ITS Academy
Adriano
Olivetti

TCP / IP - Livello di Rete (IP)

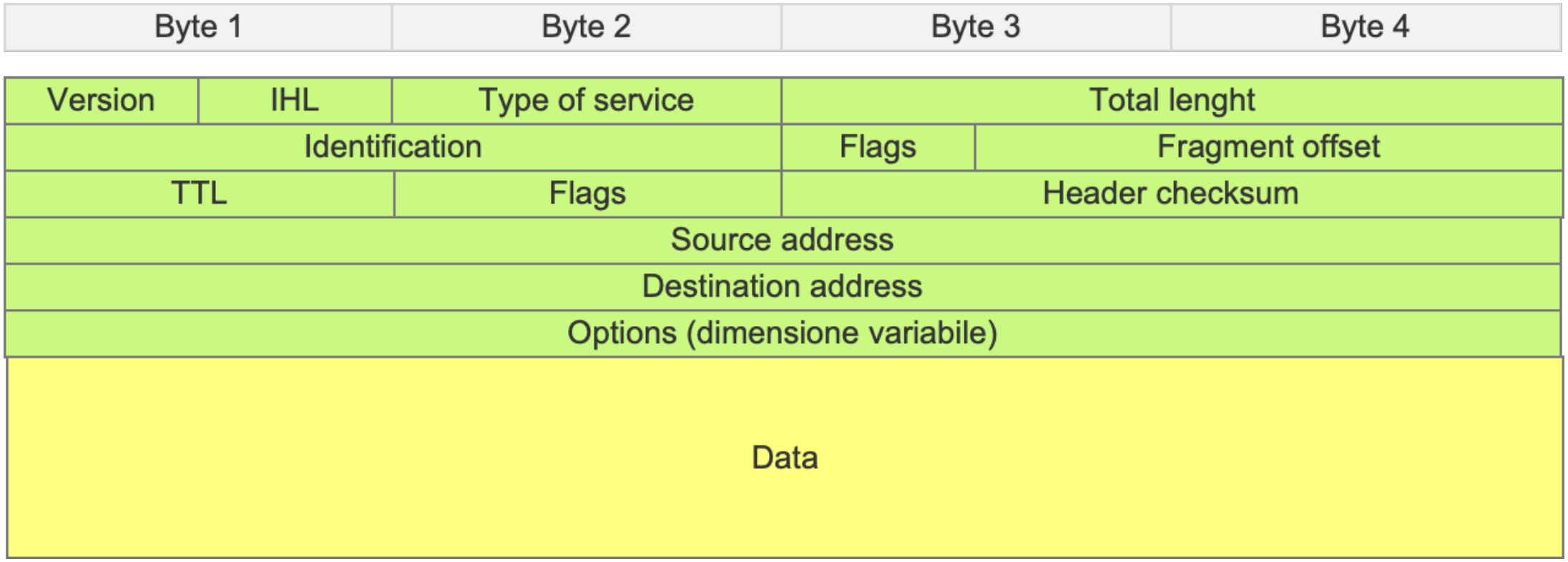
Modello TCP / IP – Livello di Rete (IP)

Il livello di rete è gestito dal protocollo IP (Internet protocol). Si affida ai servizi del livello di Fisico e pertanto è indipendente dal particolare mezzo trasmissivo utilizzato.

IP si occupa principalmente di:

- Definire indirizzi logici a livello di rete, detti indirizzi IP
- Mappare gli indirizzi IP con gli indirizzi fisici del livello sottostante (p.e. MAC address)
    - Gestendo i casi in cui non è possibile effettuare il mapping
- Frammentare i dati provenienti dai livelli superiori in datagrammi di dimensioni più contenute
- Inoltrare i pacchetti verso il destinatario, secondo la strada corretta (Routing)

Modello TCP / IP – Livello di Rete (IP)



Modello TCP / IP – Livello di Rete (IP)

- Version: Formato dell'intestazione. Attualmente è 4
- IHL: Lunghezza dell'intestazione espressa in parole di 32 bit. Lunghezza minima = 5
- Type of service: indicazione sul tipo di servizio. Usato anche come priorità
- Total lenght: lunghezza totale del datagramma espressa in byte. Lunghezza massima 65535
- Identification: valore che identifica univocamente un datagramma. Per determinare a quale datagramma appartiene un frammento
- Flag: Permette di specificare se il datagramma si può frammentare e se è stato frammentato
- Fragment offset: indica la posizione nel datagramma del frammento attuale. Espresso come distanza in multipli di 64 bit.
- Time to live: Indica il numero massimo di nodi attraversabili prima di essere scartato.

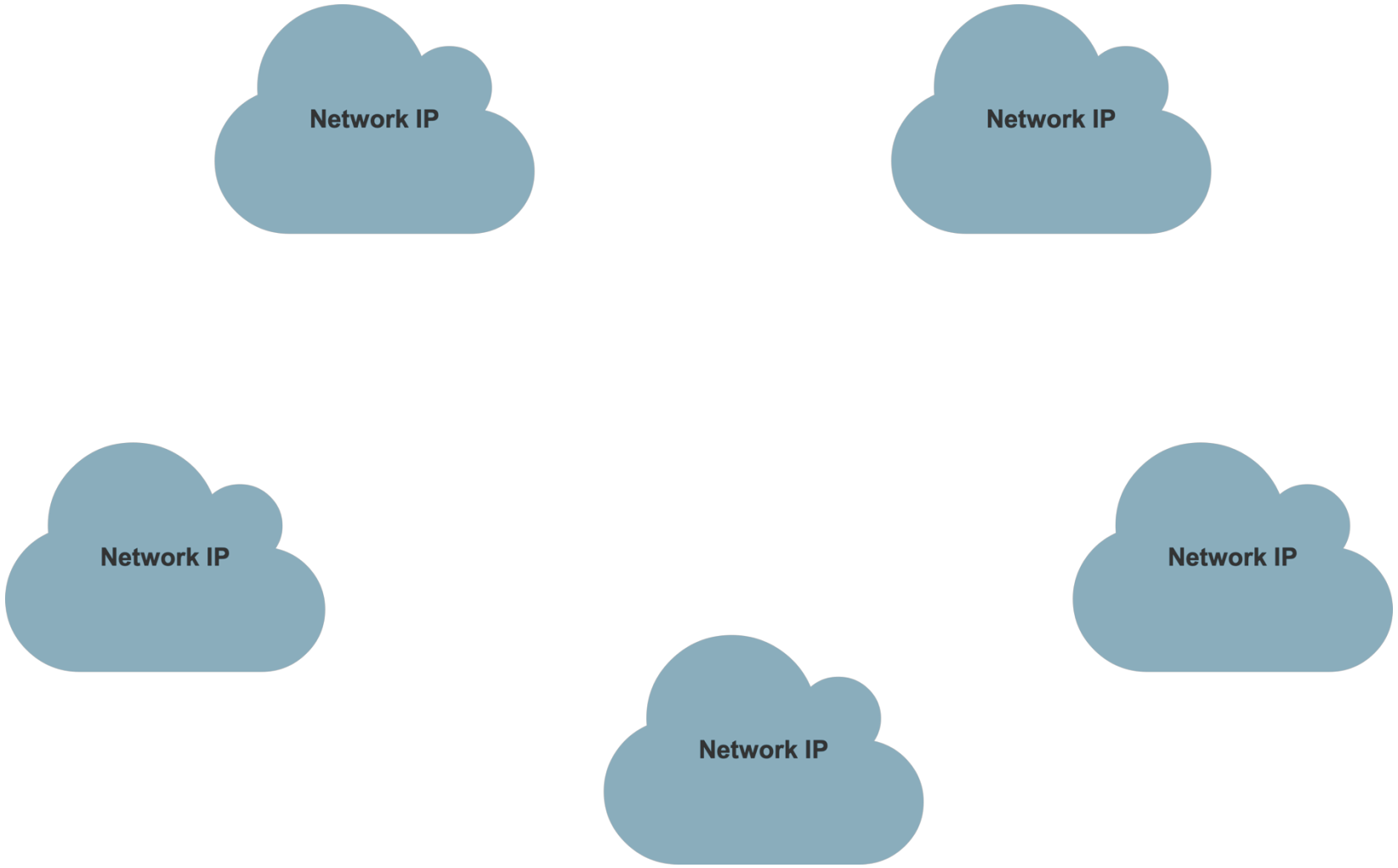
Modello TCP / IP – Livello di Rete (IP)

- Protocol: indica il protocollo di livello superiore a cui appartengono i dati nel datagramma
- Header Checksum: controllo dell'errore. Ricalcolato dopo il passaggio da ogni nodo
- Source address: Indirizzo IP sorgente
- Source address: Indirizzo IP di destinazione
- Options: Contiene opzioni varie relative al trasferimento del datagramma. È una sezione di lunghezza variabile

Modello TCP / IP – Livello di Rete (IP) – Routing

- Il protocollo IP è responsabile dell'instradamento dei dati, ovvero della loro trasmissione verso l'host più opportuno.
- Non è un compito semplice in quanto, tipicamente, esistono più modi per unire una sorgente a una destinazione.
- Il ruouting IP sfrutta la struttura a reti interconnesse (già vista in precedenza) propria di internet.
- Nella terminologia TCP / IP si utilizza il termine Network IP per identificare una singola rete, interconnessa con le altre.
- Una network IP può essere vista come una "isola" dentro la quale sono contenuti gli host
- Le varie "isole" sono tra di loro interconnesse tramite ponti che chiamiamo router o gatway

Modello TCP / IP – Livello di Rete (IP) – Routing



Modello TCP / IP – Livello di Rete (IP) – Routing

Ogni network IP può essere realizzata con tecnologie differenti, anche non compatibili tra di loro:

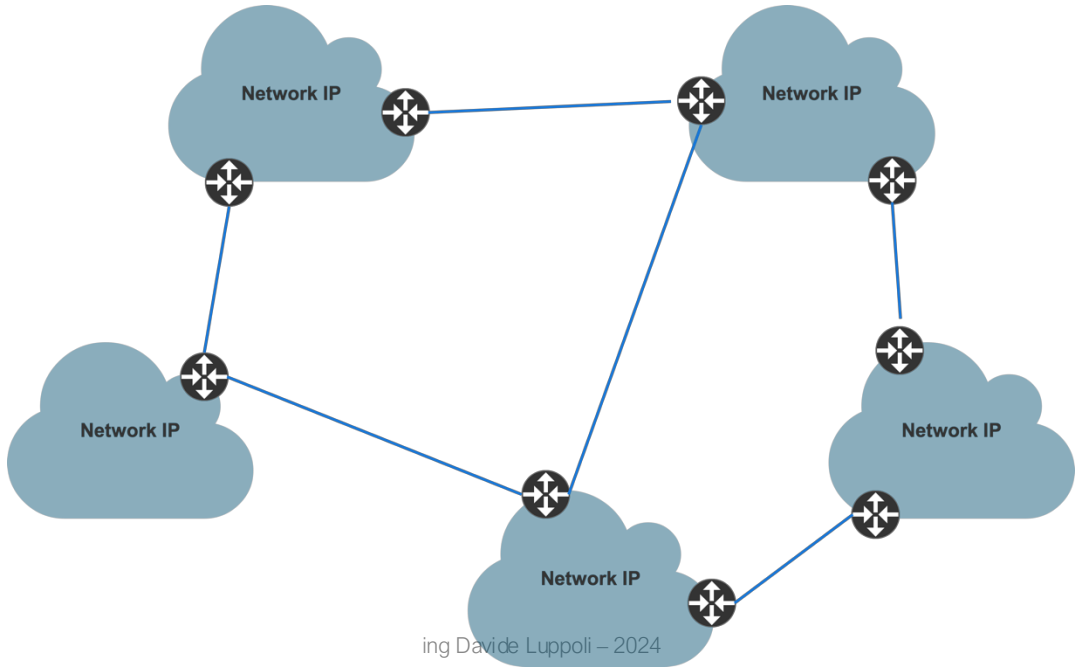
- WiFi
- Ethernet
- 4G / 5G
- …

Gli host che appartengono ad una rete sono connessi alla medesima infrastruttura di rete fisica (primo livello stack tcp / ip, primi due livelli dello stack iso / osi). Tutti gli host sono pertanto in grado di comunicare tra di loro utilizzando solamente il livello fisico.

Modello TCP / IP – Livello di Rete (IP) – Routing

Affinché le Network IP possano comunicare tra di loro è necessario che:

- Ci siano dei collegamenti fisici tra le isole, anche utilizzando tecnologie differenti
- Vi siano apparati in grado di usare tali collegamenti (router o gateway)
- Ci sia la possibilità di stabilire verso quale router inviare i dati per raggiungere la network IP desiderata



Modello TCP / IP – Livello di Rete (IP) – Routing

Nel momento in cui un host ha un datagramma da inviare si pone una domanda:

- Il destinatario è nella mia stessa Network IP o devo usare un gateway?
- Se il destinatario è sulla stessa rete allora i dati gli vengono inviati direttamente (utilizzando la network interface)
- Se il destinatario è su una rete diversa allora i dati vengono inviati al gateway, con la richiesta di inviarli a destinazione (utilizzando la network interface)

Per rispondere alla domanda, ogni host mantiene alcune informazioni, nella forma di:

- Proprio indirizzo IP
- Subnet mask

} → Per determinare se il destinatario è nella propria Network IP

- Routing table → Per determinare a quale gateway inviare di dati

Non bastavano i MAC address?

Il protocollo IP definisce il proprio sistema di indirizzamento per alcuni semplici motivi:

- Il livello fisico può utilizzare varie tecnologie ognuna con il proprio sistema di indirizzamento
- Gli indirizzi IP possono essere creati in modo adatto alle esigenze del livello di trasporto, senza essere influenzato dal livello di rete.
- Gli indirizzi IP sono logici e non sono associati alle schede di rete:
  - Più semplicità di manutenzione, in caso di guasto di una scheda di rete e/o dell'aggiornamento hardware di un server
  - Possibilità di spostare un indirizzo IP da un PC ad un altro

Modello TCP / IP – Livello di Rete (IP) – Indirizzi IP v4

Ad ogni host deve essere associato un indirizzo IP:

- Un indirizzo IP è composto da 32 bit ed è rappresentato da 4 numeri a 8 bit (da 0 a 255), separati da punto
- Gli indirizzi IP sono quindi in numero finito e vengono assegnati da una organizzazione centrale (IANA) e le sue delegate
- Esistono alcuni indirizzi utilizzabili liberamente ma solo in rete locale (indirizzi locali)
- Gli indirizzi IP sono suddivisi in due parti:
  - Network ID: prefisso che identifica la Network IP a cui appartiene l'indirizzo
  - Host ID: suffisso che identifica l'host all'interno di una Network IP
  - Le due parti sono contigue. Il Network ID occupa i bit più significativi (a sinistra)
- Gli indirizzi ip si dividono in classi

Modello TCP / IP – Livello di Rete (IP) – Indirizzi IP v4

Indirizzi IP v4 di classe A:

- Primo bit a 0
- 7 bit per il network id → da 1 a 126 (0 e 127 sono riservati)
- 24 bit per l'host id → da 0 a 16.777.214
- Gli indirizzi completi vanno quindi da 1.0.0.0 a 127.255.255.255
- Sono quindi possibili 126 reti, ognuna di 16.777.214 host.
- Sono utilizzate per grandissime reti ed organizzazioni

Modello TCP / IP – Livello di Rete (IP) – Indirizzi IP v4

Indirizzi IP v4 di classe B:

- Primi due bit a 10
- 14 bit per il network id → da 0 a 16.384
- 16 bit per l'host id → da 0 a 65.534
- Gli indirizzi completi vanno quindi da 128.0.0.0 a 191.255.255.255
- Sono quindi possibili 16.384 reti, ognuna di 65.534 host.
- Sono utilizzate per grandi reti ed organizzazioni (per esempio università)

Modello TCP / IP – Livello di Rete (IP) – Indirizzi IP v4

Indirizzi IP v4 di classe C:

- Primi tre bit a 110
- 21 bit per il network id → da 0 a 2.097.152
- 8 bit per l'host id → da 0 a 254
- Gli indirizzi completi vanno quindi da 192.0.0.0 a 233.255.255.255
- Sono quindi possibili 2.097.152 reti, ognuna di 254host.
- Sono utilizzate per reti medio-piccole

Modello TCP / IP – Livello di Rete (IP) – Indirizzi IP v4

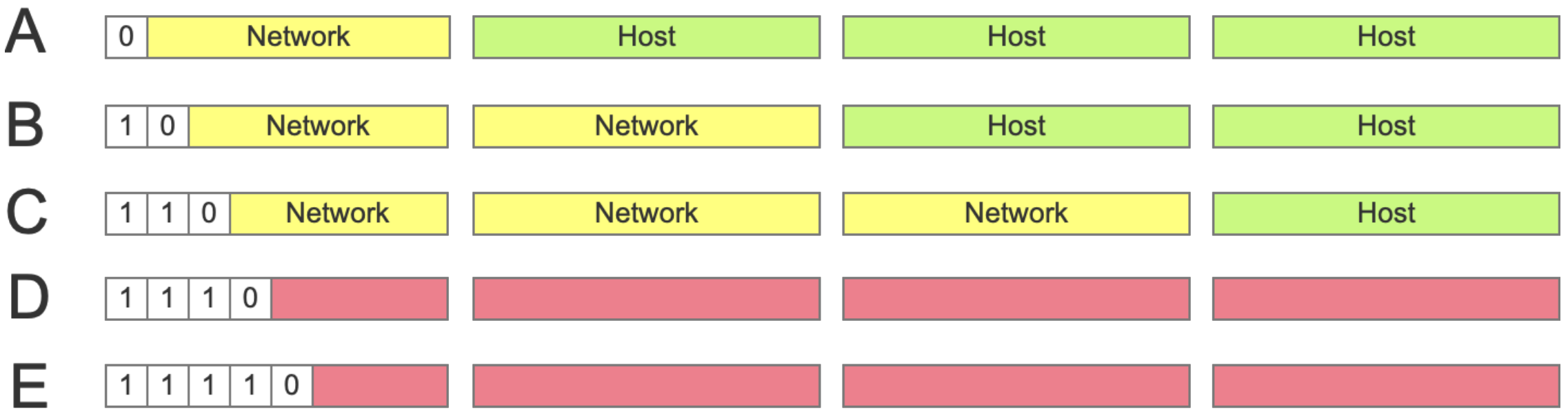
Indirizzi IP v4 di classe D:

- Primi quattro bit a 1110
- Sono indirizzi usati per trasmissioni multicast
- Gli indirizzi completi vanno quindi da 224.0.0.0 a 239.255.255.255

Indirizzi IP v4 di classe E:

- Primi cinque bit a 11110
- Sono indirizzi usati per estensioni future
- Gli indirizzi completi vanno quindi da 224.0.0.0 a 239.255.255.255

Modello TCP / IP – Livello di Rete (IP) – Indirizzi IP v4



Modello TCP / IP – Livello di Rete (IP) – Indirizzi IP v4

All'interno delle classi A, B, C esistono sottoreti con indirizzi IP privati, ovvero non assegnati dallo IANA e utilizzabili da chiunque solamente in rete locale:

Classe	Numero sottoreti	Range
A	1	10.0.0.0 – 10.255.255.255
B	16	172.16.0.0 – 172.31.255.255
C	256	192.168.0.0 – 192.168.255.255

La rete di classe A numero 127 (quindi da 127.0.0.0 a 127.255.255.255) contiene indirizzi che rappresentano l'interfaccia di loopback. È una interfaccia di rete virtuale che invia indietro ogni pacchetto ricevuto. È utilizzata principalmente per motivi di test.

Modello TCP / IP – Livello di Rete (IP) – subnet mask

- La divisione dell'indirizzo IP nella sua componente di Network ID e di Host ID avviene tramite la maschera di sottorete (o subnet mask o netmask).
- Ad ogni indirizzo host deve essere associato un IP e una maschera, affinché l'host sia in grado di dividere i due ID.
- La subnet mask è la medesima per tutti gli host della stessa rete
- Tramite la subnet mask è possibile realizzare reti di dimensioni minori rispetto a quanto previsto dalle classi IP A,B,C

La maschera di sottorete è un numero a 32 bit i cui primi n bit sono a 1 e i restanti bit sono a zero. Per esempio: 11111111.11111111.00000000.00000000

I bit a 1 della maschera identificano i bit dell'indirizzo IP che determinano la network id

Modello TCP / IP – Livello di Rete (IP) – subnet mask

Esempio:

- Ip: `137.204.191.25`
- In binario: `10001001.11001100.10111111.00011001`
- Sottomaschera: `11111111.11111111.11111111.11000000`
- Network ID: `10001001.11001100.10111111.00`
- Host ID: `011001`
- Fanno parte della stessa sottorete gli host da:
  `10001001.11001100.10111111.00000000` a
  `10001001.11001100.10111111.00111111`
- Ovvero gli IP da `137.204.191.0` a `137.204.191.63`
  - `137.204.191.0` è usato per identificare la rete, `137.204.191.63` per il broadcast

Modello TCP / IP – Livello di Rete (IP) – subnet mask

- Nell'esempio precedente si è realizzata una rete con massimo 64 host partendo da un indirizzo di classe B
- È possibile creare altre Network ID per meglio segmentare gli indirizzi disponibili

Esempio:

- Network ID: `10001001.11001100.10111111.01000000` `(137.204.191.64)`
- Sottomaschera: `11111111.11111111.11111111.11000000`
- Fanno parte della stessa sottorete gli host da:
  `10001001.11001100.10111111.01000000` a
  `10001001.11001100.10111111.01111111`
- Ovvero gli IP da `137.204.191.64` a `137.204.191.127`
  - `137.204.191.64` è usato per identificare la rete, `137.204.191.127` per il broadcast

Modello TCP / IP – Livello di Rete (IP) – subnet mask

La sottomaschera può essere espressa in più modi:

- In modo binario, separando con un punto ogni 8 bit:
  `11111111.11111111.11111111.11000000`
- Rappresentando in modo decimale ogni gruppo di 8 bit: `255.255.255.192`
- Rappresentando in modo esadecimale ogni gruppo di 8 bit: `FF.FF.FF.C0`
- Specificando solamente il numero di bit a 1: `/26`

Modello TCP / IP – Livello di Rete (IP) – Tabelle di routing

Le informazioni necessarie per instradare correttamente i datagrammi sono contenute in una tabella di routing.

Ogni host ne possiede una ma sono di maggior utilizzo sui router.

Ogni sistema operativo memorizza la tabella di routing in modo differente. Sono tutte però composte da:

- Righe che rappresentano i route. Una riga per ogni route.
- Colonne che rappresentano i parametri del route. Tra cui:
  - Network ID o host ID di destinazione (coppia IP + subnet)
  - Indirizzo del gateway
  - Identificativo della scheda di rete da utilizzare
  - Eventuali metriche per scegliere tra più route possibili

Modello TCP / IP – Livello di Rete (IP) – Tabelle di routing

Destinazione	Gateway	Interface	Metric
default	192.168.10.1	ppp0	1
137.204.64.0/24	137.204.64.254	en0	1
137.204.65.0/24	137.204.65.254	en1	1
192.168.10.0/30	192.168.10.2	ppp0	1

Quando un router deve inoltrare un datagramma, ne estrae l'indirizzo IP di destinazione e lo confronta con la routing table, verificando prima le righe con più 1 nella maschera.

Se l'indirizzo IP corrisponde con una delle sottoreti allora viene inoltrato verso la rispettiva interfaccia di rete.

Se non c'è nessun match viene utilizzato il route di default.

In assenza del route di default viene restituito un errore.

Modello TCP / IP – Livello di Rete (IP) – Tabelle di routing

Ricapitolando, quando deve inviare un datagramma un host esegue il seguente algoritmo:

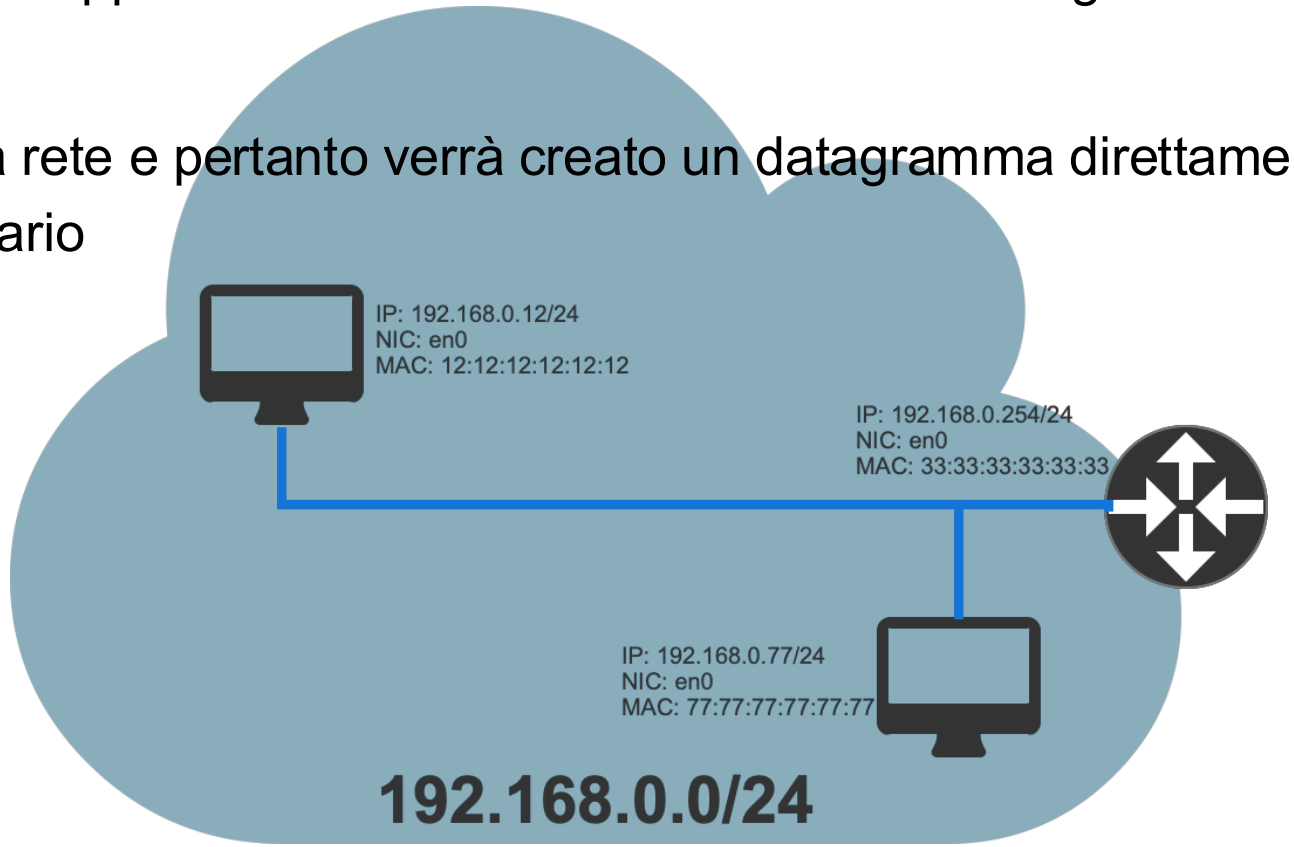
1. L'indirizzo IP del destinatario è nella mia stessa sottorete?
2. Se SI:
    1. Il datagramma viene inviato direttamente al destinatario
3. Se NO:
    1. Viene consultata la tabella di routing e viene identificato il gateway da utilizzare
    2. Il datagramma viene inviato al gateway

In entrambi i casi avviene comunque un invio diretto, o verso il destinatario finale o verso il gateway. È pertanto necessaria la conoscenza del relativo MAC

Modello TCP / IP – Livello di Rete (IP) – Tabelle di routing

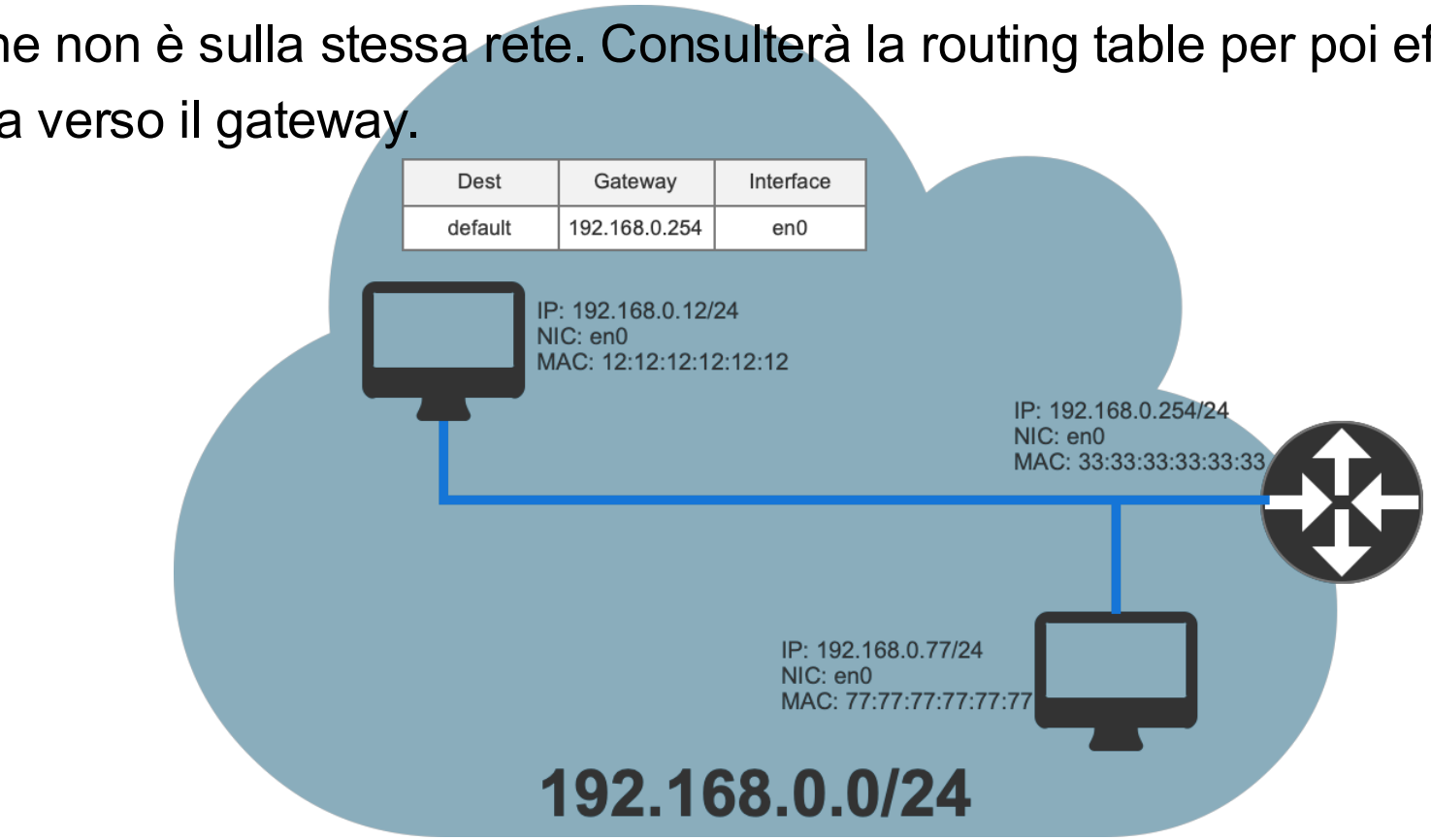
Consegna diretta: supponiamo che l'host di IP 192.168.0.12 voglia inviare dati a 192.168.0.77.

Sono sulla stessa rete e pertanto verrà creato un datagramma direttamente contenente il MAC del destinatario



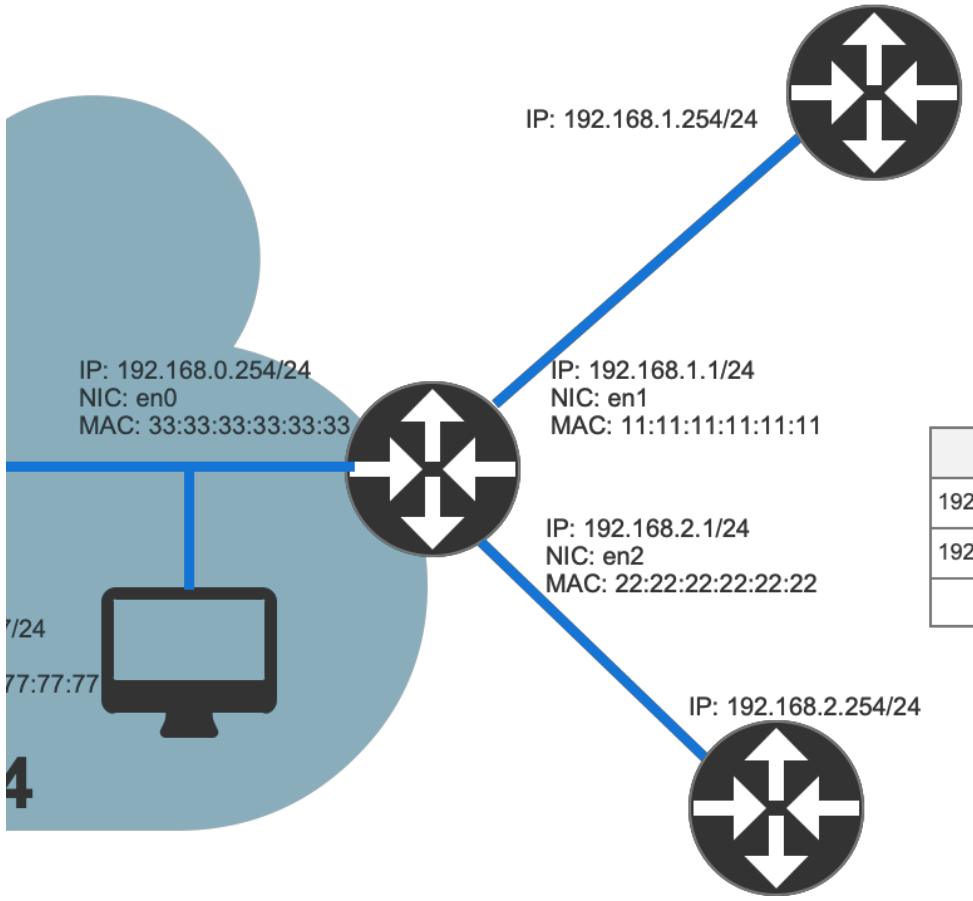
Modello TCP / IP – Livello di Rete (IP) – Tabelle di routing

Consegna indiretta: supponiamo che l'host di IP 192.168.0.12 voglia inviare dati a 192.168.2.39 che non è sulla stessa rete. Consulterà la routing table per poi effettuare una consegna diretta verso il gateway.



Modello TCP / IP – Livello di Rete (IP) – Tabelle di routing

Il router implementa lo stesso algoritmo, valutando se è possibile la consegna diretta su una delle sue interfacce, oppure esaminando la sua tabella di routing



Dest	Gateway	Interface
192.168.3.0/24	192.168.1.254	en1
192.168.7.0/25	192.168.1.254	en1
default	192.168.2.254	en2

Algoritmi di routing

Come tenere aggiornate le tabelle di routing?

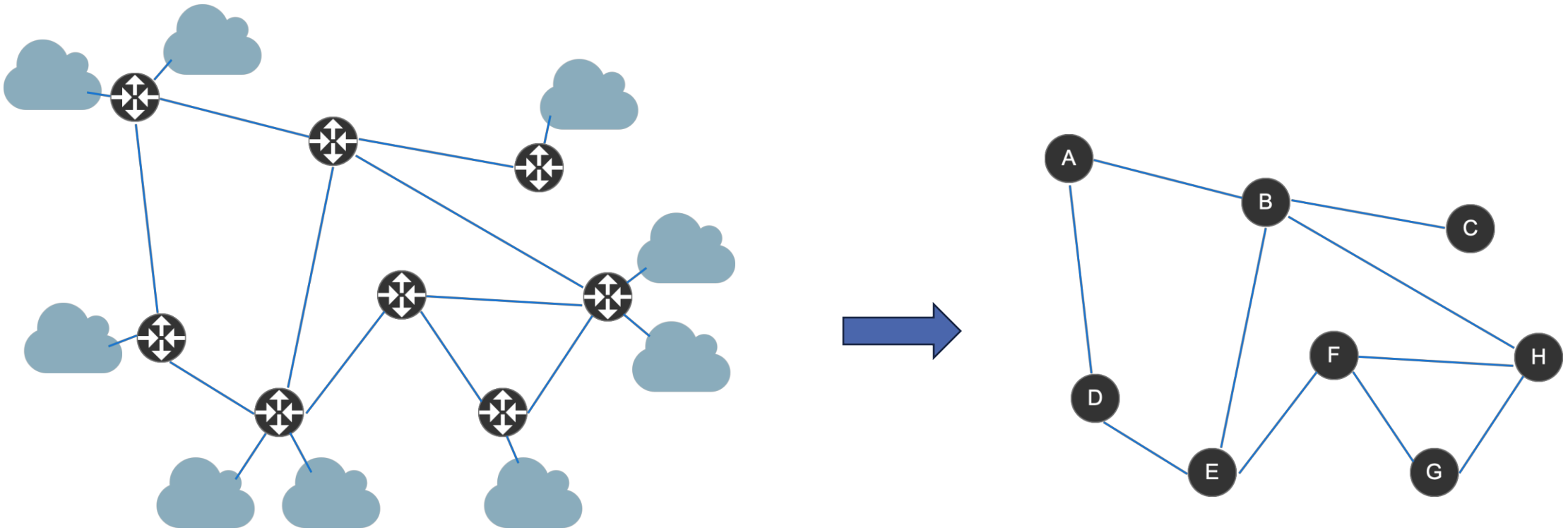
- Per i singoli host e per reti con topologia semplice (p.e. LAN) è possibile procedere manualmente eventualmente utilizzando protocolli di configurazione quali DHCP (lo vedremo in seguito)
- Per reti complesse è necessario che le tabelle di routing si aggiornino in automatico. Non è infatti possibile, manualmente, definire il percorso più conveniente. Sono disponibili molteplici protocolli, tra cui i più utilizzati sono
  - OSPF (Open Shortest Path First)
  - RIP (Routing Information Protocol)

Algoritmi di routing

Entrambi gli algoritmi, sebbene con differenti implementazioni, approcciano il problema nello stesso modo:

- La rete viene rappresentata come un grafo pesato
  - I nodi del grafo sono i router
  - Il peso rappresenta quanto sia "conveniente / sconveniente" percorrere quel ramo
- Viene impiegato un algoritmo per stabilire il percorso migliore (con peso inferiore)
- Viene definito un protocollo per la condivisione delle informazioni tra i vari router, in modo che tutti convergano verso lo stesso routing

Algoritmi di routing



Algoritmi di routing

OSPF e RIP definiscono i pesi in più modi:

- OSPF:
  - Il peso è associato alla banda del collegamento. Maggiore è la banda minore è il peso.
  - L'algoritmo privilegia i percorsi a velocità trasmissiva maggiore
- RIP:
  - Tutti i percorsi hanno peso 1
  - L'algoritmo privilegia i percorsi con meno "hop"

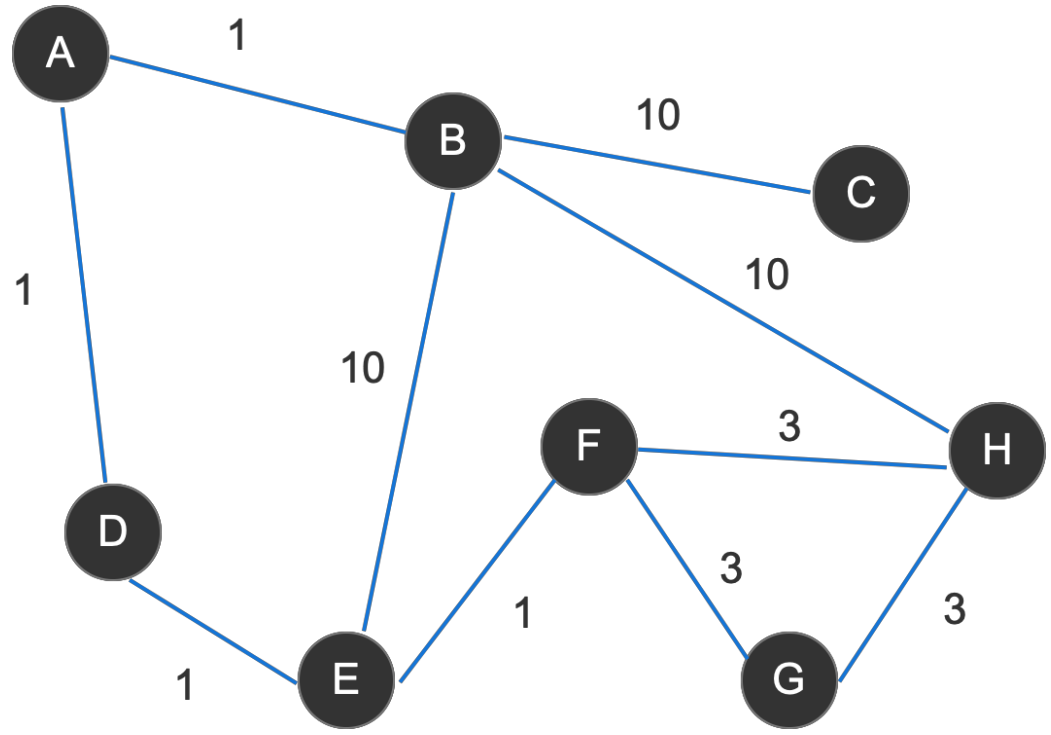
NB: In entrambi i casi potrebbero anche esistere collegamenti unidirezionali e/o pesi differenti in base al senso di trasmissione

Algoritmi di routing

Gli algoritmi di "Shortest Path" determinano, per ogni coppia di nodi, il percorso con la minore somma dei pesi.

- Qual è il percorso migliore da A a H?
- Qual è il percorso migliore da C a G?

Sarebbero stati gli stessi in caso di RIP, ovvero di pesi tutti unitari?



Modello TCP / IP – Livello di Rete (IP) – Internet Control Protocols

Il livello di rete prevede altri protocolli, oltre IP, utilizzati per gestire alcuni aspetti specifici.

In particolare vedremo:

- ARP – Address Resolution Protocol
- ICMP – Internet Control Message Protocol

Modello TCP / IP – Livello di Rete (IP) – Protocollo ARP

ARP (Address Resolution Protocol) è un protocollo utilizzato per ottenere la corrispondenza tra indirizzi IP e indirizzi MAC. Corrispondenza necessaria per poter eseguire consegne dirette.

ARP lavora in broadcast. L'host che necessita di conoscere un indirizzo MAC associato ad un indirizzo IP invia un datagramma ARP Request a tutti gli altri host della sottorete, chiedendo*:*

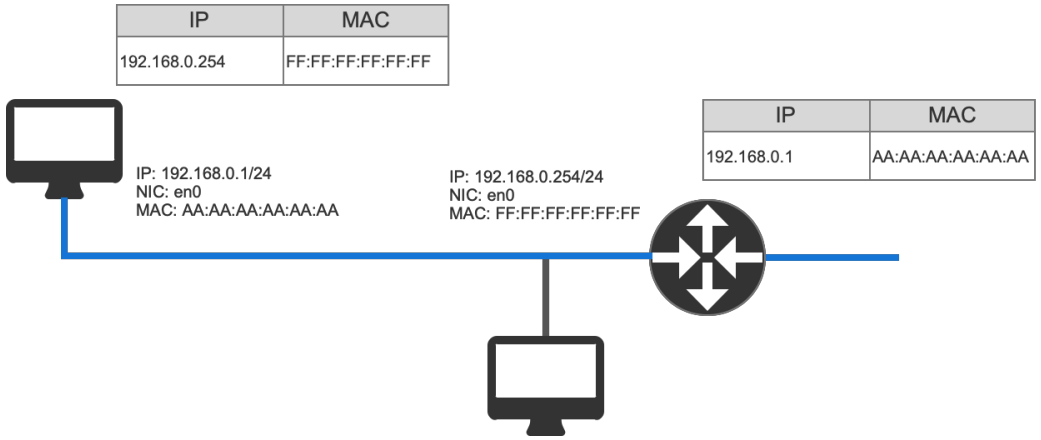
"A chi appartiene l'ip xxx.xxx.xxx.xxx?".

Tutti gli host ricevono il datagramma e solo quello interessato risponde inviando il proprio MAC. La risposta avviene con un datagramma ARP Response.

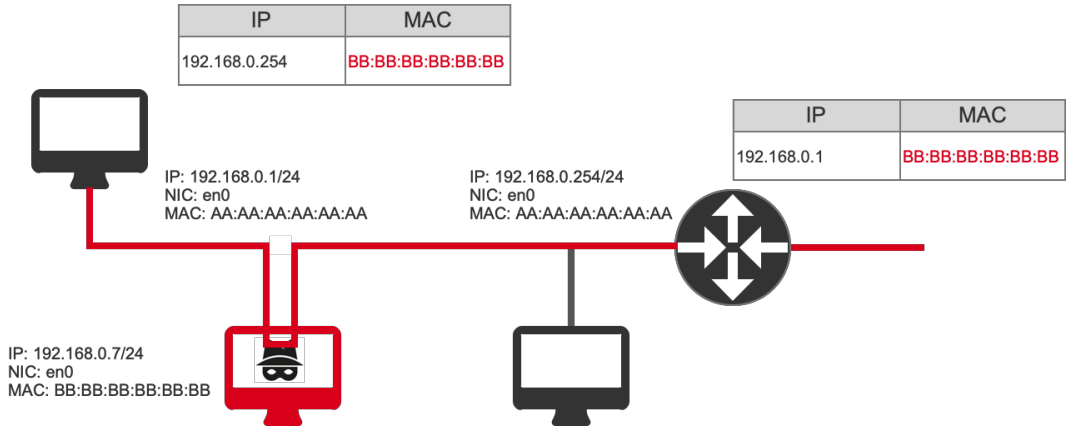
Gli host fanno caching delle associazioni IP/MAC per evitare di doverli richiedere tutte le volte

ARP Poisoning

- È una tecnica di attacco volta a modificare la cache di associazione IP / MAC, con lo scopo di dirottare il traffico verso un Man In The Middle
- Consiste nell'inviare un numero molto alto di ARP Responses nelle quali si associa l'IP del gateway al MAC della macchina dell'attaccante
- Le vittime inizieranno ad inviare il traffico verso l'attaccante piuttosto che verso il gateway



Normal gateway routing



MITM routing

Modello TCP / IP – Livello di Rete (IP) – Protocollo ICMP

ICMP (Internet Control Message Protocol) è un protocollo per inviare "messaggi" tra due host.

È utilizzato per segnalare la presenza di errori di comunicazione e per testare la connettività Internet.

Esistono numerose tipologie di messaggi ICMP. I principali sono riportati in tabella:

Tipo di messaggio ICMP	Descrizione
Destination Unreachable	Il datagramma non può essere consegnato
Time Exceeded	TTL ha raggiunto 0 (usato in tracerout)
Parameter Problem	Datagramma con header errato
Echo e Echo Reply	Per verificare se un host è attivo (usato in ping)
Timestamp request / reply	Analogo a echo ma con l'aggiunta di timestamp

I dati sono incapsulati all'interno dell'area dati di un datagramma IP

Protocollo ICMP – Ping e Traceroute

Ping e traceroute sono utilizzati per motivi di diagnostica ma possono anche essere utilizzati da un attaccante per effettuare una ricognizione.

PING:

- Verifica se un determinato IP è associato ad un host attivo (alive) e raggiungibile
- Invia un ICMP Echo Request e attende il relativo messaggio Echo Response
- In caso di risposta l'IP è considerato attivo e raggiungibile
- La mancata risposta può invece essere associata a più scenari:
    - IP non associato ad host
    - IP associato ma host non raggiungibile
    - IP associato, host raggiungibile ma configurato per non rispondere agli Echo Request

Protocollo ICMP – Ping e Traceroute

TRACEROUTE:

- Determina il percorso verso un IP di destinazione, determinando gli IP dei route intermedi
- Sfrutta i messaggi ICMP di tipo Time Exceeded
- Invia una sequenza di datagrammi verso la destinazione con TTL variabile
  - Nel primo invio TTL vale 1 → Il route successivo lo porterà a zero e invierà un messaggio time exceded (rivelando il proprio IP nel datagramma di risposta)
  - Nel secondo invio TTL vale 2 → Sarà il secondo route ad inviare il messaggio di time exceeded (rivelando il proprio IP nel datagramma di risposta)
  - …

Modello TCP / IP – Livello di Rete (IP) – Indirizzi IP v6

IP v4 ha un numero di IP insufficienti per le richieste di connessioni odierne (nel prossimo capitolo vedremo un modo per limitare il problema).

IP v6 è una versione migliorata di IP v4, che ne riprende molte caratteristiche cercando eliminare le criticità:

- IP v6 utilizza indirizzi a 128 bit (contro i 32 bit di IP v4)
- Gli IP v6 sono espressi in notazione esadecimale → 32 numeri esadecimali divisi in gruppi di 4 (ogni numero esadecimale rappresenta 4 bit)
  - 50B2:6400:0000:0000:6C3A:B17D:0000:10A9
- IP v6 è retrocompatibile con IP v4. Un set di indirizzi è infatti riservato agli indirizzi v4
  - 0:0:0:0:0:FFFF:C0A8:5909 equivale a 192.168.89.9

ITS Academy
Adriano
Olivetti

TCP / IP - Livello di Rete (IP)

HANDS ON SESSION

(con Cisco Packet Tracer)

Cisco Packet Tracer

- Cisco Packet Tracer è un software di "network simulation" creato dall'omonima azienda
- E' uno strumento didattico che permette di creare topologie di rete sia semplici che complesse
- E' lo strumento di riferimento per il programma di formazione "Cisco Networking Academy Program"
- Permette di simulare tutti i dispositivi di rete Cisco, ma integra anche alcuni dispositivi generici
- E' disponibile per i sistemi operativi Windows, Linux (Ubuntu) e MacOs

Cisco

- Cisco nasce nel 1984 in California, fondata da gruppo di ricercatori provenienti dall'Università di Stanford
- L'azienda inizialmente produce router ma diventa presto leader di riferimento per tutti gli apparati di networking
- Oggi è attiva nel mercato dei dispositivi "enterprise", utilizzabili in aziende e data center.
    - In passato è stata attiva anche nel mercato "consumer", tramite il marchio Linksys
- Attualmente impiega più di 70.000 lavoratori

Cisco Packet Tracer

- Cisco Packet Tracer permette di:
  - Creare topologie di rete composte da apparati Cisco e/o generici
  - Configurare tramite GUI e CLI gli apparati
    - L'emulazione della CLI prevede solo un sottoinsieme delle funzionalità disponibili sull'hardware fisico
  - Ispezionare dinamicamente e in tempo reale lo stato di ogni dispositivo e il traffico di rete

Cisco Packet Tracer - Installazione

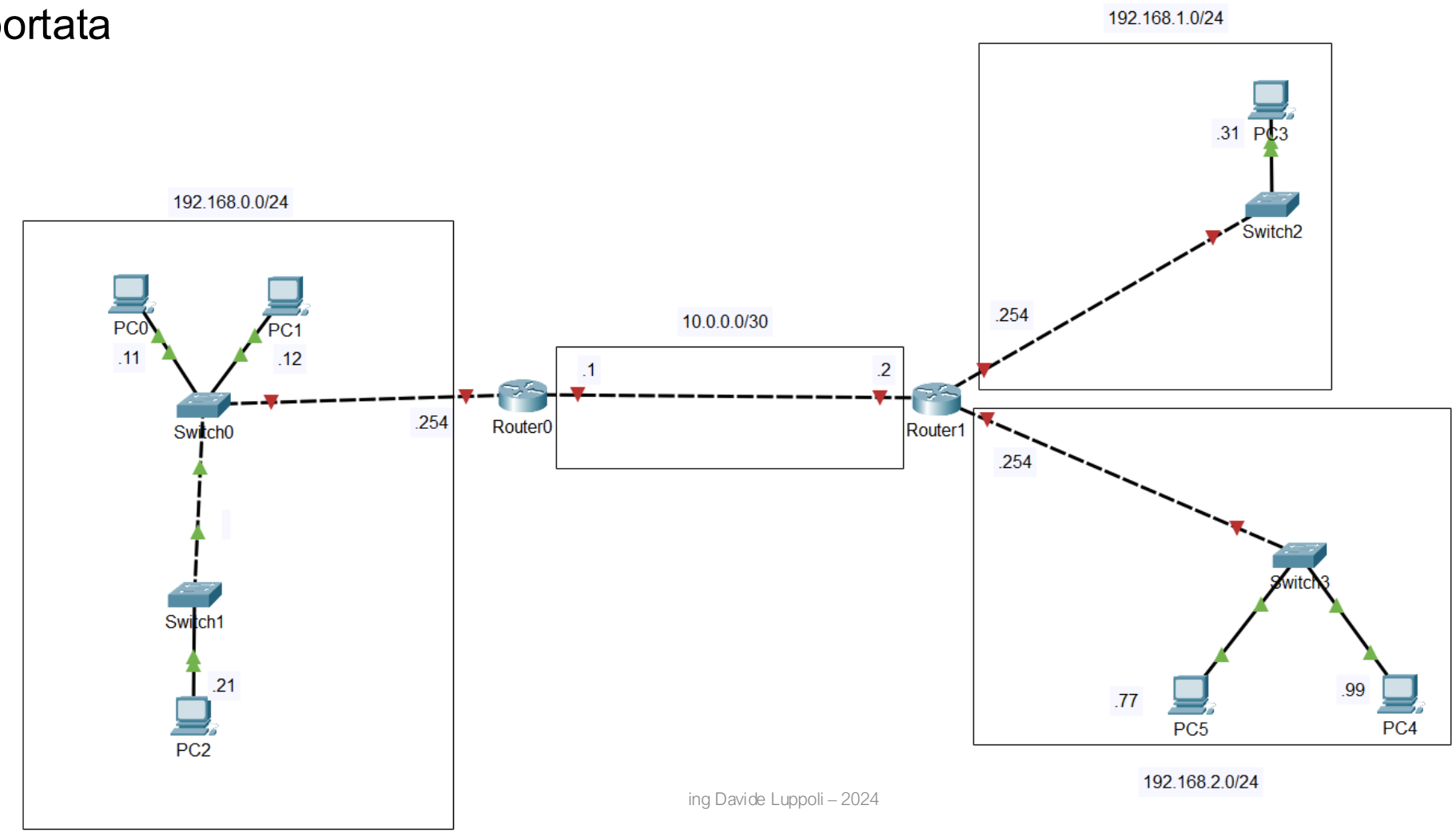
- Cisco Packet Tracer è disponibile solo per gli iscritti ad uno dei corsi del Cisco Networking Academy Program (https://www.netacad.com)
- Esistono numerosi corsi gratuiti, utilizzeremo il seguente:
  - https://www.netacad.com/courses/getting-started-cisco-packet-tracer
- Una volta iscritti al corso sarà disponibile il link per il download (all'interno del modulo 1)
- Per velocizzare le operazioni trovate il file su Classroom
  - Per l'avvio dell'applicazione è comunque necessario un account presso netacad

Modello TCP / IP – Livello di Rete (IP) – Alcuni comandi

Comando	Windows	Linux	Mac
Indirizzo/i IP del proprio pc	`ipconfig`	`ip a (ip addr)`	`ifconfig`
Tabella di routing	`route print`	`ip r (ip route)`	`netstat -rn`
Cache ARP	`arp -a`	`ip n (ip neigh)`	`arp -a`
Test raggiungibilità host	`ping IP`	`ping IP`	`ping IP`
Percorso di routing	`tracert IP`	`traceroute IP`	`traceroute IP`

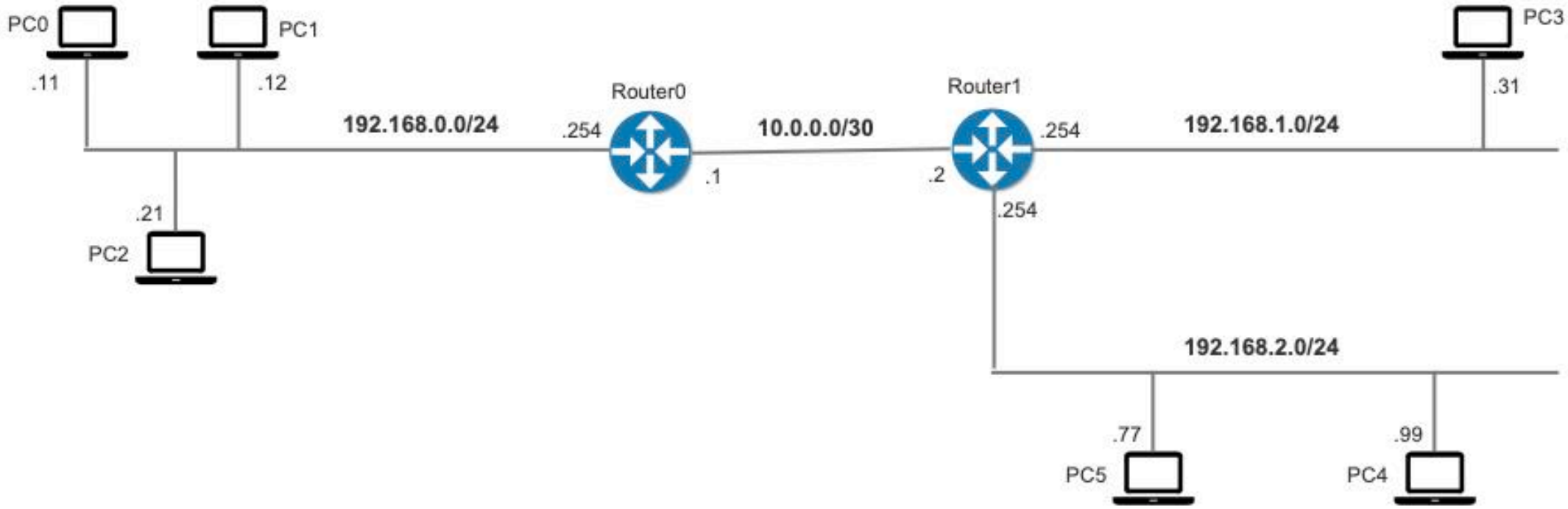
Esercizio 1

- Su Classroom trovate il file Cisco Packet Tracer che implementa la topologia sotto riportata



Esercizio 1

- La topologia può essere rappresentata anche secondo il seguente schema logico



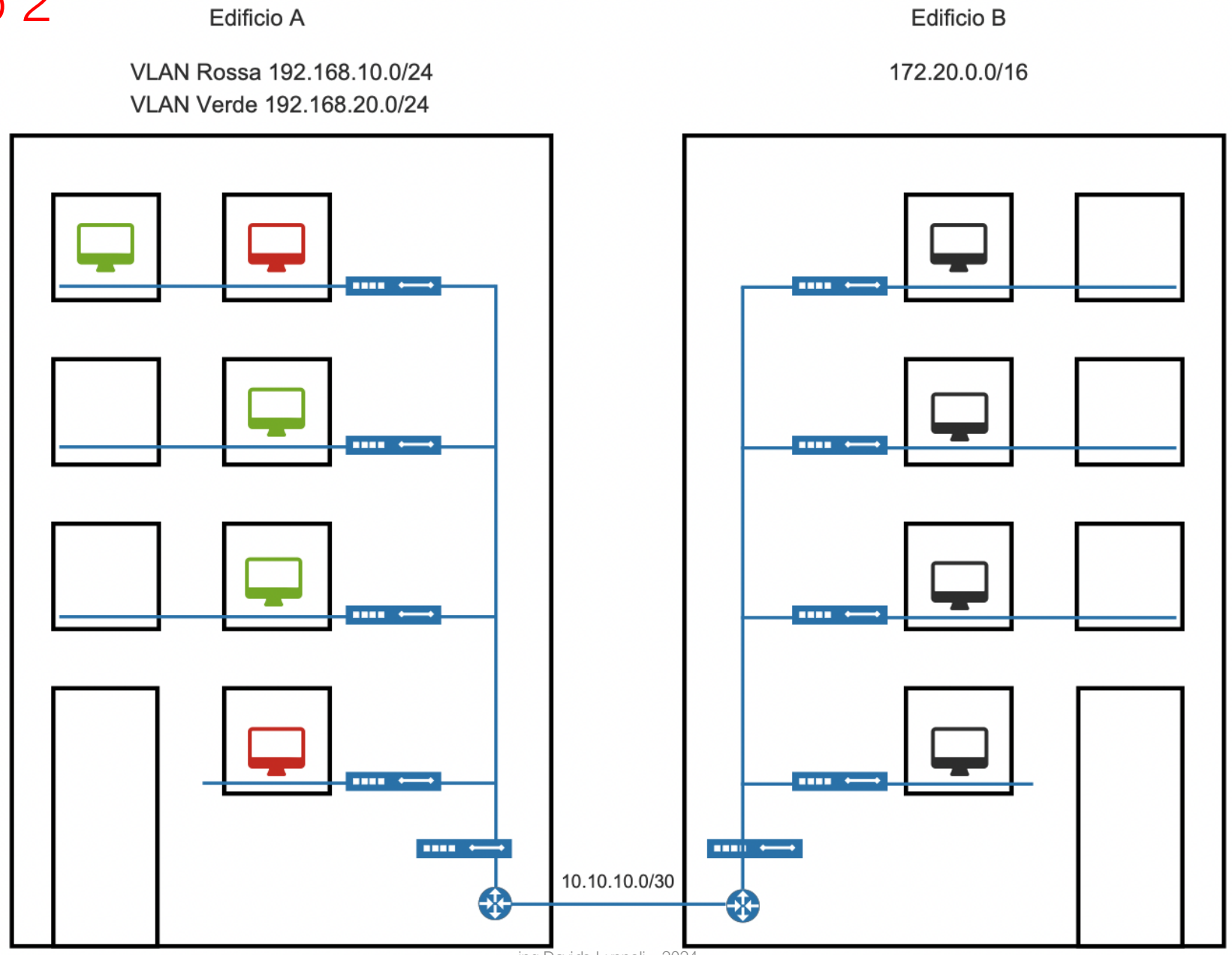
Esercizio 1

- Configurare tutti gli host e tutti i router in termini di:
  - Indirizzi IP
  - Tabelle di routing
  - Default Gateway
- Verificare la raggiungibilità degli host tramite ping
- Verificare il percorso seguito dai datagrammi tramite traceroute e tramite funzionalità di Simulation

Esercizio 2

- Una azienda è distribuita su due edifici, A e B
- Entrambi gli edifici hanno un cablaggio che utilizza switch collegati in cascata
- Nell'edificio A sono presenti due VLAN
  - 192.168.10.0/24 (in rosso nello schema della pagina seguente)
  - 192.168.20.0/25 (in verde nello schema della pagina seguente)
- L'edificio B non ha VLAN e tutti gli host sono nella rete 172.20.0.0/16
- I due edifici sono collegati tramite due router. Il colliegamento diretto tra di essi utilizza indirizzi nella rete 10.10.10.0/30

Esercizio 2


Edificio A
VLAN Rossa 192.168.10.0/24
VLAN Verde 192.168.20.0/24
Edificio B
172.20.0.0/16
10.10.10.0/30

Esercizio 2

- Realizzare l'intera topologia con Cisco Packet Tracer
- Assegnare gli indirizzi IP compatibilmente con le sottoreti specificate
- Configurare i router in modo che tutti gli host possano comunicare con tutti gli altri
  - Gli host della VLAN rossa possono comunicare con quelli della VLAN verde e viceversa
  - Gli host dell'edificio A possono comunicare con gli host dell'edificio B e viceversa

Playgroung

- Intro to LAN (https://tryhackme.com/room/introtolan)
- L2 Mac Flooding & ARP Spoofing (https://tryhackme.com/room/layer2)
- Active Reconnaissance (https://tryhackme.com/room/activerecon)