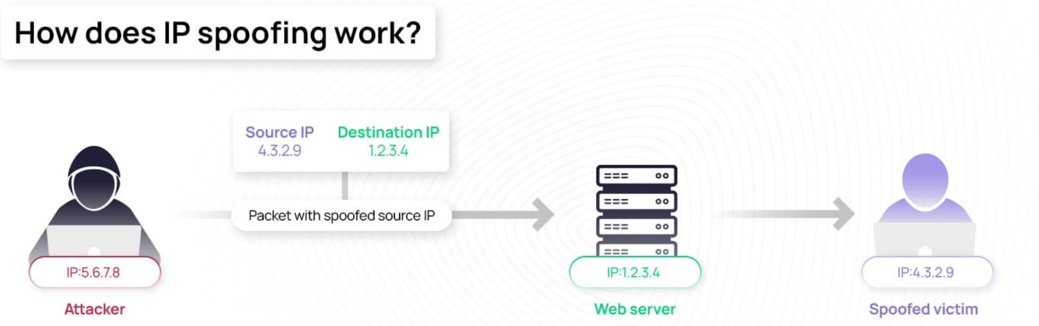
Outline

- Network Security Threads
- Securing end-to-end connections
  - Transport Layer Security (TLS)
- Security at Transport Layer
  - TCP, UDP, QUIC
- Security at Network Layer
  - IP/ICMP, IPsec, VPNs, IPv6 Security

Network Layer: IP/ICMP Attacks

1. IP spoofing

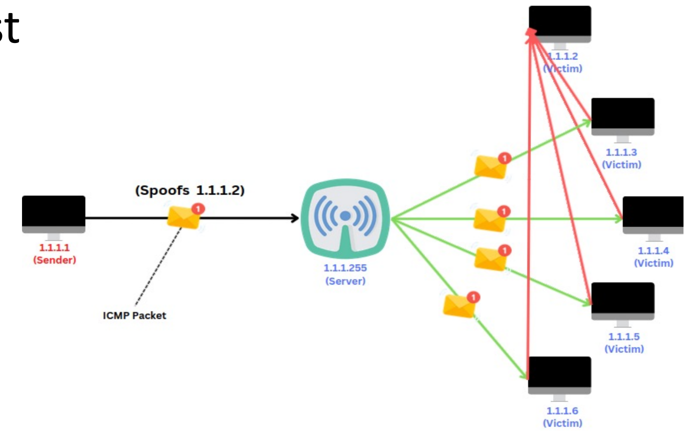
- attackers forge IP headers to impersonate another host
- used in, e.g., DDoS amplification attacks
- the target system or intermediate network devices believe the packet is from a legitimate source
- the attacker can either flood the victim or trick the victim into interacting with a spoofed host
- Mitigation: Ingress/Egress packet filtering (RFC 2827, a.k.a. BCP 38); IPsec



Network Layer: IP/ICMP Attacks

2. ICMP flood attack (ping flood)
   - overwhelm target w/ large volume of `ICMP Echo Request` packets, leading to DoS
   - Mitigation: ICMP rate limiting; firewall rules to block/validate ICMP requests
3. Smurf attack
   - ICMP-based amplification attack
   - the attacker sends `ICMP Echo Request(s)` to a broadcast address with a spoofed source IP, resulting in a large amount of traffic directed to the victim
   - Mitigation: same as above; disable ICMP broadcast
4. Ping of death
   - sending oversized packets (> 64 kBytes) that crash, freeze or reboot the target
   - Mitigation: modern OS resilient to reassembly, firewalls, IDS/IPS can easily detect and block

Concern: legacy systems; IoT devices



Network Layer: IP/ICMP Attacks

5. ICMP Redirect attacks
   - attacker manipulates routing tables via ICMP Redirect messages to divert traffic, indicating the attacker's IP as the "new best route" (e.g., spoofing the default R)
   - Mitigation: disable ICMP Redirect; use of secure routing protocols (e.g. secure OSPF)

6. Fragmentation attacks (e.g., Teardrop, Tiny Fragment Attack)
   - exploits the fragmentation process to cause DoS or bypass filters
   - attacker sends fragmented packets with overlapping fragment offsets or incomplete fragment headers, causing a crash or malfunction on reassembling
   - Mitigation:
     - current OS are robust; patch OS against fragmentation vulnerabilities, if needed
     - packet inspection and drop abnormal fragments
     - disable fragmentation; set MSS on routers to avoid fragmentation
     - IPv6

Outline

- Network Security Threads
- Securing end-to-end connections
  - Transport Layer Security (TLS)
- Security at Transport Layer
  - TCP, UDP, QUIC
- Security at Network Layer
  - IP/ICMP, IPsec, VPNs, IPv6 Security

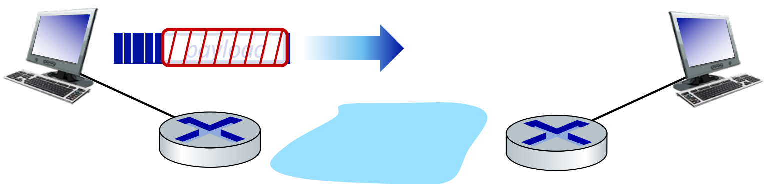
Network Layer: IPsec

IPsec

- Goal: secure IP communications providing confidentiality, integrity, and authentication
- Operation modes: *transport mode* (E2E) vs *tunnel mode* (hop-by-hop)
- Protocols:
  - Authentication Header (AH): provides data integrity and authentication [RFC 4302] (less used)
  - Encapsulating Security Payload (ESP): provides CIA [RFC 4303] (widely used)
- Security Associations (SA): to negotiate and maintain secure channels
- Key exchange: uses IKE (Internet Key Exchange) protocol for establishing secure communication

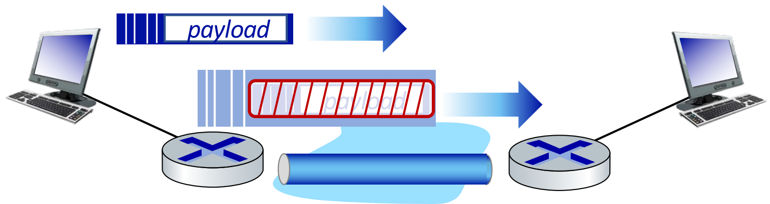
Network Layer: IPsec

- provides datagram-level encryption, authentication, integrity
  - for both user traffic and control traffic (e.g., BGP, DNS messages)
- two "modes":



transport mode:

- *only* datagram *payload* is encrypted, authenticated

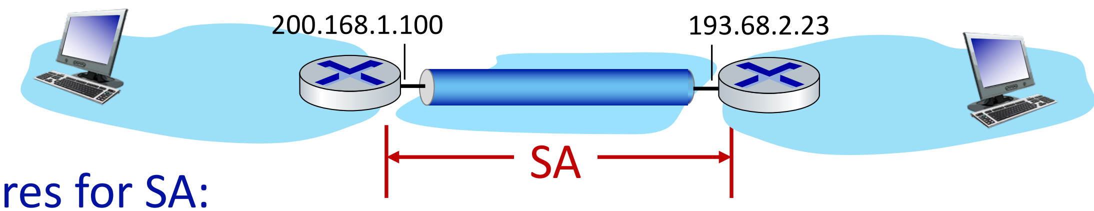


tunnel mode:

- *entire* datagram is encrypted, authenticated
- encrypted datagram encapsulated in new datagram with new IP header, tunneled to destination

Network Layer: IPsec – SA

- before sending data, a security association (SA) is established from sending to receiving entity (directional)
  - using the Internet Key Exchange (IKEv2) protocol [RFC 4306]
- ending, receiving entities maintain *state information* about SA
  - IP is connectionless; IPsec is connection-oriented!



R1 stores for SA:

- 32-bit id: *Security Parameter Index (SPI)*
- origin SA interface (200.168.1.100)
- destination SA interface (193.68.2.23)
- security protocol (AH or ESP) and mode
- type of encryption used
- type of integrity check used
- encryption key; auth key
- seq# (prevent replay attacks)

Network Layer: IPsec – SA

- *example:* manual establishment of IPsec SAs in IPsec endpoints:

  Example SA:

  SPI: 12345
  Source IP: 200.168.1.100
  Dest IP: 193.68.2.23
  Protocol: ESP
  Encryption algorithm: AES
  HMAC algorithm: SHA-2
  Encryption key: 0x7aeaca…
  HMAC key:0xc0291f…

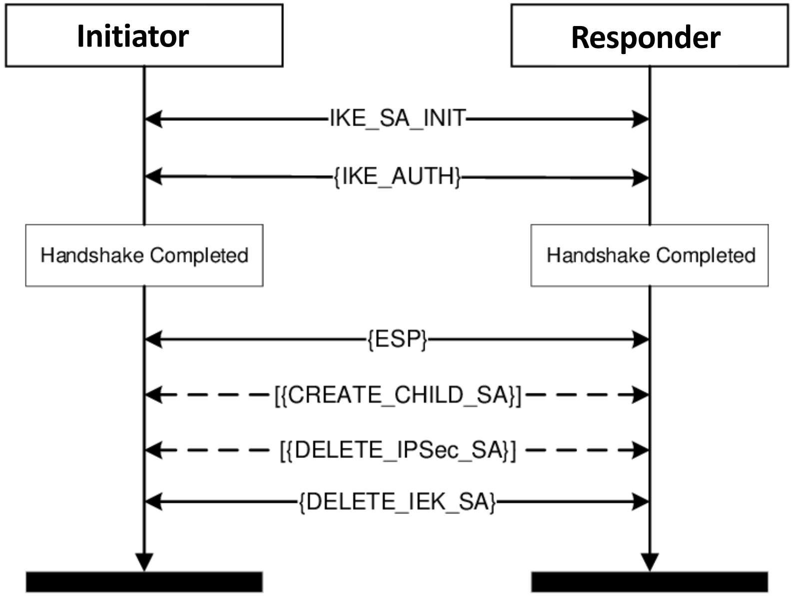
- manual keying is impractical for VPN with 100s of endpoints
- instead use IPsec IKE (Internet Key Exchange) (recommended standard)

Network Layer: IPsec – IKE

- authentication (prove who you are) with either
  - pre-shared secret (PSK) or
  - public key infrastructure (PKI)
- PSK: both sides start with secret
  - run IKE to authenticate each other and to generate IPsec SAs (one in each direction), including encryption, authentication keys
- PKI: both sides start with public/private key pair, certificates
  - run IKE to authenticate each other, obtain IPsec SAs (one in each direction)
  - similar to handshake in TLS

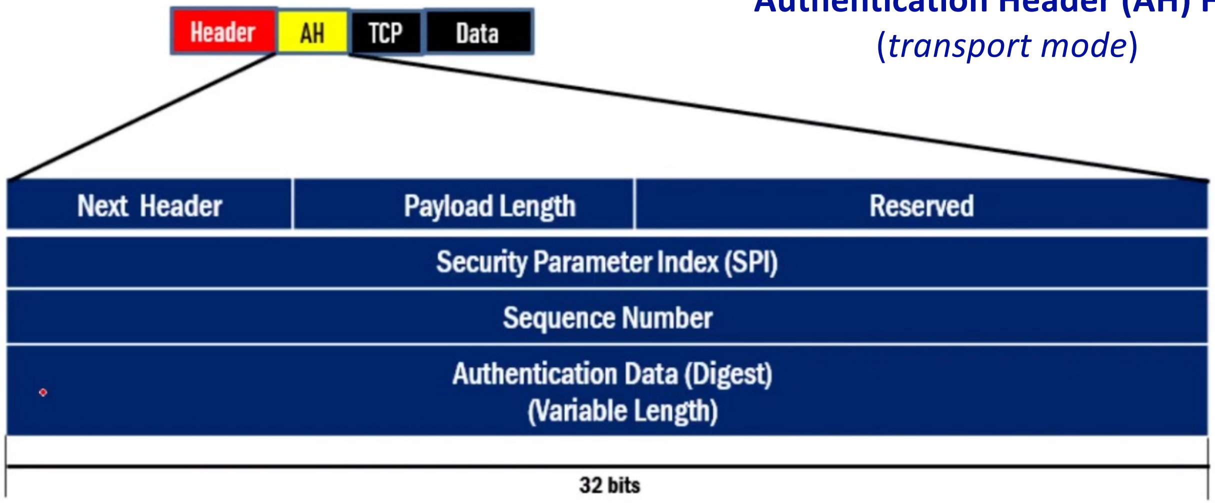
Network Layer: IPsec – IKEv2 handshaking

- IKE_SA_INIT
  - negotiates security parameters and performs Diffie-Hellman key exchange
- IKE_AUTH
  - authenticates the peers, establishes IPsec SAs, and defines the traffic to be protected



Network Layer: IPsec protocols

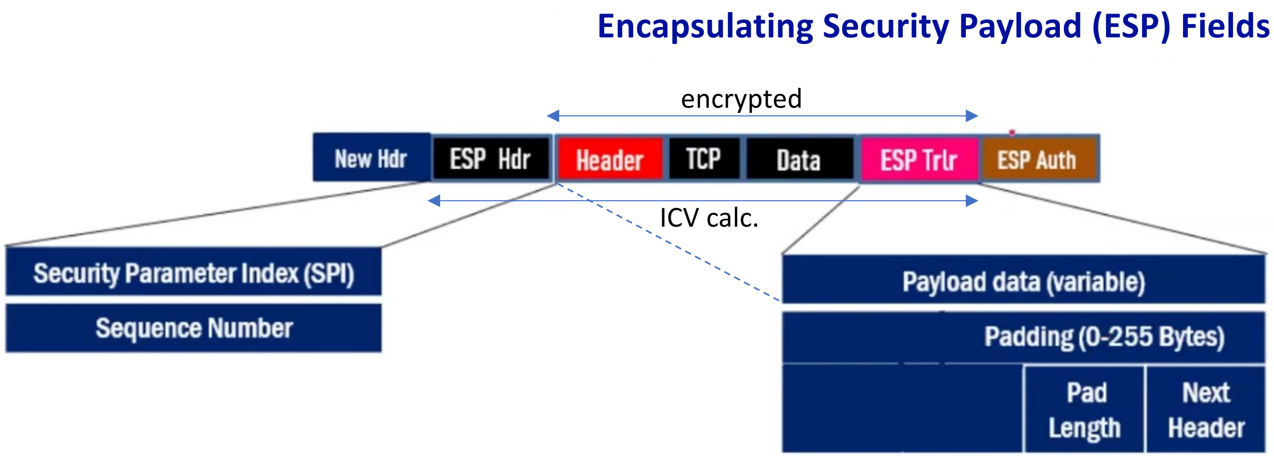
Authentication Header (AH) Fields
(*transport mode*)



- Next Header – payload type (TCP, UDP, IP, OSPF, etc.) of the original IP datagram
- Payload Length – AH length in multiple of 4 bytes
- Security Parameter Index (SPI) – identifies the security association between sender and receiver
- Sequence Number – nonce to avoid replay attacks
- Authentication Data – digest from hashing the full datagram (immutable fields); its length is determined by the MAC algorithm negotiated for the SA (HMAC-SHA256, HMAC-SHA384, etc.)

Note: * In Tunnel Mode, a new IP header is added, and the entire original IP packet is encapsulated. The AH header is placed between the new and the original IP header.

Network Layer: IPsec protocols



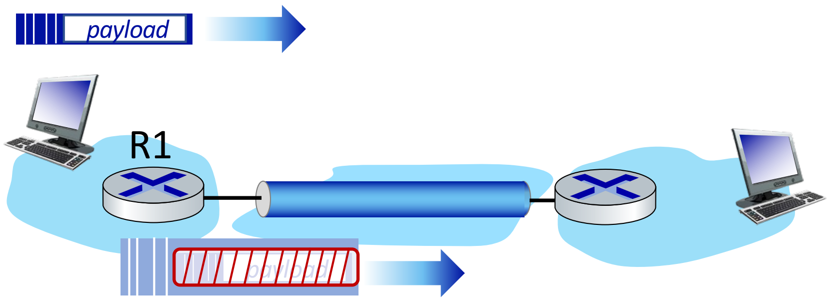
tunnel mode ESP

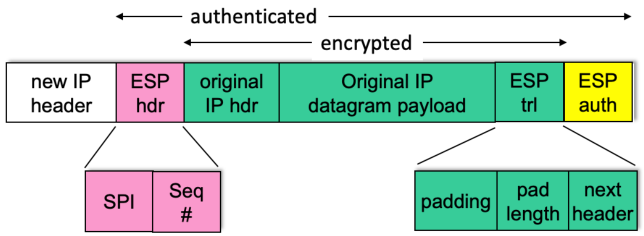
- Payload data – original datagram
- Padding (and Pad Length) – added to meet the required length for block ciphers (e.g., 16-byte blocks)
- Next Header – payload type (TCP, UDP, IP, OSPF, etc.) of the original IP datagram
- Security Parameter Index (SPI) – identifies the security association between sender and receiver
- Sequence Number – nonce to avoid replay attacks; incremented per datagram sent
- ESP Auth or Integrity Check Value (ICV) – digest from hashing original datagram, ESP header and trailer
- New Hdr - new header for tunnel mode with protocol field value 50 (ESP)

Network Layer: ESP tunnel mode

Actions at R1:

- appends ESP trailer to original datagram (which includes original header fields!)
- encrypts result using algorithm and key specified by SA
- appends ESP header to front of this encrypted quantity
- creates authentication MAC (ESP auth) using algorithm and key specified in SA
- appends MAC forming *new payload*
- creates new IP header, new IP header fields, addresses to tunnel endpoint





Network Layer: IPsec sequence numbers

- for new SA, sender initializes seq # to 0
- each time datagram is sent on SA:
  - sender increments seq # counter
  - places value in seq # field
- goal:
  - prevent attacker from sniffing and replaying a packet
  - receipt of duplicate, authenticated IP packets may disrupt service
- method:
  - destination checks for duplicates
  - doesn't keep track of *all* received packets; instead, uses an anti-replay sliding window to save state
  - legitimate packets may be dropped if net causes severe out-of-order delivery*

* In this case, admins may need to increase win size (typically 64 packets)

Network Layer: IPsec deployment

- VPNs – IPsec is a foundational technology in many VPN solutions Specifically, IPsec in tunnel mode is used in
  - site-to-site VPNs: to connect corporate branches over the Internet securely
  - remote access VPNs: allow employees to connect to their corporate network from anywhere using secure encrypted tunnels
- Enterprise Networks – large enterprises use IPsec to secure internal traffic, especially when dealing with sensitive or critical data, e.g.,
  - between data centers
  - for ensuring that internal comm. across parts of the network are protected
- Telecom and ISPs
  - some use IPsec in their backbone to secure traffic between regional points of presence (POPs) and between their infrastructure elements

Network Layer: IPsec summary

- IKEv2 message exchange for cryptographic algorithms, secret keys, SPI numbers; establishes IPsec SAs
- use AH or ESP protocols
  - AH provides integrity, source authentication
  - ESP protocol additionally provides encryption
- IPsec peers can be two end-systems, two routers/firewalls, or a router/firewall and an end system
- Still security vulnerabilities?
  - yes, mainly resulting from: IPSec misconfiguration or implementation flaws, use of weak cypher suites, or unpatched systems; it doesn't obfuscate traffic char

Network Layer: IPsec summary

Trudy sits somewhere between R1, R2; she doesn't know the keys

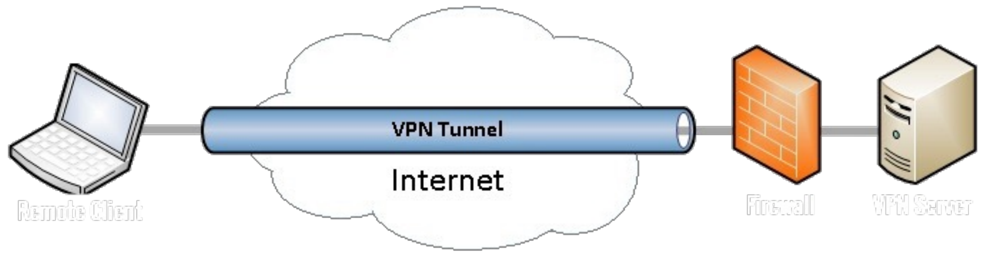
- will Trudy be able to see original contents of datagram?
- how about source, dest IP addresses, transport protocol, application ports?
- flip bits without detection?
- masquerade as R1 using R1's IP address?
- replay a datagram?

Outline

- Network Security Threads
- Securing end-to-end connections
  - Transport Layer Security (TLS)
- Security at Transport Layer
  - TCP, UDP, QUIC
- Security at Network Layer
  - IP/ICMP, IPsec, VPNs, IPv6 Security

Network Layer: Virtual Private Networks

- A VPN creates a secure, encrypted connection between a user's device and a remote server or network over the Internet



- Key goals: CIA, anonymity, access control
- Operation (Tunneling)
  - VPNs encapsulate data inside another protocol (e.g., IPsec ESP, TLS) and add an outer IP header, allowing the data to traverse public networks securely
  - Full tunneling: all user traffic is sent through the VPN
  - Split tunneling: only selected traffic (e.g., corporate resources) passes through the VPN, while the rest uses the public network directly

Network Layer: Types of VPNs

- Remote Access VPN
  - involves a VPN client that connects the user's device to a VPN server on the corporate network
  - protects data transmitted between the user's device and the company network
- Site-to-Site VPN
  - connects entire networks (e.g., two or more office locations) securely over the Internet
  - either Intranet-based or Extranet-based Site-to-Site VPN
  - often implemented using IPsec in tunnel mode
- TLS VPN
  - commonly used in web-based applications (no additional client sw required)
  - uses TLS protocols to encrypt traffic, allowing users to connect through their browsers; IPsec-based VPNs offer greater privacy (in ESP tunnel mode)

Network Layer: Types of VPNs

- Personal VPN
  - used by individuals for privacy, anonymity, and bypassing geographic restrictions (e.g., accessing content that is restricted in certain countries)
  - routes user's traffic through a remote VPN server, masking original IP address
- Cloud VPN
  - crucial way to secure communication between on-premises infrastructure and cloud services
  - helps org to protect data in hybrid environments, and secure remote work in the cloud
- Double VPNs
  - often used in privacy-conscious settings, route traffic through two VPN servers, providing an extra layer of anonymity and security
  - address privacy-focused use cases and help mitigating threats such as traffic correlation attacks

Network Layer: Open-Source VPN protocols

VPN Protocol	Security Strength	Speed	Overhead	Known Vulnerabilities	Key Features
OpenVPN (L7/L4)	Strong (AES-256, RSA, HMAC, TLS)	Moderate	High (TCP/UDP, encryption overhead)	No major vulnerabilities but requires proper config	Multiple platforms, customizable, highly secure, flexible with TCP/UDP
WireGuard (L3)	Strong (ChaCha20, Curve25519, Poly1305)	High	Low (lean codebase, smaller attack surface)	Early versions had protocol-level issues, now secure	Simplicity, very fast, minimal code, ideal for modern use cases
IKEv2/IPsec (L3)	Strong (AES-256 or ChaCha20, RSA, or ECDH, SHA-2)	High	Moderate (efficient for mobile)	Resistant to most known attacks if correctly config	Stable and secure for mobile devices, supports mobility, multihoming, fast reconnects
L2TP/IPsec (L2,L3)	Moderate (IPsec security)	Moderate	High	Vulnerable to MITM attacks without proper IPsec config	Older but still used in legacy systems
SoftEther (L2,L7/L4) (L3 optional)	Strong (SSL/TLS)	Moderate	Moderate	No major vulnerabilities known	Multi-protocol support (L2TP, OpenVPN, SSTP, etc.), easy to set up

Outline

- Network Security Threads
- Securing end-to-end connections
  - Transport Layer Security (TLS)
- Security at Transport Layer
  - TCP, UDP, QUIC
- Security at Network Layer
  - IP/ICMP, IPsec, VPNs, IPv6 Security

Network Layer: IPv6 security

- IPv6 includes security directly in its design, conversely to IPv4
    - one of its focus: be resilience to network attacks
- Main security-related features:
  - Expanded address space
    - from 2^{32} to 2^{128}
    - limits scanning and spoofing attacks, making random address guessing of active hosts impractical
  - IPsec support
    - initially mandatory, currently recommended (RFC 6434) (extension headers)
  - Simplified header structure
    - eases header inspection; decreases attack surface
  - No broadcast

Network Layer: IPv6 security

- Neighbor Discovery Protocol (NDP)
  - replaces ARP with NDP, which uses multicast instead of broadcast
  - to counter NDP spoofing, adds a security extension (SEcure ND) for cryptographic address verification
  - SEND uses Cryptographically Generated Addresses (CGAs)
  - CGAs link an IPv6 address to a public key, verifying that the source is the legitimate owner of that address
- Built-in privacy extensions (RFC 8981)
  - for temporary, random IP address assignment, reducing the risk of user tracking and identification by rotating device addresses
- Removal of NAT
  - reduces attack surface
- Fragmentation
  - no fragmentation by default; restricted to source

Network Layer: IPv4 vs IPv6 security

Feature	IPv4	IPv6
Address Space	32-bit, IP address exhaustion, easy to scan	128-bit, vast space reduces scanning attacks
IPsec Support	Optional, requires additional configuration	Native support, standardized implementation
Header Structure	Complex, contains optional fields	Simplified, fixed base header, extension hdrs
Broadcasting	Supports broadcasting (e.g., ARP, Smurf attacks)	Broadcast eliminated, relies on multicast
Neighbour Discovery	Uses ARP, vulnerable to spoofing and DoS	NDP w/ Secure Neighbour Discovery (SEND)
Routing Security	No integrated support for routing security	Supports route optimization, secure NDP
Privacy Extensions	Not natively supported	Privacy extensions prevent tracking
Extension Headers	Limited support, often requires workarounds	Allows flexible extension without modifying base header
Multicast and Anycast	Limited multicast support, anycast uncommon	Multicast and anycast built-in and standardized

Network Layer: IPv6 security

- However, IPv6 also introduces complexity in deployment, especially with extension headers and NDP, which may require additional security

Copyright © 2003 David Farley, d-farley@ibiblio.org
http://ibiblio.org/Dave/drfun.html
This cartoon is made available on the Internet for personal viewing only. Opinions expressed herein are solely those of the author.

The brave new world of IPv6

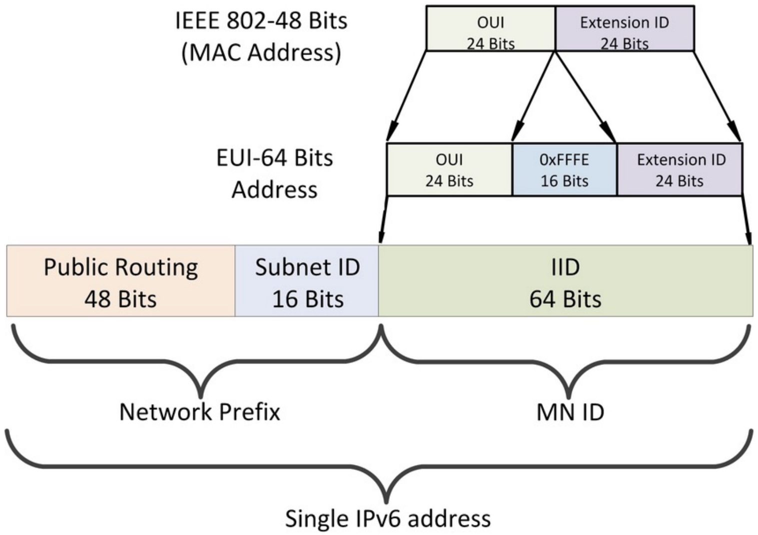
Network Layer: IPv6 security

- Extension Headers Manipulation and Fragmentation Attacks
  - IPv6 EHs allow to add optional information, for flexible packet handling
  - headers such as Destination Options or Routing Headers can create processing overhead, leading to potential DoS attacks
  - attackers can exploit EH by
    - crafting packets with unusual header chains to bypass filtering rules in firewalls and IDS/IPS
    - attacker could use Routing Header Type 0 (RH0), which specifies that packets should be routed through multiple intermediate nodes ("ping-pong" DoS amplification attack)
    - RH0 currently deprecated (RFC 5095)
  - Mitigation:
    - firewalls and IDS/IPS to inspect and handle IPv6 EH correctly, blocking headers known for evasion tactics
    - network devices must be configured to discard fragmented packets with dangerous header types (ensuring that all fragments of a packet are received before forwarding)

Network Layer: IPv6 security

- Addressing and Privacy
  - IPv6 allows for a large address space, including both link-local addresses (for local networks) and global unicast addresses
  - MAC-derived IPv6 address (EUI-64 format)* reveals information about the hardware of the device, compromising anonymity

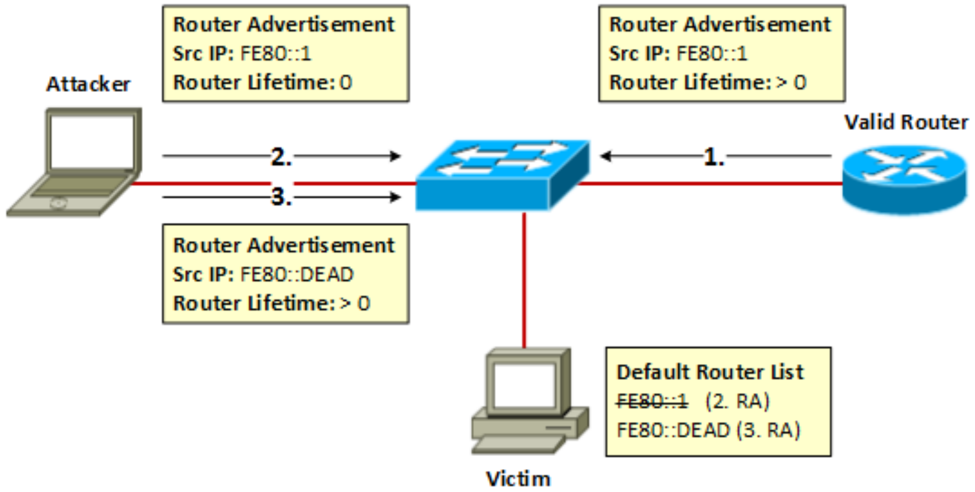
- Mitigation
  - use Temporary Addresses (RFC 8981), randomizing IID bits frequently
  - use Stable Privacy Addresses (RFC 7217) where address is not related on MAC address (not hardware- but hashed-based)



* Extended Unit Identified

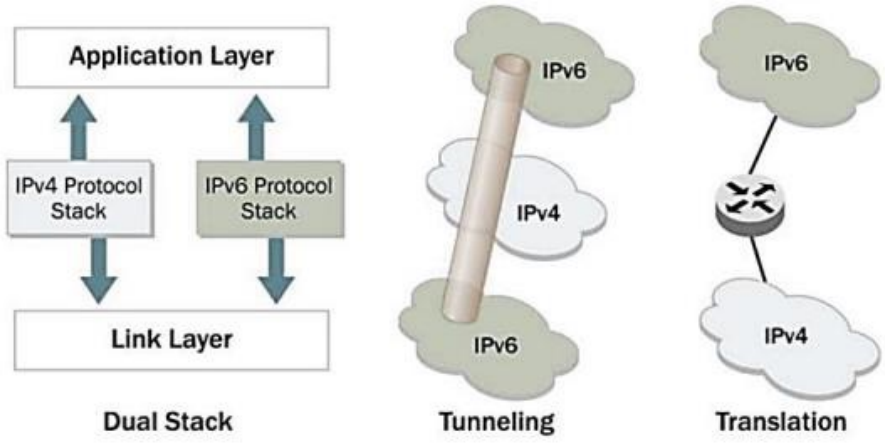
Network Layer: IPv6 security

- Neighbor Discovery Protocol (NDP)
  - NDP replaces ARP in IPv6, handling essential functions like address resolution, router discovery, and reachability detection
  - NDP is vulnerable to attacks similar to ARP spoofing, such as ND spoofing and router advertisement (RA) flooding, leading to DoS or MitM attacks
- Mitigation
  - RA guard and dynamic host configuration protections on network devices can also help limit RA flooding
  - implement SEND (SEND adoption is currently limited due to its complexity and lack of universal support)



Network Layer: IPv6 security

- IPv4 ↔ IPv6
  - IPv4 and IPv6 interoperability relies on various transition mechanisms, including dual stack, tunneling (e.g., 6to4, ISATAP, Teredo) or translation
  - transition mechanisms create additional attack surfaces, e.g., tunneling protocols can be used to bypass firewall policies and encapsulate malicious IPv6 traffic over IPv4
- Mitigation
  - avoid using insecure tunneling protocols, prefer native IPv6 deployments whenever possible
  - disable unused transition services, such as Teredo or 6to4, if not required



Network Security Summary

- Introduction
- Network Security Threads and Attacks
- Securing End-to-End Connections
  - Transport Layer Security (TLS)
- Security at Transport Layer: TCP, UDP, QUIC
- Security Network Layer
  - IP/ICMP, IPSec, VPNs, IPv6 Security