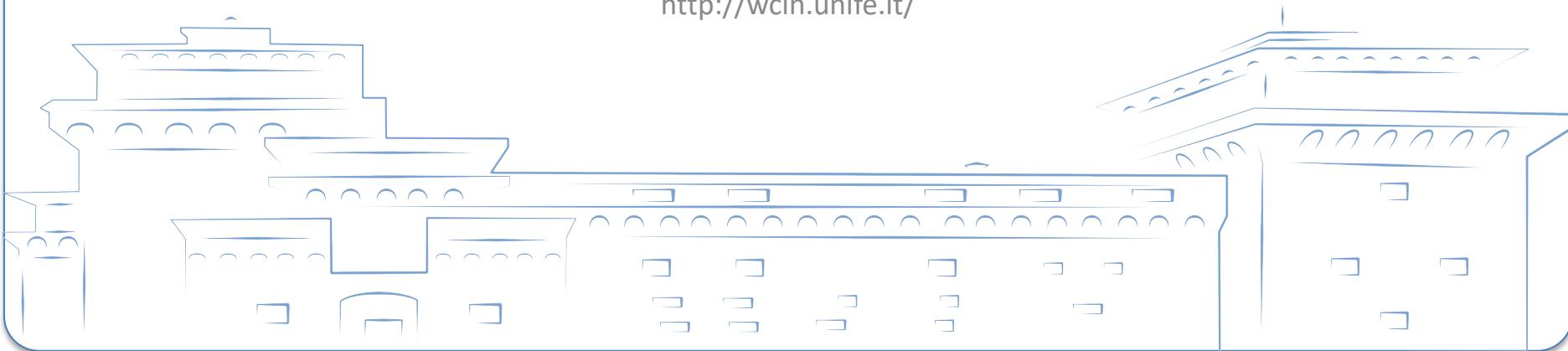


Reti di Telecomunicazioni (e Internet)

Prof. Andrea Conti

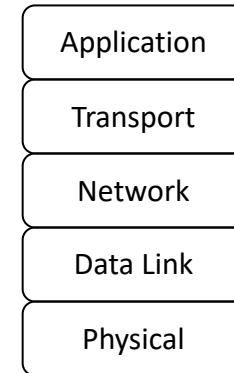
Wireless communication and localization networks laboratory
University of Ferrara
<http://wcln.unife.it/>



INTERNETWORKING

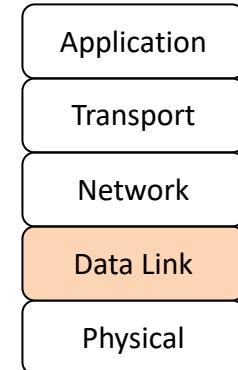
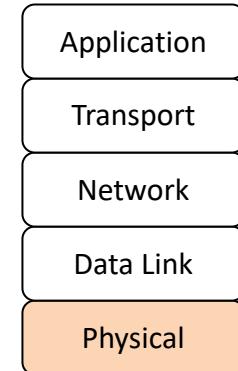
Internetworking

- Interconnessione di reti allo scopo di rendere disponibili a tutti gli utenti e le macchine interconnesse i servizi offerti dalla rete.
 - Protocolli e strategie dell'Internet Engineering Task Force (IETF) descritti in documenti chiamati Request for Comment (RFC)
- Dispositivi hardware per far transitare i pacchetti tra le reti
 - Differenziabili sulla base del layer sul quale operano e quindi sulla loro complessità realizzativa



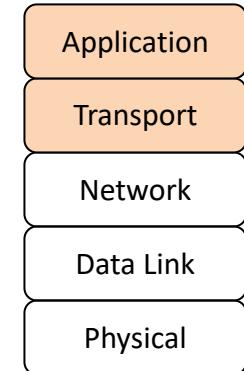
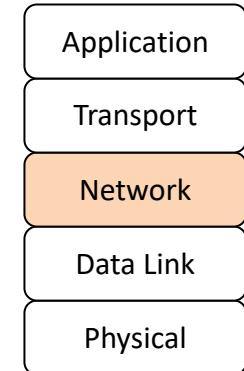
Internetworking

- **REPEATER:** Ripetitore a livello fisico
 - Rigenera il segnale modificandone il formato per adattarli a reti con strati fisici diversi.
 - Usato per suddividere una rete in sezioni più piccole.
 - Il repeater ha 2 porte. La versione multiporta si chiama **HUB**.
- **BRIDGE:** Ripetitore a livello di collegamento
 - Fa comunicare reti con diversi protocolli di livello 2 e diverse velocità di trasmissione (**logico non fisico**).
 - Deve avere qualche conoscenza di dove si trova il destinatario e dell'instradamento per raggiungerlo per evitare di generare traffico verso uscite non necessarie (**filtraggio**).
 - Ha 2 porte (collega due reti), la versione multiporta si chiama **SWITCH**.



Internetworking

- **ROUTER:** Ripetitore a livello di rete
 - Fa comunicare reti diverse (**internetworking**)
 - Realizza l'instradamento dei pacchetti
 - Può comprendere operazioni più sofisticate di processamento dei pacchetti (controllo di legittimità, gestione della qualità del servizio, tariffazione, ...)
- **GATEWAY:** Ripetitore per livelli superiori a quello di rete.
 - Viene utilizzato per il processamento ad alto livello dei pacchetti



LIVELLO 2

BRIDGE

- Deve essere trasparente e avere velocità di processamento tale da analizzare i pkt provenienti dalla rete più veloce a cui è interconnesso
- Vista la varietà di reti interconnesse al bridge occorre un buffer finito e dimensionato per memorizzare i pkt in attesa di essere trasmessi + controllo di flusso (blocco su ingresso).
- A livello 2 l'instradamento dipende da indirizzo MAC del destinatario.

Livello 2 – Indirizzamento

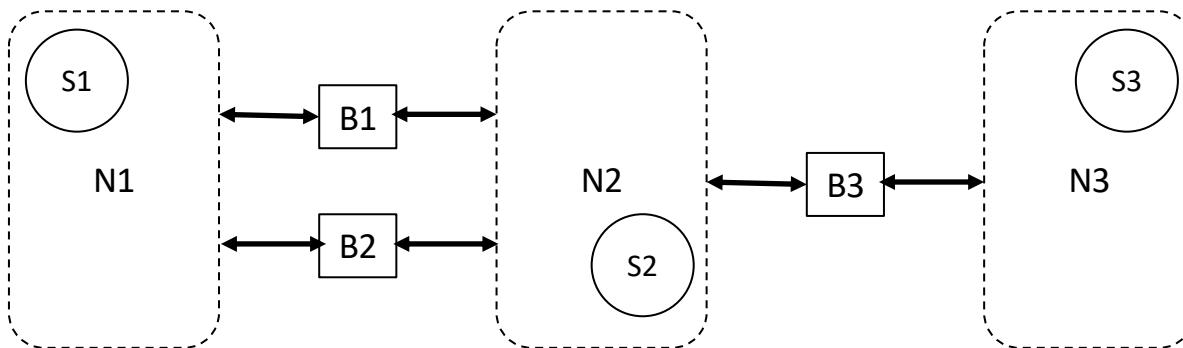
- Il media access control (MAC) ha un indirizzo di livello 2 composto da 2B o 6B (comunemente 6B) che indirizza univocamente una scheda di rete a livello mondiale:
3B id produttore e **3B seriale scheda del produttore**. Viene tipicamente espresso utilizzando cifre esadecimale

ab:cd:ef:mn:lo:pq

- Spazio di indirizzamento globale: 2^{48} indirizzi (circa 2.8×10^{14})
- Spazio di indirizzamento per ogni produttore: 2^{24} indirizzi (circa 16.77 milioni)
 - Apple Inc. ha un range per i suoi laptop mac su DC:09:04 da 00:00:00 a FF:FF:FF.
- Indirizzo broadcast: FF:FF:FF:FF:FF:FF
 - Invio di un pacchetto a tutte le stazioni di livello 2
 - Indirizzo di destinazione e non di sorgente

BRIDGE: instradamento a percorsi fissati

- Ogni possibile percorso rete sorgente—rete destinazione è mappato a priori.
 - ogni stazione è associata, sulla base del proprio indirizzo MAC, a una rete.
 - tutti i bridge devono conoscere le tabelle di associazione stazione-rete.
- Problemi
 - Non è adattativo (la tabella non varia al variare delle condizioni di rete, e.s., guasto)
 - Possibile duplicazione di risorse e di pacchetti



	N1	N2	N3
N1	X	B1	B1
N2	B1	X	B3
N3	B3	B3	X

BRIDGE: instradamento con autoapprendimento

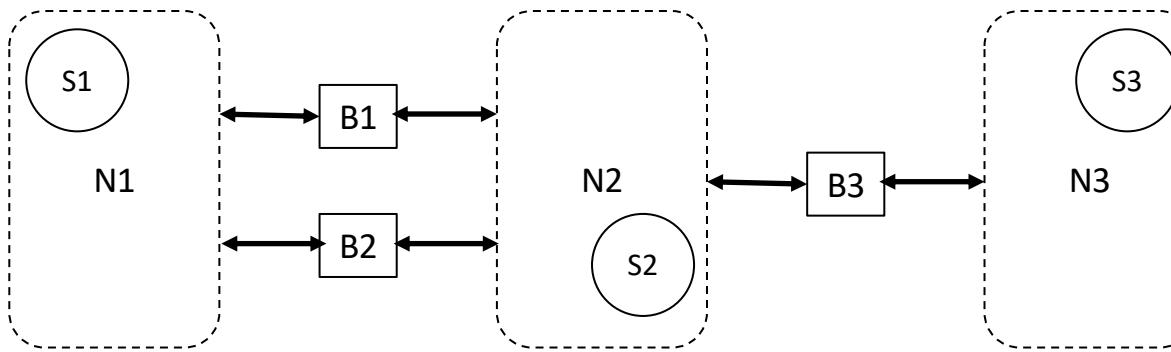
- Per rendere adattativo il sistema a percorsi fissati, ogni bridge viene dotato della capacità di compilare autonomamente la tabella di associazione
 - associazione basata sull'analisi dei pacchetti che transitano attraverso il bridge tramite estrazione dell'indirizzo MAC sorgente.
 - associazione cancellata dopo un tempo chiamato timeout dall'ultima acquisizione. Per stazioni mobili le associazioni sono indicizzate e una sola associazione per MAC address può essere presente.
- Problemi
 - Ogni bridge può conoscere solo la parte della tabella di associazione riferita alle reti ad esso collegate

BRIDGE: instradamento con autoapprendimento

Metodo per evitare la propagazione delle tabelle di associazione e di instradamento fra reti

- Viene cercata all'interno della tabella di associazione la porta corrispondente a MAC_DEST cioè la porta verso la rete che ospita la stazione indirizzata da MAC_DEST
- Se la porta destinataria è la stessa di arrivo il pkt non viene replicato, altrimenti il pkt viene ripetuto sulla porta identificata
- Se nessuna porta destinataria è identificata (es. timeout associazione) allora il filtraggio non è possibile e conservativamente si ripete il pkt sulla porta diversa da quella di arrivo per propagare nella rete
 - Il MAC_DEST broadcast è trattato allo stesso modo
 - c'è rischio di **loop** che sono eliminabili mediante la costruzione automatica di un albero di bridge e permettendo ai pkt di muoversi solo lungo l'albero (no cicli)

BRIDGE: esempio



B1	PORT
S1	1
S2	2
S3	2

B3	PORT
S1	1
S2	1
S3	2

BRIDGE: spanning tree

Algoritmo per la creazione dell'albero di bridge introdotto da IEEE802.1: ad ogni bridge assegnato un identificativo univoco (priorità-unicità); indirizzo MAC unico e noto per ciascun bridge; identificazione univoca di ogni porta

1. scelto inizialmente il bridge radice prendendo quello con identificativo più basso
2. ogni bridge determina quale sua porta, detta *porta radice*, è nella direzione a costo inferiore (velocità maggiore) verso la radice e fra tutti viene scelto quello a costo inferiore
3. ogni bridge lascia attiva la sua porta radice e tutte le porte selezionate per interconnettere una rete, le altre vengono bloccate e restano inutilizzate
4. il processo di costruzione dello spanning tree avviene attraverso lo scambio di informazioni tra bridge mediante Bridge Protocol Data Unit (BPDU) che contengono informazioni sul bridge radice e sulle funzioni di costo. Tale procedura è ripetuta periodicamente

Ci sono altri algoritmi per particolari topologie di rete (es. bridge source routing per token ring)

LIVELLO 3

Internet Protocol (IP)

- E' il protocollo di livello 3 alla base di **Internet**, la rete a pacchetto attualmente più diffusa al mondo
- IP è un protocollo datagram sviluppato negli anni '80 dal DoD americano nel progetto ARPANET (creazione rete per interconnettere postazioni della difesa americana e mantenere connessione anche se una parte fosse distrutta → commutazione pacchetto)
- è un protocollo a pacchetti senza connessione e di tipo *best effort*, che non garantisce cioè alcuna forma di affidabilità della comunicazione
- no controllo di errore, controllo di flusso e controllo di congestione, l'affidabilità può essere realizzata dai protocolli di trasporto (livello 4)

Internet Protocol (IP)

- due versioni del protocollo IP: l'originaria v4 e la più recente v6, quest'ultima nata dall'esigenza di gestire meglio il crescente numero di dispositivi connessi ad Internet
- nasce prima del modello OSI e si occupa anche della frammentazione; riceve dal livello 4 dei pkt di 64KB e li frammenta in segmenti, che riassembra in ricezione per formare i 64KB da restituire al livello 4
- Pacchetti composti da header + dati

Pacchetto IPv4

Header (parte fissa 20B + parte variabile)

- Version: 4 bit per versione protocollo e permettere la coesistenza di pkt che rispondono a versioni diverse
- IHL: 4 bit di Internet header length espressi a multipli di 4B (minimo 20B)
- TS: 8 bit di type of service per specificare affidabilità, throughput, tempo di accesso e quindi trasportare diversi tipi di traffico
- TL: 16 bit per lunghezza totale campo dati (fino a 64KB)
- ID: 16 bit di identification per distinguere i datagram indirizzati alla stessa stazione dalla stessa sorgente (ordinamento)
- Flags: 3 bit di cui il primo fisso al momento, il secondo per specificare se possibile frammentare il pkt, il terzo per indicare se è l'ultimo frammento
- FO: 13 bit fragment offset per indicare la posizione del frammento (8 volte FO) nel pkt complessivo. Ogni frammento ha una dimensione multipla di 8B
- TTL: 8 bit contatore time to live che si incrementa a ogni router attraversato per limitare la vita del pkt ed evitare che stia in un loop
- Protocol: 8 bit che specificano il protocollo di livello superiore usato dal ricevitore (e.g., TCP o UDP)
- HC: 16 bit header checksum per verifica errori sull'header
- SA: 32 bit source address
- DA: 32 bit destination address
- Options: lunghezza variabile, per ridefinire il protocollo su aspetti di sicurezza, errori, instradamento, debug
- Pad: lunghezza variabile con bit senza significato inseriti solo per assicurare che l'header sia lungo un multiplo di 4B

Indirizzi IPv4

- Indirizzo IPv4 è composto da 32 bit. Viene tipicamente espresso utilizzando una notazione a punti (dot notation) che separano quattro campi di 8 bit ciascuno
 - Es. 192.168.1.6
- 4 diversi schemi di indirizzamento (rete e stazione)
 - Classe A: un bit 0, 7bit per ID 128 reti, 24bit per ID 16M host
 - da 0.0.0.0 a 127.255.255.255
 - Classe B: due bit 10, 14bit per ID 16384 reti, 16bit per ID 64K host
 - da 128.0.0.0 a 191.255.255.255
 - Classe C: tre bit 110, 21bit per ID 2M reti, 8bit per ID 256 host
 - da 192.0.0.0 a 223.255.255.255
 - Classe D: quattro bit 1110, 28bit lasciati per ID gruppi host (es. multicast)
 - da 224.0.0.0 a 239.255.255.255
 - quattro bit 1111 per usi futuri

Indirizzamento intra/internet

- Nella vita reale quando vogliamo inviare una lettera la inseriamo in una busta su cui scriviamo gli indirizzi di mittente e destinatario. Poi portiamo la busta con la lettera a una cassetta postale che ha due bocche, una per la città e una per fuori città.
- In Internet, gli indirizzi IP di sorgente e destinatario non sono sufficienti per capire se il payload (lettera) è destinato sulla stessa rete o all'esterno.

Esempio:

S: 195.32.69.2

D: AAA.BBB.CCC.DDD

Indirizzi MAC nel payload (nell'header di livello 2)

Indirizzamento intra/internet

- Se destinatario nella stessa rete (intranet) allora il pkt può essere messo sulla rete e il destinatario lo vedrà. Altrimenti (internet) occorre inviare il pkt fuori affidandolo alla macchina che identifica l'accesso al mondo esterno detta **gateway**
- Ma come si fa a capire se il destinatario è locale o remoto?

S nella rete X. D è nella rete X? Se si pkt a macchina locale, se no pkt a gateway di default e da lì verso la rete esterna.

NETMASK permette di risolvere il problema di cosa è locale e cosa è remoto verificando se IP_DEST è dentro l'intervallo di indirizzi della rete locale

Indirizzi IPv4

- Gli indirizzi pubblici sono rilasciati e regolamentati dall'ICANN (Internet Corporation for Assigned Names and Numbers) e da altri enti internazionali
- Gli enti detentori di una classe possono suddividere ulteriormente la classe
- Per ogni rete due indirizzi sono dedicati (uno per identificare la rete stessa e uno per il broadcast, gli altri sono indirizzi unicast
 - 192.167.215.X con X=0 rete e X=255 broadcast (solo destinatario)
- Nelle diverse classi alcuni indirizzi sono riservati per applicazioni intranet (A: 10.0.0.0–10.255.255.255; B: 172.16.0.0–172.31.255.255; C: 192.168.0.0–192.168.255.255) o per scopi intrahost (A: 127.0.0.0–127.255.255.255; con 127.0.0.1 *localhost* per ogni host anche privo di scheda di rete per scrivere applicazioni di rete indirizzando sull'host stesso)

NETMASK

- La rete di un indirizzo IP è l'**<AND>** logico fra l'indirizzo IP e la NETMASK

Es. IP_DEST 195.32.62.2

NETMASK 255.255.255.0

Rete IP_DEST <AND> NETMASK = 195.32.62.0 e nella rete ci sono tutti gli indirizzi 195.32.62.X

Es. Due macchine con indirizzo IP 195.32.68.2 e 195.32.69.2 sono nella stessa rete?

NO se NETMASK 255.255.255.0

SI se NETMASK 255.255.254.0

NETMASK notevoli

255.255.255.0 classe C 2^8 -2 ID (.0 rete e .255 broadcast)

255.255.255.192 divide classe C in 4 sottoreti ciascuna con 2^6 -2 ID

255.255.255.128 divide una rete di 256 ID in due di 2^7 -2 ID

255.255.255.252 è la più piccola rete usabile con 2^2 -2 ID

255.255.255.255 rappresenta il solo host

255.255.0.0 classe B 2^{16} -2 ID (256 classi C)

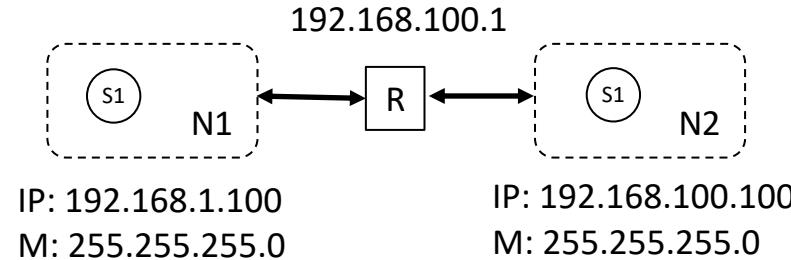
255.0.0.0 classe A 2^{24} -2 ID (256 classi B)

0.0.0.0 intero spazio degli indirizzi IP

ROUTER e instradamento

- Supponiamo di voler inviare un pacchetto di livello 3
 - Se il destinatario è nella rete locale, allora è possibile operare una trasmissione a livello 2
 - Altrimenti è necessario affidare il pacchetto ad un router

IP_NET	NET_MASK	NEXT_HOP
192.168.100.0	255.255.255.0	192.168.100.1



- Ogni nodo ed ogni router posseggono una tabella di instradamento che indichi il router (next hop) a cui affidare i pacchetti che non appartengono alla rete locale
 - diversi protocolli di instradamento per la compilazione della tabella: RIP, OSPF, BGP, ...

Il protocollo ARP

- Una volta noto il successivo nodo di destinazione di livello 3, è necessario effettuare una comunicazione di livello 2 (tra macchine locali)
 - Necessario un meccanismo di conversione tra indirizzo di livello 3 e di livello 2
- Address resolution protocol (ARP)
 1. L'entità interessata alla associazione invia sulla rete locale un pacchetto broadcast (indirizzo MAC FF:FF:FF:FF:FF:FF) chiedendo la risoluzione dell'IP desiderato
 2. La stazione con l'IP indicato nel pkt broadcast risponde all'entità sorgente sfruttando il MAC sorgente del pacchetto stesso
 3. L'entità sorgente riceve il pacchetto ed effettua la risoluzione
- Per evitare eccessivo traffico di segnalazione le risoluzioni ARP vengono mantenute in una tabella che viene aggiornata periodicamente

ARP - Esempio

- Esempio reale: L'indirizzo 192.168.1.183 vuole risolvere l'indirizzo 192.168.1.251
 - Fase 1: broadcast (ricerca del destinatario)

```
▼ Ethernet II, Src: Apple_c8:99:39 (8c:85:90:c8:99:39), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  > Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  > Source: Apple_c8:99:39 (8c:85:90:c8:99:39)
  Type: ARP (0x0806)

▼ Address Resolution Protocol (request)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: request (1)
  Sender MAC address: Apple_c8:99:39 (8c:85:90:c8:99:39)
  Sender IP address: 192.168.1.183
  Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
  Target IP address: 192.168.1.251
```

Livello 2 – 802.3
Pkt. Broadcast

Livello "2.5" – ARP
Dati richiedente

ARP - Esempio

- Esempio reale: L'indirizzo 192.168.1.183 vuole risolvere l'indirizzo 192.168.1.251
 - Fase 2: risposta (il destinatario risponde)

```
▼ Ethernet II, Src: AsustekC_fa:ec:c4 (14:da:e9:fa:ec:c4), Dst: Apple_c8:99:39 (8c:85:90:c8:99:39)
  > Destination: Apple_c8:99:39 (8c:85:90:c8:99:39)
  > Source: AsustekC_fa:ec:c4 (14:da:e9:fa:ec:c4)
    Type: ARP (0x0806)
    Padding: 0000000000000000000000000000000000000000000000000000000000000000
▼ Address Resolution Protocol (reply)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: reply (2)
  Sender MAC address: AsustekC_fa:ec:c4 (14:da:e9:fa:ec:c4)
  Sender IP address: 192.168.1.251
  Target MAC address: Apple_c8:99:39 (8c:85:90:c8:99:39)
  Target IP address: 192.168.1.183
```

Livello 2 – 802.3
Pacchetto verso richiedente

Livello "2.5" – ARP
Dati destinatario

DHCP

- Ogni nodo deve essere configurato per poter operare in una rete
 - Es. Indirizzo IP, netmask, default router, ...
- Il dynamic host configuration protocol (DHCP) è un protocollo applicativo che permette a un nodo di apprendere autonomamente la configurazione della rete a cui si connette
 1. L'host interessato invia una richiesta di configurazione in broadcast
 2. Se è presente un server DHCP nella rete, questo risponde all'host sorgente con la configurazione da adottare e il tempo di validità della configurazione stessa
- Scaduto il tempo di validità della configurazione (lease time), in assenza di comunicazioni da parte dell'host, il server DHCP considera la macchina spenta

DHCP - Esempio

- Esempio reale: configurazione di un host in DHCP
 - Fase 1: DHCP discover (ricerca di un server DHCP)

```
> Ethernet II, Src: Apple_c8:99:39 (8c:85:90:c8:99:39), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 68, Dst Port: 67
< Dynamic Host Configuration Protocol (Discover)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x9808042e
    Seconds elapsed: 1
    > Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 0.0.0.0
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
```

Livello 2 – 802.3
Livello 3 – IP
Pkt. Broadcast

Livello 7 – DHCP
Richiesta

DHCP - Esempio

- Esempio reale: configurazione di un host in DHCP
 - Fase 2: DHCP offer (il server propone una configurazione al richiedente)

```
> Ethernet II, Src: Technico_b7:5f:b4 (a4:91:b1:b7:5f:b4), Dst: Apple_c8:99:39 (8c:85:90:c8:99:39)
> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.183
> User Datagram Protocol, Src Port: 67, Dst Port: 68
< Dynamic Host Configuration Protocol (Offer)
    Message type: Boot Reply (2)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x9808042e
    Seconds elapsed: 0
    > Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 192.168.1.183
    Next server IP address: 192.168.1.1
    Relay agent IP address: 0.0.0.0
```

Livello 2 – 802.3
Indirizzo noto
Livello 3 – IP
Indirizzo offerto

Livello 7 – DHCP
Configurazione
offerta

DHCP - Esempio

- Esempio reale: configurazione di un host in DHCP
 - Fase 2 (cont.): DHCP offer (il server propone una configurazione al richiedente)
 - > Option: (53) DHCP Message Type (Offer)
 - > Option: (54) DHCP Server Identifier (192.168.1.1)
 - > Option: (51) IP Address Lease Time
 - > Option: (58) Renewal Time Value
 - > Option: (59) Rebinding Time Value
 - > Option: (1) Subnet Mask (255.255.255.0)
 - > Option: (28) Broadcast Address (192.168.1.255)
 - > Option: (3) Router
 - > Option: (6) Domain Name Server
 - > Option: (15) Domain Name
 - Fase 3 e 4: DHCP request e ACK (client e server si confermano a vicenda la configurazione)
 - Fasi necessarie per evitare problematiche di conflitti

ICMP

L'Internet control message protocol (**ICMP**) è il protocollo di segnalazione di IP

I primi 32 bit sono fissi (8 tipo messaggio, 8 codice messaggio, 16 checksum)

La parte seguente dipende dal tipo di segnalazione. Fra le più frequenti vi sono i seguenti.

- Rapporto di errori: *destination unreachable* (pkt scartato per non aver raggiunto la destinazione), *time exceed* (pkt scartato da router per aver terminato il TTL), *parameter error* (parametro header non interpretabile)
- Test di raggiungibilità e prestazioni: *echo request/echo reply* (raggiungibilità e stima tempo A/R)
- Controllo congestione: (diminuisce la freq di trasmissione dei pkt)
- Cambiamento routing: *redirect* (informa macch di usare un altro router per spedire pkt verso una destinazione)
- Richiesta parametri rete: *Address Mask Request/Reply* (per ottenere NETMASK)

IPv6

- Nasce per superare alcuni limiti di IPv4
- Spazio di indirizzamento esteso a 16B (128 bit) superando i concetti di classi per maggiore flessibilità e con gerarchie per semplificare le tabelle di instradamento
- IPv4 ha il type of service ma i router non ne tengono conto e pertanto il funzionamento è best effort. IPv6 supporta la QoS in maniera nativa
- Gestione degli header più semplice per controllo più veloce
- Funzioni di sicurezza e di controllo di integrità
- Implementa ICMPv6 che ha alcune funzionalità aggiuntive rispetto a v4

LIVELLO 4

TCP

- Il **transmit control protocol (TCP)** è il livello di trasporto (4) tipicamente usato con IP.
 - spesso non si distingue fra livelli 3 e 4 e si parla di TCP/IP
- Ha lo scopo di rendere affidabile le comunicazioni end-to-end
 - Il protocollo IP non è affidabile a causa, ad esempio, delle code finite nei router
- Il protocollo TCP crea una connessione virtuale fra sorgente e destinatario per ogni flusso di pacchetti, i pacchetti sono numerati in modo sequenziale e si implementa un meccanismo ARQ basato su ACK e timeout
- Il flusso di pacchetti è identificato da:
 - Indirizzi (Sorgente, Destinazione) di livello 3
 - Porte (Sorgente, Destinazione) di livello 4

TCP

Implementa:

- Fasi di connessione e disconnessione
- Trasferimento dei segmenti
- Controllo degli errori
- Controllo di flusso
- Controllo della congestione (meccanismo a finestra)

TCP

Il TCP accetta pkt di lunghezza arbitraria e li frammenta in segmenti di lunghezza 64KB accettabili da IP.

TCP riordina e riassembra i pkt

TCP sovraintende alla connessione E2E e decide la velocità con cui immettere i pkt nel circuito virtuale di livello 4 che instaura. Questo consente di controllare il flusso e la congestione nella rete

Essendo un protocollo di comunicazione E2E opera solo in modalità unicast e non multicast o broadcast

Pacchetto TCP

Formato Header + Dati (<=64KB). Ecco l'header:

- Source port: 16 bit, indirizzo porta sorgente
- Destination port: 16 bit, indirizzo porta destinazione
- Sequence number: 32 bit
- ACK number: 32 bit, ack implicito nella direzione opposta mediante piggybacking
- Data offset: 4 bit, lunghezza header a multipli di 4B
- Flags: 12 bit (6 per future espansioni)
 - URG (urgent) per dare precedenza alle info nel pkt
 - ACK campo acknowledgment valido
 - PSH (push) causa la trasm immediata delle info ricevute dallo strato superiore
 - RST (reset) indica che si vuole fermare flusso e resettare connessione
 - SYN (synchronize) specifica il valore della seqenza al destinatario per sincronizzare
 - FIN (final) specifica che il trasm ha finito di trasmettere su questa connessione virtuale di livello 4
- Window: 16 bit indica # byte che il ricevitore è in grado di ricevere per influenzare trasmissione e controllo di flusso
- Checksum: 16 bit per verifica errori su header
- Urgent pointer: 16 bit, se presenti dati urgenti sono all'inizio della parte dati e il puntatore segna la fine
- Options: variabile, info su dimensioni buffer, gestione operazioni, etc.
- PAD: variabile affinché header con dimensione multipla di 4B

UDP & RTP

L'**User Datagram Protocol (UDP)** è un altro modo per effettuare il trasporto mediante datagram senza circuito virtuale

Sono le applicazioni a livello superiore che riordinano i pkt e chiedono la ritrasmissione

Il **Real Time Protocol (RTP)** è un modo di fare trasporto per gestire dati isocroni (ad esempio video e audio per videoconferenza).

È simile a UDP ma fornisce alle applicazioni pkt ordinati e cadenzati anche accorpando sorgenti diverse (es. video e audio)