Università degli Studi di Roma "Tor Vergata"
Laurea in Informatica

Sistemi Operativi e Reti
(modulo Reti)
a.a. 2023/2024

Livello di rete: piano di controllo (parte3)

dr. Manuel Fiorelli

manuel.fiorelli@uniroma2.it

https://art.uniroma2.it/fiorelli

Basate sulle slide del libro di testo:
https://gaia.cs.umass.edu/kurose_ross/ppt.php

Livello di rete: tabella di marcia del “piano di controllo”

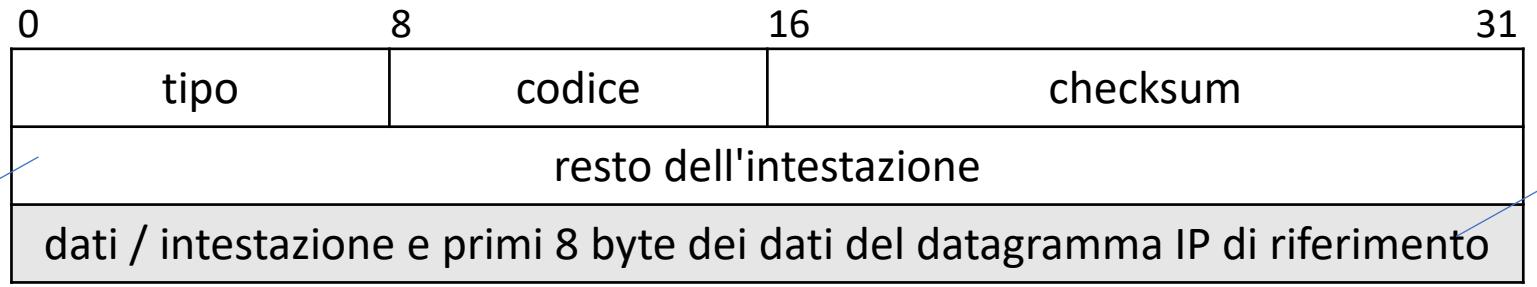
- introduzione
- algoritmi di instradamento
  - link state
  - distance vector
- instradamento interno al sistema autonomo: OSPF
- instradamento tra sistemi autonomi: BGP
- piano di controllo SDN
- Internet Control Message Protocol

- gestione e configurazione della rete
  - SNMP
  - NETCONF/YANG

ICMP: internet control message protocol

- utilizzato da host e router per comunicare informazioni a livello di rete
  - segnalazione di errori: host, rete, porta, protocollo non raggiungibile
  - richiesta/risposta echo (usato da ping)
- livello di rete "sopra" l'IP:
  - messaggi ICMP trasportati nei datagrammi IP
  - non viene considerato un protocollo di trasporto perché non usato dalle applicazioni di rete per trasferire i propri messaggi

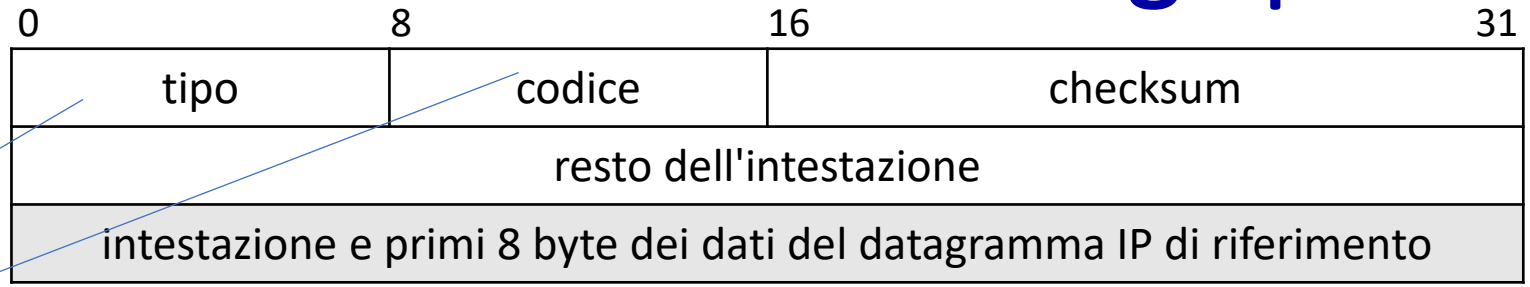
Messaggio ICMP:



la struttura dipende dal tipo di messaggio

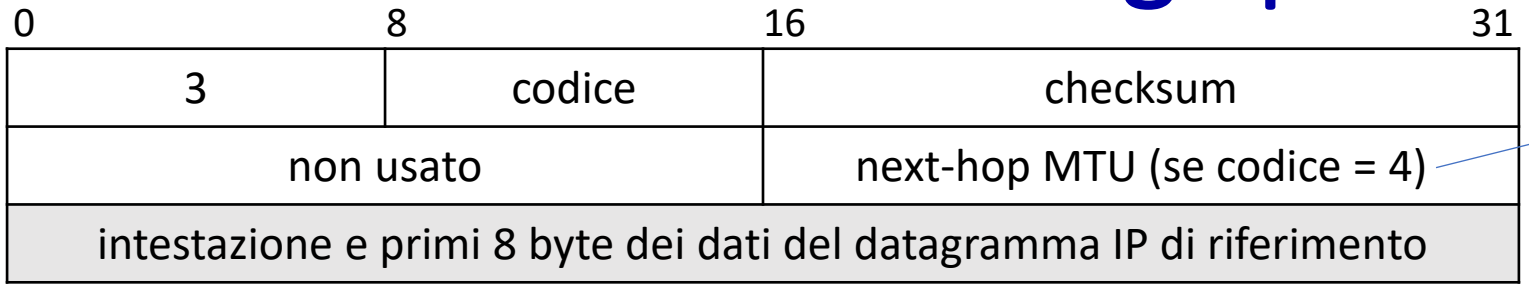
in alcuni casi, usato per determinare il datagramma che ha causato il messaggio e determinare il processo corrispondente (assumendo che i numeri di porta si trovino nei primi 8 byte)

ICMP: internet control message protocol



Tipo	Codice	Descrizione
0	0	echo reply (ping)
3	0	dest. network unreachable
3	1	dest host unreachable
3	2	dest protocol unreachable
3	3	dest port unreachable
3	4	fragmentation required
3	6	dest network unknown
3	7	dest host unknown
4	0	source quench (congestion control - not used)
8	0	echo request (ping)
9	0	route advertisement
10	0	router discovery
11	0	TTL expired
12	0	bad IP header

ICMP: internet control message protocol



si rammenti *Path MTU Discovery* (PMTUD)

Tipo	Codice	Descrizione
0	0	echo reply (ping)
3	0	dest. network unreachable
3	1	dest host unreachable
3	2	dest protocol unreachable
3	3	dest port unreachable
3	4	fragmentation required
3	6	dest network unknown
3	7	dest host unknown
4	0	source quench (congestion control - not used)
8	0	echo request (ping)
9	0	route advertisement
10	0	router discovery
11	0	TTL expired
12	0	bad IP header

possibilmente inviati dai router lungo il percorso. Una rete è irraggiungibile ad esempio se risulta avere distanza infinita, mentre per un host può derivare dal fallimento della risoluzione ARP. L'essere sconosciuto deriva al non trovare una rotta idonea.

dovrebbero essere inviati dall'host di destinazione, quando il protocollo o la porta non sono attivi. Il protocollo TCP gestisce il secondo caso attraverso l'invio di segmenti RST. Tuttavia, il lato mittente (di qualunque protocollo di trasporto) deve gestire anche l'analogo messaggio ICMP.

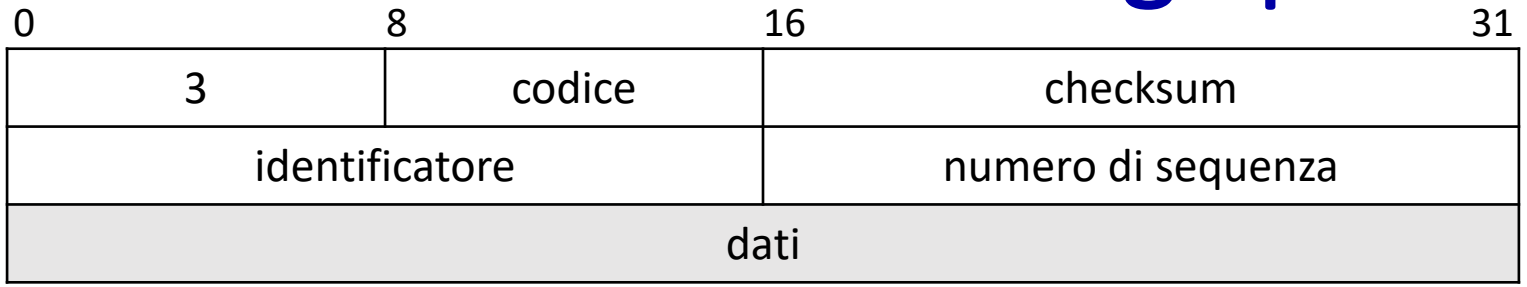
I messaggi *destination unreachable* devono essere passati dal livello di rete a quello di trasporto, che dovrebbe farne un uso appropriato (es. riportare il problema all'applicazione)

ICMP: internet control message protocol

Tipo	Codice	Descrizione
0	0	echo reply (ping)
3	0	dest. network unreachable
3	1	dest host unreachable
3	2	dest protocol unreachable
3	3	dest port unreachable
3	4	fragmentation required
3	6	dest network unknown
3	7	dest host unknown
4	0	source quench (congestion control - not used)
8	0	echo request (ping)
9	0	route advertisement
10	0	router discovery
11	0	TTL expired
12	0	bad IP header

Può essere inviato da un router congestionato per forzare l'host mittente a ridurre il tasso di trasmissione. Permette una forma di controllo della congestione informato dalla rete. **Oggi deprecato**. Si ricordi, invece, il meccanismo ECN discusso in precedenza.

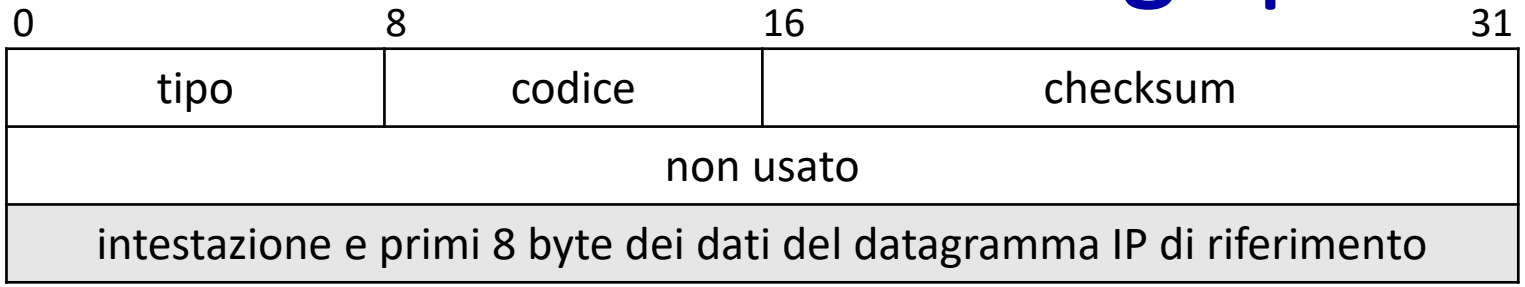
ICMP: internet control message protocol



Tipo	Codice	Descrizione
0	0	echo reply (ping)
3	0	dest. network unreachable
3	1	dest host unreachable
3	2	dest protocol unreachable
3	3	dest port unreachable
3	4	fragmentation required
3	6	dest network unknown
3	7	dest host unknown
4	0	source quench (congestion control - not used)
8	0	echo request (ping)
9	0	route advertisement
10	0	router discovery
11	0	TTL expired
12	0	bad IP header

La risposta *ping* contiene gli stessi dati della richiesta *ping*: tra le altre cose può includere un timestamp per calcolare RTT in maniera stateless

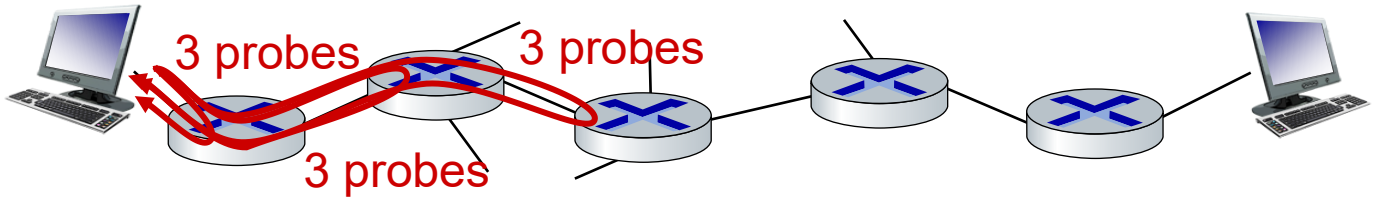
ICMP: internet control message protocol



Tipo	Codice	Descrizione
0	0	echo reply (ping)
3	0	dest. network unreachable
3	1	dest host unreachable
3	2	dest protocol unreachable
3	3	dest port unreachable
3	4	fragmentation required
3	6	dest network unknown
3	7	dest host unknown
4	0	source quench (congestion control - not used)
8	0	echo request (ping)
9	0	route advertisement
10	0	router discovery
11	0	TTL expired
12	0	bad IP header

viene usato da *traceroute*

Traceroute e ICMP



- la sorgente invia serie di segmenti UDP alla destinazione (con un numero di porta "improbabile")
  - 1˚ insieme ha TTL =1, 2˚ insieme ha TTL=2, ...
- un datagramma nella *n*-esimo insieme arriva all'*n*-esimo router:
  - il router scarta il datagramma e invia il messaggio ICMP alla sorgente (tipo 11, codice 0)
    - l'indirizzo IP del router si trova nel campo indirizzo sorgente dell'intestazione del datagramma che incapsula il messaggio ICMP

criteri di arresto:

- Il segmento UDP arriva eventualmente a destinazione
  - la destinazione restituisce il messaggio ICMP “port unreachable” (tipo 3, codice 3)
- la sorgente si ferma

- quando il messaggio ICMP arriva alla sorgente: registrare gli RTT

ICMP: internet control message protocol

- ICMPv6 per IPv6:
  - nuovi tipi e codici
  - ridefinizione di alcuni tipi e codici esistenti

Per esempio, invece di "*destination unreachable – fragmentation required*" c'è il messaggio "*packet too big*".

Livello di rete: tabella di marcia del “piano di controllo”

- introduzione
- algoritmi di instradamento
  - link state
  - distance vector
- instradamento interno al sistema autonomo: OSPF
- instradamento tra sistemi autonomi: BGP
- piano di controllo SDN
- Internet Control Message Protocol

- gestione e configurazione della rete
  - SNMP
  - NETCONF/YANG

Cos'è la gestione della rete (*network management*)?

- sistema autonomo (noto altrimenti come “rete”): migliaia di componenti software e hardware che interagiscono tra loro

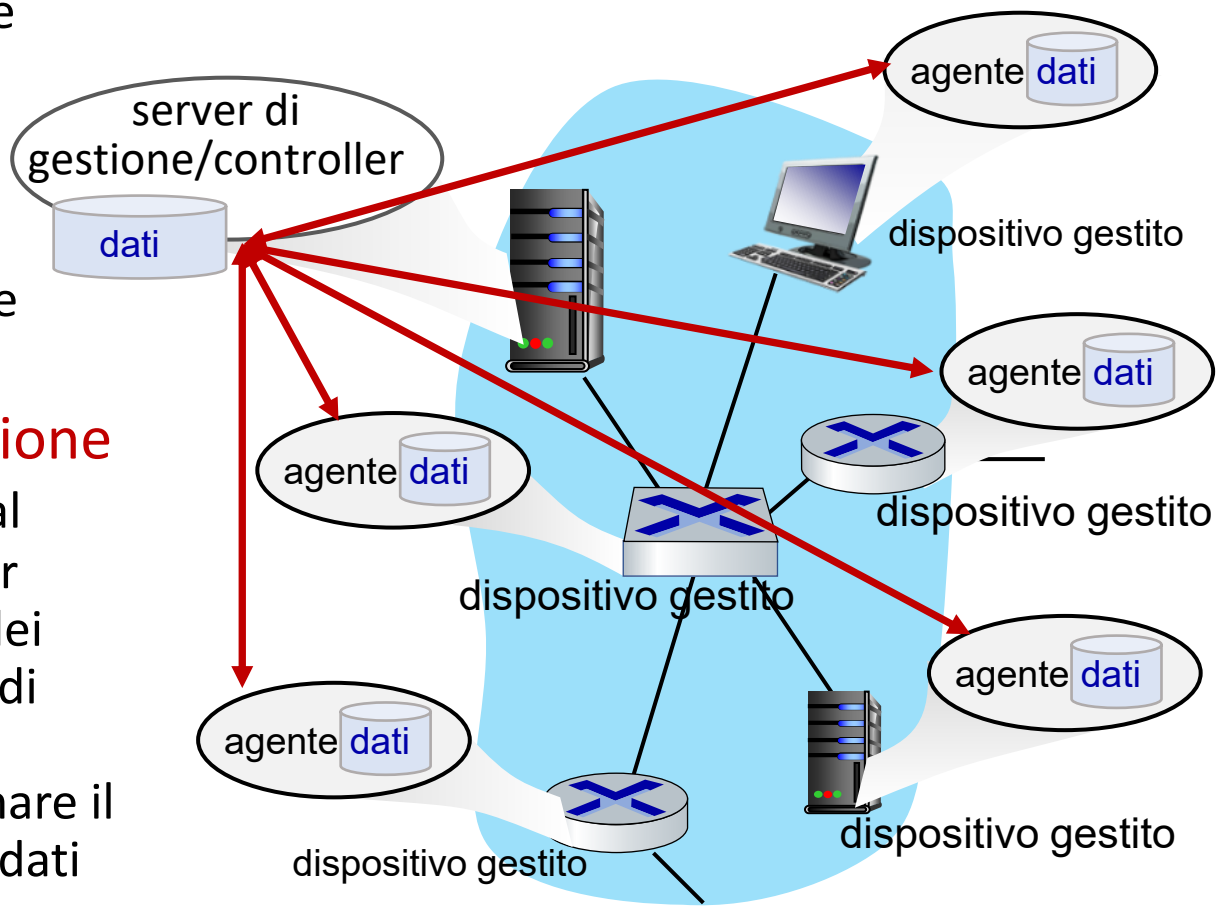
Saydam 1996

"La gestione della rete comprende il funzionamento, l’integrazione e il coordinamento di hardware, software e personale tecnico per monitorare, verificare, configurare, analizzare, valutare e controllare le risorse della rete affinché soddisfino le funzionalità in tempo reale e i requisiti di qualità del servizio a un costo accettabile"

Componenti della gestione della rete

Server di gestione: raccolta, elaborazione e analisi delle informazioni, invio di informazioni e comandi, in genere con i gestori della rete (umani) nel loop

Protocollo di gestione di rete: utilizzato dal server di gestione per interrogare lo stato dei dispositivi e agire su di essi; utilizzato dai dispositivi per informare il server di gestione di dati ed eventi.



Dispositivo di rete gestito: apparecchiature con componenti hardware e software gestibili e configurabili

Dati: "stati" del dispositivo: dati di configurazione (assegnati dall'amministratore, come indirizzo IP), dati operativi (acquisiti da dispositivo, come i vicini OSPF), statistiche

Approcci dell'operatore di rete per gestire la rete

CLI (Command Line Interface)

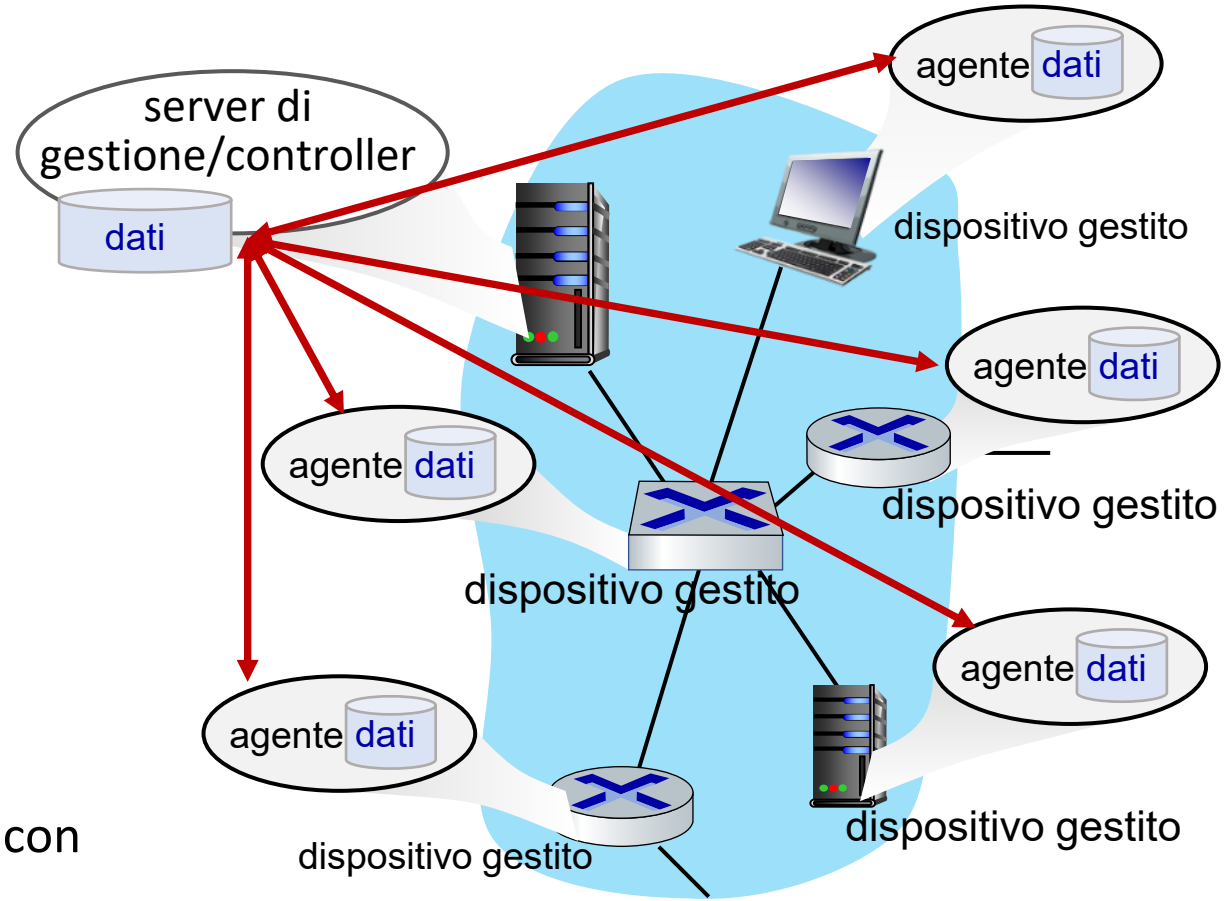
- l'operatore scrive comandi su una console del dispositivo o esegue script da remoto, per esempio, attraverso un ssh
- molti dispositivi hanno anche una UI web

SNMP/MIB

- l'operatore interroga/imposta i dati contenuti negli oggetti MIB (*management information base*) utilizzando il Simple Network Management Protocol (SNMP)

NETCONF/YANG

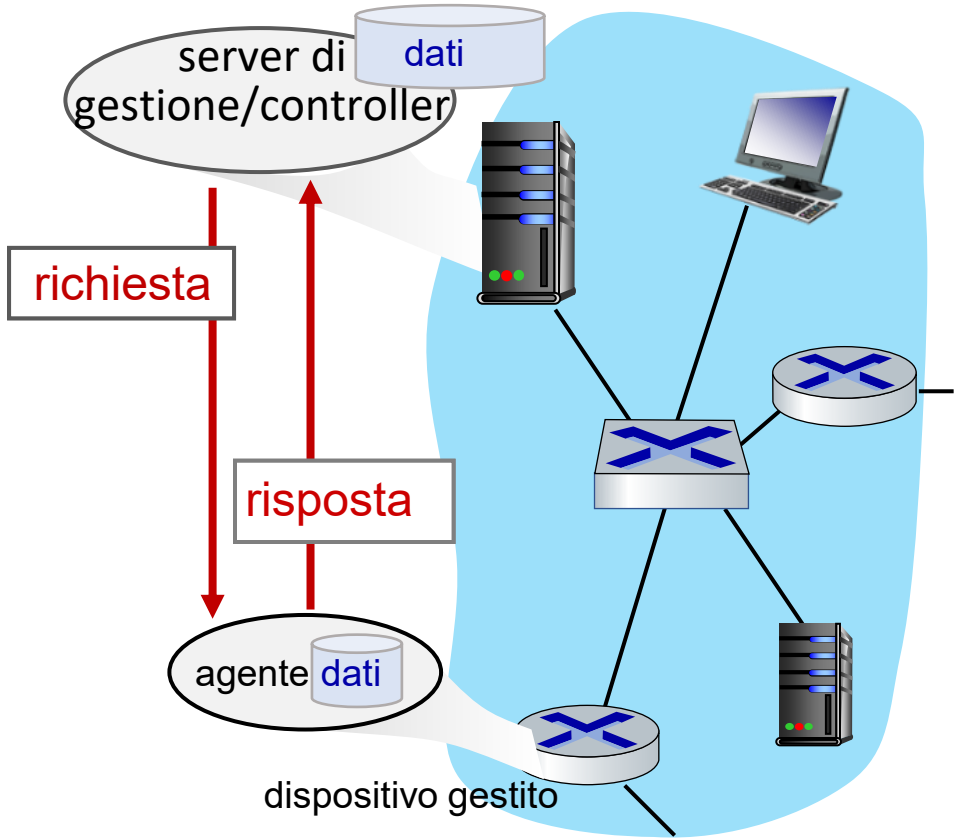
- più astratto, a livello di rete, olistico
- enfasi sulla gestione della configurazione multidispositivo
- YANG: linguaggio di modellazione dei dati
- NETCONF: comunicare azioni/dati compatibili con YANG a/da/tra dispositivi remoti



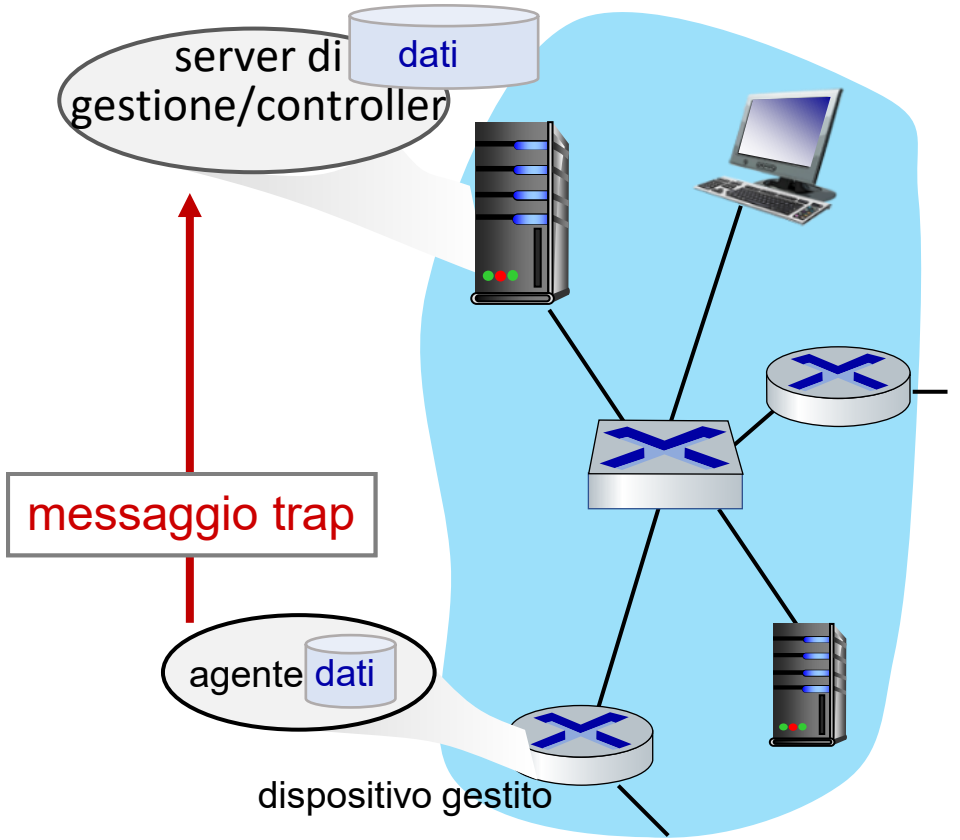
Protocollo SNMP

Due modi per trasmettere le informazioni MIB e comandi:

SNMP utilizza in genere il protocollo di traporto UDP



modalità richiesta/risposta

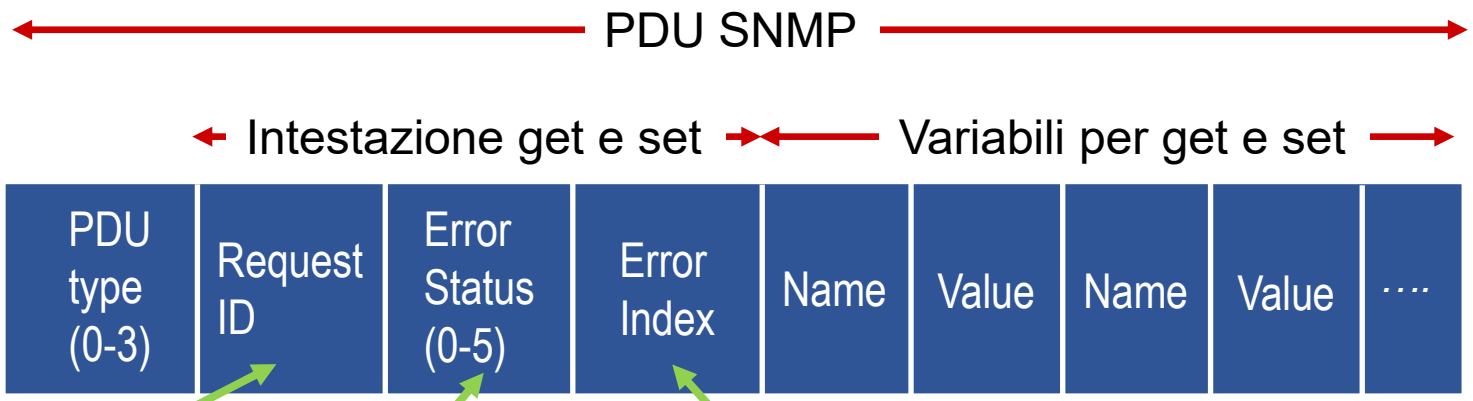


trap mode

Protocollo SNMP: tipi di messaggio

Tipo di messaggio	Funzione
GetRequest GetNextRequest GetBulkRequest	manager→agente: “dammi dati” (istanze di oggetto, prossima istanza di oggetto in lista o tabella, blocco di dati).
SetRequest	manager→agente: imposta il valore di una o più istanze di oggetti MIB
Response	agente→manager: generato in risposta a una richiesta
Trap	agente→manager: informa il manager di un evento inatteso

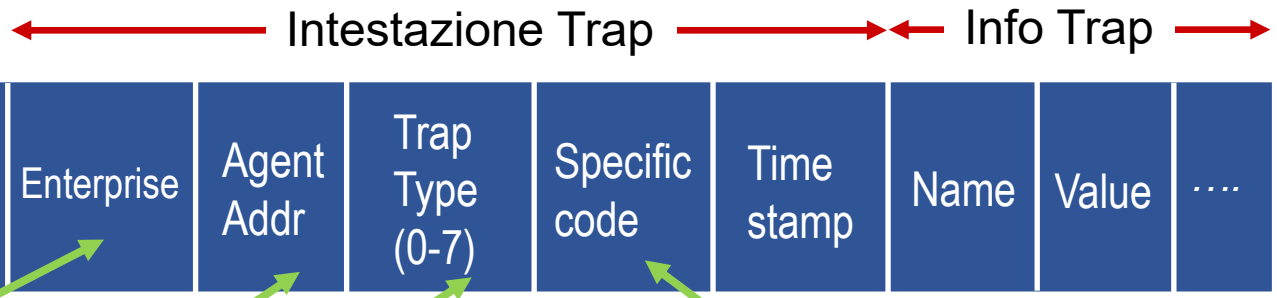
Protocollo SNMP: formati dei messaggi



Identificatore usato per associare richieste e risposte (veicolate tramite UDP)

riporta un errore

per alcuni *error status*, quali *noSuchName*, fornisce l'indice della variabile cui si riferisce l'errore



OID che descrive il tipo di agente che ha inviato la trap

indirizzo IP dell'agente che ha inviato la trap

tipo di trap. Il valore 6 indica una *enteprise-specific trap*

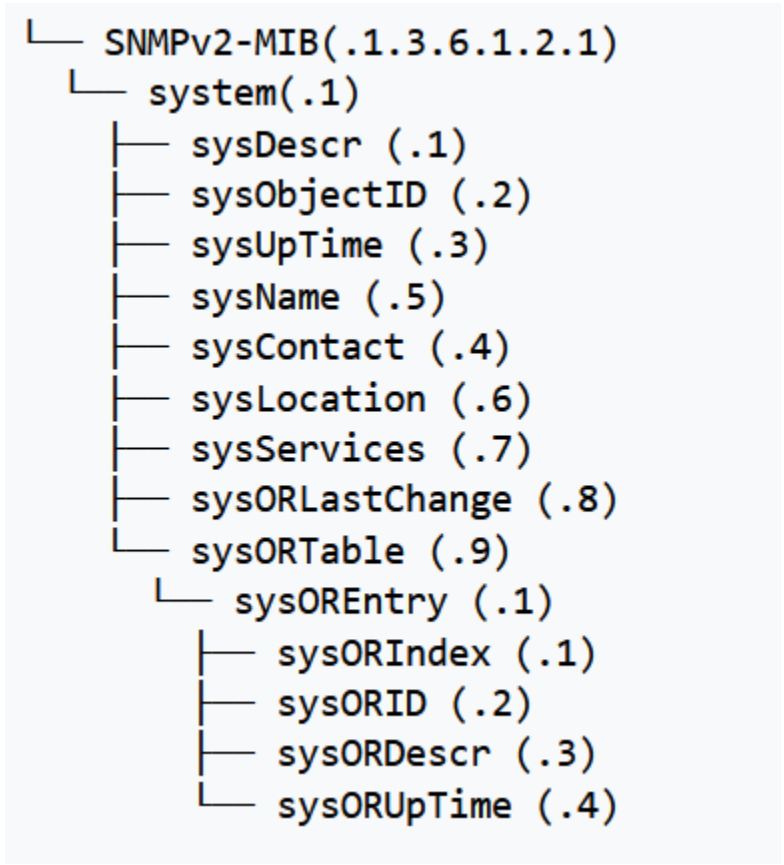
qualifica il tipo di una *enterprise-specific trap*

SNMP: Management Information Base (MIB)

- i dati operativi (e alcuni dati di configurazione) del dispositivo gestito
- raccolti moduli MIB
  - 400 moduli MIB definiti da RFC; molte più moduli MIB specifici del fornitore
- Structure of Management Information (SMI): linguaggio di definizione dei dati
- esempio di variabili MIB per il protocollo UDP:

Object ID	Name	Type	Comments
1.3.6.1.2.1.7.1	UDPInDatagrams	32-bit counter	numero totale di datagrammi consegnati
1.3.6.1.2.1.7.2	UDPNoPorts	32-bit counter	numero di datagrammi non consegnabili (nessuna applicazione alla porta)
1.3.6.1.2.1.7.3	UDInErrors	32-bit counter	numero di datagrammi non consegnabili (qualsiasi altra ragione)
1.3.6.1.2.1.7.4	UDPOutDatagrams	32-bit counter	numero totale di datagrammi inviati
1.3.6.1.2.1.7.5	udpTable	SEQUENCE	una voce per ogni porta in uso

SNMP: Management Information Base (MIB)

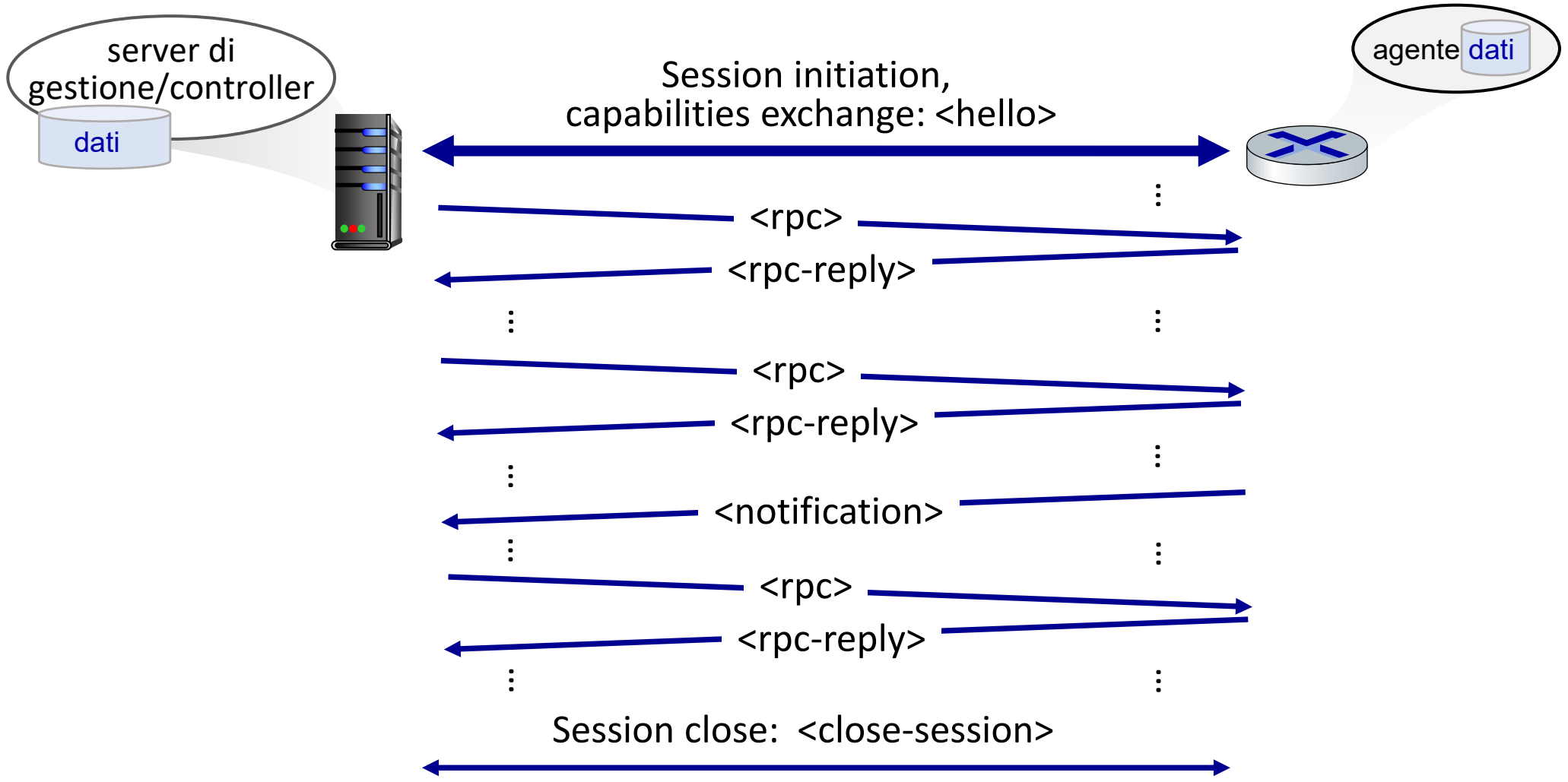


- gerarchico
- ogni voce è indirizzata da un OID (*object identifier*)

Panoramica di NETCONF

- obiettivo: gestire/configurare in maniera attiva dispositivi a sulla rete
- opera tra il server di gestione e i dispositivi di rete gestiti
  - azioni: retrieve, set, modify, activate configurations
  - commit atomico di azioni su molteplici dispositivi
  - interrogare i dati operativi e le statistiche
  - sottoscrivere le notifiche dai dispositivi
- Paradigma a chiamata di procedura remota (*remote procedure call*, RPC)
  - messaggi del protocollo NETCONF codificati in XML
  - scambiati attraverso un protocollo di trasporto affidabile e sicuro (e.g., TLS)

NETCONF: inizializzazione, scambio, chiusura



Operazioni NETCONF selezionate

Operazione	Descrizione
<get-config>	Recupera tutta o parte di una data configurazione. Un dispositivo può avere più configurazioni. C'è sempre una configurazione *running*, che descrive la configurazione corrente (in esecuzione) dei dispositivi.
<get>	Recupera tutti o parte dei dati operativi e della configurazione running.
<edit-config>	Modifica la configurazione (possibilmente in esecuzione) del dispositivo gestito. Quest'ultimo invia un <rpc-reply> contenente <ok>; altriemnti viene inviato un <rpcerror> con rollback.
<lock>, <unlock>	Bloccare (sbloccare) il datastore di configurazione sul dispositivo gestito (per bloccare i comandi NETCONF, SNMP o CLI da altre fonti).
<create-subscription>, <notification>	Abilita la sottoscrizione di notifiche di eventi dal dispositivo gestito

Esempio di messaggio NETCONF RPC

```
01 <?xml version="1.0" encoding="UTF-8"?>
02 <rpc message-id="101"
03   xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
04   <edit-config>
05     <target>
06       <running/>
07     </target>
08     <config>
09       <top xmlns="http://example.com/schema/
         1.2/config">
10         <interface>
11           <name>Ethernet0/0</name>
12           <mtu>1500</mtu>
13         </interface>
14       </top>
15     </config>
16   </edit-config>
17 </rpc>
```

nota l'id del messaggio

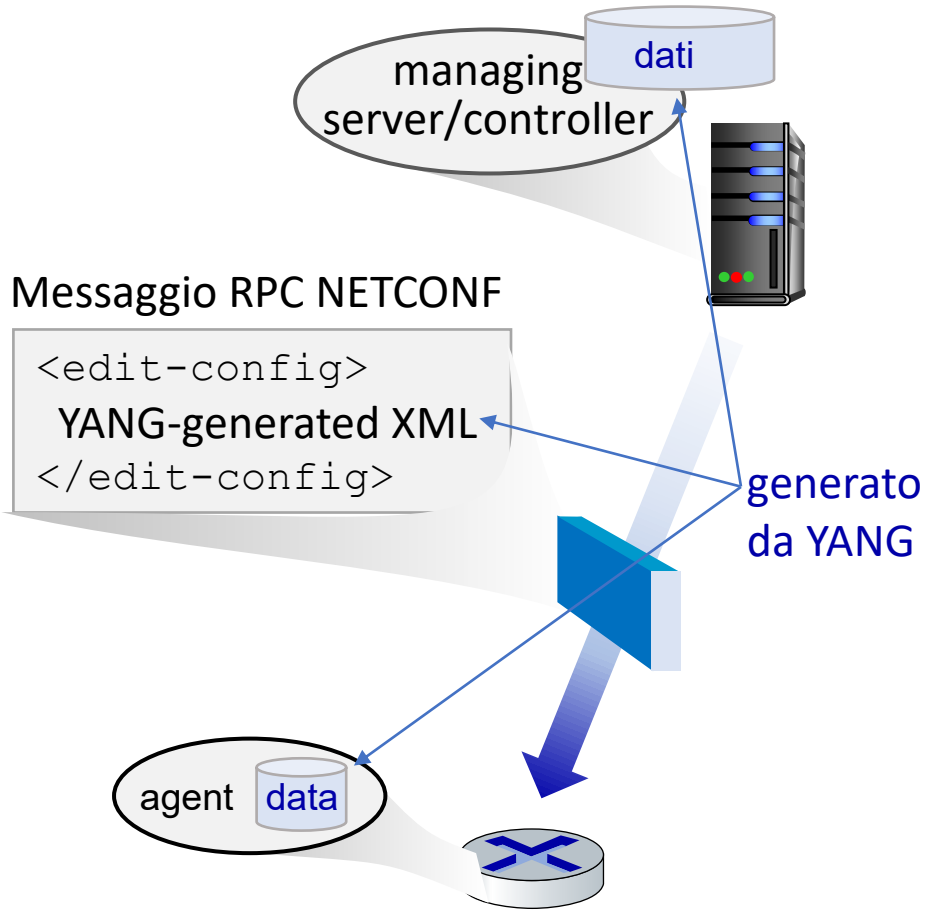
cambia una configurazione

cambia la configurazione in esecuzione

cambia la MTU dell'interfaccia Ethernet 0/0 in 1500

YANG

- linguaggio di modellazione dei dati utilizzato per specificare la struttura, la sintassi e la semantica dei dati di gestione della rete NETCONF
  - tipi di dati incorporati, come SMI
- documento XML che descrive il dispositivo; può essere generato dalla descrizione YANG
- può esprimere vincoli tra i dati che devono essere soddisfatti da una configurazione NETCONF valida
  - garantire che le configurazioni NETCONF soddisfino i vincoli di correttezza e di coerenza



YANG (continua)

Esempio YANG:

```
container system {
        container login {
                leaf message {
                        type string;
                        description "Message given at start of login session";
                }
        }
}
```

Esempio NETCONF:

```
 <system>
        <login>
                <message>Good morning</message>
        </login>
</system>
```

Livello di rete: Riassunto

Abbiamo imparato molto!

- approcci al piano di controllo della rete
  - controllo per router (tradizionale)
  - controllo centralizzato logicamente (software defined networking)
- algoritmi di instradamento tradizionali
  - implementazione in Internet: OSPF , BGP
- controller SDN
  - implementazione in pratica: ODL, ONOS
- Internet Control Message Protocol
- network management

Prossima fermata: livello di collegamento!

Livello di rete: “piano di controllo” Fatto!

- introduzione
- algoritmi di instradamento
  - link state
  - distance vector
- instradamento interno al sistema autonomo: OSPF
- instradamento tra sistemi autonomi: BGP
- piano di controllo SDN
- Internet Control Message Protocol

- gestione e configurazione della rete
  - SNMP
  - NETCONF/YANG