

Principi architetturali di Internet (Clark' 88)

In ordine di importanza:

- 0 **Connessione delle reti già esistenti**
inizialmente: ARPANET, ARPA packet radio, rete a pacchetto satellitare
1. **Sopravvivenza (survivability)**
garantire comunicazione anche in caso di guasti a nodi/link
2. **Supporto a molteplici tipi di servizi**
3. **Possibilità di estensione a grande varietà di reti**
4. **Permettere gestione distribuita**
5. **Permettere che un host si attacchi alla rete con minimo sforzo**
6. **Efficiente in termini di costi**
7. **Permettere monitoraggio e tariffazione delle risorse utilizzate**

Un diverso ordinamento delle priorità porta a architetture diverse!

I. Sopravvivenza

- ❖ Continuare a operare anche in caso di perdita di componenti della rete (e.s., guasti a link e router)
 - due nodi terminali devono continuare a poter comunicare fintantochè la rete sottostante non è partizionata
 - qualunque altro guasto interno (eccetto la partizione della rete) deve restare **trasparente** ai nodi terminali
 - concetto di “fate sharing”
- ❖ Decisione: mantenere solo stato a livello di trasporto, nei nodi terminali
 - elimina il problema di gestire inconsistenza dello stato e recupero dello stato in caso di guasto a nodi/link
- ❖ Internet: architettura a livello rete senza stato (**stateless**)
 - Non c'è nozione di sessione/chiamata a livello rete

2. Tipi di servizio

- ❖ aggiunta di UDP a TCP per supportare applicazioni diverse
 - e.s., applicazioni “real-time”
- ❖ forse la ragione principale della separazione TCP, IP
- ❖ astrazione “datagram”: comune denominatore su cui i servizi di livello superiore possono essere costruiti
 - la differenziazione dei servizi a livello rete fu inizialmente considerata (il campo ToS), ma mai adottata su larga scala (perchè?)

3. Varietà di reti

- ❖ Grande successo (perchè?)
 - grazie a requisito minimalistico; si richiede alla rete sottostante solo di consegnare un pacchetto con “ragionevole” probabilità di successo
- ❖ ...non si richiede: affidabilità, consegna in sequenza
- ❖ *mantra*: IP su qualunque cosa
 - allora: ARPANET, X.25, rete satellitare DARPA ...
 - oggi: Ethernet, SONET, WiFi, reti cellulari, WDM...

Altri obiettivi (secondari)

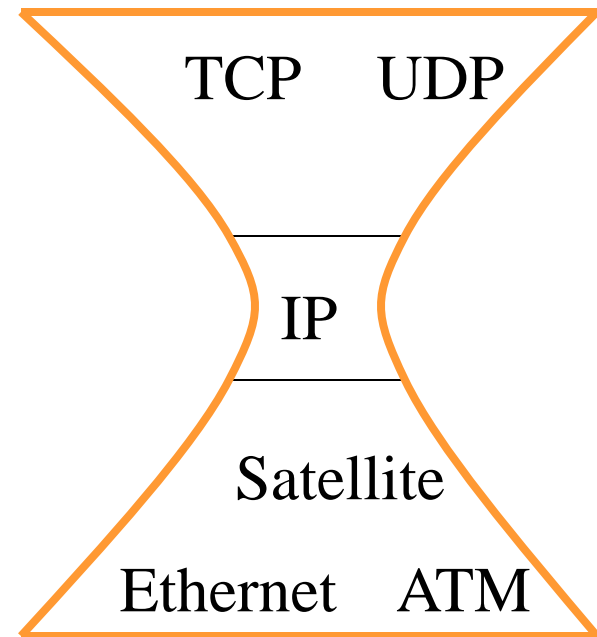
- ❖ Permettere **gestione distribuita**
 - Autonomia amministrativa: IP interconnette reti diverse
 - ogni rete può essere gestita da una diversa organizzazione
 - le diverse organizzazioni interagiscono solo ai bordi della rete
 - ... ma questo modello complica molto l'istradamento
- ❖ **Efficacia in termini di costi**
 - presenti diverse inefficienze:
 - overhead di pacchetti (e.g.: telnet)
 - ritrasmissioni end-to-end
 - routing può non essere ottimale
 - ...ma raggiungere prestazioni "ottimali" non è mai stata una priorità

Altri obiettivi (secondari)

- ❖ **Basso costo per attaccare un nuovo host**
 - non un punto di forza → costo più alto rispetto ad altre architetture poichè **intelligenza risiede negli host** (e.s., telefono vs computer)
 - cattive implementazioni o utenti malevoli possono produrre danni considerevoli (fate-sharing...)
- ❖ **Tariffazione**
 - complicata se non impossibile

Summario: Architettura di Internet

- ❖ rete a datagramma basata su commutazione di pacchetto
- ❖ IP fa da collante
- ❖ architettura a “clessidra”
 - tutti gli host e i router eseguono IP
 - architettura stateless
 - no stato per-flow dentro la rete



IP hourglass

E in futuro?

- ❖ Il “datagram” non è la migliore astrazione per:
 - gestione delle risorse, tariffazione, QoS
- ❖ nuova astrazione: **flusso** (vedi IPv6)
 - ma nessuno sa cosa è un flusso
- ❖ routers dovrebbero mantenere informazione di stato per ogni flusso
- ❖ gestione dello stato: il recupero di informazione di stato andata persa è difficile
- ❖ qui (1988) troviamo la prima idea di “soft state”!
 - **soft-state: sistemi terminali** responsabili del mantenimento dello stato

Lista di priorità rivista (1988 vs 2008)

1988

1. Sopravvivenza (survivability)
2. Supporto a molteplici tipi di servizi
3. Possibilità di estensione a grande varietà di reti
4. Permettere gestione distribuita
5. Permettere che un host si attacchi alla rete con minimo sforzo
6. Efficiente in termini di costi
7. Permettere monitoraggio e tariffazione delle risorse utilizzate

2008

1. Sicurezza
2. Availability and resilience
3. Convenienza economica
4. Migliore gestione
5. Venire incontro ai bisogni della società
6. Longevità
7. Predisposizione a supportare e sfruttare tecnologie future
8. Assolvere al suo compito (funziona...)