Lo strato di Trasporto
UDP

Corso di
Reti di Calcolatori
AA. 2023-2024

Federica Paganelli

UDP

- Servizio di consegna a massimo sforzo
  - I datagrammi UDP possono essere perduti o consegnati fuori sequenza
  - Nota: L'affidabilità può essere aggiunta al livello applicazione

- Orientamento al messaggio
  - Ogni datagramma UDP indipendente dall'altro
  - I processi devono inviare messaggi di dimensioni limitate, che possono essere incapsulati in un datagramma UDP

Rispetto al TCP l'UDP è meno complesso, offre meno servizi, ma è più indicato in contesti dove occorre un completo controllo della temporizzazione (applicazioni time-sensitive come la trasmissione di dati multimediali)

UDP: User Datagram Protocol [RFC 768]

INTERNET STANDARD

RFC 768

J. Postel
ISI
28 August 1980

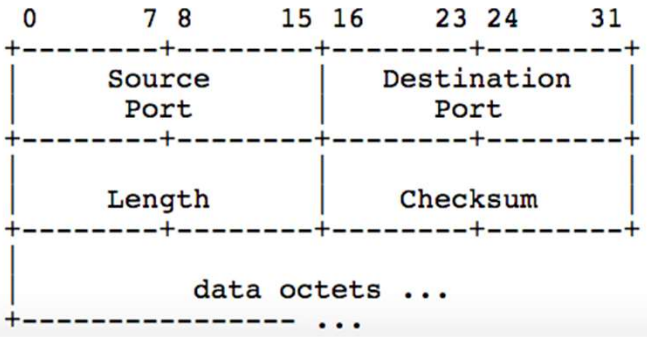
User Datagram Protocol

Introduction

This User Datagram Protocol (UDP) is defined to make available a datagram mode of packet-switched computer communication in the environment of an interconnected set of computer networks. This protocol assumes that the Internet Protocol (IP) [1] is used as the underlying protocol.

This protocol provides a procedure for application programs to send messages to other programs with a minimum of protocol mechanism. The protocol is transaction oriented, and delivery and duplicate protection are not guaranteed. Applications requiring ordered reliable delivery of streams of data should use the Transmission Control Protocol (TCP) [2].

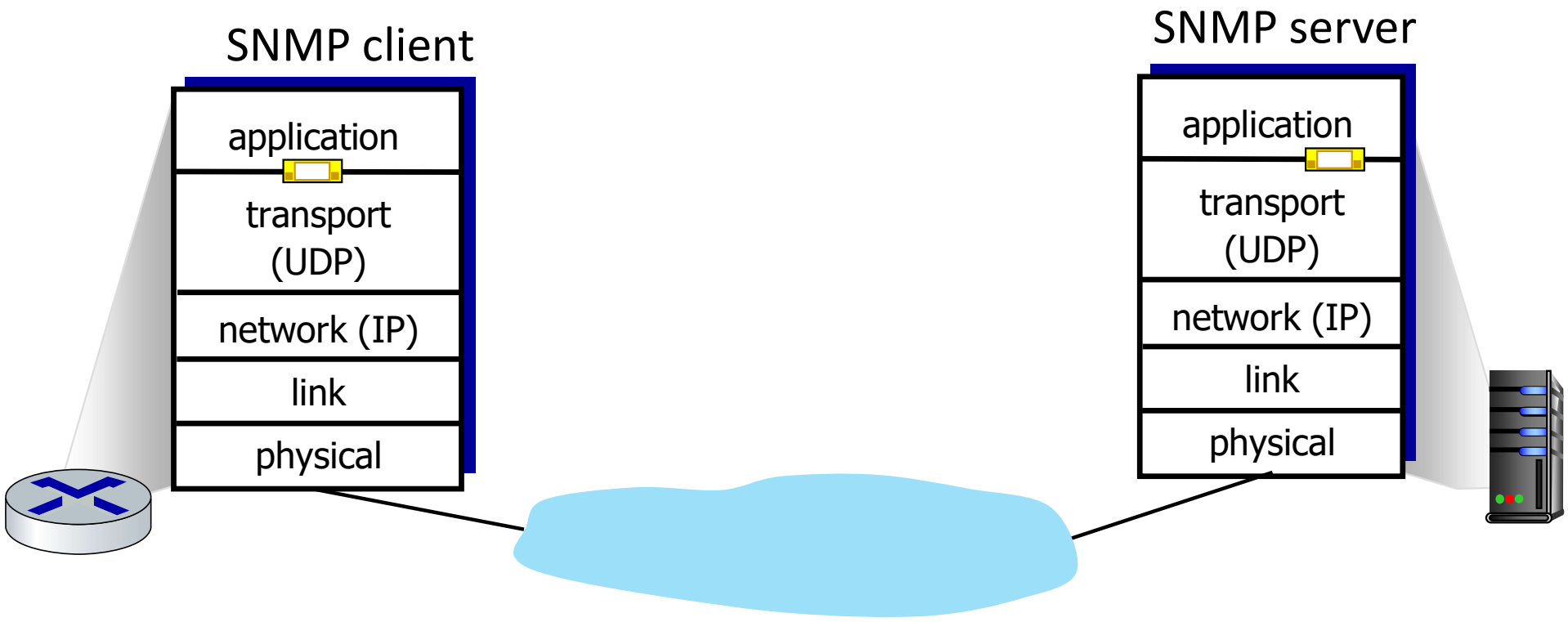
Format



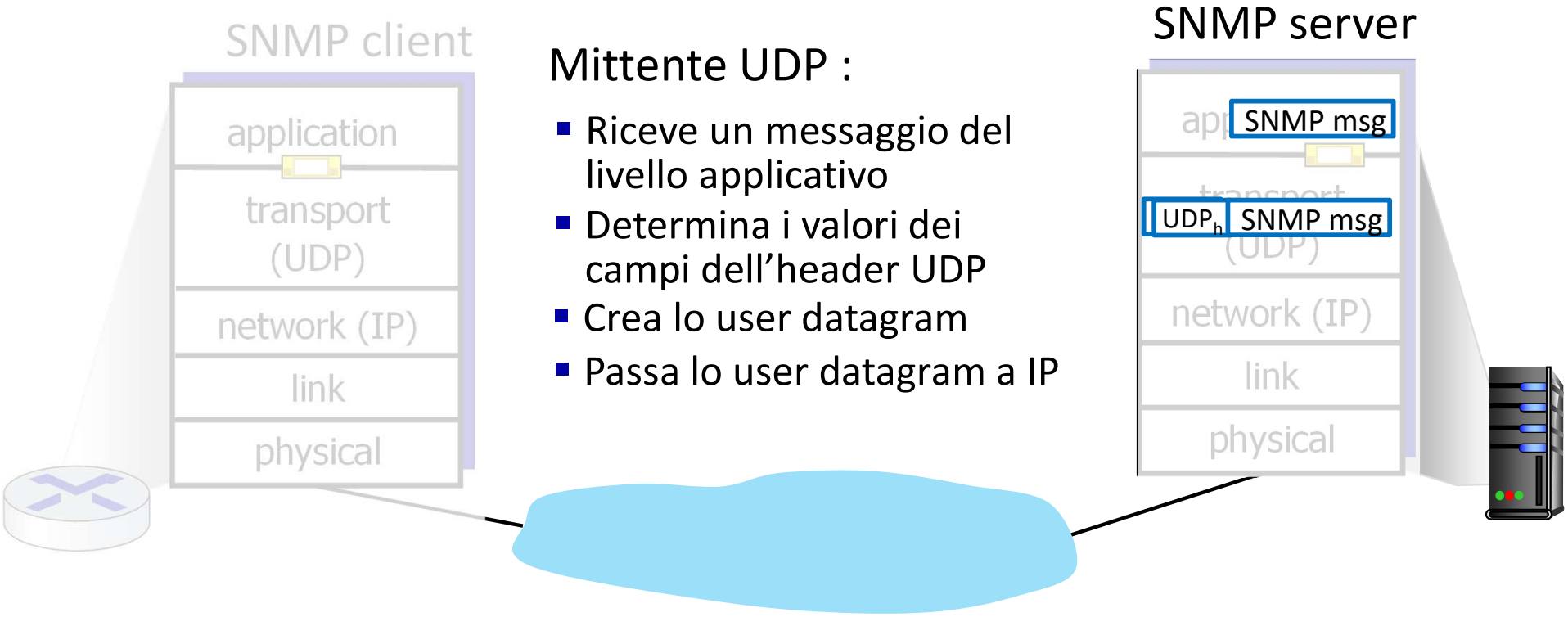
Proprietà del servizio UDP

- Nessuna connessione (non si introduce ritardo)
  - Semplice: non viene gestito lo stato di connessione
  - Intestazioni di 8 byte
  - Senza controllo di congestione e di flusso: UDP può sparare dati a raffica
- Il checksum è facoltativo
- E' facile e leggero da gestire (non richiede particolari meccanismi)
- Utilizzato spesso in applicazioni multimediali
  - Tolleranza piccole perdite
  - Sensibilità alla frequenza
- Altri impieghi: DNS, SNMP (Simple Network Management Protocol)

UDP: Transport Layer Actions



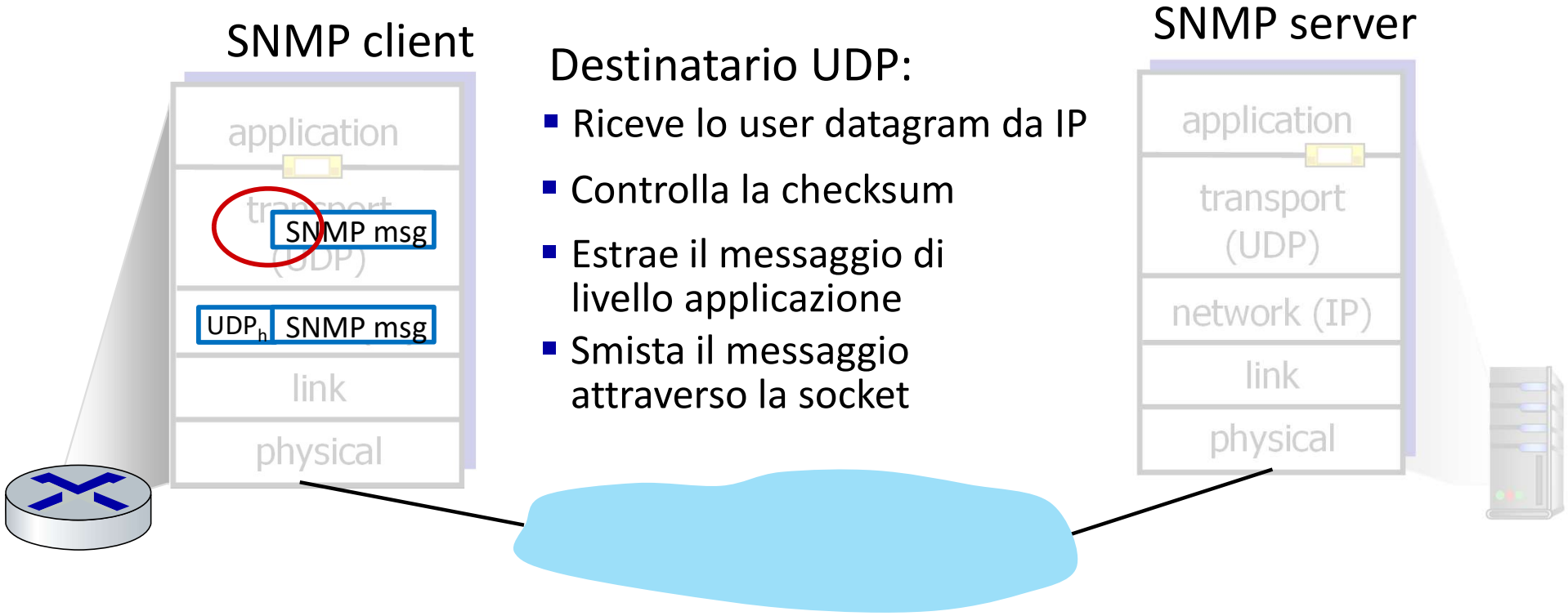
UDP: Transport Layer Actions



Mittente UDP :

- Riceve un messaggio del livello applicativo
- Determina i valori dei campi dell'header UDP
- Crea lo user datagram
- Passa lo user datagram a IP

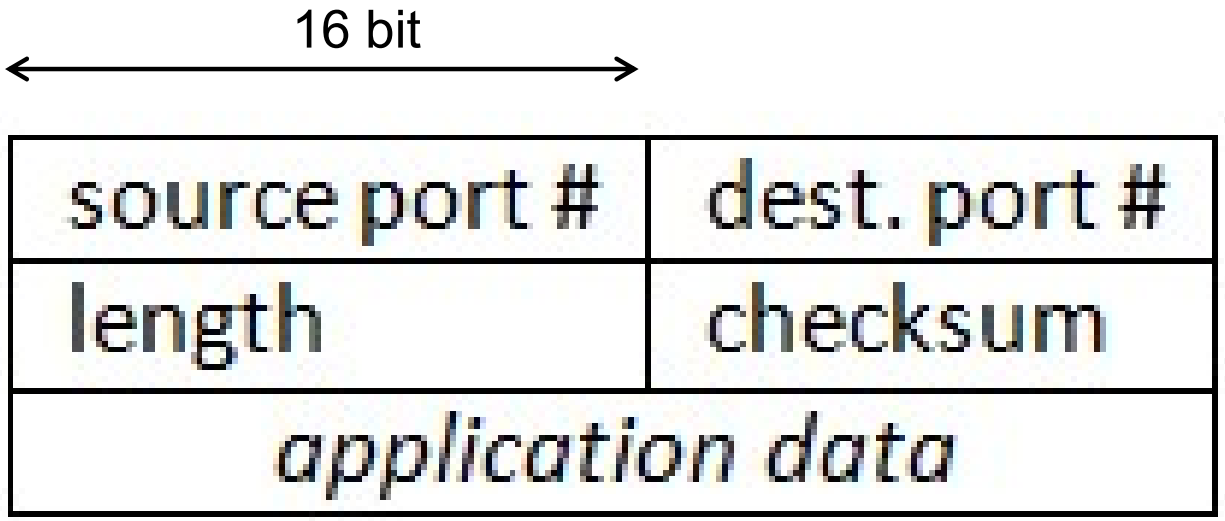
UDP: Transport Layer Actions



Destinatario UDP:

- Riceve lo user datagram da IP
- Controlla la checksum
- Estrae il messaggio di livello applicazione
- Smista il messaggio attraverso la socket

Datagramma UDP

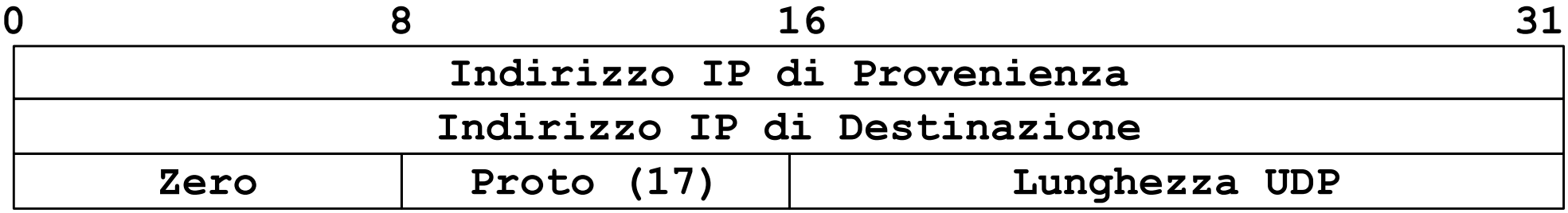


- 8 byte di intestazione
- **Porta**: numeri di porta della comunicazione (per il demultiplexing è usato solo quello di destinazione).
- **Lunghezza del messaggio***:* lunghezza totale (header + dati) del datagramma UDP (16 bit -> max 65535 byte)

Datagramma UDP: campi

- **Checksum**: checksum dell'intero datagramma
- E' opzionale in UDP.
  - Controllo errore end-to-end
  - Il pacchetto corrotto viene scartato, ma il mittente non ne riceve notifica
- Calcolata sull'intero datagramma UDP più lo pseudo-header (ovvero parte dell'header IP)

Pseudoheader – usato per calcolo checksum



Calcolo checksum UDP

Mittente

- Campo checksum a 0
- Tratta il contenuto del datagramma UDP come una sequenza di parole da 16 bit
- checksum: somma le parole di 16 bit in complemento a uno
  - Somma dei singoli bit
  - Eventuale riporto viene aggiunto al risultato
- Complemento a uno del risultato della somma
  - Inversione dei bit
- Il mittente pone il valore della checksum nel campo checksum del datagramma UDP

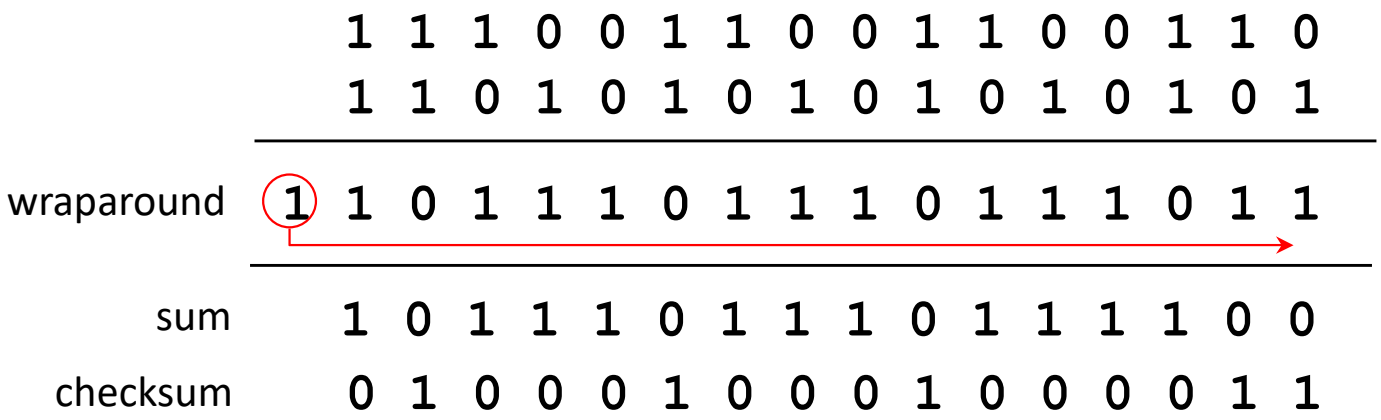
Ricevente

- calcola la checksum del segmento ricevuto (campo checksum incluso)
- Il valore della checksum è 0?
  - No - errore rilevato, il messaggio viene scartato
  - Si - Nessun errore rilevato.

- Analogo per TCP
- In TCP la checksum è obbligatoria

Internet checksum: esempio

example: add two 16-bit integers



Note: when adding numbers, a carryout from the most significant bit needs to be added to the result

I servizi forniti dai protocolli di trasporto di Internet

Servizio UDP:

- trasferimento dati non affidabile tra mittente e destinatario
- non fornisce: setup della connessione, affidabilità, controllo di flusso, controllo della congestione, timing, o garanzia di banda
- Richiede minor overhead

Servizio TCP:

- *connection-oriented:* richiesto handshake tra client e server
- *trasporto affidabile* tra i processi mittente e destinatario
- *controllo di flusso:* il mittente non saturerà il destinatario
- *controllo della congestione:* limita il mittente quando la rete è sovraccarica
- *non fornisce:* timing, banda minima garantita

TCP vs UDP

Nella programmazione di rete si deve ricordare che:

- il TCP offre un servizio di trasporto a stream, quindi si può leggere da un input di rete quanti byte si desiderano.
- l'UDP offre un servizio a messaggi, quindi occorre leggere tutto il messaggio in arrivo.

TCP vs UDP

- UDP adeguato per
  - processi che richiedono uno scambio di dati con volume limitato con scarso interesse al controllo di flusso e degli errori
  - processi che hanno meccanismi interni di controllo di flusso e degli errori
  - trasmissioni multicast (destinatari multipli)
  - applicazioni interattive in tempo reale che non tollerano ritardi variabili

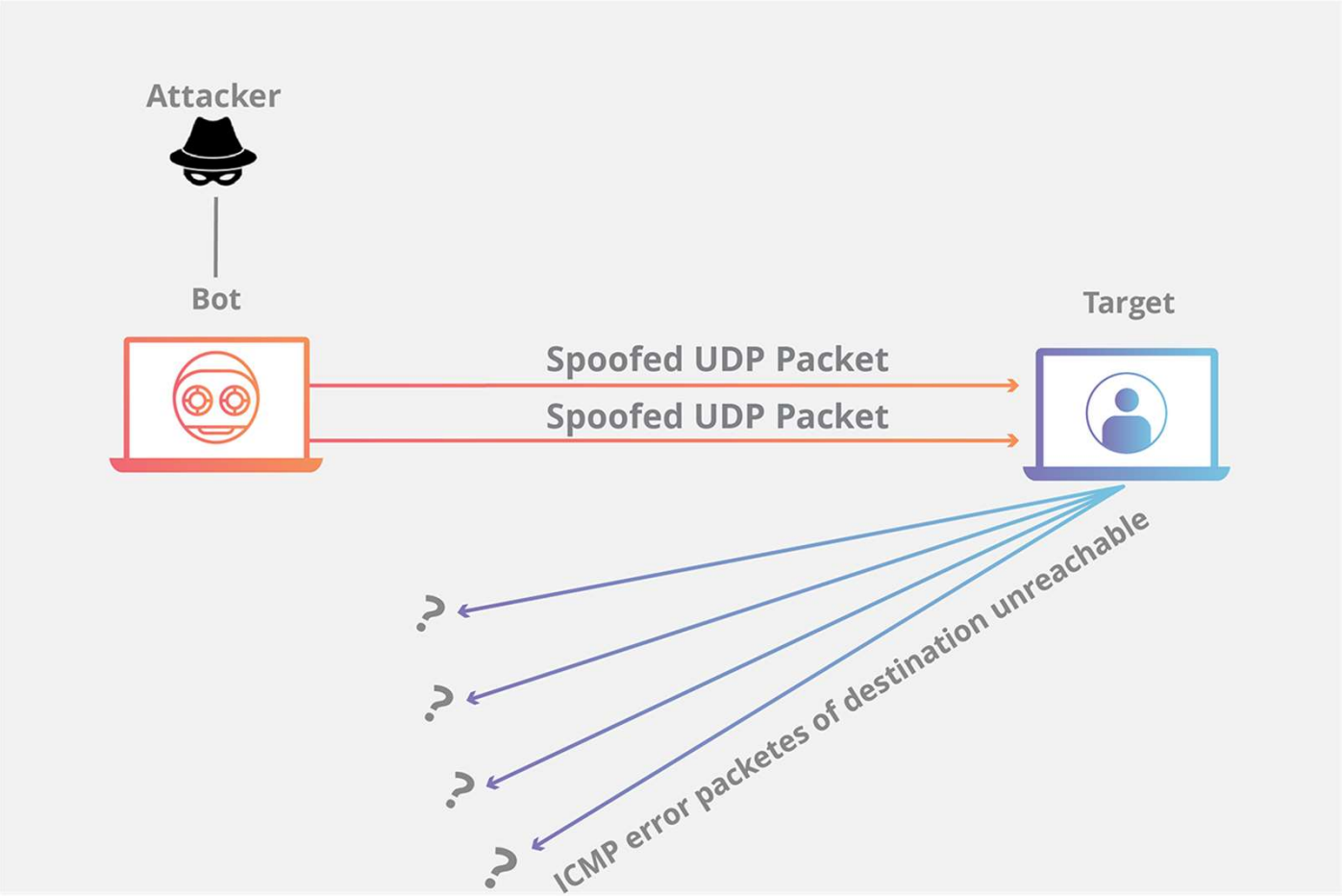
Attacco UDP Flood

- Un UDP flood è un tipo di attacco denial-of-service in cui un gran numero di pacchetti UDP viene inviato a un server obiettivo e porta destinazione scelta in modo random
- Attacco volumetrico con l'obiettivo di sovraccaricare la capacità del dispositivo di elaborare e rispondere.
  - Il server prima controlla se sono in esecuzione programmi che sono attualmente in attesa di richieste sulla porta specificata.
  - Se nessun programma riceve pacchetti su quella porta, il server risponde con un pacchetto ICMP (prossime lezioni) per informare il mittente che la destinazione non è raggiungibile.
  - Come risultato dell'utilizzo delle risorse da parte del server di destinazione per controllare e quindi rispondere ad ogni pacchetto UDP ricevuto, le risorse possono esaurirsi rapidamente, con conseguente denial-of-service al traffico normale…

fonte: https://www.cloudflare.com/learning/ddos/udp-flood-ddos-attack/
The UDP flood attack explained: how it works and available security measures - IONOS

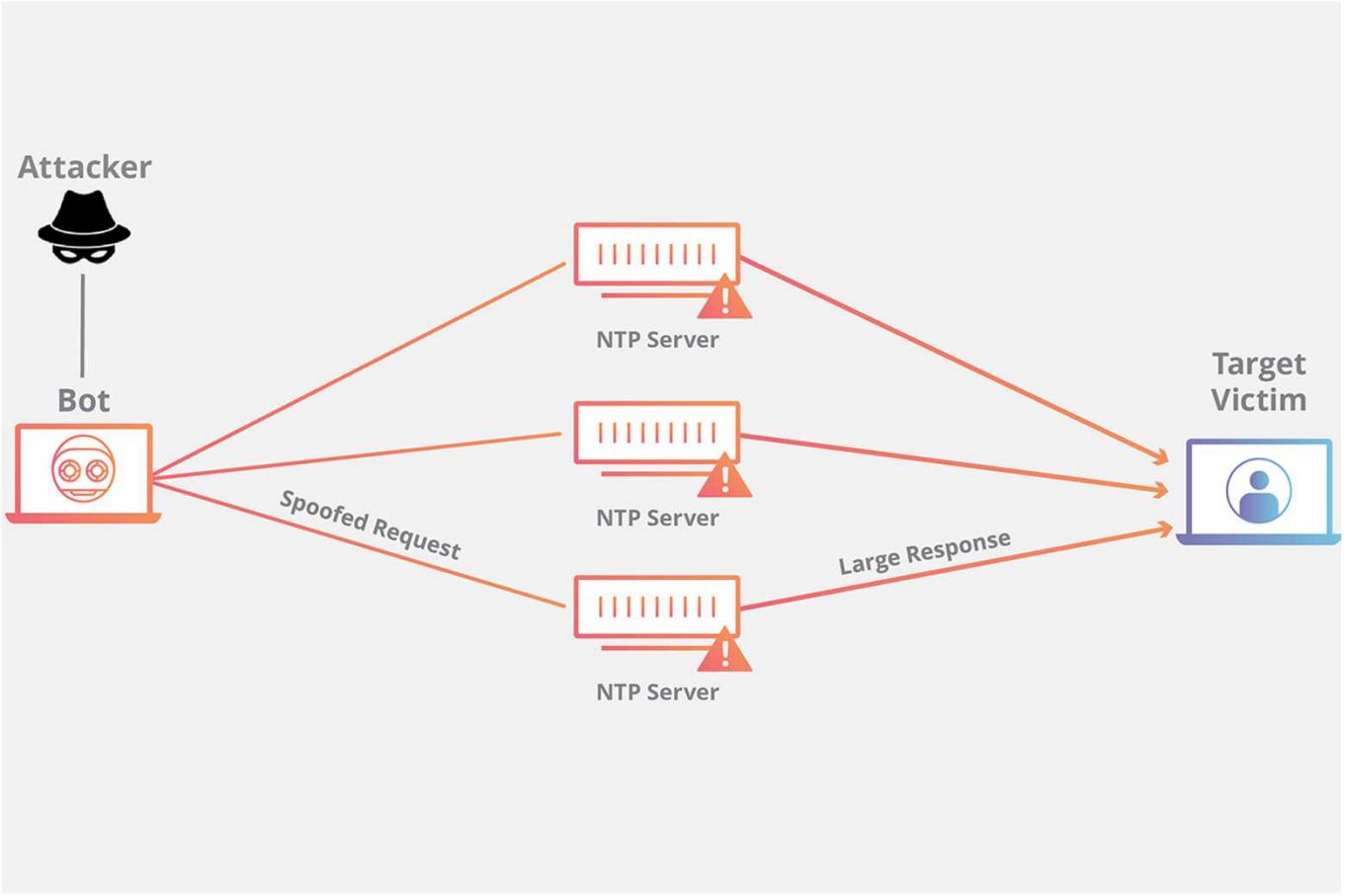
Attacco UDP Flood

- L'attaccante tipicamente inserisce nel pacchetto del messaggio UDP un indirizzo IP spoofed



fonte: https://www.cloudflare.com/learning/ddos/udp-flood-ddos-attack/

UDP Amplification attack



fonte: https://www.cloudflare.com/learning/ddos/ntp-amplification-ddos-attack/

Attacco UDP Amplification

- UDP è un protocollo senza connessione che non controlla gli indirizzi IP (Internet Protocol) di origine
- Un utente malintenzionato può facilmente forgiare un pacchetto per usare un indirizzo IP di origine arbitrario (in questo caso è l'IP della vittima).
- L'attaccante invia numerosi pacchetti UDP con l'indirizzo IP di origine falsificato ad un server di destinazione (o amplificatore).
- Il server risponde alla vittima (anziché all'attaccante), creando un attacco DoS (Denial of Service) riflesso.
- Si basa sul fatto che alcuni protocolli applicativi che usano UDP possono generare risposte molto più grandi della richiesta iniziale.
  - DNS, Network Time Protocol (NTP)
  - Lista di protocolli «vettori» di attacco e fattore di amplificazione in https://www.cisa.gov/uscert/ncas/alerts/TA14-017A

fonte: https://www.cisa.gov/uscert/ncas/alerts/TA14-017A /