ICT 4010 Data and Communication Networks

VPNs and Network Address Translation

Lecture 13

Phyela Mbewe
LIS Department
University of Zambia

September 2023

addressing schemes for Private Networks:

- There are 3 choices of addressing schemes for Private Networks:

  - Use IP addresses from the Internet Authority – use them without connection to the Internet. Pro: if there is a decision to join the Internet, could be done easily. Con: wasted addresses

  - Use the IP addresses without registering the addresses. This will work because the network is isolated. Con: users could confuse the private addresses with the global addresses

  - Use the **reserved IP addresses** for overcoming options above. There are 3 sets of reserved addresses for this case

Addresses Reserved for private networks

Range	*Total*
10.0.0.0 to 10.255.255.255	2^{24}
172.16.0.0 to 172.31.255.255	2^{20}
192.168.0.0 to 192.168.255.255	2^{16}

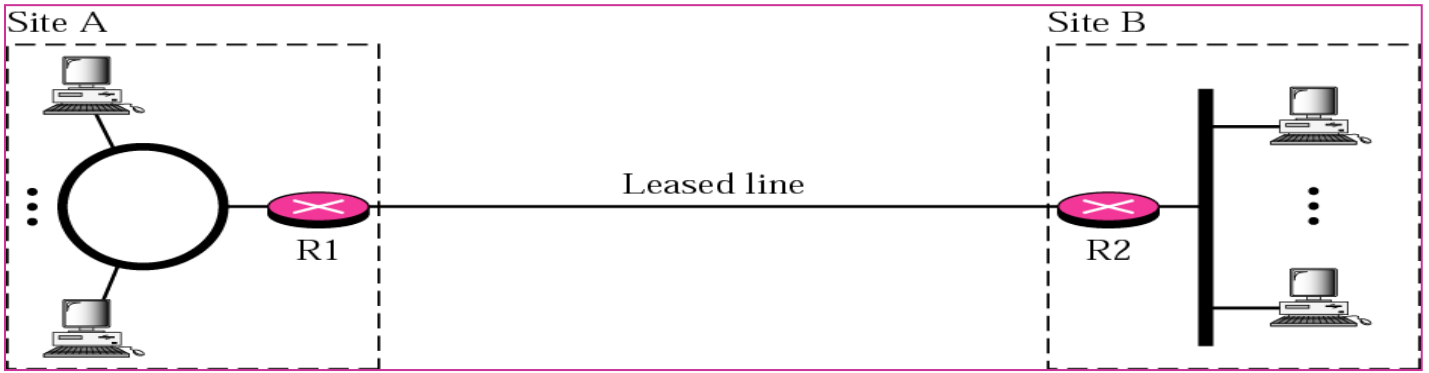
Private Network Strategy

- In Achieving Privacy for VPNs: can use the
  - private network
  - hybrid network or
  - virtual private network

Private Network Strategy

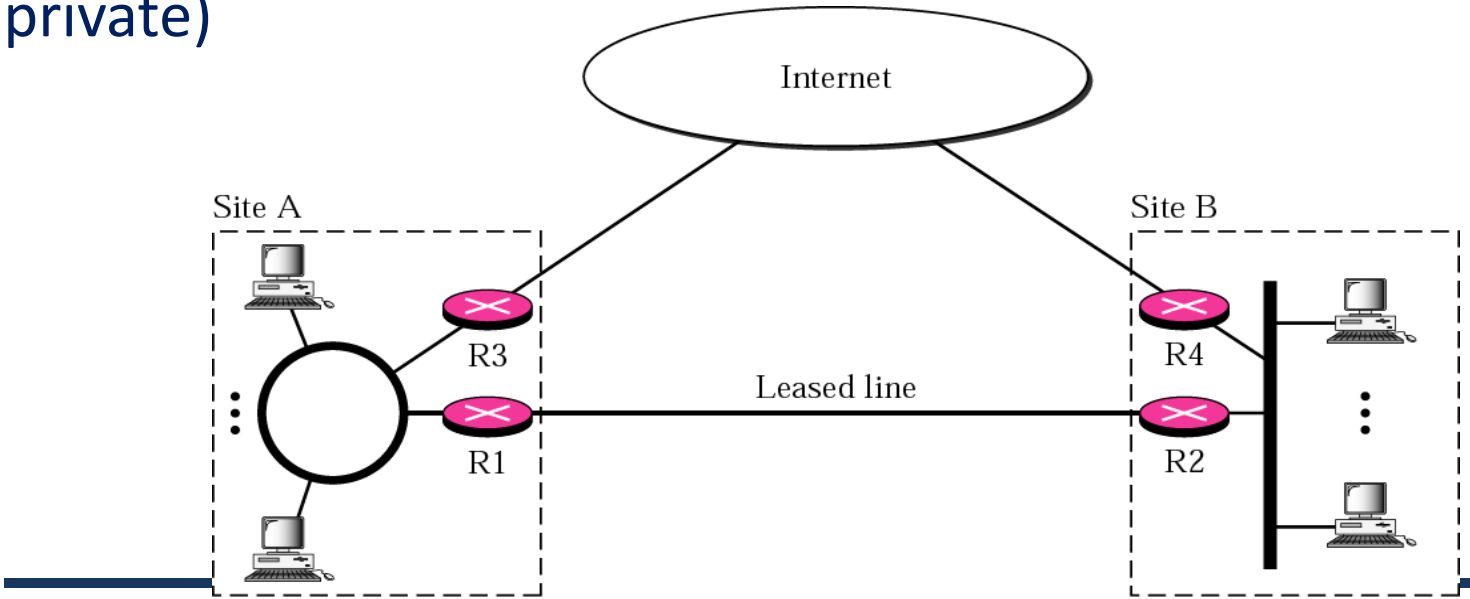
- If an organization has a single LAN, it could be detached from the Internet

- If an organization has multiple LANs in different locations, the routers of each LAN could be connected via a leased line



Hybrid Network Strategy

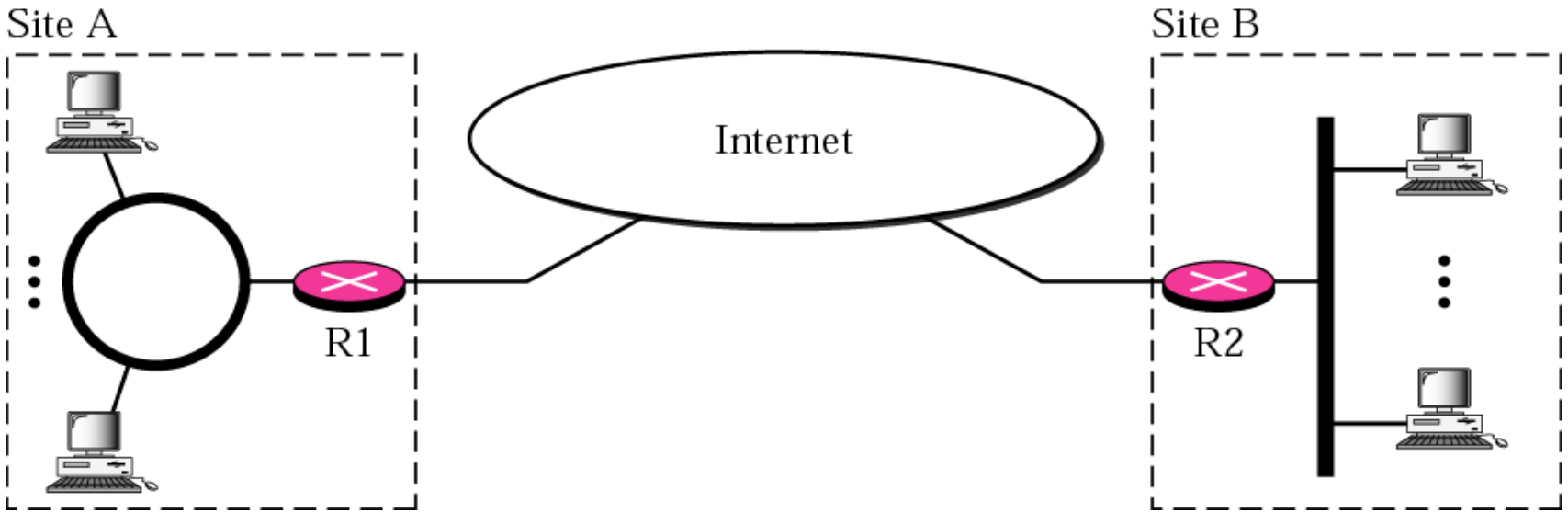
- Organization could have: routers connect to the global Internet (global)
- **and** Routers connect to the organization's private network (private)



Virtual Private Network Strategy

- With a Virtual Private Network
  - Routers R1 & R2 connect to the global Internet and use the VPN technology in guaranteeing privacy for the organization
- The VPN technology uses two techniques in implementing privacy:
  - Tunneling
  - and IPSec

Virtual Private Network Strategy



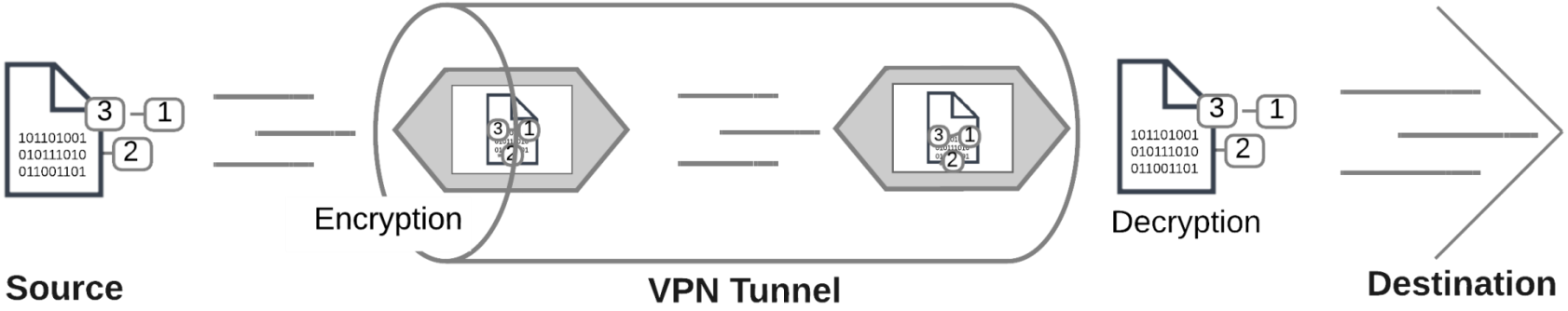
Virtual Private Network Strategy

- Both the Private and Hybrid strategies could be expensive.
- For a VPN, the users can use the Global Internet for private network access. For the VPN, the network is physically public but virtually private

VPN Technique 1: Tunneling

- A VPN tunnel
  - an encrypted link between the users computer or mobile device and an outside network.
    - A VPN tunnel connects the users smartphone, laptop, computer, or tablet to another network in which the users IP address is hidden and all the data generated while surfing the web is encrypted
  - The ‘tunnel’ is created by a VPN, however, the tunnel on its own can’t be considered private unless it’s accompanied with encryption strong enough to prevent governments or ISPs from intercepting and reading the users Internet activity.
  - The level of encryption the tunnel has depends on the type of tunneling protocol used to encapsulate and encrypt the data going to and from the users device and the internet.

VPN Technique 1: Tunneling

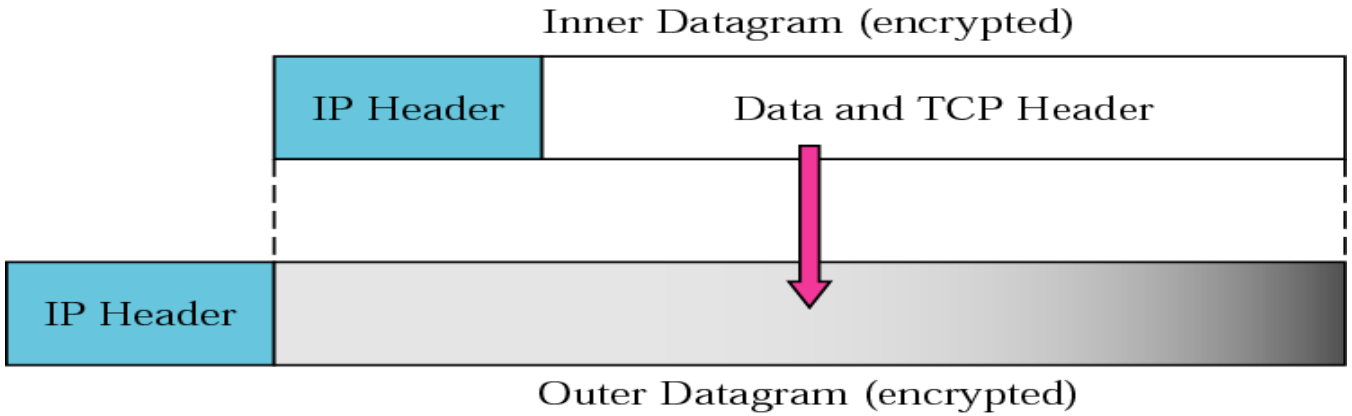


VPN Technique 1: Tunneling

- For router, R1, the IP datagrams sent are encapsulated into other IP datagrams, hiding them during their travel across the global Internet. The datagrams are “de-capsulated” at router, R2

VPN Technique 1: Tunneling

- a packet is the Internet layer datagram
- a frame is the network access layer datagram
  - a frame will include encapsulated information (hidden data) when transmitted via a VPN



VPN Technique 2: IPSec

- Internet Protocol Security (IPSec)
  - a network layer protocol that provides IP security
  - Host-to-Host communications must occur before applying IPSec
    - this connection is called Security Association (SA)
  - Three Elements of Security Association (SA):
    - 32-bit security parameter (ie virtual circuit id)
    - The type of protocol used for security (AH or ESP)
    - Source IP address

IPSec Mode

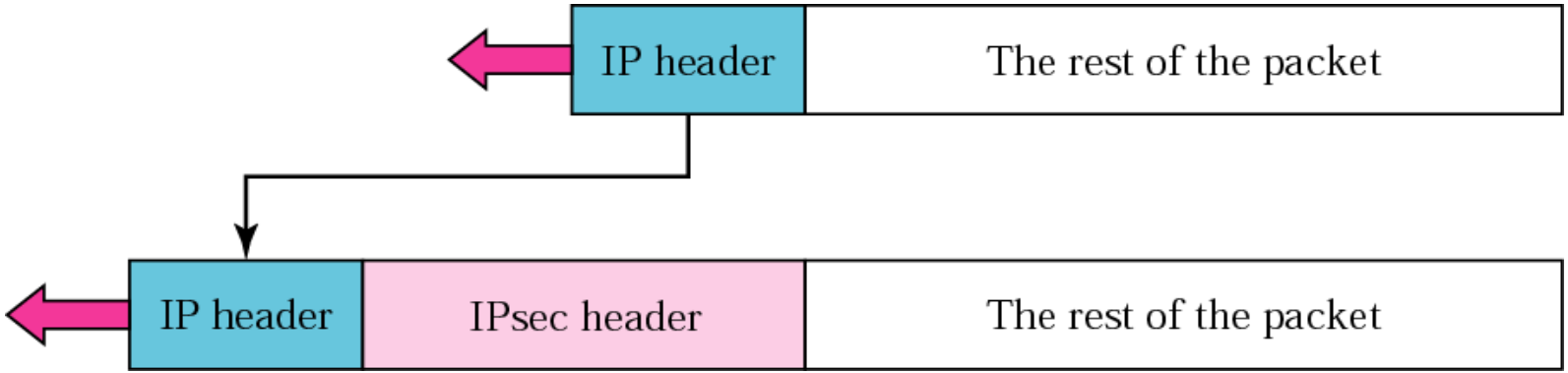
- The Mode defines where the IPSec header is added to the IP packet.

- Transport Mode
  - IPSec header added after the IP header

- Tunnel Mode
  - IPSec header is place in front of IP header and a NEW IP header is added in front of the IPSec header – attempting to hide the original header & payload
    - payload is the main data(content) to be transmitted

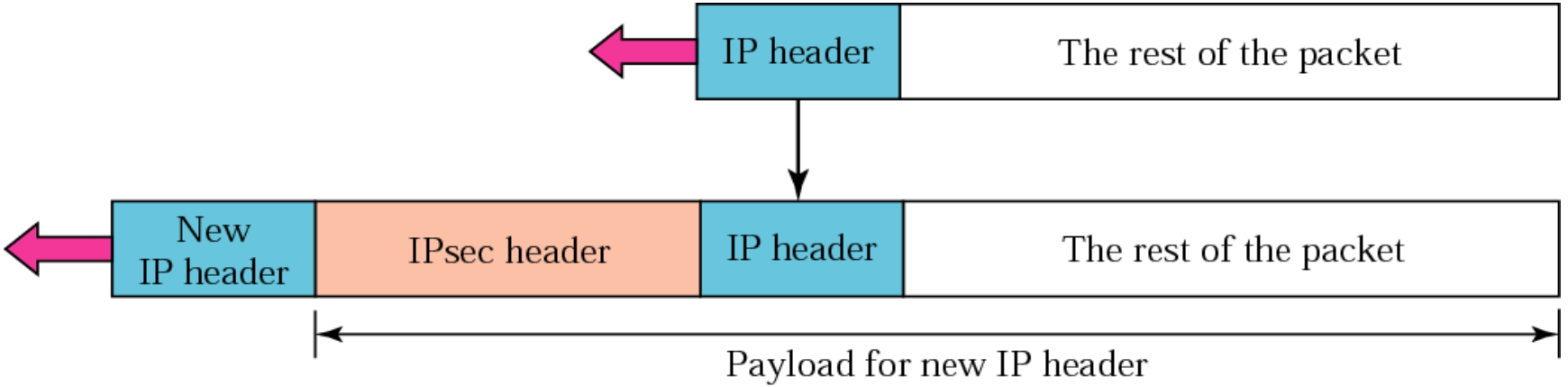
IPSec Mode

Transport Mode



IPSec Mode

Tunnel Mode



IPSec - protocols:

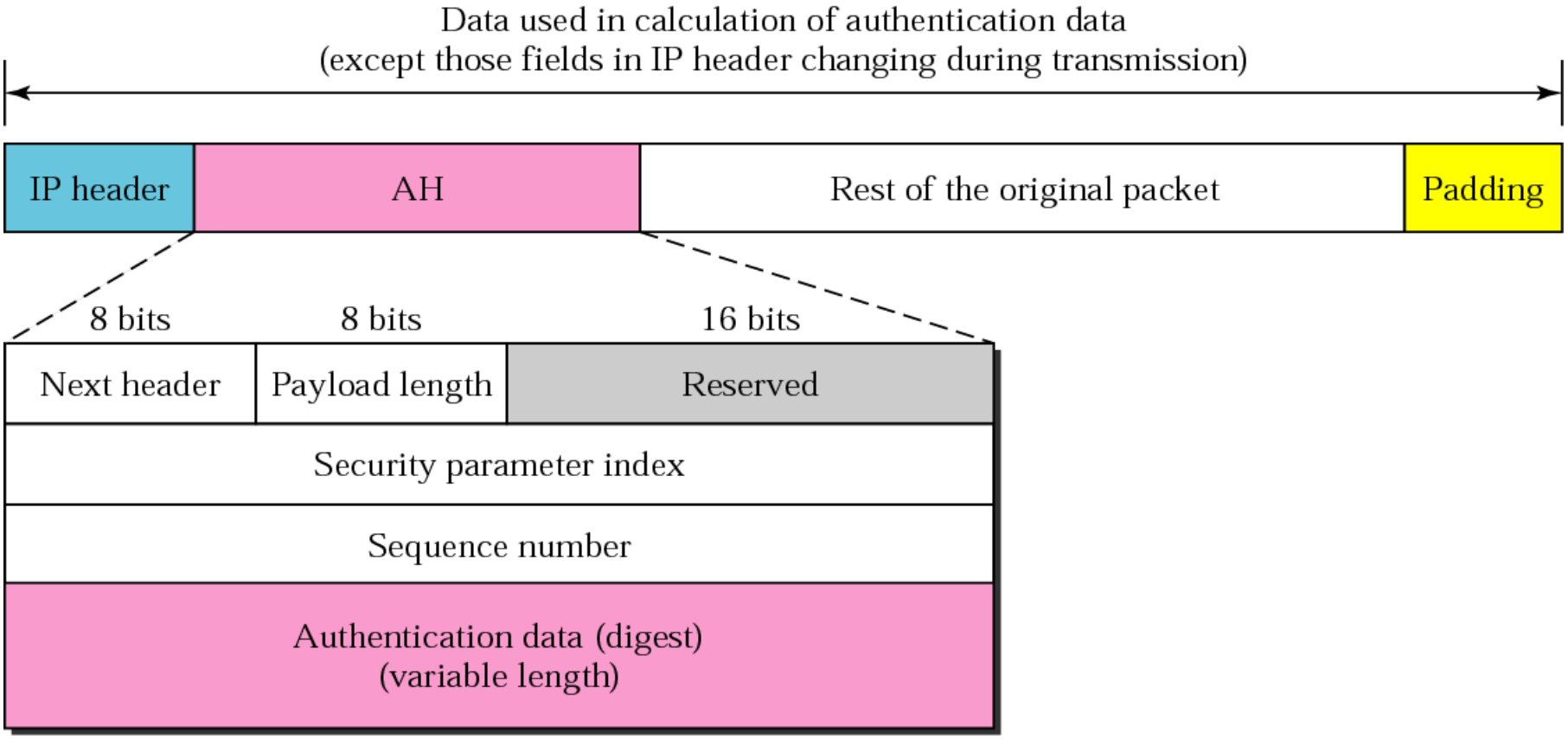
- IPSec includes 2 protocols:
  - Authentication Header (AH) Protocol
  - Encapsulation Security Payload (ESP) Protocol

AH Protocol:

- Using a hashing function and symmetric key, AH calculates a message digest (unique)

- AH inserts the message digest in the authentication header
- Based on either the tunneling or transport modes, the AH is placed in the appropriate location

AH Protocol


Data used in calculation of authentication data
(except those fields in IP header changing during transmission)
IP header
AH
Rest of the original packet
Padding
8 bits
8 bits
16 bits
Next header
Payload length
Reserved
Security parameter index
Sequence number
Authentication data (digest)
(variable length)

AH Protocol

- The AH protocol provides message authentication and integrity, but does **not provide privacy**

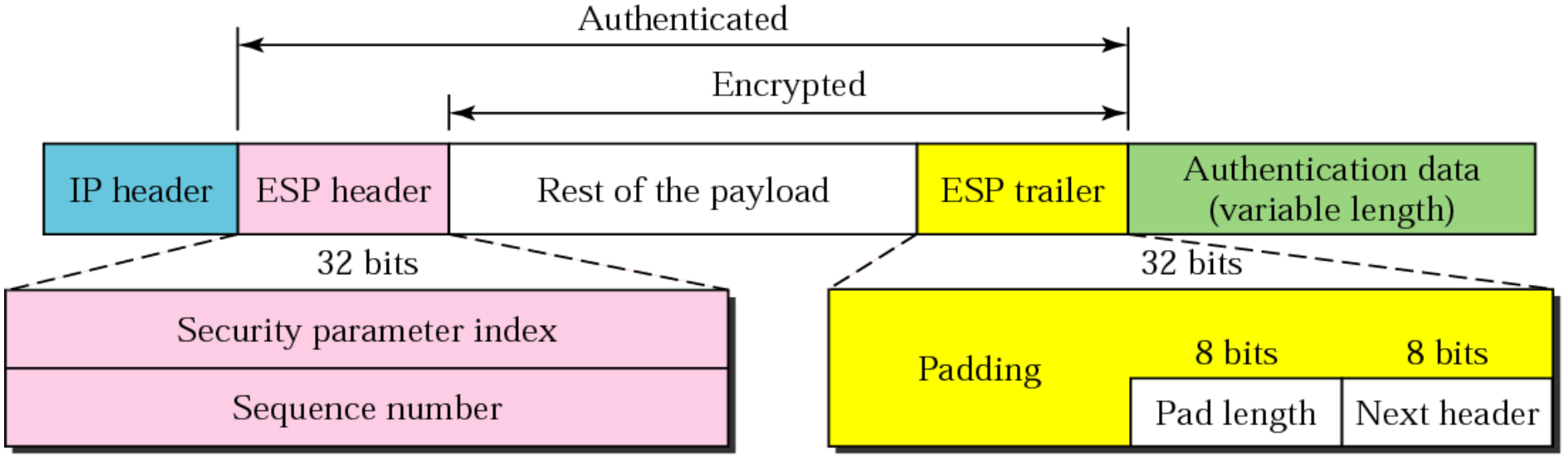
ESP Protocol:

- IPSec defines an alternative protocol that provides **privacy** (AH doesn't)
- ESP adds a header and trailer (AH only added a header)
- 50 is placed in the IP datagram "protocol" field and the "protocol" is placed in the "next header" field of the ESP trailer
- ESP trailer is added and both the payload and the trailer are encrypted
- Then the ESP header is added

ESP Protocol:

- Then the ESP header, payload and trailer are used to create the authentication data
- Then the newly created authentication data is ADDED AFTER the trailer
- Then the IP header is added
- ESP provides message authentication, integrity, and privacy

ESP Protocol:



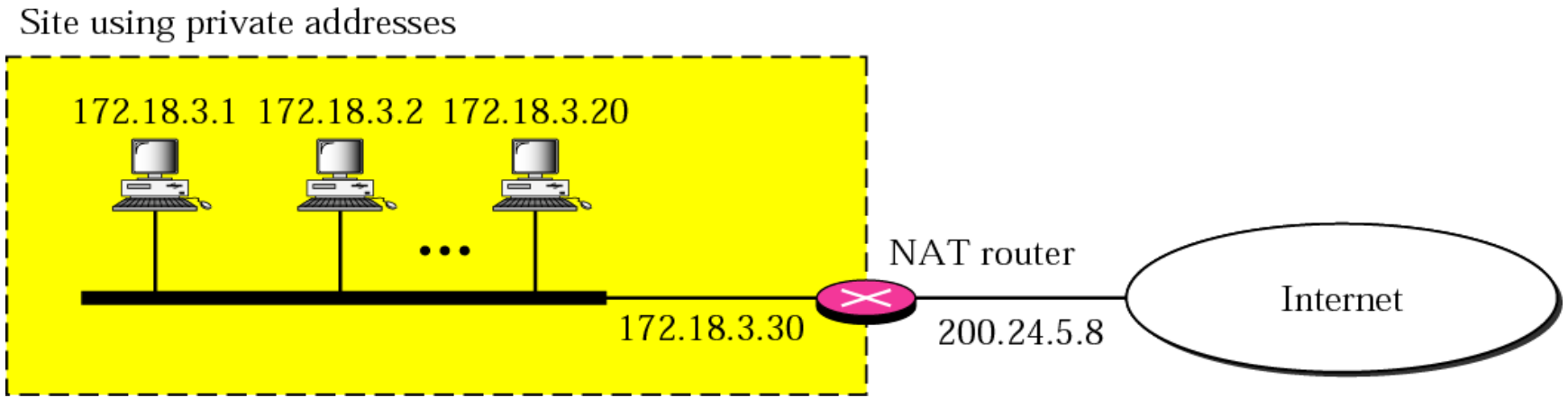
Network Address Translation (NAT)

- NAT allows a site to use a set of private addresses for internal communication and a set of global Internet addresses for communication with another site.

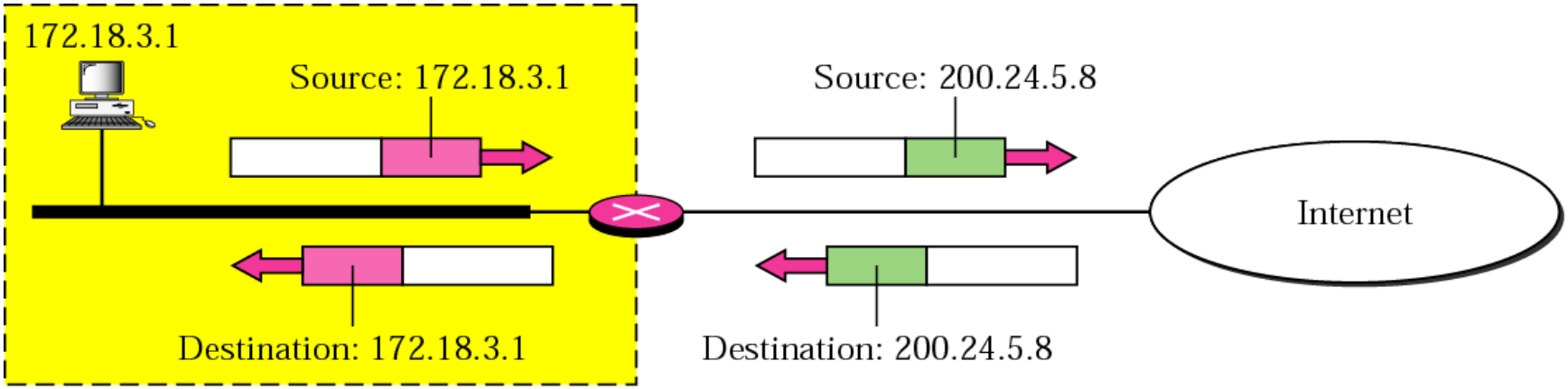
- The site must have only one single connection to the global Internet through a router that runs NAT software.

- The routers only 2 address: (1) the global IP address and (2) one private address

NAT


Site using private addresses
172.18.3.1
172.18.3.2
172.18.3.20
172.18.3.30
NAT router
200.24.5.8
Internet

Address Translation



Address Translation

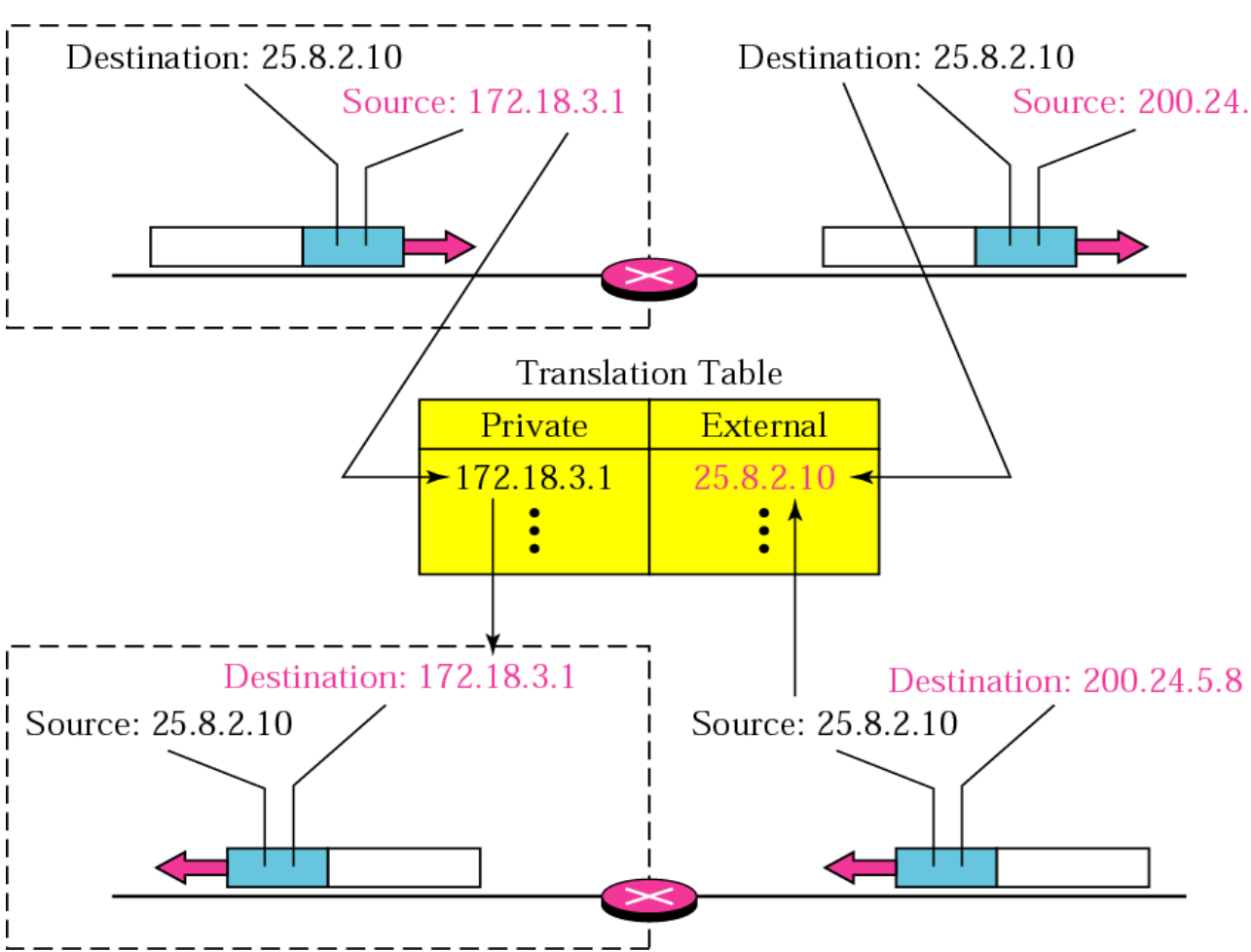
- All packets leaving the network get assigned the global address as the source address

- All packets coming into the network get their global destination address replaced with the appropriate private address

Address Translation

- Packet: From Private Network to Internet
  - with in the private network, the original source address is a private address representing the original source in the private network.
  - Just before the packet leaves the router
    - the router makes note of the global destination address and cross-references with the private source address
    - the router changes the packet's private source address to the global source address (i.e. the global source address of the router)

Translation



Router Translation Table - keeps track of private and global source addresses

Five-column Translation Table

Private Address	*Private Port*	*External Address*	*External Port*	*Transport Protocol*
172.18.3.1	1400	25.8.3.2	80	TCP
172.18.3.2	1401	25.8.3.2	80	TCP
. . .	. . .	. . .	. . .	. . .

An ISP and NAT

- An ISP serving Internet customers can conserve addresses by using NAT.
  - Consider the customers as being part of the ISP's private network before gaining access to the Global Internet.
  - The ISP could assign a private address to each customer and when the customer leaves the private network, a translation would occur
  - Let an ISP with 100,000 customers be granted only 1000 global addresses
    - the ISP could assign private addresses to each 100,000 customers and the ISP then translates the 100,000 source addresses for the outgoing packets with the 1000 global addresses

An ISP and NAT