

Luigi SCIOLLA

Università di Genova

Network Security

Fondamenti di reti di calcolatori



<https://cybersecnatlab.it>

License & Disclaimer

2

License Information

This presentation is licensed under the Creative Commons BY-NC License



To view a copy of the license, visit:

<http://creativecommons.org/licenses/by-nc/3.0/legalcode>

Disclaimer

- We disclaim any warranties or representations as to the accuracy or completeness of this material.
- Materials are provided “as is” without warranty of any kind, either express or implied, including without limitation, warranties of merchantability, fitness for a particular purpose, and non-infringement.
- Under no circumstances shall we be liable for any loss, damage, liability or expense incurred or suffered which is claimed to have resulted from use of this material.

Obiettivi

3

- Avere una conoscenza di base del modello ISO/OSI
- Capire il funzionamento del modello TCP/IP
- Conoscere la struttura degli indirizzi IPv4
- Capire a cosa servono e come funzionano le tabelle di routing
- Sapere riconoscere le differenze tra TCP e UDP
- Comprendere il funzionamento del Domain Name System (DNS)

Indice

4

- Modello ISO/OSI, modello TCP/IP
- Layer 3: IP e routing
- Layer 4: TCP e UDP
- Modello Client/Server

Indice

5

- **Modello ISO/OSI, modello TCP/IP**
- Layer 3: IP e routing
- Layer 4: TCP e UDP
- Modello Client/Server

Modello ISO/OSI – Perché?

6

- Sviluppato nel 1984 dall'International Organization for Standardization (ISO)
- Fornisce la logica per la comunicazione tra dispositivi all'interno di reti di calcolatori
- **Non** è lo standard implementato abitualmente su Internet

OSI Layers

7



Una guida per lo sviluppo di protocolli di rete.

- Sette layers (strati)
- Basato su un approccio *divide et impera*: ogni problema viene risolto all'interno di un singolo layer
- Forte flessibilità: può adattarsi a nuovi protocolli e servizi di rete

OSI Layers

8

Applicazione

Fornisce il servizio all'utente

Presentazione

Responsabile per la formattazione delle informazioni (ad esempio decompressione)

Sessione

Responsabile di instaurare, mantenere e chiudere connessioni tra applicazioni

Trasporto

Permette un trasferimento affidabile di dati tra due host

Rete

Responsabile di trasferire i pacchetti da una sorgente ad una destinazione indipendentemente dagli strati superiori. Gestisce l'indirizzamento dei nodi e le problematiche relative

Collegamento dati

Combina i bit in una struttura dati per la comunicazione tra due nodi fisicamente connessi

Fisico

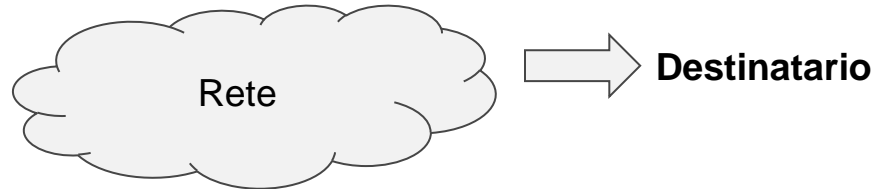
Il collegamento fisico su cui vengono trasmessi i segnali

OSI Layers: trasferimento di dati

9

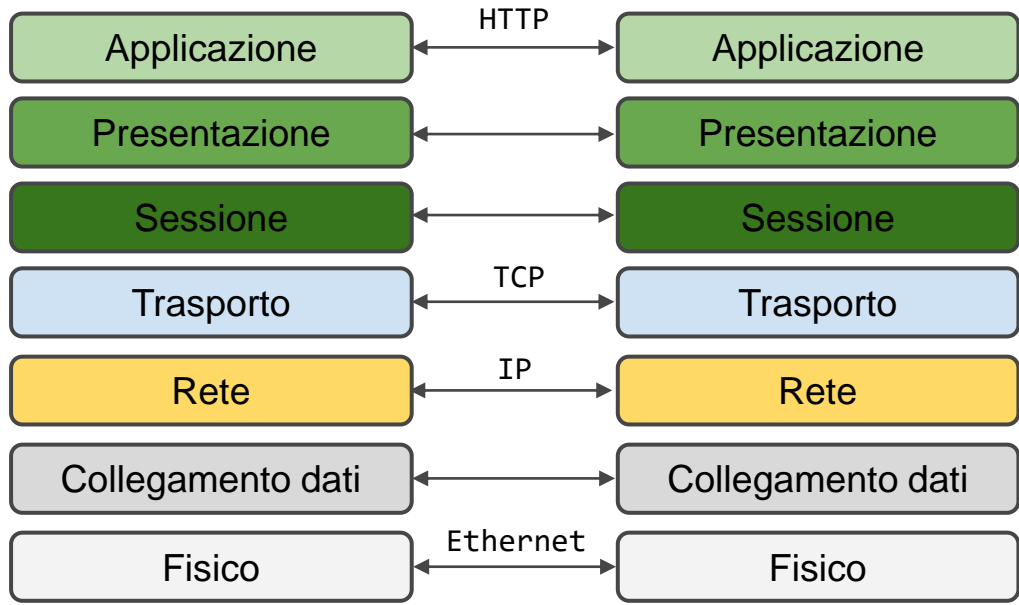


- Ogni layer può comunicare **solo** con i layer a esso adiacenti
- Il trasferimento di dati inizia dal livello applicativo del mittente
- La comunicazione avviene dall'alto verso il basso nel dispositivo del mittente e viceversa nel dispositivo del destinatario



OSI Layers: protocolli

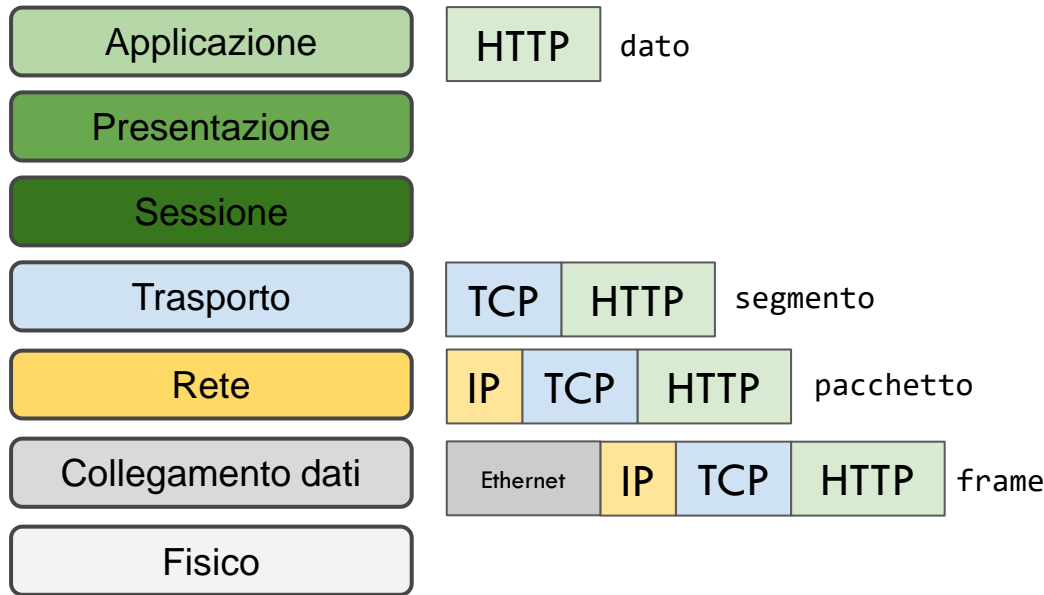
10



- Il modello fornisce delle linee guida, ma non specifica i protocolli per ciascuno strato
- Un *protocollo* è una procedura standard utilizzata tra due dispositivi per poter comunicare
- La comunicazione è quindi definita da diversi protocolli, ciascuno dei quali fa riferimento a uno specifico layer

OSI Layers: Protocols Data Unit (PDU)

11



- Ogni strato inserisce all'interno del pacchetto informazioni relative al suo protocollo, dopodiché trasferisce il pacchetto allo strato successivo
- Ogni pacchetto è formato da informazioni di controllo inserite dal protocollo stesso (Protocol Control Information - PCI) e dai dati da trasmettere (Service Data Unit - SDU)
- L'insieme del PCI e del SDU formano un pacchetto
- A ogni livello i pacchetti vengono chiamati con nomi differenti (datato, segmento, pacchetto o frame)

Modello TCP/IP

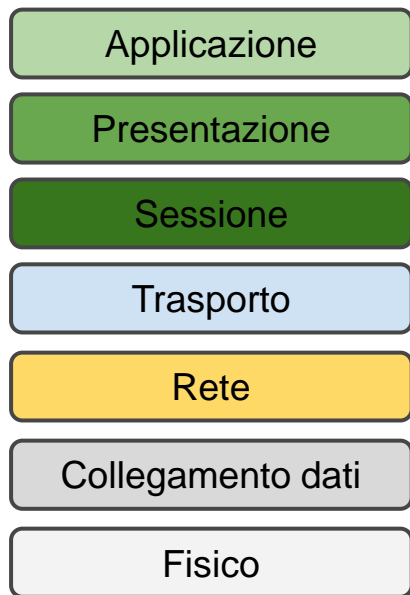
12

Il modello TCP/IP è un insieme di protocolli utilizzati per la comunicazione all'interno di reti.

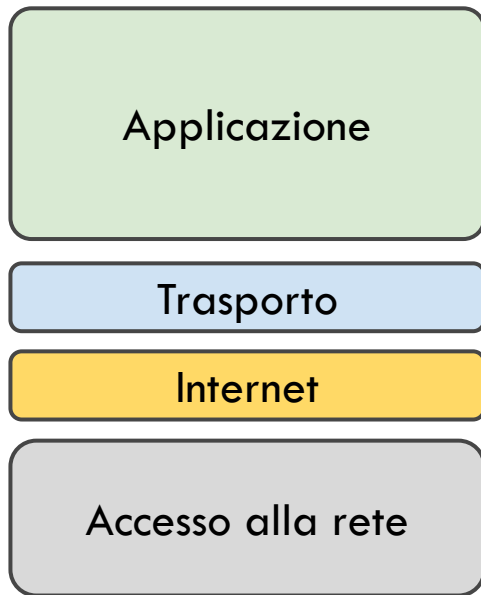
- È basato su quattro livelli
- È basato sui protocolli sviluppati e applicati su Internet (quindi è protocollo-dipendente)
- È lo standard utilizzato su Internet

Modello TCP/IP

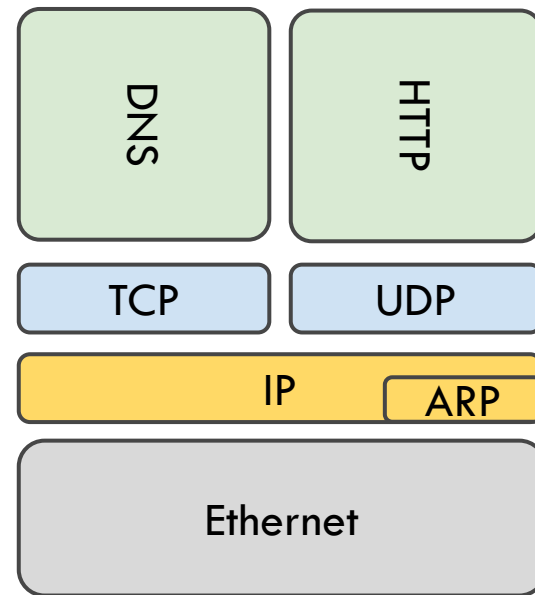
13



ISO/OSI



TCP/IP



Protocolli standard

Indice

14

- Modello ISO/OSI, modello TCP/IP
- **Layer 3: IP e routing**
- Layer 4: TCP e UDP
- Modello Client/Server

Internet Protocol (IP)

15

L'Internet Protocol (IP) è il protocollo utilizzato nel layer 3 (rete).

- È lo standard per l'instradamento di pacchetti all'interno delle reti
- Incapsula i dati e li passa in forma di pacchetti
- Ogni pacchetto include:
 - l'indirizzo IP della sorgente
 - l'indirizzo IP del destinatario

Indirizzamento IP

- Gli indirizzi IP, nella versione 4, sono:
 - Formati da 32 bits
 - Raggruppati in quattro ottetti da 8 bit
 - Rappresentati da un numero decimale, ogni ottetto è separato dagli altri attraverso un punto

11000000 10101000 01100100 11001000
192 . 168 . 100 . 200

Indirizzi IP e Netmask

17

- Un indirizzo IP ha due componenti:
 1. un componente che corrisponde alla rete (la via)
 2. un componente corrispondente all'host (il numero della casa)
- La netmask permette questa separazione in due componenti: combinando la netmask e l'indirizzo IP con un AND logico, viene fuori la componente corrispondente alla rete

11000000 10101000 01100100 11001000 address

192 . 168 . 100 . 200

11111111 11111111 11111111 00000000 netmask (/24)

255 . 255 . 255 . 0

network 11000000 10101000 01100100 00000000 **host**

192 . 168 . 100

Indirizzi IP e Netmask

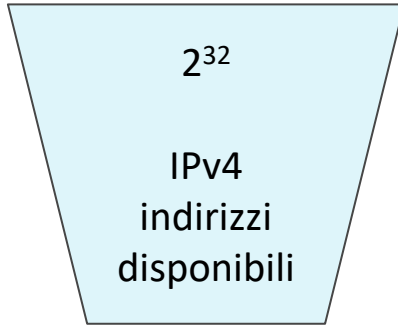
18



192.168.100.200
(indirizzo dell'host)



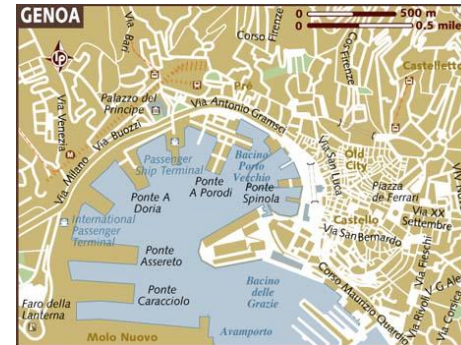
192.168.100
(indirizzo di rete)



35
(civico)



via Dodecaneso
(via)



Indirizzi IP riservati

19

In ogni rete ci sono due indirizzi IP riservati che non possono essere utilizzati dagli host

- **Indirizzo della rete:** Il primo indirizzo della rete (quello in cui tutti i bit relativi all'host sono uguali a 0), esso identifica la rete
- **Indirizzo di Broadcast:** l'ultimo indirizzo della rete (quello in cui tutti i bit relativi all'host sono uguali a 1). I pacchetti inviati a questo indirizzo si intendono inviati a tutti i nodi di quella rete

```
11000000 10101000 01100100 11001000 address
    192 . 168 . 100 . 200
11111111 11111111 11111111 00000000 netmask (/24)
    255 . 255 . 255 . 0
```

```
11000000 10101000 01100100 00000000 network addr.
    192 . 168 . 100 . 0
11000000 10101000 01100100 11111111 broadcast addr.
    192 . 168 . 100 . 255
```

Indirizzi IP privati

20

Alcuni indirizzi IP, detti *privati*, non vengono trasmessi all'interno di Internet

- Gli indirizzi IP privati sono validi solo all'interno di reti locali.
 - Indirizzi da 10.0.0.0 a 10.255.255.255
rete 10.0.0.0 con 255.0.0.0 o /8 (8-bit) mask
 - Indirizzi da 172.16.0.0 a 172.31.255.255
rete 172.16.0.0 con 255.240.0.0 o /12 (12-bit) mask
 - Indirizzi da 192.168.0.0 a 192.168.255.255
rete 192.168.0.0 con 255.255.0.0 or /16 (16-bit) mask

Neighbor Table and Address Resolution Protocol (ARP)

21

- Se un nodo vuole comunicare con un host all'interno della stesso livello 2
 - Ha l'indirizzo fisico del nodo destinatario (generalmente l'indirizzo MAC), oppure
 - Invia una richiesta ARP (Address Resolution Protocol), essa è una richiesta attraverso l'indirizzo broadcast che chiede "Qual è l'indirizzo fisico del nodo con indirizzo IP X.X.X.X ?"
- Se il destinatario è disponibile risponde con il suo indirizzo

IP Routing

22

- L'IP Routing è il processo che permette di inviare pacchetti tra host di reti differenti
 - Ciascun nodo esamina l'indirizzo IP di destinazione e determina il successivo host (next-hop) a cui inoltrare il pacchetto.
 - Per determinare l'indirizzo del passo successivo si utilizzano le tabelle di routing

Tabelle di routing

23

- La tabella di routing è utilizzata dai nodi per determinare il percorso per arrivare alla rete di destinazione
- Ogni tabella di routing fornisce le seguenti informazioni:
 - Rete di destinazione
 - Indirizzo IP del dispositivo successivo che gli permette di raggiungere la rete di destinazione
 - Interfaccia di rete da utilizzare per raggiungere la rete di destinazione

Tabelle di routing (esempio)

24

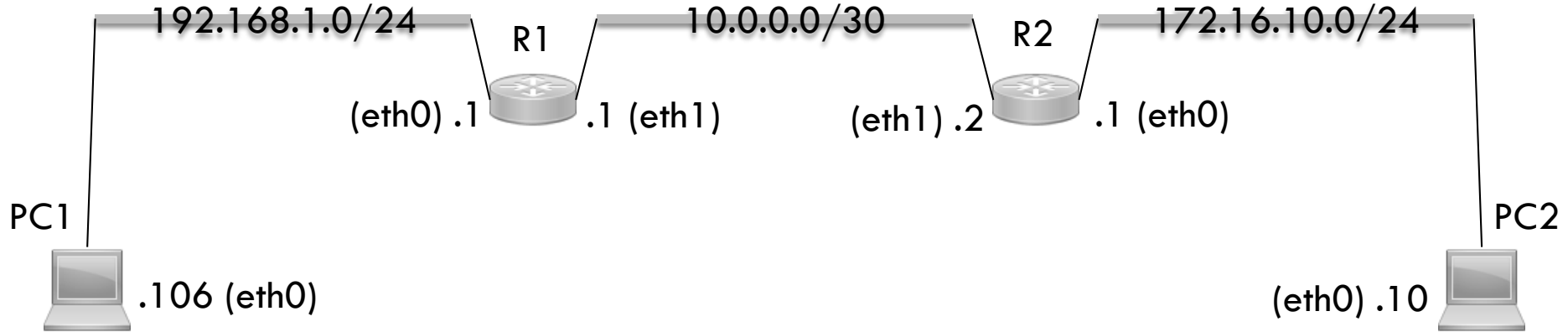
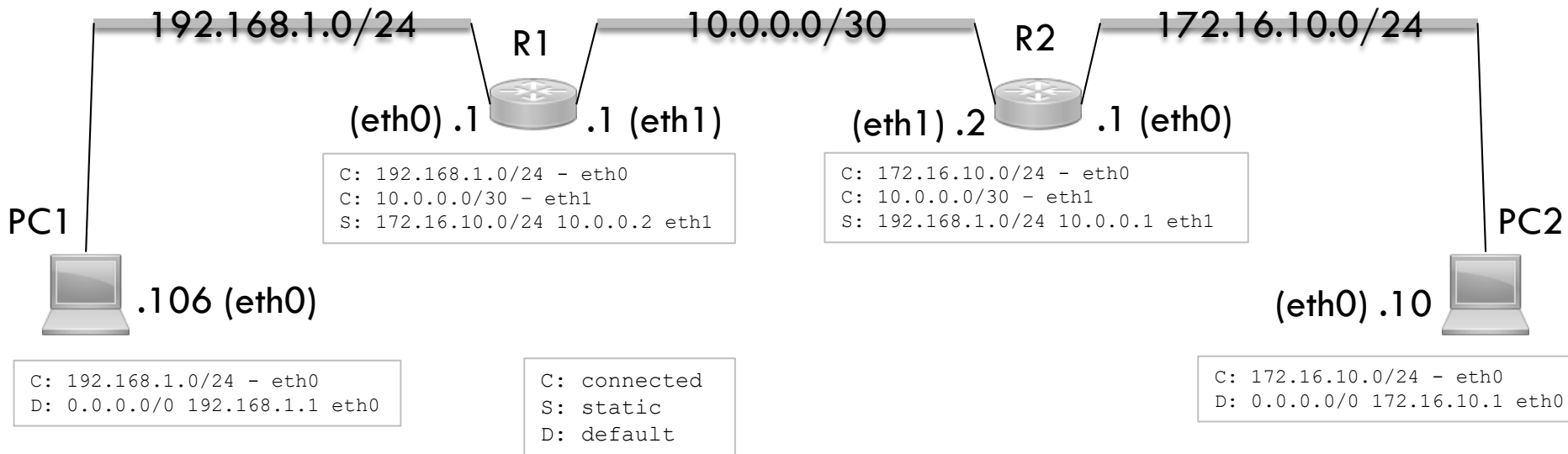


Tabelle di routing (esempio)

25



Indice

26

- Modello ISO/OSI, modello TCP/IP
- Layer 3: IP e routing
- **Layer 4: TCP e UDP**
- Modello Client/Server

TCP vs UDP

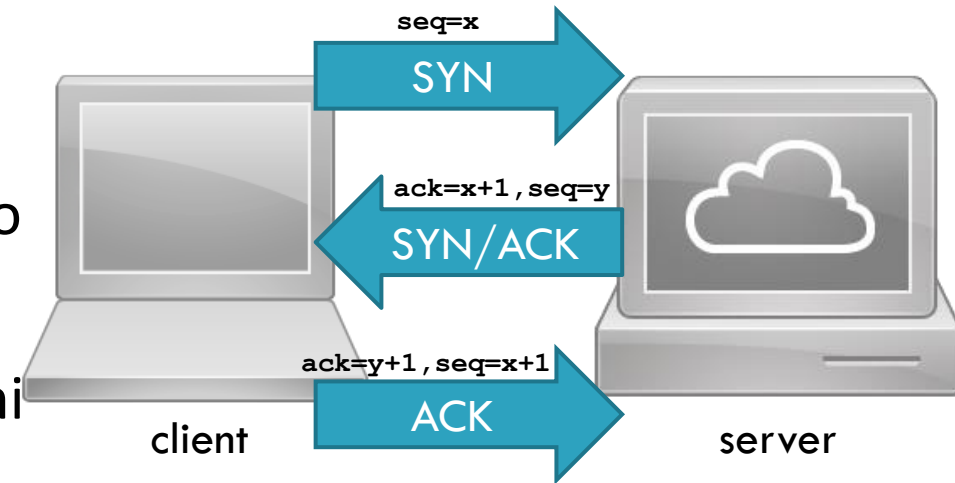
27

- TCP e UDP sono I protocolli più utilizzati nel layer 4
 - TCP prima crea una connessione, poi invia il contenuto della comunicazione. UDP trasmette direttamente dati
 - Entrambi controllano errori attraverso checksum, ma UDP non fa nessuna azione a riguardo. TCP invece è in grado di correggere gli errori
 - TCP ordina I pacchetti, UDP invece non ha un ordine predefinito per I pacchetti
 - I pacchetti TCP sono più grandi in termini di spazio rispetto ai pacchetti UDP

TCP - Three-Way Handshake

28

- TCP utilizza il *three-way handshake* per stabilire una connessione affidabile
- L'utilizzo di un numero di sequenza (seq) e un numero di accettazione (ack), permette a entrambe le parti di rilevare dei problemi all'interno della comunicazione



Layer 4 indirizzamento: porte

29

- Il layer 4 si occupa anche della comunicazione tra processi remoti
- Questi processi sono identificati attraverso porte così definite:
 - 16-bit unsigned integer (0-65535, 0 riservato)
 - **Well-known ports** (0-1023): usate da processi di Sistema particolarmente rilevanti
 - **Registered ports** (1024-49151): assegnate da IANA a particolari applicazioni previa registrazione
 - **Ephemeral ports** (49152–65535): porte dinamiche o per servizi private.
- Nonostante questa convenzione, qualsiasi servizio può ascoltare su qualsiasi porta!

Indice

30

- Modello ISO/OSI, modello TCP/IP
- Layer 3: IP e routing
- Layer 4: TCP e UDP
- **Modello Client/Server**

Il modello client-server

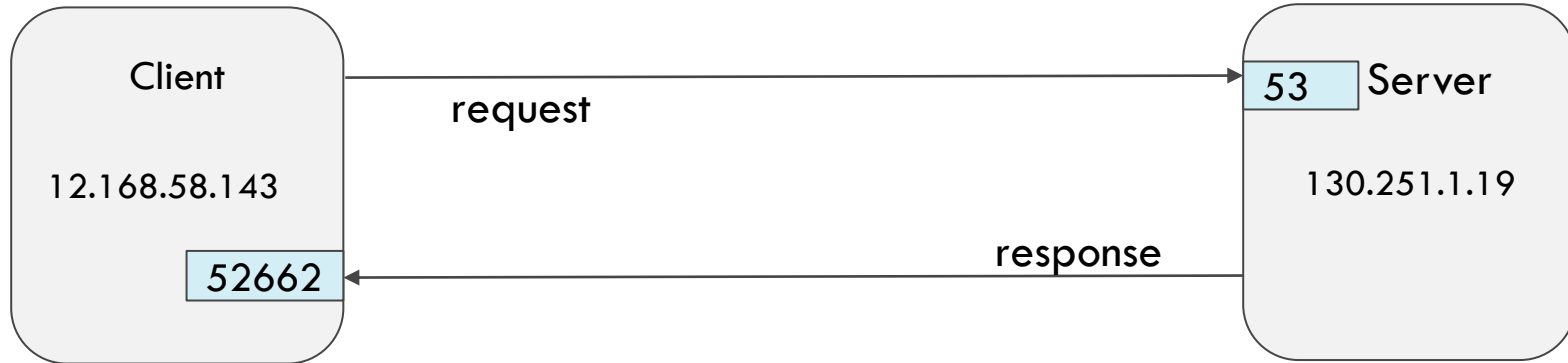
31

- Il modello client-server è il paradigma più utilizzato per la comunicazione all'interno di reti
 - Si ha una relazione per cui un programma (client) richiede un servizio o una risorsa a un altro programma (server)
 - Il client deve conoscere l'indirizzo del server
 - Il server non per forza deve conoscere l'indirizzo (o l'esistenza) del client prima della connessione

Il modello client-server (esempio DNS)

32

12.168.58.143	52662 (ephemeral)	130.251.1.19	53 (well-known)	<pre>Queries olicyber.it: type A, class IN Name: olicyber.it Type: A (Host address) Class: IN (0x0001)</pre>
Source IP	Source Port	Destination IP	Destination Port	Data



Data	Destination Port	Destination IP	Source Port	Source IP
------	------------------	----------------	-------------	-----------

<pre>Answers [...] olicyber.it: type A, class IN Name: olicyber.it Type: A (Host address) Class: IN (0x0001) Addr: 104.21.89.84 [...]</pre>	52662 (ephemeral)	12.168.58.143	53 (well-known)	130.251.1.19
---	-------------------	---------------	-----------------	--------------

Luigi SCIOLLA

Università di Genova

Network Security

Fondamenti di reti di calcolatori



<https://cybersecnatlab.it>