



Guida del Gioco di Ruolo Cappuccetto **Rosso** 2.0

RICONNESSIONI
educazione al futuro

Questa guida ha l'intento di rendere chiare le dinamiche e le tematiche che caratterizzano il gioco di ruolo Cappuccetto Rosso 2.0, proposto durante la seconda giornata del corso Essere Digitali del progetto Riconessioni (<https://www.riconessioni.it/notizie/laboratori/essere-digitali/>).

Sulla falsa riga di un regolamento di un comune gioco da tavolo, di seguito verranno presentati nell'ordine:

1. **il background narrativo**, utile per incuriosire i giocatori incorniciando il gioco in un contesto diverso da quello tecnico;
2. **il background tecnico** che renda consapevole l'insegnante che intende proporre il gioco ai propri studenti delle semplificazioni apportate al modello di rete Internet, su cui si basa il regolamento del gioco, rispetto a quello reale;
3. **il materiale e il campo di gioco** da predisporre prima di iniziare a giocare;
4. **le regole di gioco**;
5. **alcune idee per espandere il regolamento** e personalizzarlo in base al contesto classe o ai processi che si intende approfondire maggiormente;
6. **tabelle di sintesi**, per una consultazione rapida del regolamento durante la partita.

1. Background narrativo

E' estate, e una vivace bambina sta trascorrendo le vacanze con la famiglia in una ridente località di montagna. Durante un'escursione nel bosco, poco distante dal loro campeggio, la bambina scorge tra gli alberi un piccolo ponticello rosso su un calmo ruscello. Rapita da questo paesaggio, scatta una foto col cellulare e decide di inviarla subito alla nonna rimasta in città.

Nello stesso momento però, in un luogo sconosciuto, un losco hacker si intromette nella comunicazione e riesce a ottenere l'indirizzo email della nonna. In un attimo scrive un messaggio ingannevole, con cui spera di impossessarsi dei dati della carta prepagata su cui l'anziana riceve i soldi della pensione. E glielo invia. Riuscirà la nonna a ricevere il messaggio della nipote e a non cadere nella trappola dell'hacker?

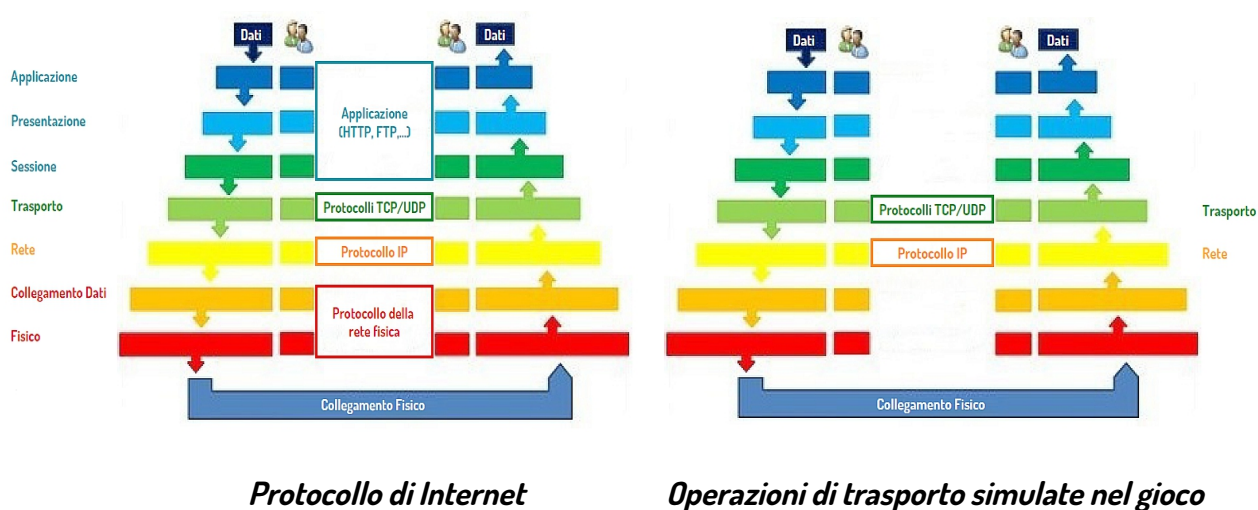
Il compito dei giocatori sarà quello di recapitare i due messaggi al computer della nonna, attraverso la rete Internet, e di evitare che l'email dell'hacker venga letta.

2. Background tecnico

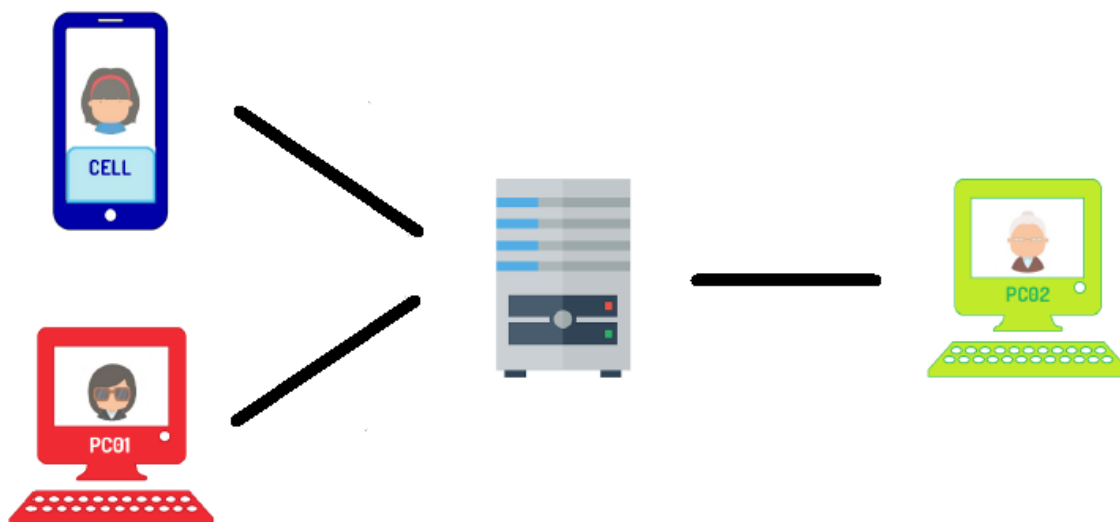
Il gioco ha lo scopo di far comprendere a chi non ha particolari competenze informatiche il funzionamento che regola la trasmissione di dati tra computer connessi in rete. Per poterlo fare in maniera efficace e ludica, rendendo l'attività fruibile a una classe di scuola primaria o secondaria, si è quindi scelto di creare un modello semplificato dell'intero processo e di simularlo con azioni semplici e attraverso materiali di uso comune.

In questo paragrafo saranno quindi messe in evidenza queste semplificazioni.

- i. Il tipo di rete che si intende simulare è Internet (quella maggiormente nota e diffusa, ma non l'unica, né la prima ad essere stata realizzata), e basata sul cosiddetto *protocollo TCP/IP*. Di questo insieme di regole e operazioni (raggruppabili nelle 4 macroaree raffigurate in basso a sinistra), tuttavia, verranno solamente simulate nel gioco quelle relative al trasporto dei dati sulla rete (immagine in basso a destra).






- ii. Nel gioco, ogni porzione di rete è costituita da 4 device o nodi. In particolare 2 pc, 1 telefono cellulare e 1 server. Ognuna di queste porzioni non comunica con le altre.

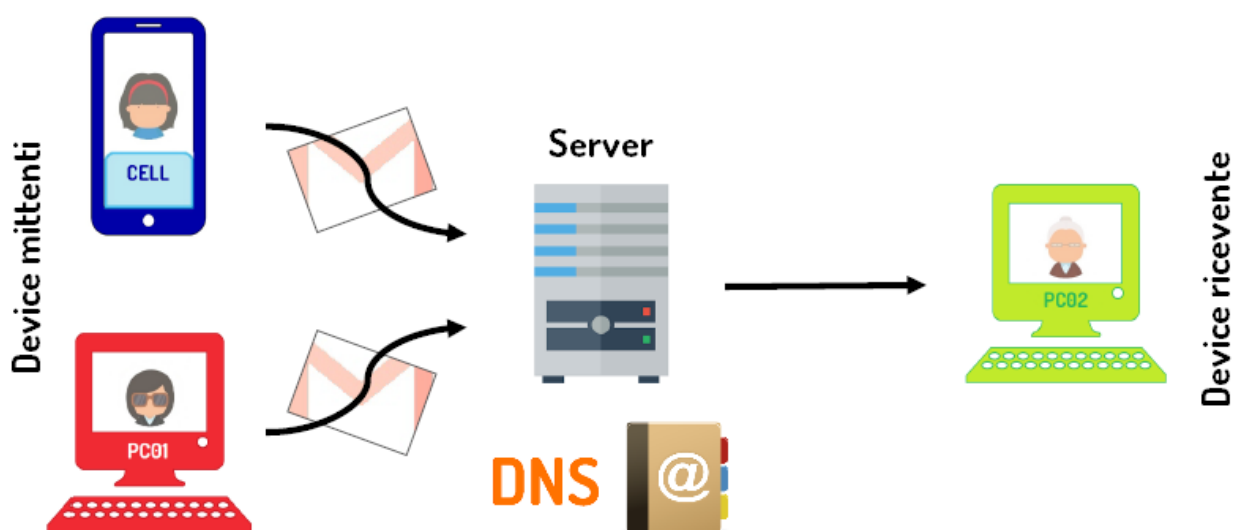


I 4 device che compongono una porzione di rete

- iii. Ogni device possiede un indirizzo numerico con il quale viene riconosciuto in maniera univoca all'interno della stessa porzione di rete (IP address). In questo modello il server non ha assegnato nessun indirizzo.

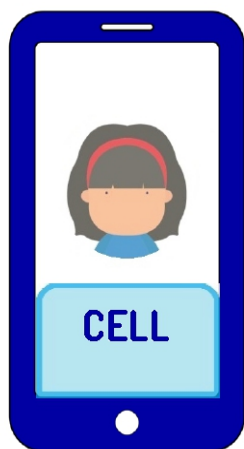
<i>Icona</i>	<i>Nome</i>	<i>Indirizzo</i>
	CELL	194.24.12.3
	PC01	194.24.12.1
	PC02	194.24.12.2

- iv. Il flusso dei dati di ciascuna porzione di rete segue una sola direzione. Questo significa che ogni device, escluso il server, ha un solo ruolo ben specifico: o è mittente o è ricevente. Tutte le porzioni di rete hanno in comune il DNS che regola il traffico dei dati sull'intera rete.



Suddivisione device tra mittenti e riceventi, il DNS governa il traffico di ogni dispositivo

- v. Esistono solo due tipi di messaggi inviati sulla rete, e ognuno dei due messaggi può essere inviato solo da un device specifico.



ID Messaggio:	
<p>Ciao Nonna!</p> <p>Guarda in che bel posto mi hanno portato mamma e papà... 😊</p> <p>Ci sentiamo presto!</p>	
From: CELL	To: PC02

Messaggio inviato dal cellulare



ID Messaggio:	
<p>Gentile utente,</p> <p>a seguito di attività sospette sul suo conto, le abbiamo bloccato la sua carta postepay.</p> <p>Per sbloccarla vada al seguente link e segua le istruzioni indicate.</p> <p>web.poste.it</p>	
From: PC01	To: PC02

Messaggio inviato dal PC 01

3. Materiale e campo di gioco

Il campo di gioco deve prevedere una postazione fissa per ogni device (un banco andrà benissimo). Questo significa che, per una partita tipo tra 2 squadre, serviranno almeno 9 postazioni (4 per squadra più una riservata al DNS che durante la partita si occuperà di regolare i flussi dei dati di tutte le squadre). Non è tuttavia indispensabile che, per la stessa squadra, le postazioni del *Cellulare della nipote* e del *PC 01 dell'hacker* siano separate.

Serviranno inoltre:

- 1 paio di forbici per squadra;
- 1 matita per squadra;
- 1 nastro adesivo per squadra;
- 1 contenitore per squadra (di cartone o plastica per raccogliere ritagli di fogli A4);
- 1 timbro a inchiostro o un pennarello per squadra;
- 8 copie delle Schede Messaggi Compilate Fronte Retro per squadra, da stampare fronte-retro;
- 1 copia della Rubrica DNS da ritagliare in modo da ricavare dei biglietti (17 per dispositivo) con un **Nome del device** e il relativo **Indirizzo**;
- 1 copia delle Schede Nodi Fronte Retro per squadra, da stampare fronte-retro;
- (Facoltativo) 1 copia delle Schede Personaggio Fronte Retro per squadra, da stampare fronte-retro.

I file da stampare si possono scaricare ai seguenti link:

Riconessioni/Gioco di Ruolo Cappuccetto Rosso 2.0
<https://www.riconessioni.it/notizie/laboratori/essere-digitali/>

Weschool
<https://app.weschool.com/#group/91085/boards/369355>

4. Regole di gioco

4.1. Caratteristiche generali e condizioni di vittoria

Come anticipato nel paragrafo precedente, il gioco è a squadre.

Ogni squadra rappresenta una porzione di rete Internet, composta dai 4 device descritti nel *background tecnico*, e su cui si verifica lo stesso scambio di messaggi tra nipote, hacker e nonna descritto nel *background narrativo*.

La squadra che consegna per prima tutti i messaggi della nipote e dell'hacker al *PC 02 della nonna* vince.

Per la prima partita si consiglia di impostare a 2 il numero di messaggi da inviare su ciascuna porzione di rete (1 della nipote e 1 dell'hacker). Una volta compreso il meccanismo da tutti i giocatori sarà possibile aumentarlo a piacere (con il materiale indicato, due squadre potranno scambiare fino a 16 messaggi ciascuna: 8 dalla nipote e 8 dall'hacker).

4.2. Composizione delle squadre

Ogni squadra è composta da 7 giocatori, ognuno con un ruolo specifico.

Ogni ruolo rappresenta un attore del protocollo TCP/IP e appartiene a un preciso device della rete. Questo significa che ogni giocatore potrà compiere le azioni pertinenti al ruolo assegnatogli solo per il proprio device.

In ogni partita deve essere presente almeno un giocatore esterno a ciascuna squadra: il DNS. Il suo ruolo sarà fondamentale per ogni squadra e imparziale.

I ruoli di ciascuna squadra, divisi per device, sono:

Cellulare della nipote: 1 IP Blu, 1 TCP Blu;

Pc 01 dell'hacker: 1 IP Rosso, 1 TCP Rosso;

Pc 02 della nonna: 1 IP Verde, 1 TCP Verde, 1 Antivirus Verde.

Durante la spiegazione delle regole, si consiglia di assegnare i ruoli dei giocatori già a questo punto. Prima cioè di spiegare le azioni di ciascun ruolo. Per agevolare il riconoscimento dei ruoli da parte di tutti i giocatori si possono usare, come cartelli da indossare, le Schede Personaggio Fronte Retro. Per riconoscere le postazioni invece si possono usare le Schede Nodi Fronte Retro.

4.3. Azioni dei ruoli: TCP Blu e TCP Rosso

La partita inizia dalle postazioni dei device mittenti (il *Cellulare della nipote* e il *PC 01 dell'hacker*), all'interno delle quali i relativi TCP e IP lavorano per inviare i messaggi del proprio dispositivo. I messaggi hanno due facciate che devono essere compilate dal TCP (Schede Messaggi Compilate Fronte Retro).

In particolare, sul fronte del messaggio il TCP deve scrivere l'**ID Messaggio** che si trova in alto a sinistra. Può scegliere qualsiasi nome, purché non l'abbia già scritto in un **ID Messaggio** precedente (per semplificare l'operazione si consiglia comunque una compilazione progressiva del tipo "0001", "0002", "0003"...). Gli altri campi "From" e "To" sono già precompilati.

ID Messaggio:	
Ciao Nonna!	
Guarda in che bel posto mi hanno portato mamma e papà... 😊	
Ci sentiamo presto!	
	
From: CELL	To: PC02

Fronte messaggio nipote

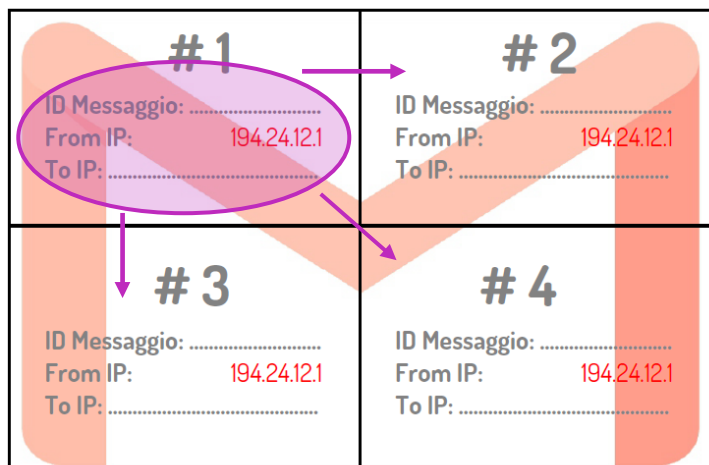
ID Messaggio:	
Gentile utente,	
a seguito di attività sospette sul suo conto, le abbiamo bloccato la sua carta postepay.	
Per sbloccarla vada al seguente link e segua le istruzioni indicate.	
web.poste.it	
From: PC01	To: PC02

Fronte messaggio hacker

Sul retro del messaggio, in ciascun riquadro, il TCP deve scrivere lo stesso l'**ID Messaggio** inserito sul fronte.

Nella voce **To IP** deve invece scrivere l'**Indirizzo** del *PC 02 della nonna* a cui è indirizzato il messaggio. Il TCP tuttavia non conosce questo dato e dovrà incaricare il proprio IP (se il TCP è Blu, incaricherà l'IP Blu, se è Rosso incaricherà l'IP Rosso) di richiederlo al DNS della rete. Una volta che l'IP è tornato alla postazione

del TCP con l'**Indirizzo** del *PC 02 della nonna*, quest'ultimo potrà completare la compilazione dei 4 riquadri presenti su retro del messaggio (le voci "From IP" sono precompilate).



Retro messaggio da compilare (hacker)

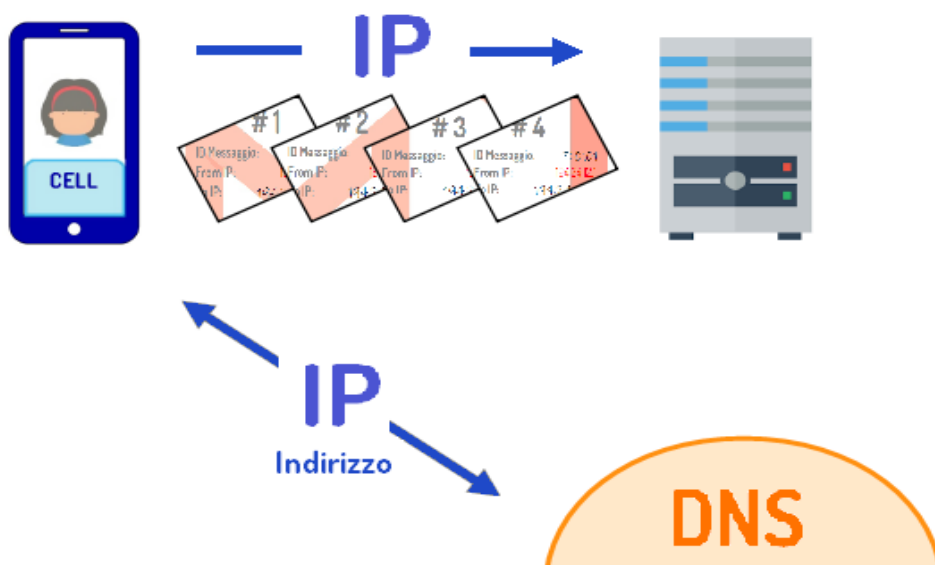
A questo punto il TCP ritaglia il messaggio in 4 parti (pacchetti), seguendo le linee che delimitano i riquadri presenti sul retro.

Le azioni dei TCP Blu e Rosso si concludono con la consegna dei pacchetti così ritagliati ai corrispondenti IP, per poi riprendere, nello stesso ordine, all'invio di un nuovo messaggio del proprio dispositivo.

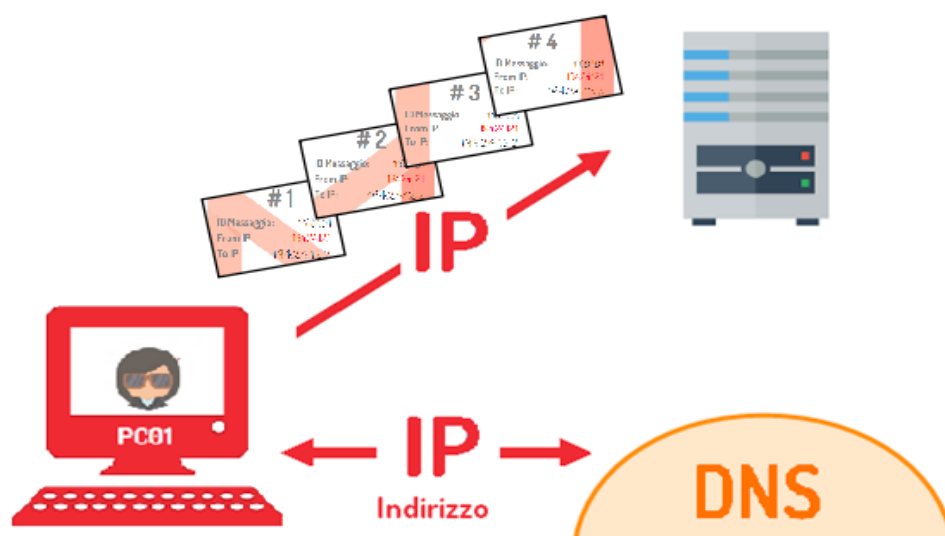
4.4. Azioni dei ruoli: IP Blu e IP Rosso

Gli IP si occupano solo di trasportare i dati attraverso le postazioni della rete.

In particolare, per ogni messaggio da inviare, recapitano la domanda del proprio TCP al DNS e riportano indietro la risposta sotto forma di biglietto (*Rubrica DNS*). Portano inoltre i pacchetti ritagliati dal proprio TCP, uno alla volta, nel raccogliitore presente nella postazione del server.



Percorsi dell'IP Blu sulla rete

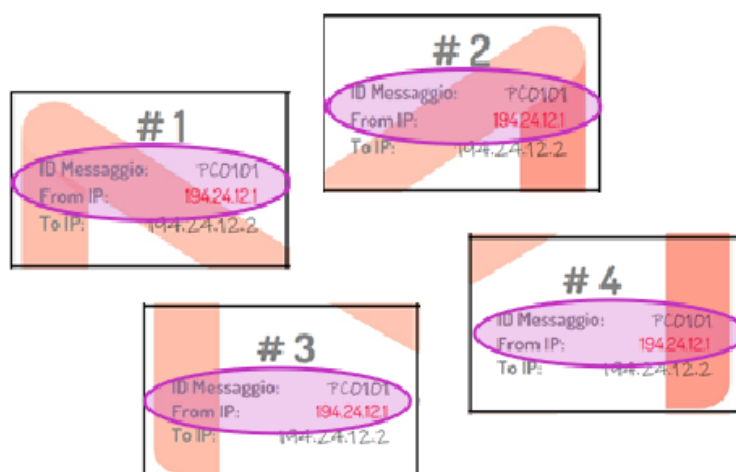


Percorsi dell'IP Rosso sulla rete

4.5. Azioni dei ruoli: IP Verde, TCP Verde e Antivirus Verde

L'IP verde deve solo portare i pacchetti depositati nel raccoglitore del server al TCP Verde nella postazione del *PC 02 della nonna*. Come per gli IP Blu e Rosso, dovrà compiere quest'azione prendendo solamente un pacchetto alla volta.

Il TCP Verde si deve invece occupare di ricostruire correttamente i messaggi ricevuti dall'IP Verde sotto forma di pacchetti. Per fare ciò dovrà raggruppare tra loro i pacchetti aventi gli stessi **ID Messaggio** e **From IP**. Una volta raccolti i 4 pacchetti dello stesso messaggio li unirà col nastro adesivo.

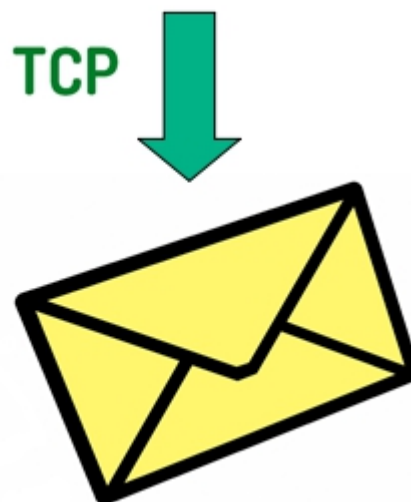
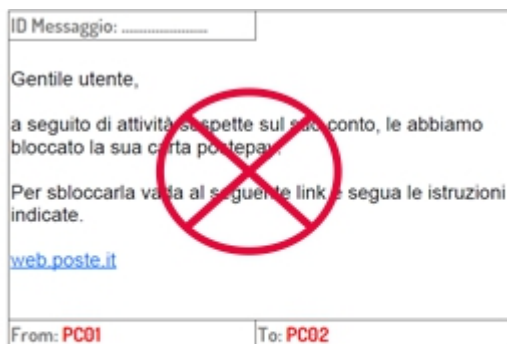


Pacchetti raggruppati per ID Messaggio e From IP

A questo punto il TCP Verde passa il messaggio ricostruito all'Antivirus Verde che dovrà valutare (anche solo leggendo il contenuto del messaggio) la pericolosità dello stesso e successivamente restituirlo al TCP

Verde. Se dovesse rilevare una minaccia per il *PC 02 della nonna* marchierà il messaggio con un timbro o con un pennarello prima di riconsegnarlo al TCP. Una volta riottenuto il messaggio dall'Antivirus Verde, il TCP Verde depositerà il messaggio nello **SPAM** (*Schede_Nodi_Fronte_Retro*) se quest'ultimo riporta il marchio dell'Antivirus, altrimenti depositerà il messaggio nella **CASELLA DI POSTA** della nonna (*Schede_Nodi_Fronte_Retro*).

Una volta che un messaggio è stato depositato nello **SPAM** o nella **CASELLA DI POSTA** avrà terminato il suo percorso sulla rete e si considera ricevuto dal *PC 02 della nonna*.



I messaggi della nipote e dell'hacker concludono il loro percorso nello spam o nella posta in arrivo

4.6. Il DNS

Il DNS partecipa al gioco di tutte le squadre ma non appartiene a nessuna di esse. Non può vincere e non può perdere. E' imparziale nei confronti di tutte le squadre e conosce gli **Indirizzi** di tutti i device di ogni squadra.

La sua unica azione consiste nel dare il biglietto (ricavato dalla Rubrica_DNS), con Nome e Indirizzo del dispositivo richiesto, a ogni IP che arriva alla sua postazione.

5. Possibili espansioni (emerse in aula durante le edizioni precedenti di Essere Digitali)

- aumentare la varietà e il numero di messaggi inviati
- aumentare il numero di device mittenti e riceventi, consentendo in particolare la possibilità per ciascun pacchetto di intraprendere percorsi diversi per arrivare al device ricevente
- consentire comunicazioni tra device di porzioni di rete diverse. In questo caso occorrerà introdurre nuovi indirizzi per i dispositivi, in modo da non avere ripetizioni, e aggiornare conseguentemente la rubrica del DNS.
- ogni device può inviare e ricevere
- adattare le dinamiche di trasporto dati da parte degli IP, simulando in maniera coerente le tecnologie di connessione (wifi – perdita di pacchetti possibile, adsl – perdita di pacchetti improbabile, fibra ottica – perdita di pacchetti pressoché nulla).
- introdurre un device che possenga il database aggiornato dei virus a cui gli Antivirus devono interfacciarsi (allo stesso modo degli altri device mittenti) per poter riconoscere nuove minacce in arrivo coi dati ricevuti da altri device
- introdurre la ricevuta di ritorno sulla consegna dei singoli pacchetti. In questo caso, se la ricevuta non arriva al device mittente entro un certo periodo fissato, quest'ultimo reinvia allo stesso device ricevente il pacchetto di cui manca la ricevuta

6. Tabelle riassuntive

Tabella Cellulare della nipote:

<i>Ruolo</i>	<i>Descrizione</i>	<i>Azioni</i>	<i>Interazioni</i>
TCP Blu	ricompone i messaggi dai pacchetti ricevuti da un device della rete	incarica l'IP Blu di ottenere dal DNS l'indirizzo del PC 02 della nonna compila le voci mancanti dei messaggi della nipote ritaglia in quattro parti il messaggio compilato e lo consegna all'IP Blu	con l'IP Blu
IP Blu	trasporta i pacchetti inviati dal proprio device attraverso i nodi della rete	interroga il DNS riguardo all'indirizzo del PC 02 della nonna e riporta la risposta al TCP Blu porta, uno alla volta, i pacchetti ritagliati dal TCP Blu al server della sua porzione di rete	con il TCP Blu con il DNS

Tabella PC 01 dell'hacker:

<i>Ruolo</i>	<i>Descrizione</i>	<i>Azioni</i>	<i>Interazioni</i>
TCP Rosso	ricompone i messaggi dai pacchetti ricevuti da un device della rete	incarica l'IP Rosso di ottenere dal DNS l'indirizzo del PC 02 della nonna compila le voci mancanti dei messaggi dell'hacker ritaglia in quattro parti il messaggio compilato e lo consegna all'IP Rosso	con l'IP Rosso
IP Rosso	trasporta i pacchetti inviati dal proprio device attraverso i nodi della rete	interroga il DNS riguardo all'indirizzo del PC 02 della nonna e riporta la risposta al TCP Rosso porta, uno alla volta, i pacchetti ritagliati dal TCP Rosso al server della sua porzione di rete	con il TCP Rosso con il DNS

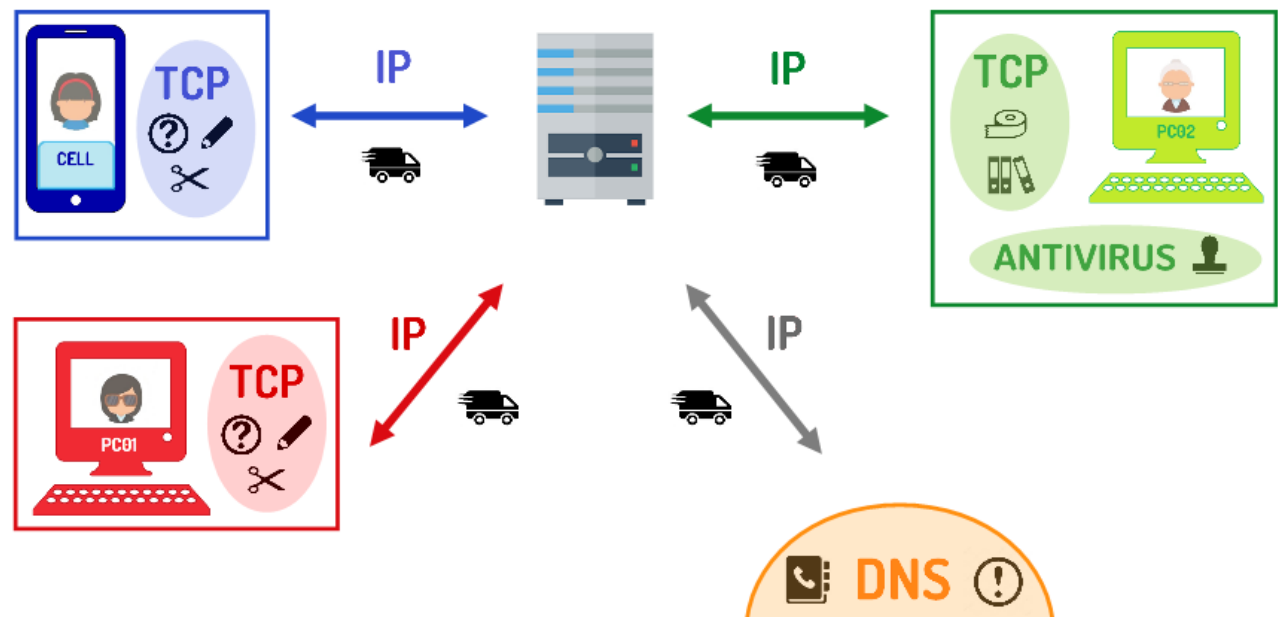
Tabella PC 02 della nonna:

<i>Ruolo</i>	<i>Descrizione</i>	<i>Azioni</i>	<i>Interazioni</i>
TCP Verde	ricompone i messaggi dai pacchetti ricevuti da un device della rete	divide in gruppi da 4 i pacchetti ricevuti dall'IP che hanno gli stessi "ID Messaggio" e "From IP" ricompone ciascun gruppo di pacchetti col nastro adesivo e consegna all'Antivirus Verde il messaggio così ricostruito smista i messaggi ricevuti dall'Antivirus Verde tra "Posta in Arrivo" e "SPAM"	con l'IP Verde con l'Antivirus Verde
IP Verde	trasporta i pacchetti inviati verso il proprio device attraverso i nodi della rete	porta i pacchetti dal server della sua porzione di rete al TCP Verde	con il TCP Verde
Antivirus Verde	filtra i messaggi in arrivo sul suo device scartando quelli pericolosi	controlla i messaggi ricevuti dal TCP Verde e marca con un timbro o un pennarello quelli ritenuti pericolosi restituisce al TCP Verde tutti i messaggi controllati	con il TCP Verde

Tabella DNS:

Ruolo	Descrizione	Azioni	Interazioni
DNS	possiede la rubrica con gli indirizzi esatti dei device connessi alla sua rete e smista il traffico sulla rete stessa	su richiesta di un IP (Blu o Rosso) consegna l'indirizzo esatto del device della rete richiesto	tutti gli IP Blu tutti gli IP Rosso

Tabella di sintesi grafica: sono messe in evidenza le postazioni dei diversi device della rete con i ruoli dei giocatori



- Manda l'IP dal DNS per chiedere l'Indirizzo del PC 02
- Compila i 4 pacchetti del messaggio
- Ritaglia in 4 pacchetti il messaggio
- Unisci i 4 pacchetti aventi gli stessi "ID Messaggio" e "From IP"
- Dai ciascun messaggio all'Antivirus. Una volta riottenuto, archivalo tra Spam e Posta in Arrivo
- Prendi i messaggi ricomposti dal TCP, marca quelli pericolosi e restituisci tutto al TCP
- Trasporta la richiesta del proprio TCP al DNS
Trasporta la risposta del DNS al proprio TCP
Trasporta i pacchetti ritagliati dal proprio TCP al Server
Trasporta i pacchetti dal Server al proprio TCP