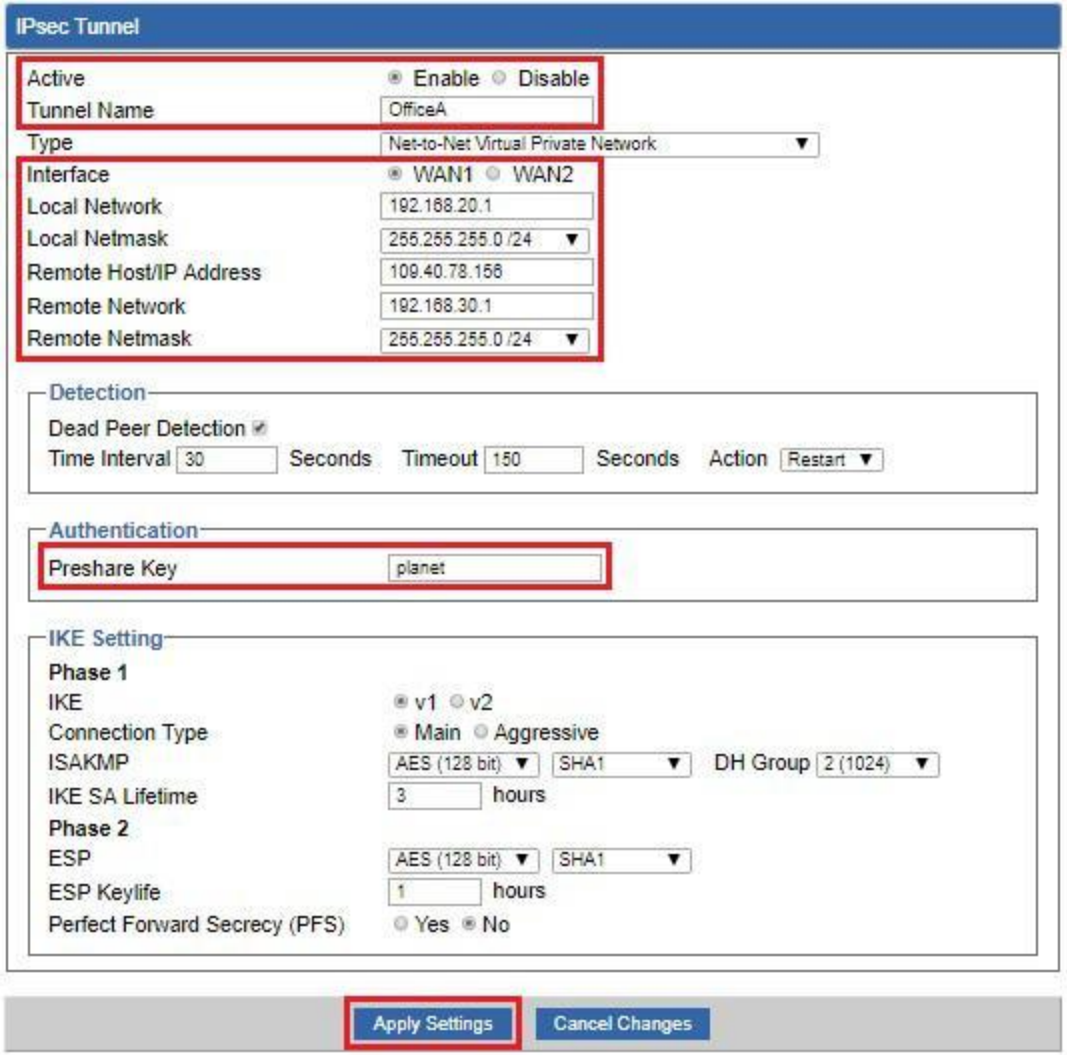
Internet-Layer Security

Outline

- ☐ Internet Protocols
- ☐ Supporting Protocols
- ☐ IPsec Protocol



IPsec Tunnel

Active ● Enable ○ Disable
Tunnel Name OfficeA
Type Net-to-Net Virtual Private Network ▼
Interface ● WAN1 ○ WAN2
Local Network 192.168.20.1
Local Netmask 255.255.255.0 /24 ▼
Remote Host/IP Address 109.40.78.156
Remote Network 192.168.30.1
Remote Netmask 255.255.255.0 /24 ▼

Detection
Dead Peer Detection ☑
Time Interval 30 Seconds Timeout 150 Seconds Action Restart ▼

Authentication
Preshare Key planet

IKE Setting
Phase 1
IKE ● v1 ○ v2
Connection Type ● Main ○ Aggressive
ISAKMP AES (128 bit) ▼ SHA1 ▼ DH Group 2 (1024) ▼
IKE SA Lifetime 3 hours
Phase 2
ESP AES (128 bit) ▼ SHA1 ▼
ESP Keylife 1 hours
Perfect Forward Secrecy (PFS) ○ Yes ● No

Internet Protocols

TCP or UDP have generated segments but now how to send them to another device on the internet?

Internet Protocols: Background (1/4)

- When a person was born, they were given a

  name

- When this person enrols to a university, they were given a

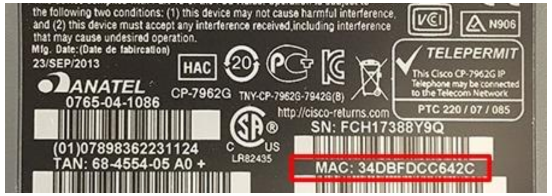
  student number

Student number helps manage records efficiently, reduce errors, and facilitate quick retrieval of information.

Internet Protocols: Background (2/4)

- When a device is manufactured for network communications, it is assigned a

  MAC address


the following two conditions: (1) this device may not cause harmful interference,
and (2) this device must accept any interference received,including interference
that may cause undesired operation.
Mfg. Date:(Date de fabircation)
23/SEP/2013
ANATEL
0765-04-1086
(01)07898362231124
TAN: 68-4554-05 A0 +
HAC
20
CP-7962G
TNY-CP-7962G-7942G(B)
C US
LR82435
http://cisco-returns.com
N906
TELEPERMIT
This Cisco CP-7962G IP Telephone may be connected to the Telecom Network
PTC 220 / 07 / 085
SN: FCH17388Y9Q
MAC: 34DBFDCC642C

- When this device connects to the broader internet, it is assigned an

  IP address

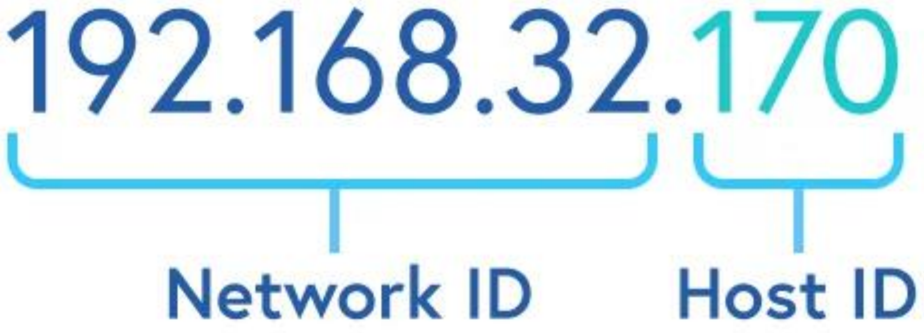
The IP address helps facilitate communication across networks, enabling efficient routing of data, reducing the potential for errors in addressing, and ensuring that information reaches the correct destination quickly.

Structure in management

Internet Protocols: Background (3/4)

Wiki:

- An Internet Protocol address (IP address) is a numerical label such as 192.168.32.170 that is assigned to a device connected to a computer network that uses the Internet Protocol for communication. (Transmit data or payload from higher-layer protocols like UDP or TCP)



- IP addresses serve two main functions:

□ network interface identification, and

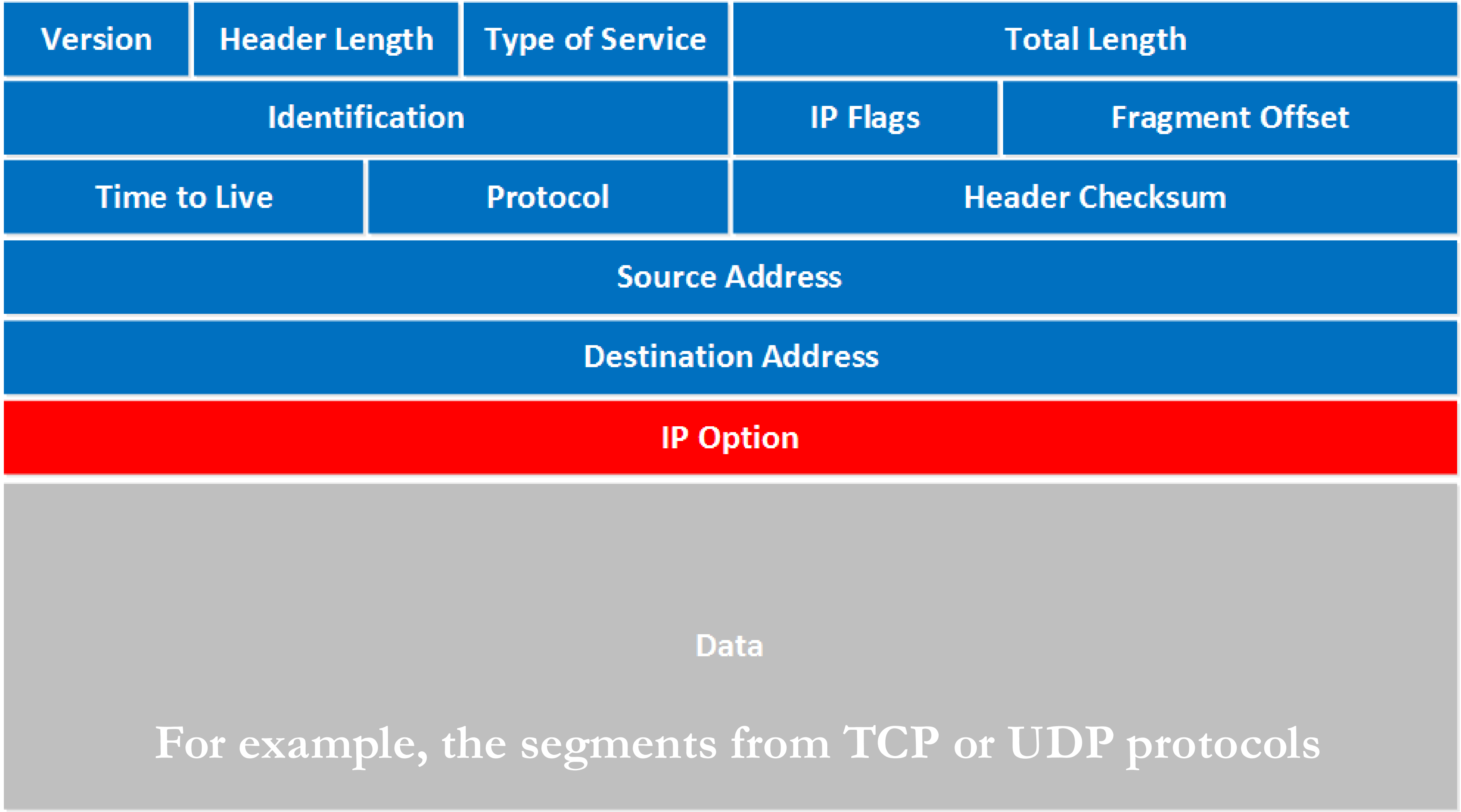
□ location addressing.

Internet Protocols: Background (4/4)

- IPv4 (Internet Protocol version 4) is the fourth version of the Internet Protocol (IP) and one of the core protocols that govern the way data is transmitted over the internet. It was introduced in the early 1980s and is still widely used today. IPv4 addresses are 32-bit numbers: 203.210.191.112 in decimal.

- IPv6 (Internet Protocol version 6) is the sixth version of the Internet Protocol, designed to replace IPv4 and address the limitations posed by its 32-bit address space. IPv6 was introduced in the late 1990s to provide a significantly larger address space, using 128-bit addresses formatted in hexadecimal and separated by colons (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334). This expanded address space accommodates the growing number of devices on the internet

Internet Protocols: IPv4 (1/7)



Version | Header Length | Type of Service | Total Length

Identification | IP Flags | Fragment Offset

Time to Live | Protocol | Header Checksum

Source Address

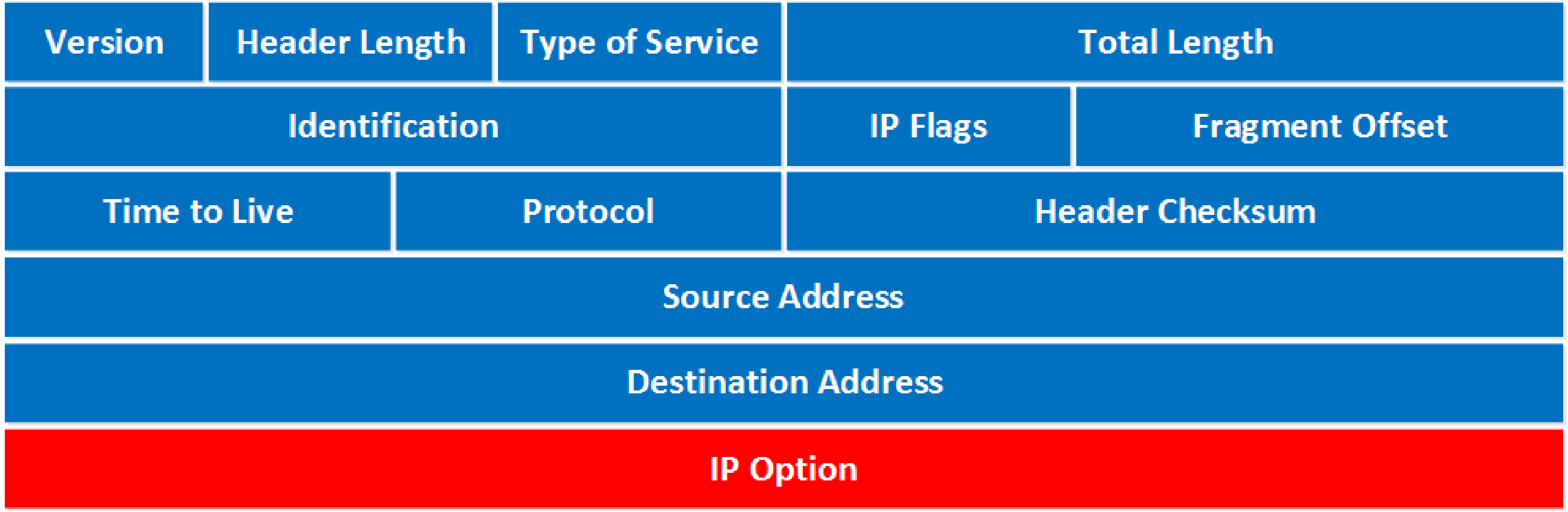
Destination Address

IP Option

Data

For example, the segments from TCP or UDP protocols

Internet Protocols: IPv4 (2/7)



Version | Header Length | Type of Service | Total Length

Identification | IP Flags | Fragment Offset

Time to Live | Protocol | Header Checksum

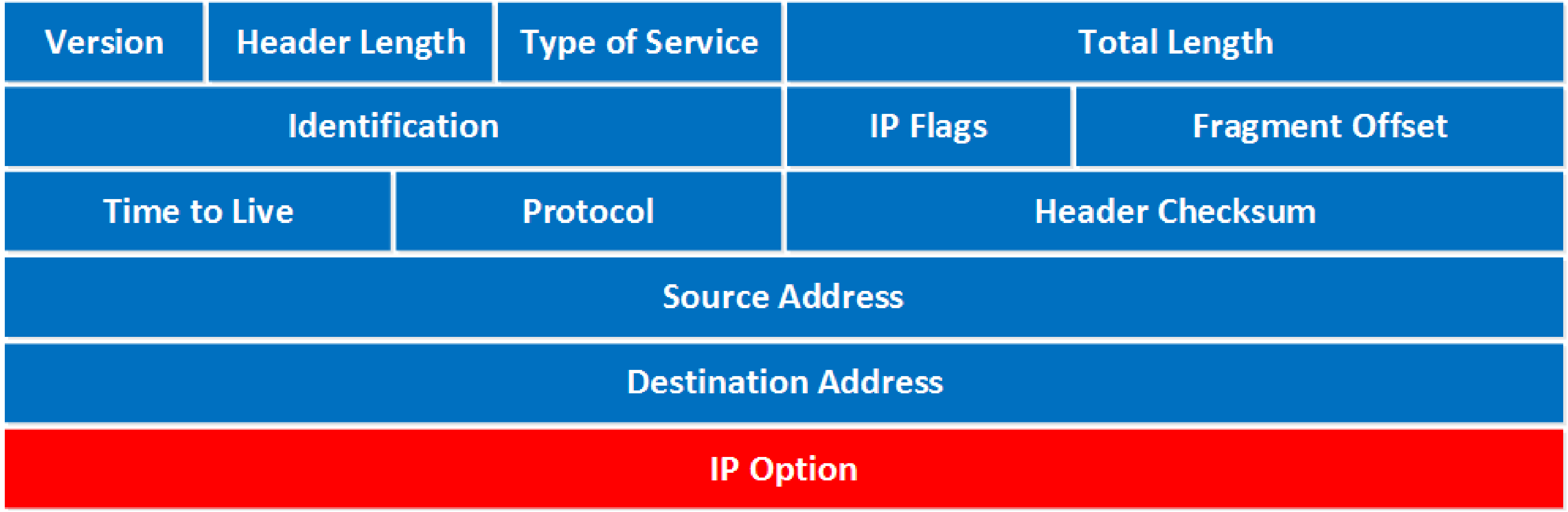
Source Address

Destination Address

IP Option

- Version (4 bits): Indicates the version of the IP protocol. For IPv4, this field always has a value of 4.
- Header Length (4 bits): Specifies the length of the header in 32-bit words (number of 32-bits). The minimum value is 5, indicating a header length of 20 bytes. If options are included, this value will be greater than 5.
- Total Length (16 bits): Specifies the entire packet size, including both the header and data, in bytes. The maximum length is 65,535 bytes.
- Identification (16 bits): This field is used for uniquely identifying the fragments of an original IP packet (same data, same ID) when fragmentation occurs. It helps reassemble the fragments at the destination.

Internet Protocols: IPv4 (3/7)



Version | Header Length | Type of Service | Total Length

Identification | IP Flags | Fragment Offset

Time to Live | Protocol | Header Checksum

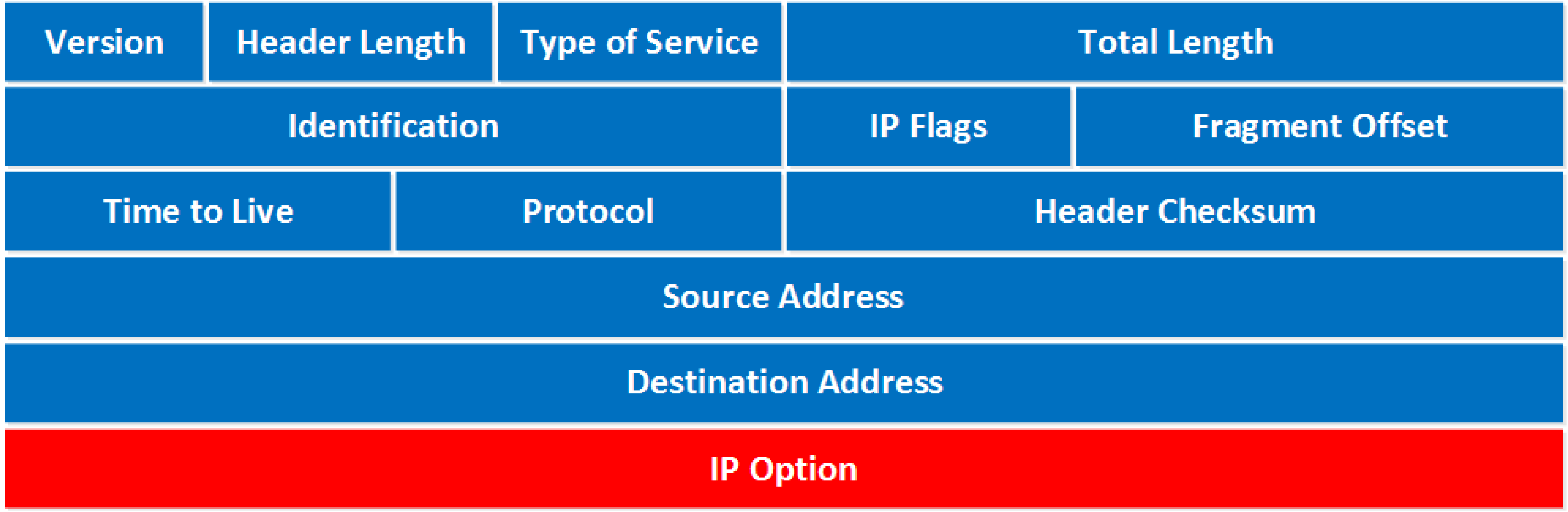
Source Address

Destination Address

IP Option

- Fragment Offset (13 bits): Specifies the position of a fragment in the original packet. This is used during reassembly to correctly order fragments.
- Time to Live (8 bits) limits the lifespan of a packet by decrementing with each hop; when it reaches zero, the packet is discarded to prevent infinite looping in the network. From 64 or 128
- Protocol (8 bits): Indicates the transport layer protocol used in the data portion of the packet, such as TCP (value 6) or UDP (value 17). This allows the receiving device to know how to process the payload.
- Header Checksum (16 bits): A checksum value used for error-checking the header. It ensures that the header has not been corrupted during transmission.

Internet Protocols: IPv4 (4/7)



Version | Header Length | Type of Service | Total Length

Identification | IP Flags | Fragment Offset

Time to Live | Protocol | Header Checksum

Source Address

Destination Address

IP Option

- Source Address (32 bits): The IP address of the originating device sending the packet.
- Destination Address (32 bits): The IP address of the intended recipient device.
- IP Options (variable length): This field is optional and may include additional control information (e.g., security options, timestamp, etc.). Multiple of 32 bits in length

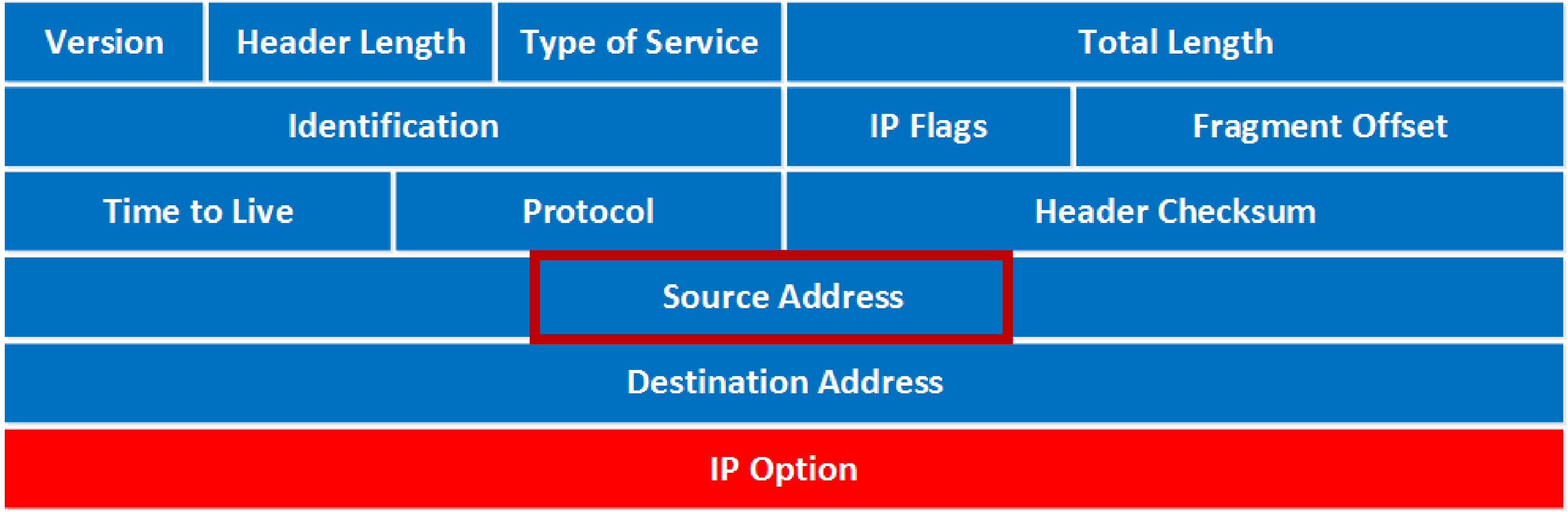
Internet Protocols: IPv4 (5/7)

Vulnerability Background:

- If Bob annoys Alice by calling her hundreds of times a day, Alice can simply block Bob's phone number using her smartphone's block feature.

- However, if Bob knows how to alter his caller ID, he can continue calling Alice from what appear to be different numbers. This forces Alice to answer, as the calls could be important, making it much harder for her to avoid picking up Bob’s phone call.

Internet Protocols: IPv4 (6/7)



Version

Header Length

Type of Service

Total Length

Identification

IP Flags

Fragment Offset

Time to Live

Protocol

Header Checksum

Source Address

Destination Address

IP Option

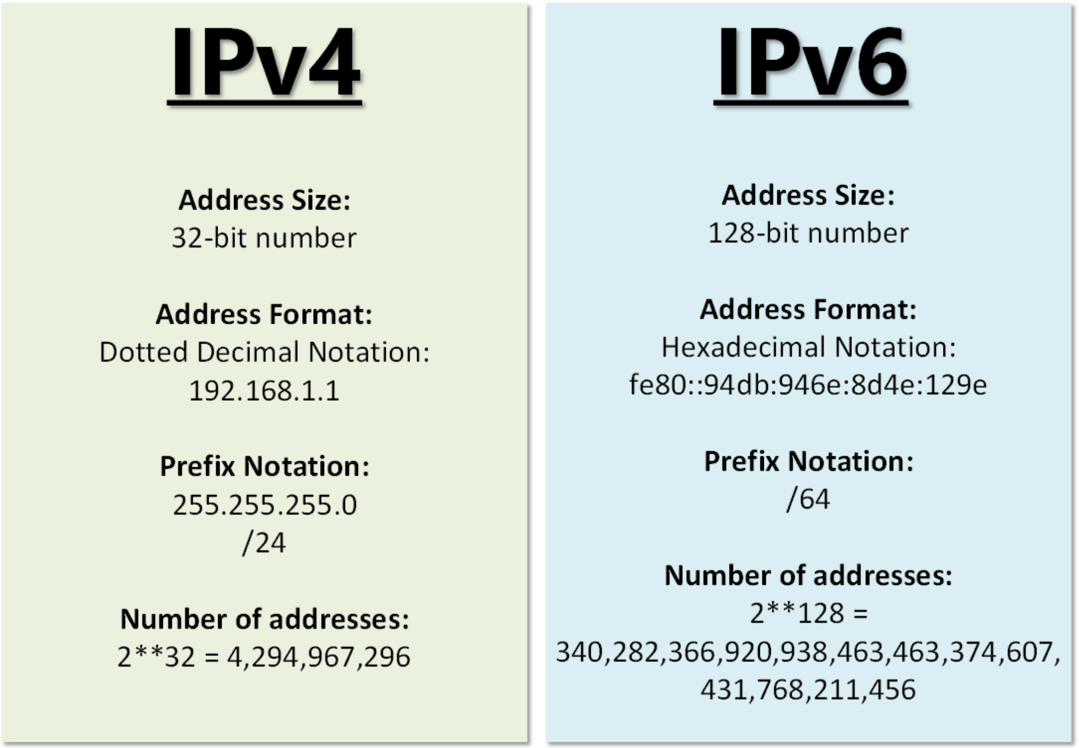
Address Spoofing: No authentication on source IP address

- Description: Attackers can forge the source IP address in packets, making it appear as though the packet originates from a trusted source.
- Impact: This can lead to various attacks, including Denial of Service (DoS) attacks where the attacker impersonates a legitimate user or device.

Internet Protocols: IPv4 (7/7)

- Step 1: Crafting and Launching the Attack. The attacker initiates the DoS attack by creating packets with forged source IP addresses. These addresses can belong to legitimate users or trusted services. The attacker sends a large volume of these packets to the target server or network (victim). The use of forged IPs makes it appear as though the traffic originates from multiple sources, masking the actual attacker.
- Step 2: Flooding the Target Server. The target server receives a flood of packets and tries to respond to the forged IP addresses. If these forged addresses belong to real devices, those devices may receive unexpected replies from the server. This can confuse those devices or even lead to an unintended amplification of the attack. However, the primary victim of this step is still the target server, which must handle all incoming requests and outgoing responses.
- Step 3: Overloading the Target Server. The target server becomes overwhelmed as it struggles to process the massive volume of requests and send replies. This exhausts critical resources, such as bandwidth, CPU, or memory. As a result, the server is unable to handle legitimate traffic, causing delays or a complete denial of service for its legitimate users.

Internet Protocols: IPv6 (1/4)

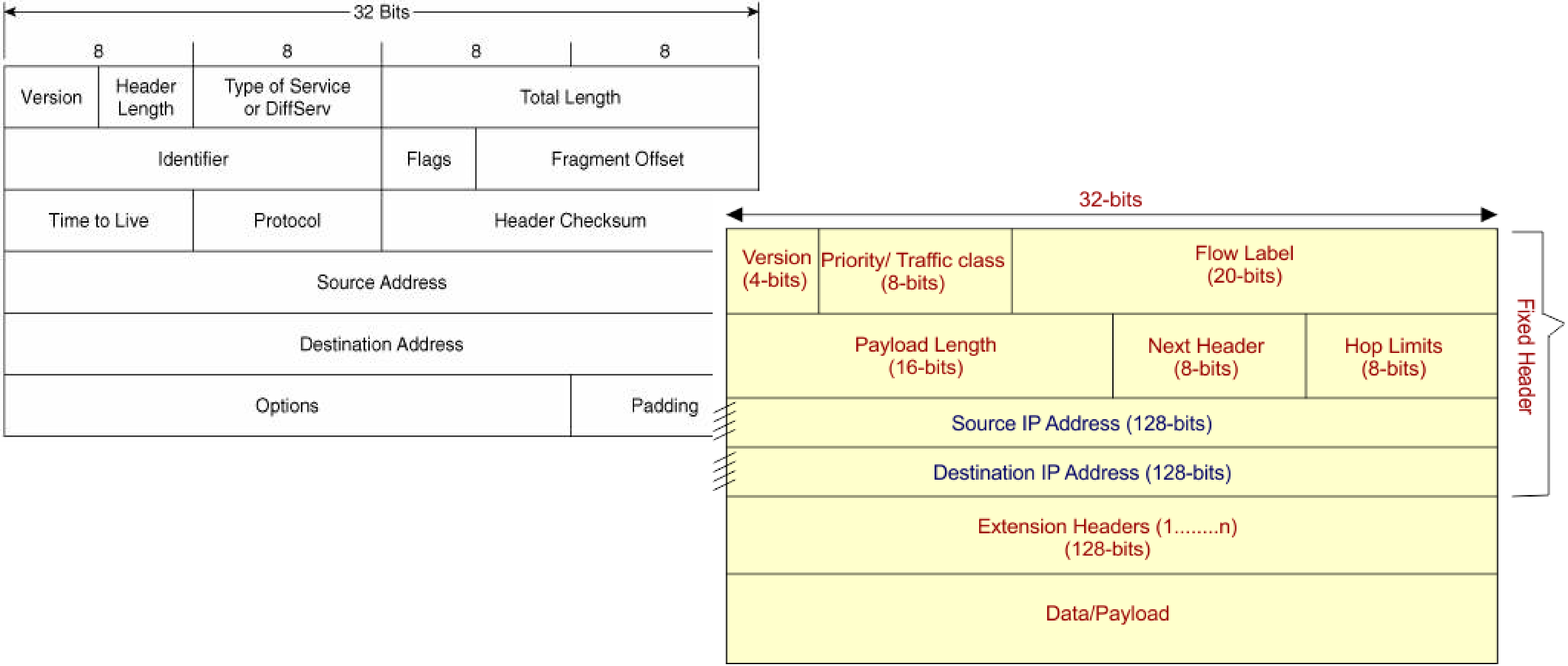


IPv4	IPv6
Address Size: 32-bit number	**Address Size:** 128-bit number
Address Format: Dotted Decimal Notation: 192.168.1.1	**Address Format:** Hexadecimal Notation: fe80::94db:946e:8d4e:129e
Prefix Notation: 255.255.255.0 /24	**Prefix Notation:** /64
Number of addresses: 2**32 = 4,294,967,296	**Number of addresses:** 2**128 = 340,282,366,920,938,463,463,374,607, 431,768,211,456

- The main motivation for IPv6 was due to the small number of IPv4 addresses. It became a pressing issue as the internet expanded globally to support the larger number of internet-connected devices, especially with the growth of mobile devices, IoT, and more users worldwide.

- IPv6 also provides manageable and future-proof solutions to meet the demands of the evolving internet.

Internet Protocols: IPv6 (2/4)



32 Bits

8 8 8 8

Version | Header Length | Type of Service or DiffServ | Total Length

Identifier | Flags | Fragment Offset

Time to Live | Protocol | Header Checksum

Source Address

Destination Address

Options | Padding

32-bits

Version (4-bits) | Priority/ Traffic class (8-bits) | Flow Label (20-bits)

Payload Length (16-bits) | Next Header (8-bits) | Hop Limits (8-bits)

Source IP Address (128-bits)

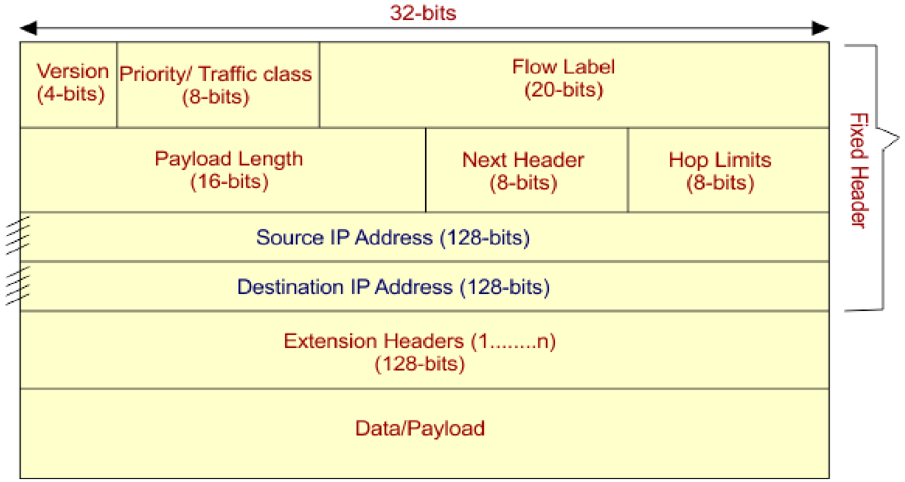
Destination IP Address (128-bits)

Extension Headers (1........n) (128-bits)

Data/Payload

Fixed Header

Internet Protocols: IPv6 (3/4)



32-bits

Version (4-bits)

Priority/ Traffic class (8-bits)

Flow Label (20-bits)

Payload Length (16-bits)

Next Header (8-bits)

Hop Limits (8-bits)

Source IP Address (128-bits)

Destination IP Address (128-bits)

Extension Headers (1........n) (128-bits)

Data/Payload

Fixed Header

- Simplified Header Structure: IPv6 reduces the number of fields in the base header from 14 to 8, resulting in faster processing and streamlined routing.
- Removal of Unnecessary Fields Using Extension Headers: IPv6 removes fields like fragmentation and options, which are now handled only when needed through extension headers, reducing the default header size and router workload.
- Expanded Address Fields: IPv6 uses 128-bit addresses instead of 32-bit, vastly increasing the number of available IP addresses to accommodate the growing number of devices.

Internet Protocols: IPv6 (4/4)

Challenge of adopting IPv6

- Compatibility and Transition Challenges: IPv4 and IPv6 are not directly compatible, requiring special mechanisms (like dual-stack or NAT64) for communication. This complicates transitions for organizations with established IPv4 infrastructure, creating resistance to upgrading.
- Cost and Infrastructure Upgrades: Transitioning to IPv6 needs significant investments in compatible hardware, software, and network configurations. The costs and training required for network administrators add to the burden, especially for large organizations and ISPs.
- Limited Immediate Incentive: Many organizations rely on existing IPv4 workarounds, like Network Address Translation (NAT), which reduces the need for IPv6.

Its advantages are mostly infrastructural and don’t provide immediate, noticeable improvements for many users.

Supporting Protocols

Suppose A and B know each party’s IP address, they can run internet protocols for communications. But how to achieve “suppose”?

Supporting Protocols: Overview

Supporting protocols of IPv4:

- Addressing Protocols: These protocols handle the assignment and management of IP addresses. Examples include the Address Resolution Protocol (ARP), which maps IP addresses to MAC addresses, and the Dynamic Host Configuration Protocol (DHCP), which dynamically assigns IP addresses to devices on a network.
- Diagnostic Protocols: These protocols are used for testing and troubleshooting network connectivity and performance. Common examples include the Internet Control Message Protocol (ICMP), which is used for error messages and diagnostics (like the ping command), and the Traceroute protocol, which helps identify the path packets take through the network.
- Routing Protocols: These protocols facilitate the routing of packets between different networks (managed by different gateway). They determine the best paths for data to travel. Examples include Routing Information Protocol (RIP) and Border Gateway Protocol (BGP).

Supporting Protocols: ARP

To be introduced in the next topic!

Supporting Protocols: DHCP (1/4)

- A gateway is a networking device that serves as a point of access to the internet, allowing a set of devices to connect and communicate with external networks.

- It acts as an intermediary between local networks and the internet, facilitating data transfer and enabling devices to send and receive information outside their own network.

TPM 2.0 Secure Element for True Platform Integrity & Assured Privacy
Quiet low-power operation with no moving parts
FastLane Model 8000
Gig Ethernet with true POE+ 802.3at OUT Power Source
Separated Interfaces for Segmented Network Security
Gig Ethernet with true POE+ 802.3at IN Powered Device
Easy In-Line Installation with Full Self-Power & Integrated Wall Mount
PoE PSE
PoE PD
1
2
3
4
5

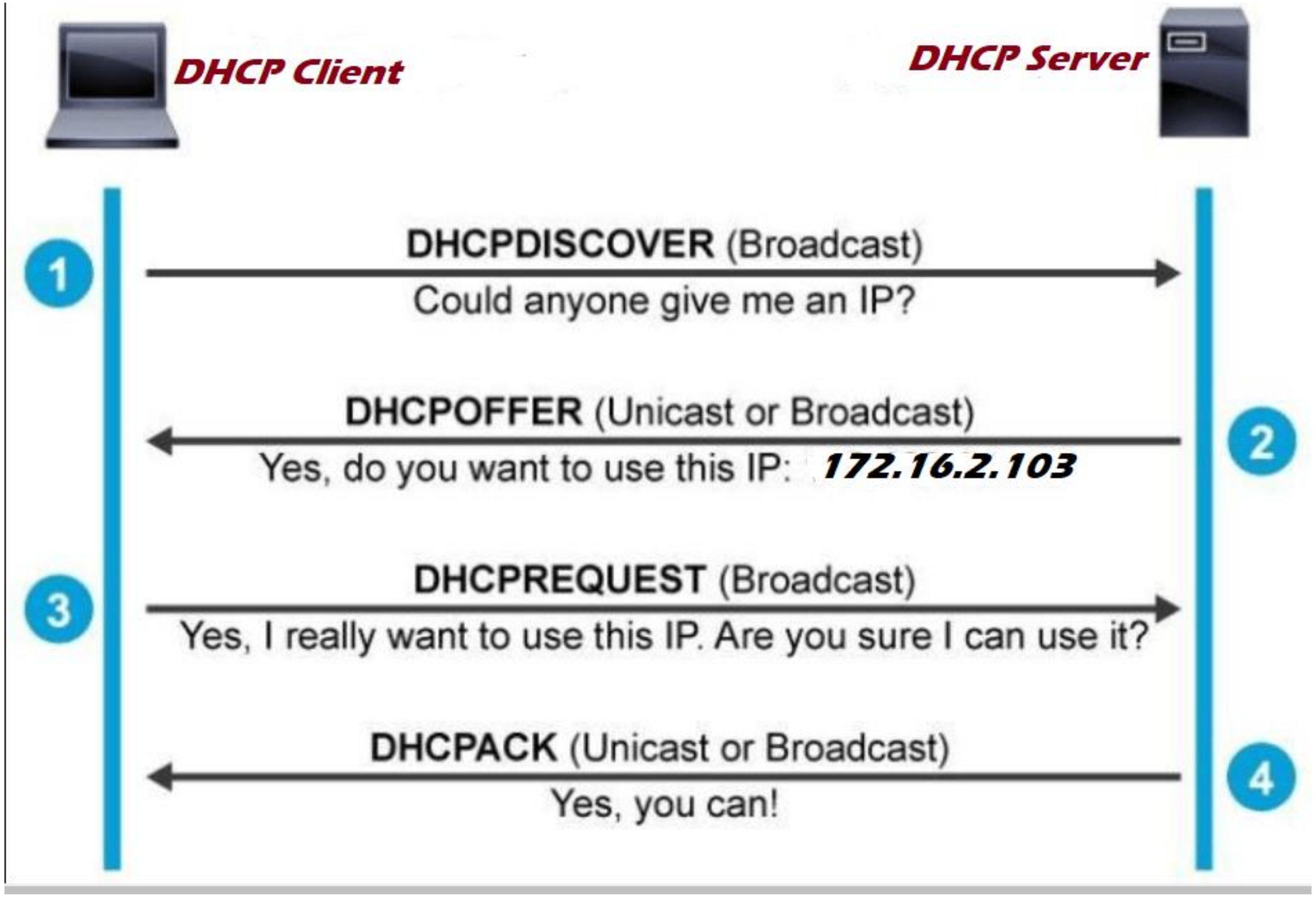
Supporting Protocols: DHCP (2/4)

DHCP Protocol Description:

- When a device connects to the network, it sends a DHCP Discover message to find available DHCP servers.
- The DHCP server responds with a DHCP Offer, which includes an available IP address and other configuration information.
- The client then sends a DHCP Request message to accept the offer, and the server sends a DHCP Acknowledgment to confirm the assignment.

Benefits: This dynamic allocation helps manage IP address space efficiently, as devices can receive different IP addresses each time they connect, and unused addresses can be reassigned to other devices.

Supporting Protocols: DHCP (3/4)


DHCP Client
DHCP Server
1
DHCPDISCOVER (Broadcast)
Could anyone give me an IP?
2
DHCPOFFER (Unicast or Broadcast)
Yes, do you want to use this IP: 172.16.2.103
3
DHCPREQUEST (Broadcast)
Yes, I really want to use this IP. Are you sure I can use it?
4
DHCPACK (Unicast or Broadcast)
Yes, you can!

Supporting Protocols: DHCP (4/4)

Vulnerability: DHCP spoofing is a type of network attack where an unauthorized (or rogue) DHCP server is set up by an attacker on a network. This rogue server can respond to DHCP requests from clients instead of the legitimate DHCP server.

- Client Request: When a device (client) connects to a network, it sends a DHCP Discover message to locate available DHCP servers.
- Rogue Server Response: The attacker's rogue DHCP server responds with a DHCP Offer that includes a malicious or incorrect IP address and network configuration settings (such as the default gateway and DNS server).
- Client Acceptance: The client accepts the offer and configures itself with the settings provided by the rogue server, believing it to be legitimate.

Potential Consequences: Denial of Service (DoS), Network Interception

Supporting Protocols: ICMP (1/4)

- ICMP (Internet Control Message Protocol) is a core protocol of the Internet Protocol Suite, primarily used for sending error messages and operational information. It operates at the network layer and is essential for network diagnostics and management.

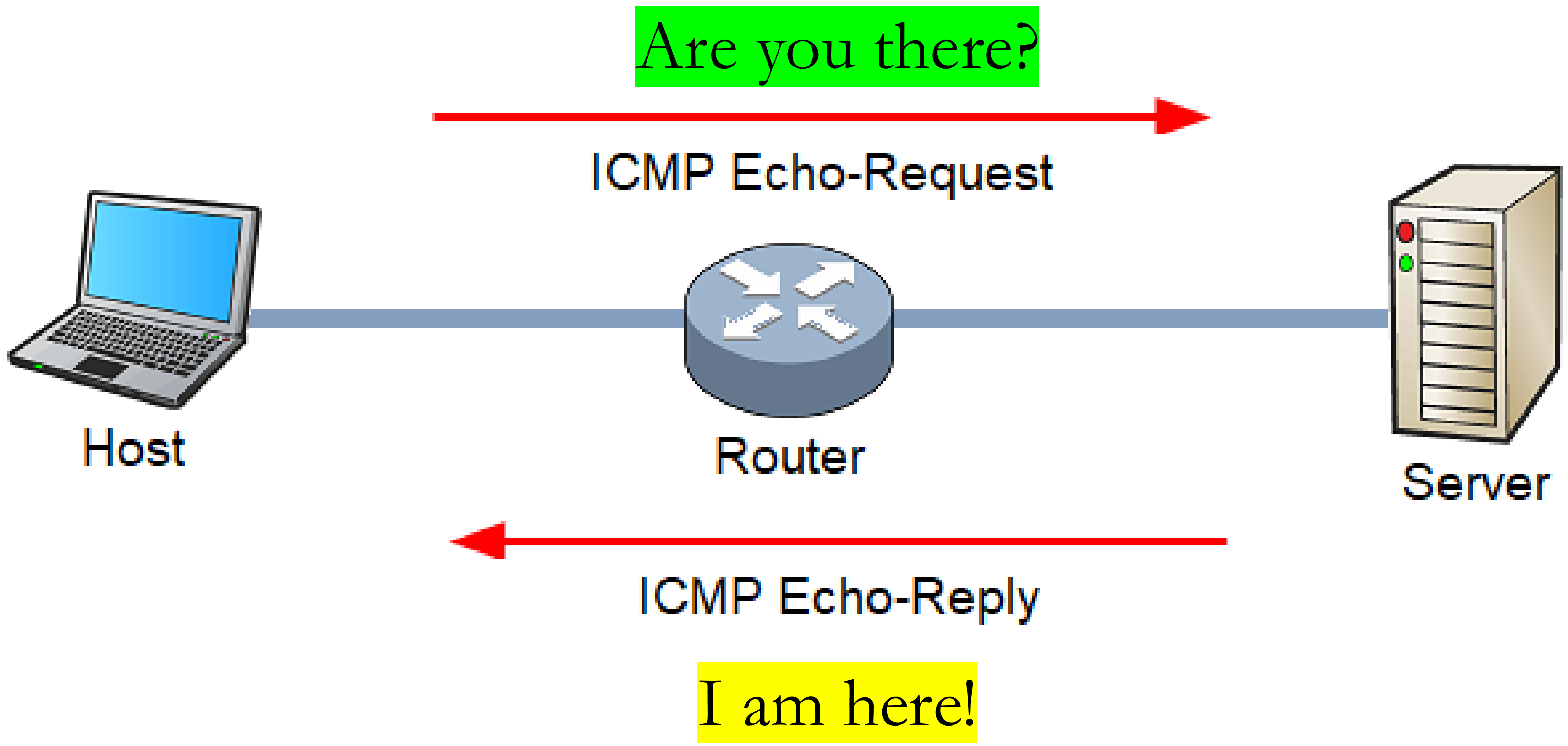
- Key Functions of ICMP
  - □Error Reporting: ICMP communicates issues like unreachable destinations, time exceeded for packet delivery, and other network errors.

  - □Network Diagnostics: It provides tools for network troubleshooting and performance monitoring, allowing administrators to assess network health.

Supporting Protocols: ICMP (2/4)

- One of the most well-known functions of ICMP is the ping utility, which is used to test the reachability of a host on a network.
- How Ping Works: When a user issues a ping command, the device sends an ICMP Echo Request message to the target IP address. If the target device is reachable and operational, it responds with an ICMP Echo Reply message.
- Purpose of Ping:
  - □Reachability Testing: Ping checks whether a particular IP address is active and responsive.
  - □Round-Trip Time Measurement: It measures the time it takes for the Echo Request to reach the target and for the Echo Reply to return, providing an indication of network latency.

Supporting Protocols: ICMP (3/4)



The ping protocol requires the server to unconditionally answer messages --> attack!

Supporting Protocols: ICMP (4/4)

ICMP Flooding (Denial-of-Service Attack):

- Description: Attackers send a high volume of ICMP Echo Request (ping) packets to overwhelm a target system's resources, leading to degraded performance or complete unresponsiveness.
- Impact: This can cause significant network disruption, making services unavailable and impacting overall network stability.

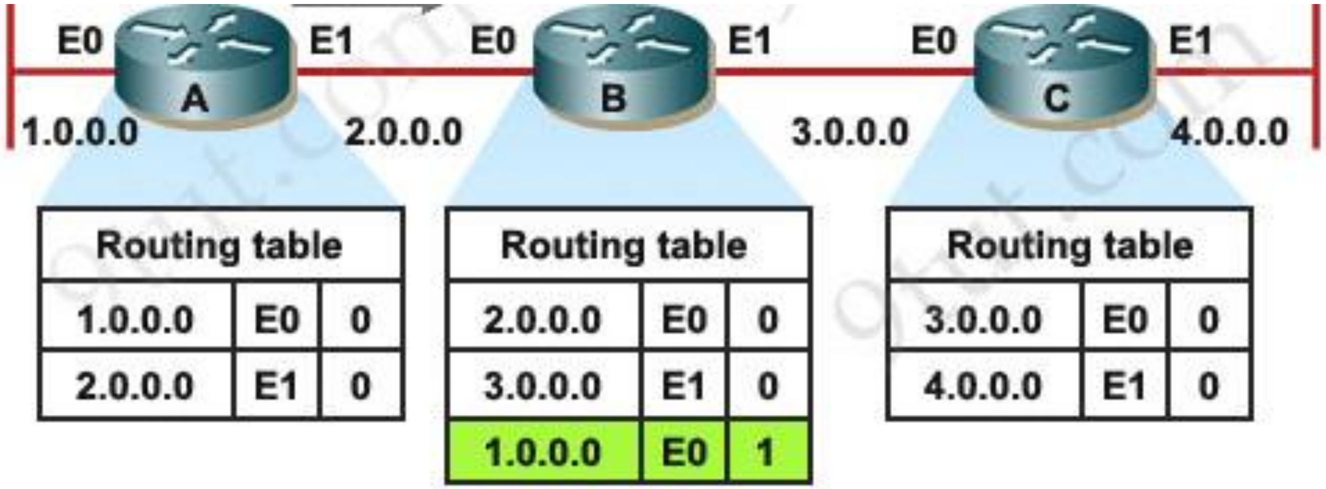
Ping of Death:

- Description: Exploits vulnerabilities in a system's handling of oversized ICMP packets, which can cause (old systems) crashes (Lack of Size Checking).
- Impact: This can lead to system crashes or reboots, affecting the availability and reliability of network services.

Supporting Protocols: RIP (1/4)

RIP (Routing Information Protocol): The RIP is a dynamic routing protocol that allows routers to

- exchange information about their connected networks and
- find optimal paths to reach different destinations.



Routing table		
1.0.0.0	E0	0
2.0.0.0	E1	0

Routing table		
2.0.0.0	E0	0
3.0.0.0	E1	0
1.0.0.0	E0	1

Routing table		
3.0.0.0	E0	0
4.0.0.0	E1	0

Supporting Protocols: RIP (2/4)

Router A<==> B <==> C are in a network, each connected to different subnetworks.

- Router A advertises its routing table to Router B, which contains a route to its connected network with a hop count (unit of distance) of 1.
- Router B receives this update, adds 1 to the hop count, and updates its table if this is a better route.
- Router B then advertises its updated table to neighbours Router C and Router A. Router A may receive updates about networks it doesn’t directly connect to.
- If any route is lost (e.g., Router B loses connection with Router D for example), Router B sends a triggered update marking the route as unreachable (with a hop count of 16), allowing other routers to update their tables promptly.

Supporting Protocols: RIP (3/4)

RIP is vulnerable to several attacks due to its simplicity and lack of robust authentication:

1. RIP Spoofing Attack (Route Injection)

How it works: In a RIP spoofing attack, an attacker sends fake RIP update messages to a router, claiming to have a route to certain networks with a low hop count. This misleads the router into using the attacker's route to reach those destinations.

Impact: The router redirects traffic through the attacker, enabling a Man-in-the-Middle (MitM) attack where the attacker can intercept, modify, or discard the traffic. This attack can result in data breaches, loss of confidentiality, and potential service disruptions.

Supporting Protocols: RIP (4/4)

2. Route Poisoning Attack

How it works: In route poisoning, the attacker sends RIP messages with a hop count of 16 (indicating that a route is unreachable) for specific networks. This tricks routers into marking legitimate routes as invalid.

Impact: This leads to denial of service (DoS) on affected networks, as routers will remove these routes from their tables, blocking legitimate traffic from reaching its intended destination.

Supporting Protocols: BGP (1/3)

BGP is another routing protocol.

- BGP (Border Gateway Protocol): Designed for large-scale inter-network routing, especially between Autonomous Systems (AS) on the internet. It is primarily used by ISPs and large organizations to manage routes across different administrative domains.

- RIP (Routing Information Protocol): Created for smaller, internal networks (Local Area Networks, or LANs) such as within one AS by one ISP. RIP is simple and used in smaller networks where complex routing policies and scalability aren't a priority.

Supporting Protocols: BGP (2/3)

Similarities (BGP VS RIP) in the Process

Route Advertisement: Like other protocols, BGP routers advertise their routing tables to neighboring routers.

Table Updates: Each router evaluates received routes, updates its routing table based on the received information, and propagates this information to its neighbors.

Handling Route Changes: When routes become unreachable, BGP routers notify their peers to ensure all routers maintain accurate and up-to-date routing information.

Key Difference: Path-Vector Mechanism in BGP. This mechanims allows it to function effectively in larger, more complex networks, particularly for inter-domain routing on the internet.

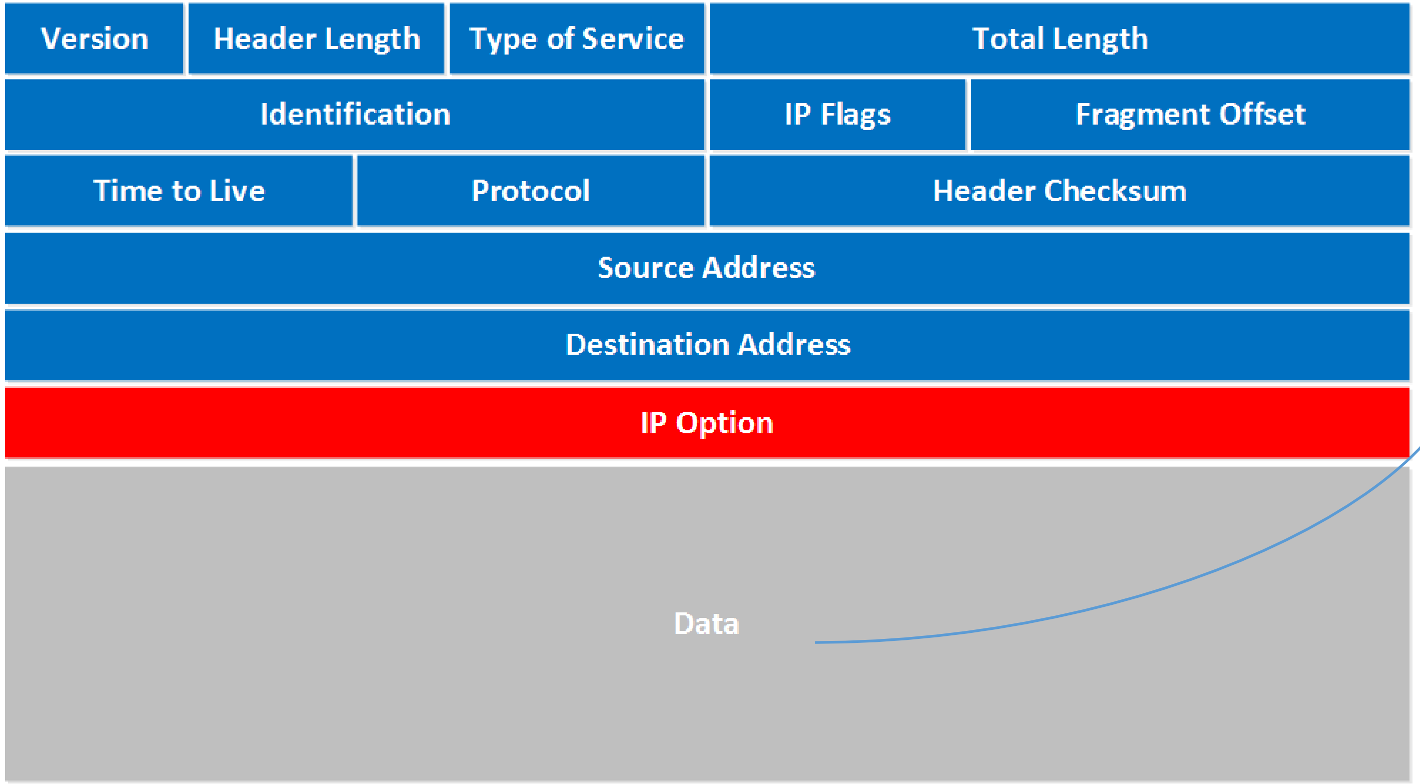
Supporting Protocols: BGP (3/3)

- Session Hijacking specifically refers to the unauthorized takeover of a session between a user and a server from a different network. This takeover can happen during a MitM attack when an attacker captures session identifiers (like cookies or tokens) while intercepting the communication between the user and the server.
- Session hijacking can occur through BGP vulnerabilities because BGP operates on a trust-based model, allowing routers to accept route updates without strict authentication. An attacker (ISP for example) can hijack routes by advertising fake paths for IP prefixes they don't own, redirecting traffic through their own router. This enables the attacker to intercept sensitive information, such as session tokens, which can then be used to take over legitimate user sessions.

IPsec

How to secure internet protocols?

IPsec: Background (1/7)



Datagram of IPv4

Data (Payload)

- could be saw
- could be modified

IPsec: Background (2/7)

- IPsec (Internet Protocol Security) is a suite of protocols designed to secure Internet Protocol (IP) communications by providing authentication, integrity, and confidentiality at the network layer.
- The development of IPsec began in the early 1990s and was standardized in in 1998. IPsec gained widespread adoption in the late 1990s and early 2000s, becoming a fundamental technology for Virtual Private Networks (VPNs) and secure site-to-site communications.
- For VPN, IPsec's ability to secure all applications with a single configuration is a significant advantage over TLS, which requires separate setups for each application.

IPsec: Background (3/7)

Two communication modes by IPsec:

- Transport Mode. In this mode, only the payload (data) of the original IP packet is encrypted or authenticated. The original IP header is not changed. This mode is often used for end-to-end communication between two hosts, where both endpoints support IPsec. (A sends to B)
- Tunnel Mode. In this mode, the entire original IP packet (including both the header and the payload) is encapsulated within a new IP packet. A new IP header is added for routing. This mode is commonly used for Virtual Private Networks (VPNs), especially in site-to-site configurations, where two networks are securely connected over an untrusted network like the Internet. (A sends to C that is fowarded to B)

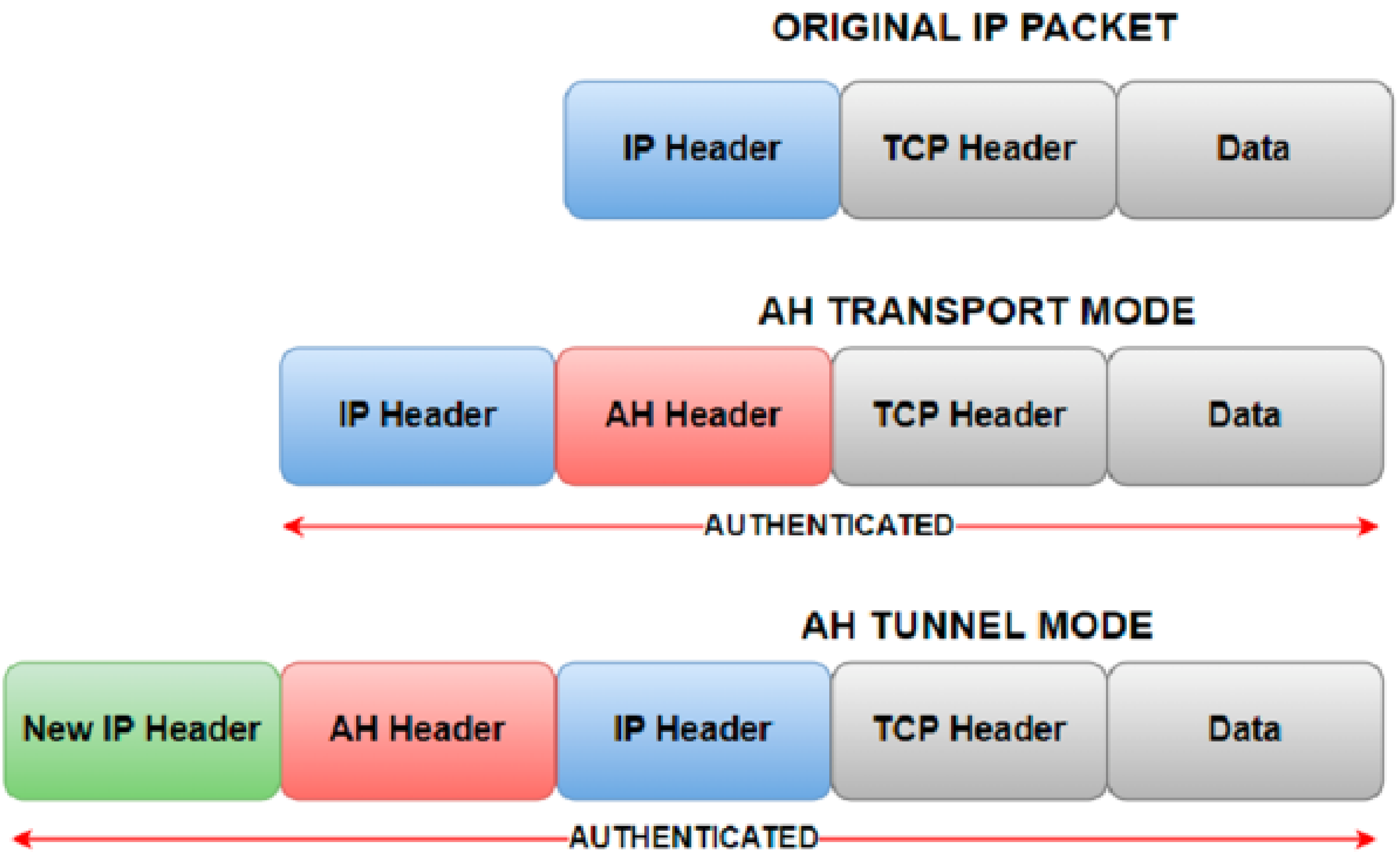
IPsec: Background (4/7)

Two different security protections from IPsec:

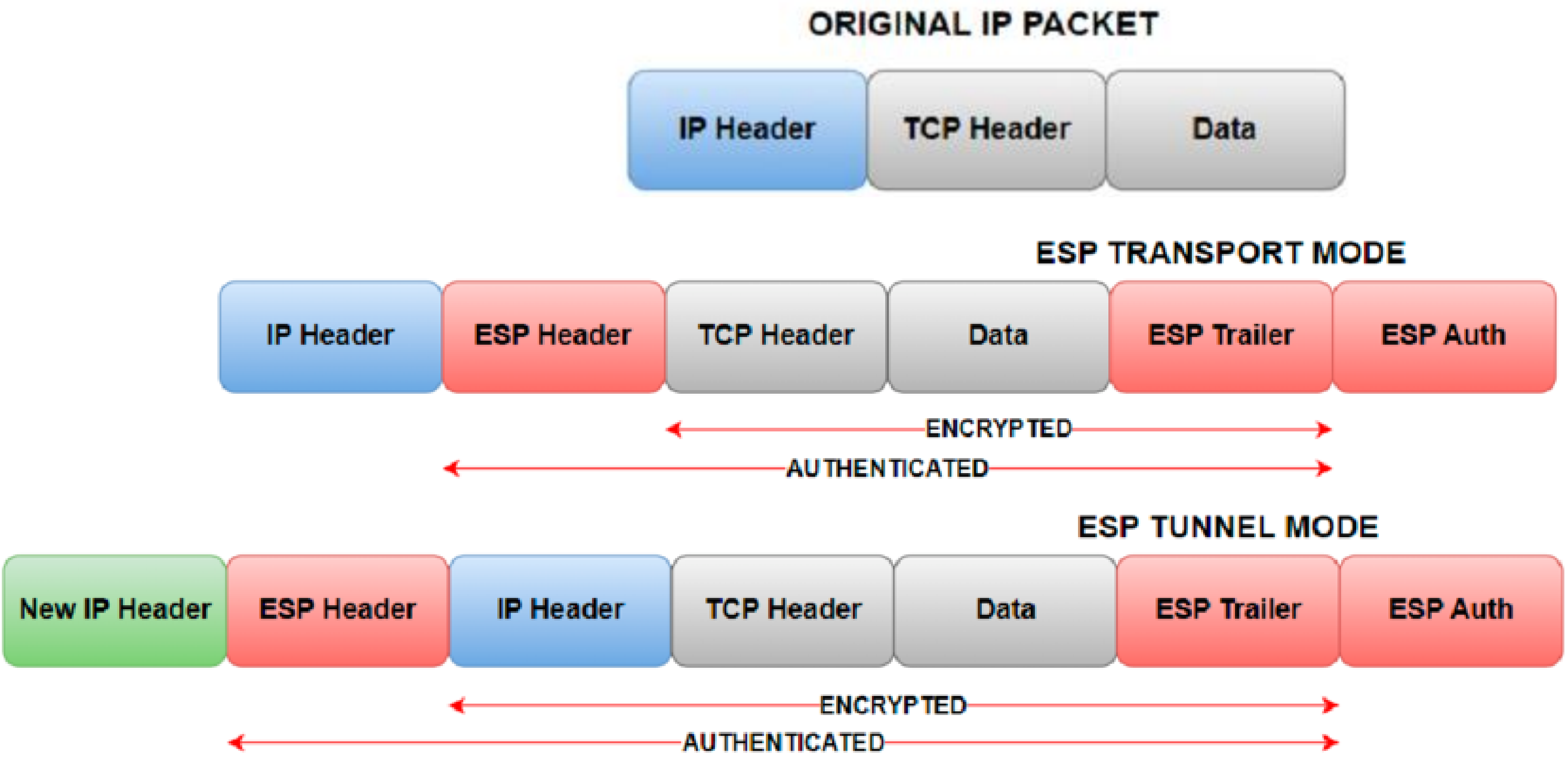
- Authentication Header (AH): This component provides integrity and authentication for the data, ensuring the packet hasn't been tampered and verifying the sender's identity. AH does not provide encryption, so it's useful for scenarios where data confidentiality isn't required. integrity

- Encapsulating Security Payload (ESP): ESP offers encryption for data confidentiality, along with optional integrity and authentication. ESP is typically used for scenarios that require secure, private communication, as it protects both the payload and offers optional tamper-proofing. confidentiality+ integrity

IPsec: Background (5/7)



IPsec: Background (6/7)



ORIGINAL IP PACKET

IP Header | TCP Header | Data

ESP TRANSPORT MODE

IP Header | ESP Header | TCP Header | Data | ESP Trailer | ESP Auth

ENCRYPTED

AUTHENTICATED

ESP TUNNEL MODE

New IP Header | ESP Header | IP Header | TCP Header | Data | ESP Trailer | ESP Auth

ENCRYPTED

AUTHENTICATED

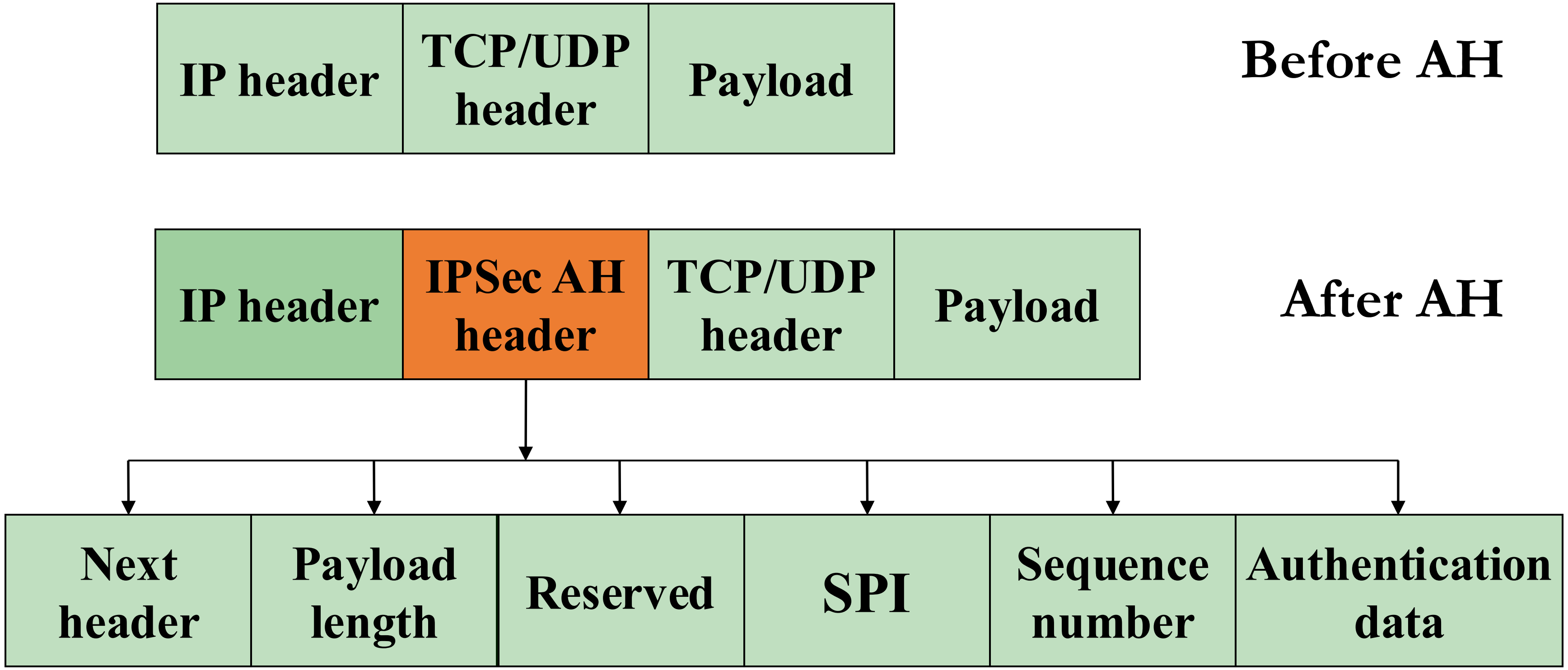
IPsec: Background (7/7)

Two main components in IPsec:

- Internet Key Exchange (IKE): IKE is a protocol for establishing Security Associations and managing keys. It automates the process of negotiating and setting up SAs, which include choosing encryption methods, exchanging keys securely, and refreshing keys periodically to maintain security.

- Security Associations (SA): The SA is a set of policies and keys established between two IPSec endpoints to define how traffic will be handled. Each SA is unidirectional and determines the specific security protocols (AH or ESP), encryption and authentication methods, and keys to be used for that connection.

IPsec: AH&Transport (1/3)

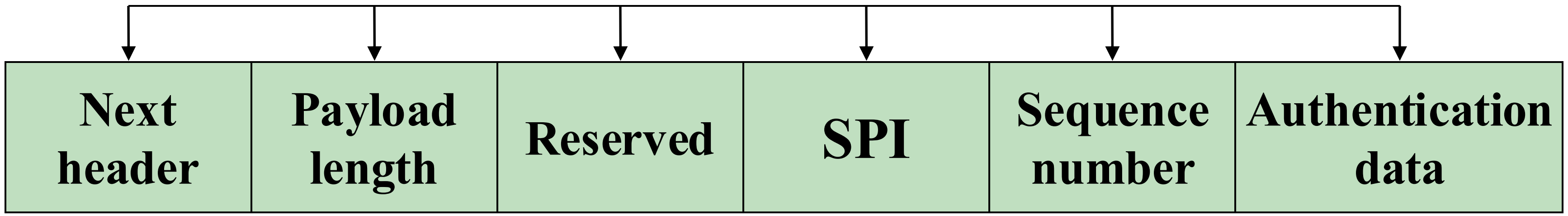


IP header | TCP/UDP header | Payload — Before AH

IP header | IPSec AH header | TCP/UDP header | Payload — After AH

Next header | Payload length | Reserved | SPI | Sequence number | Authentication data

IPsec: AH&Transport (2/3)



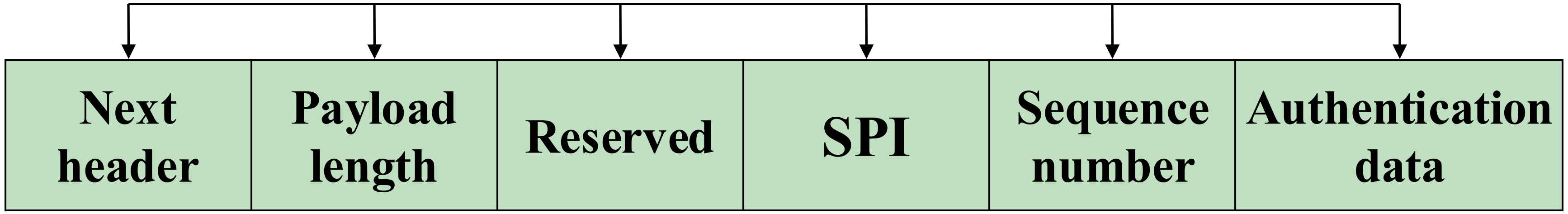
Next header	Payload length	Reserved	SPI	Sequence number	Authentication data

1. Next Header (8 bits): Indicates the type of payload protocol following the AH header (e.g., TCP, UDP). It points to the protocol type of the encapsulated data.

2. Payload Length (8 bits): Specifies the length of the AH header in 32-bit words (including the fields in the header). It helps in identifying where the AH header ends and the payload begins.

3. Reserved (16 bits): This field is reserved for future use and is always set to zero.

IPsec: AH&Transport (3/3)



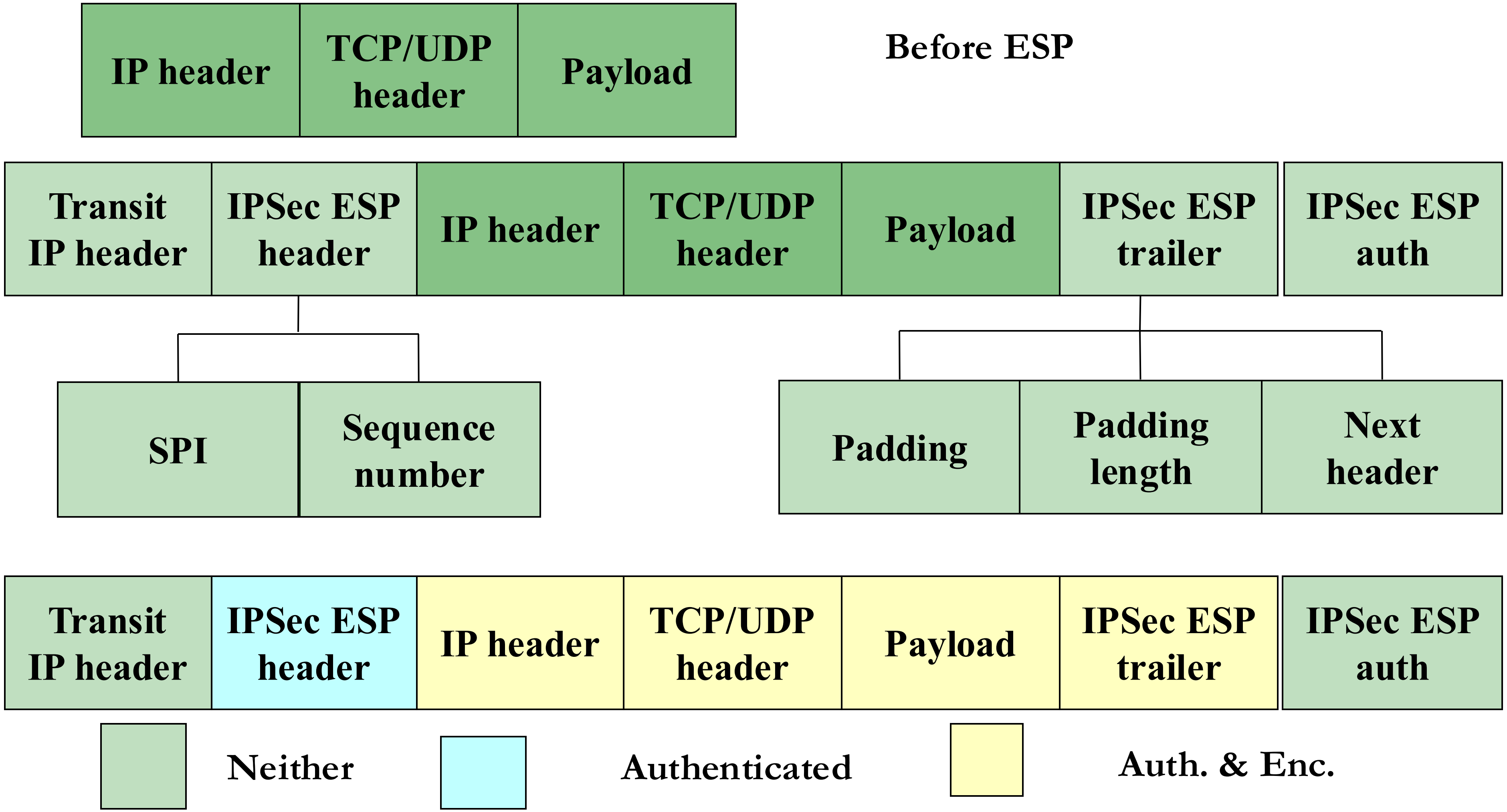
Next header | Payload length | Reserved | SPI | Sequence number | Authentication data

4. Security Parameters Index (SPI) (32 bits): A unique identifier that points to the Security Association (SA) being used. It helps the receiving party know which SA and related keys to use for authentication.

5. Sequence Number (32 bits): A counter that increases with each transmitted packet. It provides replay protection by ensuring that old packets cannot be resent or reordered by attackers.

6. Authentication Data (variable length): This field is used by the receiver to verify the authenticity and integrity of the packet. (part of IP header +AH header + Payload)

IPsec: ESP&Tunnel (1/3)



IP header | TCP/UDP header | Payload

Before ESP

Transit IP header | IPSec ESP header | IP header | TCP/UDP header | Payload | IPSec ESP trailer | IPSec ESP auth

IPSec ESP header: SPI | Sequence number

IPSec ESP trailer: Padding | Padding length | Next header

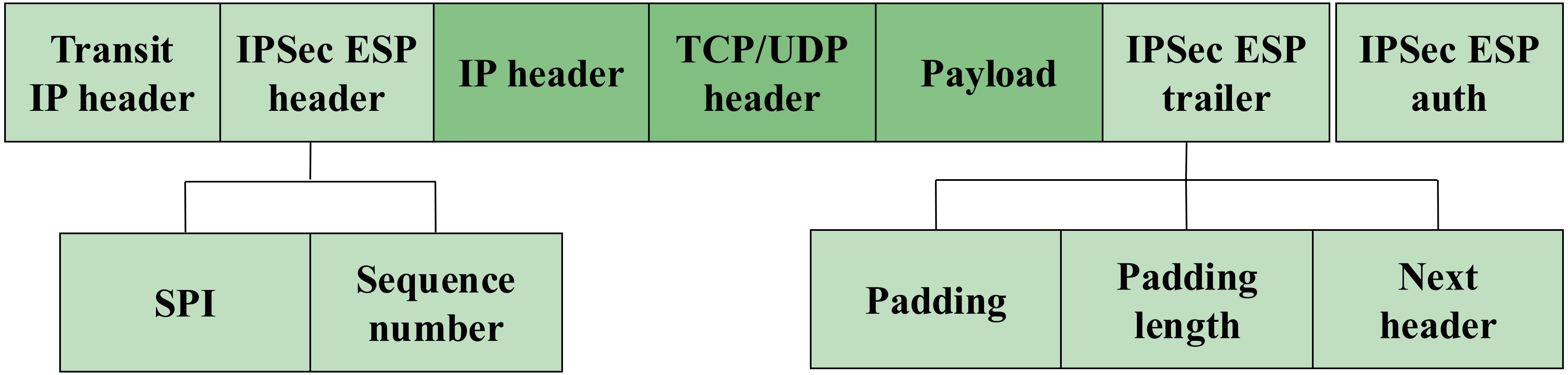
Transit IP header | IPSec ESP header | IP header | TCP/UDP header | Payload | IPSec ESP trailer | IPSec ESP auth

🟩 Neither

🟦 Authenticated

🟨 Auth. & Enc.

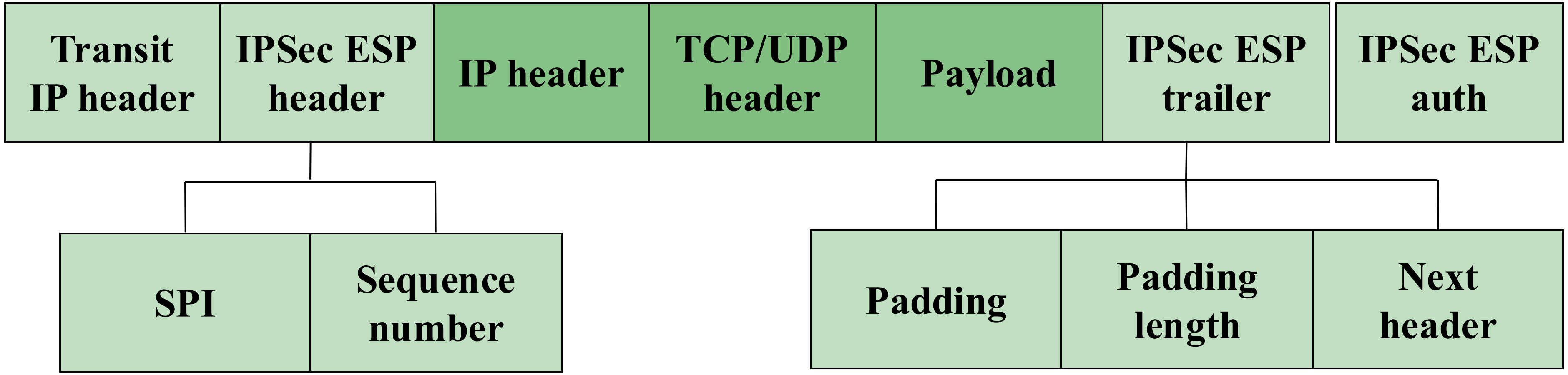
IPsec: ESP&Tunnel (2/3)



- Security Parameters Index (SPI) (32 bits): Identifies the Security Association (SA) used for this ESP packet. This value points to the specific cryptographic keys and algorithms agreed upon for securing the data.

- Sequence Number (32 bits): A counter that increments with each packet sent under a particular SA. It provides replay protection by ensuring that packets can't be reused or reordered by attackers.

IPsec: ESP&Tunnel (3/3)



- Padding and Pad Length (variable length): Padding is used to align the data to a multiple of the encryption algorithm's block size. The Pad Length field specifies the number of padding bytes added.

- Next Header (8 bits): Indicates the type of protocol within the payload data, such as TCP, UDP, or ICMP.

- Authentication Data (variable length, optional): It covers all immutable fields.

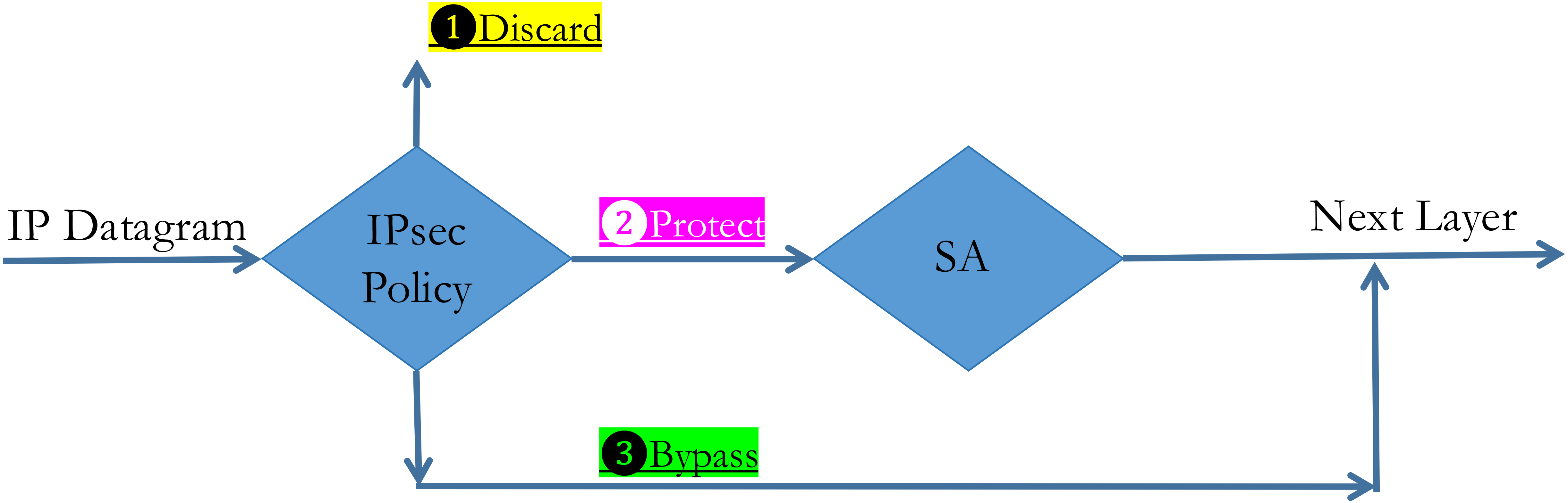
IPsec: SA (1/4)

- IPSec follows a policy-based approach to enforce the local security decisions of a system.

- On input Requirements from administrator, it generates IPsec Policy.
  - Which traffic requires IPsec protection (e.g., IP addresses, or ports).
  - Which IPsec mode to use (Transport or Tunnel).
  - Whether to use ESP or AH for encryption or authentication.

- Essentially, policies are like filters and action plans that decide which packets should trigger IPsec and what type of IPsec protection is required for those packets.

IPsec: SA (2/4)



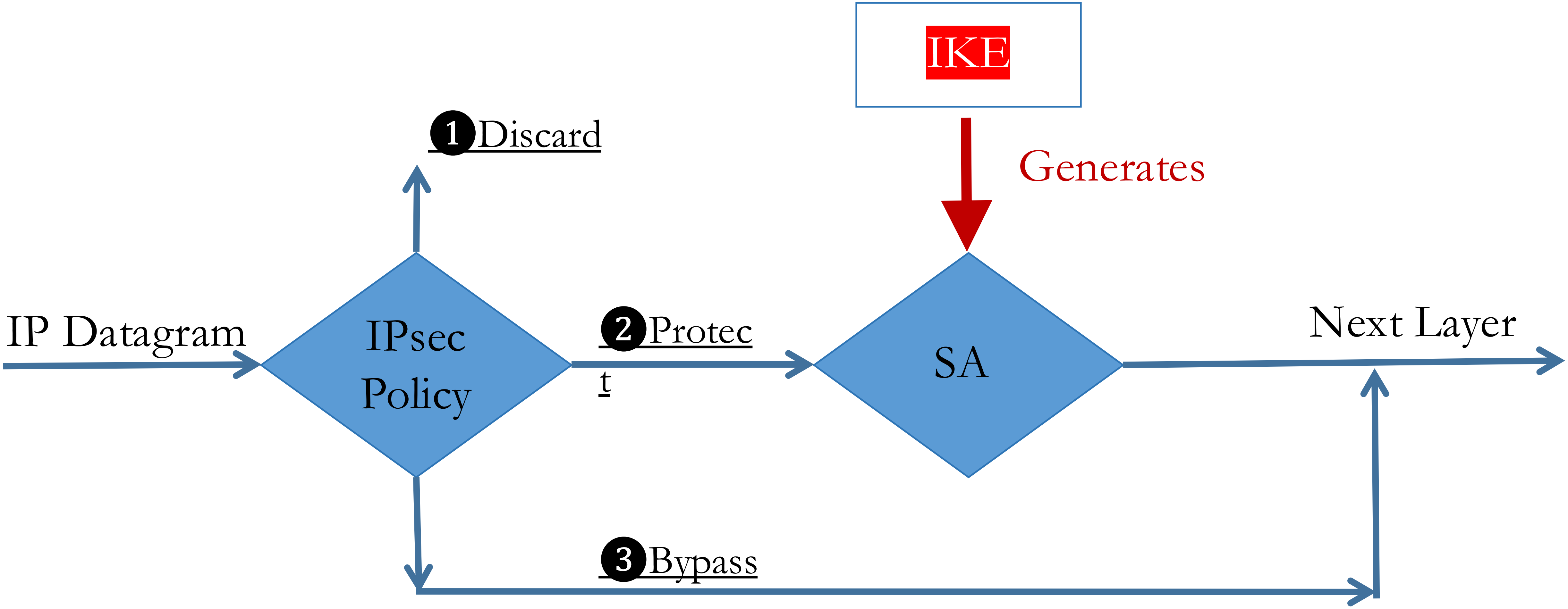
- Discard: Blocks traffic that doesn’t meet policy requirements, deleting it.
- Protect: Secures matching traffic using encryption, authentication, or integrity checks as specified.
- Bypass: Allows trusted traffic to pass without IPsec protection, optimizing performance.

IPsec: SA (3/4)

- A Security Association (SA) in IPsec is a set of parameters and keys that define how traffic will be secured for a specific data flow, both for outgoing traffic and incoming traffic under the Protect decision.

- Components:
  - SPI (Security Parameters Index): A unique identifier for the SA, helping distinguish it among multiple SAs.
  - Cryptographic Algorithms: Specifies the encryption (e.g., AES) and authentication (e.g., SHA-256) algorithms to be used.
  - Keys: Contains encryption and authentication keys generated through protocols like IKE (Internet Key Exchange).
  - Lifetime: Determines how long the SA remains valid before rekeying or re-negotiating.

IPsec: SA (4/4)


IKE
Generates
1 Discard
IP Datagram
IPsec Policy
2 Protect
SA
Next Layer
3 Bypass

IPsec: IKE (1/5)

- Internet Key Exchange (IKE) protocol is responsible for establishing and negotiating the parameters for SAs between two endpoints, including selecting cryptographic algorithms, generating shared keys, and setting lifetimes.

□ Phase 1(Secure channel): IKE first establishes a secure communication channel between the two endpoints by authenticating them and setting up an initial secure-channel SA for IKE itself. This phase ensures that both sides are legitimate and agree on the base security settings.

□ Phase 2(Negotiation): Using the secure IKE channel from Phase 1, IKE negotiates IPsec SAs for actual data protection. During this phase, IKE defines the cryptographic parameters and keys used by IPsec to secure data flow according to the agreed Protect policies.

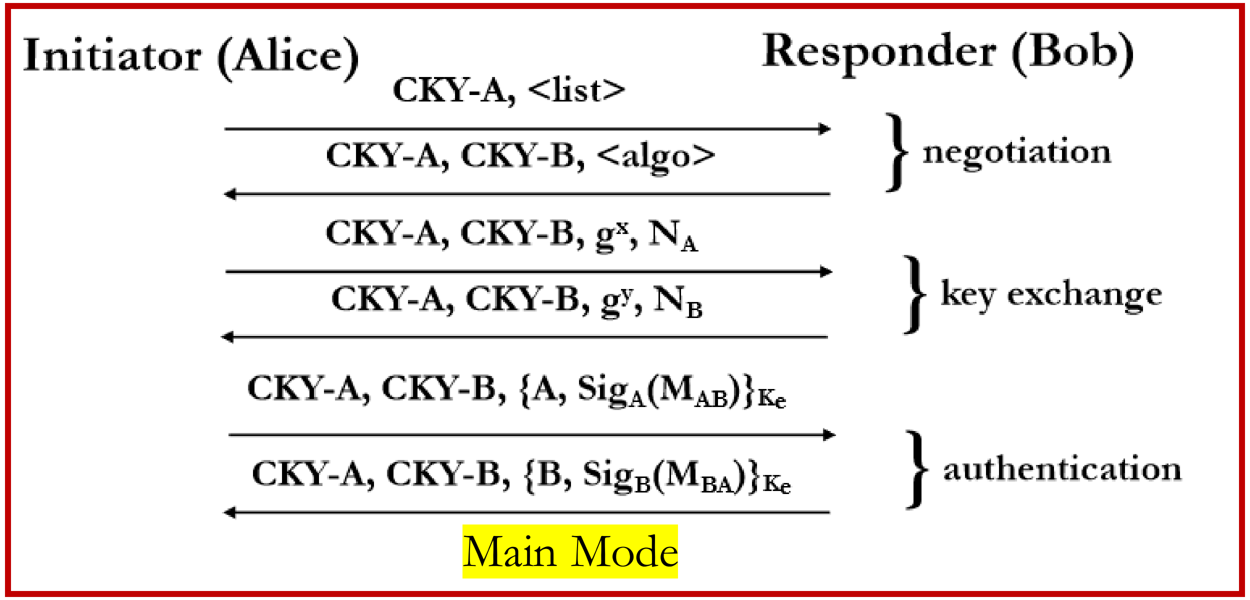
IPsec: IKE (2/5)

Phase 1(Secure channel): IKE first establishes a secure communication channel between the two endpoints by authenticating them and setting up an initial secure-channel SA for IKE itself. This phase ensures that both sides are legitimate and agree on the base security settings.

- □ There are two types of establishment in the phase-1, called *modes*:
  - □ Aggressive mode: mutual authentication and session key establishment in three messages.
  - □ Main mode: uses six messages and has additional functionality such as the ability to hide endpoint identifiers from eavesdroppers.

IPsec: IKE (3/5)

Phase 1



Initiator (Alice)

Responder (Bob)

CKY-A, <list>

CKY-A, CKY-B, <algo>

} negotiation

CKY-A, CKY-B, g^x, N_A

CKY-A, CKY-B, g^y, N_B

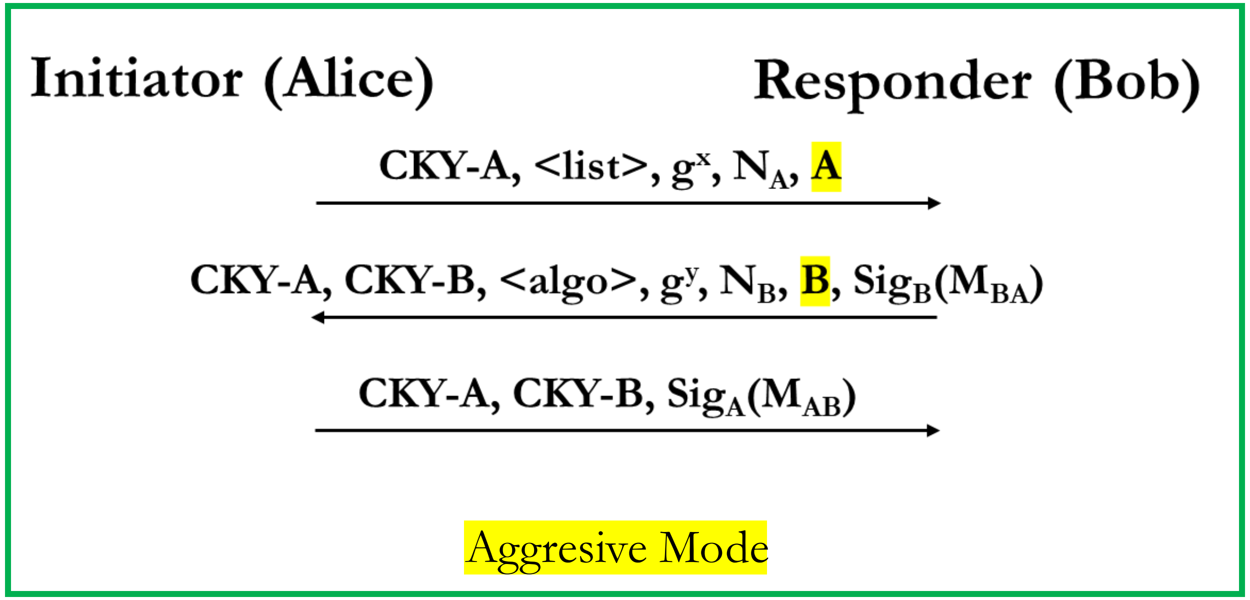
} key exchange

CKY-A, CKY-B, $\{A, Sig_A(M_{AB})\}_{Ke}$

CKY-A, CKY-B, $\{B, Sig_B(M_{BA})\}_{Ke}$

} authentication

Main Mode



Initiator (Alice)

Responder (Bob)

CKY-A, <list>, g^x, N_A, A

CKY-A, CKY-B, <algo>, g^y, N_B, B, $Sig_B(M_{BA})$

CKY-A, CKY-B, $Sig_A(M_{AB})$

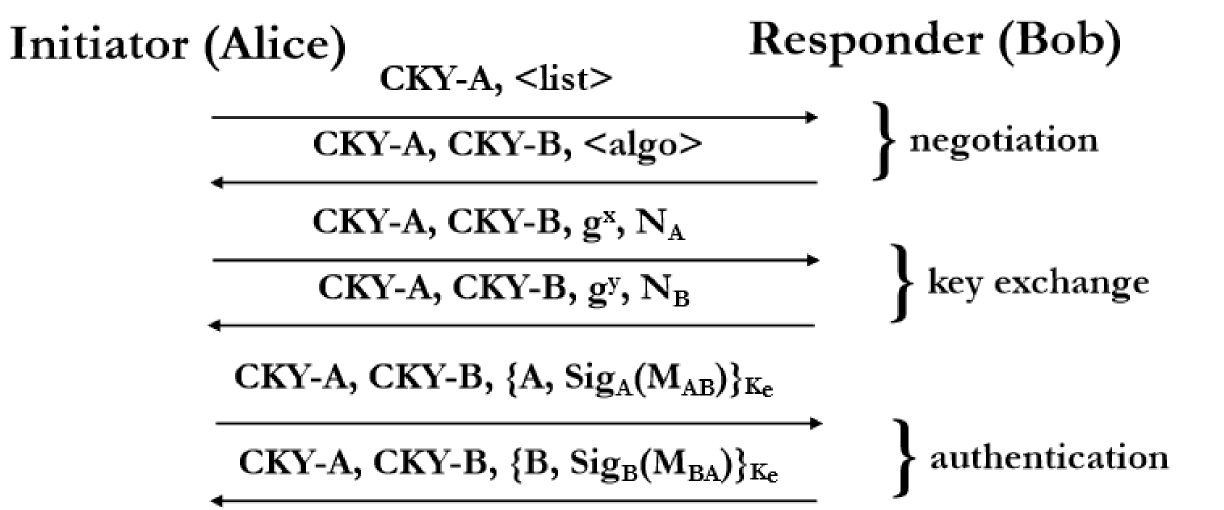
Aggresive Mode

- CKY: cookie
- KM: derived from (N_A | N_B, g^{xy})
- Ke: derived from KM
- M_{AB}: $MAC_{KM}(g^x$ | g^y | CKY-A | CKY-B | <list> | A)
- M_{BA}: $MAC_{KM}(g^y$ | g^x | CKY-B | CKY-A | <list> | B)

- Only three message flows
- No identity protection

5.3 IPsec: IKE (4/5)

Phase 1



Initiator (Alice)

Responder (Bob)

CKY-A, <list>

CKY-A, CKY-B, <algo>

negotiation

CKY-A, CKY-B, g^x, N_A

CKY-A, CKY-B, g^y, N_B

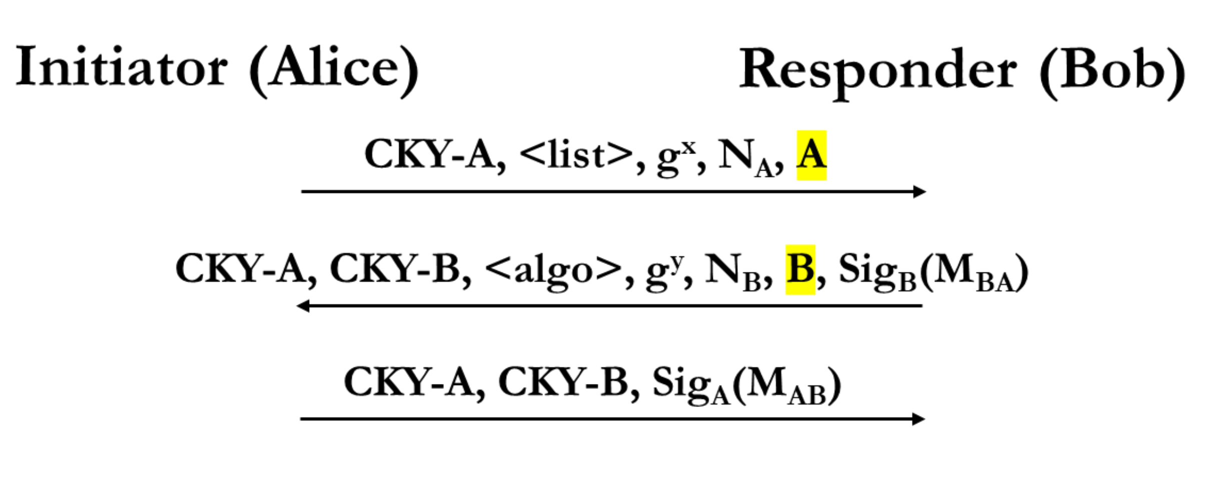
key exchange

CKY-A, CKY-B, {A, $Sig_A(M_{AB})$}$_{K_e}$

CKY-A, CKY-B, {B, $Sig_B(M_{BA})$}$_{K_e}$

authentication

Main Mode



Initiator (Alice)

Responder (Bob)

CKY-A, <list>, g^x, N_A, A

CKY-A, CKY-B, <algo>, g^y, N_B, B, $Sig_B(M_{BA})$

CKY-A, CKY-B, $Sig_A(M_{AB})$

Aggresive Mode

IPsec can use pre-shared keys, where both parties involved in the communication share a secret key in advance. This key is then used for authentication during the IPsec negotiation process. (equivalent to sk_A and sk_B in signature)

IPsec: IKE (5/5)

Phase 2

- Message 1 (Initiator → Responder): Proposal, Nonce, and optional DH Key.
- Message 2 (Responder → Initiator): Confirmed Proposal, Nonce, and optional DH Key.
- Message 3 (Initiator → Responder): Final confirmation with a Hash Payload.

□ Phase 2 is communicated in secure channel with the help of alrorithms and key in phase 1.

□ Proposal =Encryption algorithm (e.g., AES or 3DES), Integrity algorithm (e.g., HMAC-SHA1 or HMAC-MD5), and Lifetime of the SA (how long the SA is valid)

□ Optional DH Key: The secret key for encryption and integrity can be generated based on this DH or the secret key from phase 1. Aim to achieve stronger security, Perfect Forward Secrecy.

□ Hash= a MAC of all communicated message