Politecnico di Torino

Corso di Protocolli e Architetture di Routing

Domande di riepilogo

Fulvio Risso

August 25, 2011

Contents

1 Forwarding e Routing

1. I concetti di Forwarding e Routing:
   a) Sono sinonimi; individuano il processo che permette di trovare un percorso valido per un pacchetto, dal mittente al destinatario
   b) Sono sinonimi; individuano il processo che permette, a fronte di un pacchetto entrante in un nodo di rete, di determinare qual è la migliore porta di uscita verso la destinazione
   c) Sono concetti differenti; il processo di forwarding mira ad individuare un percorso valido per un pacchetto, dal mittente al destinatario; il processo di routing permette, a fronte di un pacchetto entrante in un nodo di rete, di determinare qual è la migliore porta di uscita verso la destinazione
   d) Sono concetti differenti; il processo di routing mira ad individuare un percorso valido per un pacchetto, dal mittente al destinatario; il processo di forwarding permette, a fronte di un pacchetto entrante in un nodo di rete, di determinare qual è la migliore porta di uscita verso la destinazione

2 Algoritmi di forwarding

2. La tecnica di forwarding "Label Swapping":
   a) Non è adatta qualora si abbia la necessità di fornire garanzie di qualità del servizio nell'inoltro dei pacchetti
   b) Prevede che un pacchetto dati mantenga la stessa etichetta ("label") per tutto il percorso dal nodo sorgente a quello destinazione
   c) Richiede che tutti i nodi presenti sul percorso condividano esattamente la stessa tabella di forwarding
   d) Può richiedere una fase di "Path Setup" per la determinazione del percorso

3. La tecnica di forwarding "Source Routing":
   a) Prevede l'utilizzo di client ("host") molto semplici e di nodi intermedi ("router") molto complessi
   b) È adatta quando si vuole minimizzare il numero di bytes necessari per le operazioni di instradamento e presenti in ogni pacchetto
   c) Il nodo mittente deve avere una conoscenza (almeno parziale) della topologia di rete
   d) È la tecnica comunemente utilizzata dal protocollo IP nelle operazioni di forwarding

4. Quali di queste tecnologie è più adatta a gestire percorsi multipli verso la stessa destinazione ("multipath")?
   a) Forwarding by network address
   b) Label Swapping e Source Routing
   c) Label Swapping
   d) Source Routing

3 Introduzione agli algoritmi di routing

3.1 Aspetti generali

5. Il Multipath routing:
   a) È supportato dalle maggiori implementazioni di RIP
   b) Permette ai router di utilizzare percorsi multipli durante i transitori sulla rete, così da velocizzare la diffusione delle informazioni di routing e diminuire la durata del transitorio
   c) Può essere causa di loop se si ammette che i percorsi utilizzati possano avere costi differenti
   d) È consigliato solamente se il traffico dati è composto prevalentemente da pacchetti TCP

6. Nei protocolli di routing, il periodo di transitorio:
   a) È presente solo quando vengono adottati gli algoritmi più semplici (es. Distance Vector)
   b) Non è mai presente, in quanto è una caratteristica dei protocolli che lavorano a livello data-link (es. Spanning Tree)
   c) Si verifica sempre nel periodo immediatamente successivo al rilevamento di un guasto
   d) Si verifica sempre nel momento in cui una parte della rete cambia di stato

3.2 Algoritmi di routing non adattativi

7. Il routing statico:
   a) È particolarmente apprezzato per la sua capacità di rilevare velocemente i guasti
   b) Viene utilizzato in reti in cui si ha un elevato tasso di variazione delle tabelle di routing
   c) Trova applicazione soprattutto nelle reti periferiche; ad esempio è spesso utilizzato in quelle dove vi è un solo collegamento verso il resto della rete Internet
   d) È tipicamente usato nelle aree di backbone, per l'alta affidabilità

8. Si consideri una semplice topologia di rete in cui sono presenti quattro router (A, B, C, D), collegati tra di loro ad anello (A-B-C-D-A). Se gli host utilizzano un algoritmo di routing di tipo flooding e il router A invia un pacchetto a D, quante copie del medesimo pacchetto saranno recapitate al router D?
   a) 1
   b) 2
   c) 4
   d) È proporzionale al valore del campo Time To Live presente nel pacchetto

9. Si consideri una semplice topologia di rete in cui sono presenti quattro router (A, B, C, D). I primi 3 sono collegati tra di loro ad anello (A-B-C-A), mentre il quarto è collegato a C attraverso un link punto-punto (C-D). Se gli host utilizzano un algoritmo di routing di tipo flooding e il router A invia un pacchetto a D, quante copie del medesimo pacchetto saranno recapitate al router D?
   a) 1
   b) 2
   c) 3

d) È proporzionale al valore del campo Time To Live presente nel pacchetto

10. Un algoritmo di routing di tipo selective flooding:
    a) È sostanzialmente simile all'algoritmo di flooding classico, con la differenza che ciascun pacchetto in arrivo viene ritrasmesso su tutte le linee eccetto quella su cui è stato ricevuto
    b) È sicuramente più robusto di un classico algoritmo di flooding
    c) Consente di ridurre il numero di volte in cui un pacchetto viene inviato sulla stessa porzione di rete
    d) Richiede che i pacchetti inviati contengano un numero di sequenza

3.3 Algoritmi di routing adattativi

11. Quale tra questi elementi rappresenta un notevole svantaggio nella tecnica del routing centralizzato?
    a) Scarse prestazioni nel caso in cui il traffico trasportato sia di tipo voce
    b) Difficoltà nel determinare l'effettiva topologia di rete in caso di guasti
    c) Traffico dati particolarmente intenso nell'intorno del nodo centrale
    d) Criticità del nodo centrale dal punto di vista della robustezza e della scalabilità

12. Nel routing isolato:
    a) Ogni router calcola, attraverso scambi di messaggi con i soli vicini, la propria tabella di routing
    b) Ogni router calcola, attraverso scambi di messaggi con tutti i router nella rete, la propria tabella di routing
    c) Ogni router calcola, analizzando solamente il traffico che lo attraversa, la propria tabella di routing
    d) Alcune porzioni della rete vengono isolate dai rimanenti router, impedendo il transito di dati tra la porzione pubblica della rete e quella isolata

4 Algoritmi di routing distribuiti

4.1 Distance Vector

13. L'algoritmo di routing di tipo Distance Vector:
    a) Può causare di fenomeni di "Counting to Infinity" solo in reti che presentano maglie
    b) Causa sempre fenomeni di "Counting to Infinity" in reti non magliate
    c) È caratterizzato da una minore possibilità di fenomeni di "Counting to Infinity" in reti che non presentano maglie qualora si faccia uso della tecnica "Split Horizon"
    d) Il fenomeno di "Counting to Infinity" è proprio delle reti Link State.

14. Il meccanismo dello "Split Horizon" permette di:
    a) Eliminare la possibilità che si verifichino loop (percorsi di inoltro ciclici) in seguito a cambiamenti della topologia

b) Ridurre la probabilità che si verifichino loop in seguito a cambiamenti della topologia

c) Disabilitare, durante la fase di convergenza, l'invio di pacchetti dati verso quelle destinazioni che potrebbero dare luogo a loop

d) Diminuire il traffico di routing implementando la fase di neighbor discovery con dei pacchetti appositi ("Hello Packets")

15. La tecnica di "Split Horizon":

a) Prevede che le route ricevute negli annunci di un router vicino vengano sempre annunciate a quel vicino con metrica pari a infinito

b) Prevede che un prefisso non venga annunciato al vicino che rappresenta il "next hop" verso quella destinazione

c) Prevede che una destinazione venga dichiarata irraggiungibile nel momento in cui il costo supera una certa soglia di infinito.

d) Nessuna delle risposte precedenti

4.2 Path Vector

16. Nell'algoritmo di routing di tipo Path Vector:

a) Ogni record contenuto nel Path Vector contiene la destinazione, la distanza dal router in esame, e il next hop router per raggiungere quella destinazione

b) Ogni record contenuto nel Path Vector contiene la destinazione, la distanza dal router in esame, e il prossimo Autonomous System per raggiungere quella destinazione

c) Ogni record contenuto nel Path Vector contiene la destinazione, la distanza dal router in esame, e l'elenco dei router da attaversare per raggiungere quella destinazione

d) Ogni record contenuto nel Path Vector contiene la destinazione, la distanza dal router in esame, e l'elenco degli Autonomous System da attaversare per raggiungere quella destinazione

17. La tecnica "Path Vector" permette di:

a) Risolvere il problema del count to infinity

b) Risolvere il problema delle route sovrapposte

c) Rendere il protocollo "trasparente" rispetto all'informazione trasportata

d) Nessuna delle precedenti

4.3 Diffusing Update Algorithm

18. Il Diffusing Update Algorithm (DUAL):

a) Prevede che ogni router mantenga in memoria una serie di strutture dati aggiuntive, come ad esempio tutte le distanze tra i router ad esso adiacenti e le varie destinazioni nella rete

b) Non richiede la memorizzazione di informazioni aggiuntive rispetto a quelle classiche di un algoritmo Distance Vector

c) Permette di comprimere le informazioni di routing trasportate, aumentano così le prestazioni del processo di aggiornamento delle tabelle di instradamento

d) Introduce il concetto di "vicino accettabile", cioè un nodo adiacente al router che viene utilizzato come router di default per raggiungere qualsiasi destinazione nel momento in cui si verificano dei guasti sulla rete

19. Il "vicino accettabile" di un router R, nel Diffusing Update Algorithm (DUAL):
    a) È un router adiacente ad R il cui costo verso la destinazione è minore del costo (prima del guasto) tra il router R e la destinazione
    b) È un router il cui costo verso la destinazione è minore del costo (prima del guasto) tra il router R e la destinazione
    c) È un router adiacente ad R il cui costo verso la destinazione è minore del costo attuale tra il router R e la destinazione
    d) È un router il cui costo verso la destinazione è minore del costo attuale tra il router R e la destinazione

4.4 Link State

20. Nell'algoritmo Link State a regime, tutti i router hanno in memoria:
    a) Lo stesso albero di percorsi ottimi
    b) La base di dati descrivente il dominio a cui appartengono
    c) La stessa routing table
    d) Un set di Link State di tutti i nodi adiacenti

21. Qual è un vantaggio di utilizzare un algoritmo di routing di tipo Link State rispetto ad uno di tipo Distance Vector?
    a) La presenza del Link State Database elimina la necessità di avere una routing table, con un risparmio di memoria
    b) Avendo a disposizione il Link State Database, ogni router è in grado di calcolare autonomamente i percorsi verso ogni destinazione
    c) Una minore richiesta in termini di potenza elaborativa per l'esecuzione dell'algoritmo
    d) Minori errori di instradamento in quanto i Link State sono scambiati dai router con una frequenza molto elevata

22. È possibile l'instaurazione di un loop in una rete che utilizza un routing di tipo Link State?
    a) Si
    b) No, perchè ogni router ha una visione completa della topologia della rete
    c) No, perchè gli aggiornamenti del Link State vengono inviati in flooding
    d) No, perchè viene usato un Hold-Down timer

23. Nella fase finale di un algoritmo di routing di tipo Link State, ogni router:
    a) Esegue l'algoritmo di Shortest Path First, utilizzando come input il Link State Database
    b) Invia in flooding i propri Link State ai vicini
    c) Invia in flooding tutti i Link State ai vicini
    d) Esegue l'algoritmo DUAL (Diffusing Update Algorithm)

5 Routing gerarchico e redistribuzione

24. La redistribuzione:
    a) È quel processo che va abilitato sul router per far sì che riesca a smistare i pacchetti verso l'opportuna destinazione
    b) È utilizzata per lo scambio di informazioni tra un router interno (interior gateway) ed un router esterno (exterior gateway) che usa il protocollo BGP
    c) Viene utilizzata soprattutto dai domini di routing periferici, che si collegano ad un solo Internet service provider per l'accesso ad Internet
    d) È utilizzata per permettere il passaggio delle informazioni di routing da un dominio di routing A ad un dominio di routing B

6 Routing interdominio

25. Il routing inter-dominio:
    a) Prevede che ogni router sappia esattamente il percorso, in termini di router attraversati, fatto dai pacchetti verso una destinazione
    b) Prevede che un exterior gateway operi scelte di percorsi, basate su informazioni raccolte tramite protocolli di routing inter-dominio, coerenti con gli accordi esistenti con altri autonomous system
    c) Prevede che ogni router sappia esattamente il costo di raggiungimento di qualsiasi destinazione (ad esempio in termini di banda dei link attraversati) per poter calcolare il percorso a costo minore (per esempio a banda più elevata)
    d) È un concetto che tenderà a sparire

26. Il termine "Peering" si riferisce a:
    a) Il punto di collegamento tra due router di due Internet Service Provider diversi
    b) Lo scambio di informazioni tra un router e una stazione utilizzando un protocollo di routing
    c) Lo scambio di informazioni tra due router OSPF collegati da un virtual link
    d) Lo scambio di informazioni tra due router OSPF della stessa area

27. Un Autonomous System è:
    a) Un calcolatore in grado di autoconfigurarsi
    b) Una zona di una rete IP amministrata, soprattutto da punto di vista del routing, autonomamente dalle altre e con delle connessioni con almeno altri due Autonomous System
    c) Un dispositivo di rete in grado di scoprire autonomamente la strada migliore lungo cui inoltrare pacchetti per le destinazioni
    d) La rete di un ISP

28. Si supponga l'esistenza di tre AS (Autonomous System) collegati sequenzialmente (`A-B-C`). Se l'AS intermedio B vuole impedire che la sua rete venga usato come transito da A verso C:
    a) Deve effettuare il mascheramento delle route verso A
    b) Deve impostare una access list ("packet filtering") all'ingresso del suo dominio che scarta tutti i pacchetti in ingresso da A verso C

c) Deve impostare il mascheramento delle route verso A e una access list all'ingresso del suo dominio sui pacchetti provenienti da A e diretti a C

d) L'AS B non può bloccare il traffico, in quanto ogni AS deve fornire il transito agli AS a lui adiacenti

29. Un Network Provider considerato "Tier-1":
    a) Dispone di una sola interconnessione verso un altro Autonomous System di tipo Tier-1
    b) È un Autonomous System collegato ad altri AS Tier-1 solamente con connessioni di tipo "peering", ossia non a pagamento
    c) È un Autonomous System collegato ad altri AS Tier-1 prevalentemente con connessioni di tipo "peering", ossia non a pagamento
    d) È un Autonomous System collegato ad altri AS Tier-1 prevalentemente con connessioni di tipo "transit", ossia a pagamento

30. Un Neutral Access Point è una particolare rete in cui:
    a) Più Autonomous System collegano, a livello 2, un certo numero di router in modo scambiarsi le informazioni di routing
    b) Più Autonomous System collegano, a livello 3, un certo numero di router in modo scambiarsi le informazioni di routing
    c) Un Autonomous System collega, a livello 2, un certo numero di router in modo da velocizzare lo scambio delle informazioni di routing all'interno del dominio
    d) Un Autonomous System collega, a livello 3, un certo numero di router in modo da velocizzare lo scambio delle informazioni di routing all'interno del dominio

31. Un Neutral Access Point è una particolare rete in cui:
    a) Tutti gli apparati sono collegati mediante l'utilizzo di un router centrale ad alte prestazioni, dotato di interfacce di rete multiple
    b) Il collegamento tra gli apparati è realizzato a livello 2
    c) Ogni router collegato vede a livello 3 tutti gli altri router presenti sulla rete ed in grado di effettuare peering con ognuno di essi
    d) I vari AS si scambiano il traffico in modalità "peering", ossia non a pagamento

7 Protocolli di routing

32. Per il supporto dei prefissi di rete a lunghezza variabile in una zona della rete in cui sia utilizzato routing dinamico:
    a) La netmask associata al prefisso deve essere fornita ai router in fase di configurazione (con il comando "network" sui router Cisco)
    b) La netmask viene dedotta automaticamente dalla classe degli indirizzi utilizzati
    c) Le informazioni di routing scambiate tra i router devono includere la subnet mask associata ad ogni prefisso annunciato
    d) È obbligatorio l'utilizzo dei protocolli OSPF o BGP

33. La tecnica del CIDR (Classless InterDomain Routing):

a) Permette la trasmissione degli annunci di routing in modo più efficiente rispetto alla metodologia tradizionale, nonostante il numero di annunci di routing trasmessi sia lo stesso

b) Permette di ottimizzare il trasferimento degli annunci mediante una tecnica detta "aggregazione"

c) Consente il trasporto di informazioni atte a realizzare policy routing (politiche di routing) nel routing tra autonomous system differenti (routing interdominio)

d) È il protocollo di routing utilizzato nello scambio di route tra due Autonomous Systems

7.1 RIP

34. Il protocollo RIP prevede meccanismi per ridurre la possibilità di verificarsi di loop:
    a) Attraverso l'analisi dei pacchetti in transito e l'identificazione di quelli che passano più di una volta dallo stesso router
    b) Per mezzo di processi di "traceroute" attivati periodicamente
    c) Attraverso meccanismi di "Split-Horizon" e di "Hold-Down"
    d) Nessuna delle risposte precedenti

35. La principale limitazione del protocollo di routing RIP rispetto all'IGRP è che:
    a) Essendo il RIP proprietario non è disponibile su tutti i router
    b) La metrica del RIP è meno indicativa, rispetto a quella dell'IGRP, del reale grado di preferibilità di un percorso di rete rispetto ad altri
    c) Non permette, a differenza dell'IGRP, il routing gerarchico
    d) È un protocollo di tipo Distance Vector, quindi meno scalabile dell'IGRP (Link State)

36. Il protocollo RIP è imbustato:
    a) Direttamente in IP, per limitare la dimensione dei pacchetti di routing
    b) Direttamente in IP, per consentire la trasmissione in broadcast dei pacchetti
    c) In UDP, per consentire la trasmissione in broadcast dei pacchetti
    d) In UDP, per questioni principalmente legate alla maggiore semplicità di sviluppo del software

37. Un router dotato di due interfacce di rete (*FastEthernet0* con indirizzo `192.168.0.1/24` e *FastEthernet1* con indirizzo `192.168.1.1/30`) esegue il protocollo RIPv2, configurato con l'algoritmo di split horizon (puro) abilitato. I distance vector inviati dal router sull'interfaccia FastEthernet0 conterranno le informazioni sulle seguenti reti:
    a) 192.168.1.0/24
    b) 192.168.1.0/30
    c) 192.168.0.0/24 e 192.168.1.0/30
    d) 192.168.0.0/24 e 192.168.1.0/24

38. Due router sono connessi tra loro mediante un apparato di livello 2 (switch). Entrambi hanno il protocollo di routing RIPv2 abilitato, con le opzioni di default. Se l'interfaccia di uno dei router viene spenta, l'altro rileverà il guasto:

a) Dopo pochi istanti

b) Allo scadere del Routing Update Timer

c) Allo scadere del Route Invalid Timer

d) Allo scadere del Route Flush Timer

e) Nessuna delle risposte precedenti

39. Un router R1 è connesso ad un router R2 mediante un apparato di livello 2 (switch). Entrambi hanno il protocollo di routing RIPv2 abilitato, con le opzioni di default. Se si verifica un guasto sul collegamento tra i due router, il router R1 rileverà il guasto:

    a) Dopo pochi istanti

    b) Allo scadere del Routing Update Timer

    c) Allo scadere del Route Invalid Timer

    d) Allo scadere del Route Flush Timer

    e) Nessuna delle risposte precedenti

40. Un router R1 è connesso ad un router R2 mediante un apparato di livello 2 (switch). Entrambi hanno il protocollo di routing RIPv2 abilitato, con le opzioni di default. Se il link tra R1 e lo switch viene staccato, il router R1 rileverà il guasto:

    a) Dopo pochi istanti

    b) Allo scadere del Routing Update Timer

    c) Allo scadere del Route Invalid Timer

    d) Allo scadere del Route Flush Timer

    e) Nessuna delle risposte precedenti

7.2 IGRP-EIGRP

41. Il protocollo di routing EIGRP (Enhanced IGRP) differisce dall'IGRP perchè:

    a) Usa metriche più efficaci

    b) Genera maggior traffico di routing

    c) Prevede la comunicazione di informazioni riguardanti le netmask

    d) È più sofisticato ma più sensibile al fenomeno del Count to Infinity

42. Il protocollo EIGRP impedisce l'innescarsi di loop in quanto:

    a) Utilizza un algoritmo molto conservativo che nella sua fase iniziale accetta solamente annunci che provengono dal router che, per una data destinazione D, rappresenta il next hop per quella destinazione

    b) Accetta solo annunci che arrivano dal router che, per una data destinazione D, rappresenta il next hop per quella destinazione

    c) Invia periodicamente sui link dei pacchetti di tipo "Hello" per rilevare in brevissimo tempo la caduta di un nodo

    d) Ogni router conosce l'intera topologia di rete

43. Il protocollo EIGRP impedisce l'innescarsi di loop in quanto:

a) Accetta solamente annunci che migliorano il costo di una route esistente

b) Accetta solamente annunci che arrivano dal router che, per una data destinazione D, rappresenta il next hop per quella destinazione

c) Accetta solamente annunci che (a) migliorano il costo di una route esistente, oppure (b) arrivano dal router che, per una data destinazione D, rappresenta il next hop per quella destinazione

d) Accetta solamente annunci che (a) migliorano il costo di una route esistente, oppure (b) arrivano dal router che, per una data destinazione D, rappresenta il next hop per quella destinazione, a cui fa seguito una fase di selezione del percorso alternativo che esclude ogni percorso che potrebbe essere origine di loop

44. Il protocollo EIGRP:

a) Genera un maggiore traffico di rete rispetto ad IGRP a causa della necessità di evitare i loop

b) Adotta l'algoritmo DUAL per evitare la scelta di percorsi che possano contenere dei loop

c) Garantisce che le route siano *loop-free* grazie all'algoritmo di "selezione del vicino accettabile"

d) Ignora gli annunci provenienti dai router che non sono next-hop per le destinazioni presenti nella routing table

7.3 OSPF

45. Una differenza del protocollo di routing OSPF rispetto all'IGRP è che:

a) OSPF è gerarchico

b) OSPF consente di effettuare anche routing tra AS diversi

c) OSPF permette di trasportare contemporaneamente informazioni di routing relative a diverse architetture protocollari (routing integrato)

d) OSPF è proprietario

46. Il protocollo di routing OSPF sceglie il percorso verso una destinazione tenendo conto di:

a) Lunghezza di ciascun link lungo il percorso

b) Banda e ritardo per ogni link

c) Può essere configurato ad utilizzare svariate metriche la cui semantica viene stabilita dal gestore della rete

d) Hop Count

47. Nel protocollo OSPF i router connessi ad una stessa LAN vengono rappresentati nel grafo che descrive la rete come:

a) Un unico nodo

b) Una struttura di connessioni logiche di forma stellare

c) Una struttura di connessioni logiche completamente magliata

d) Una struttura composta da un insieme di nodi su un link broadcast

48. Un "Internal Router" OSPF in un'area mantiene nell'archivio di LSA:

a) La descrizione dettagliata della topologia di tutto il dominio OSPF

b) Solo ed esclusivamente una descrizione dettagliata della topologia dell'area di cui il router fa parte

c) La descrizione dettagliata della topologia dell'area di cui il router fa parte e i sommari di tutte le destinazioni presenti nel dominio di routing OSPF

d) La descrizione dettagliata della topologia dell'area di cui il router fa parte, la descrizione dettagliata dell'area backbone, e il sommario delle restanti destinazioni presenti nel dominio di routing OSPF

49. Nel protocollo OSPF a regime tutti i router hanno in memoria:

a) Lo stesso albero di percorsi ottimi

b) La base di dati descrivente l'area cui appartengono

c) La stessa base di dati che descrive l'intero AS

d) Un set di Distance Vector di tutti i router adiacenti

50. Un Area Border Router OSPF

a) Dispone di informazioni riassuntive sulle aree su cui si affaccia e le diffonde nelle aree; non conosce i dettagli di tali aree.

b) Conosce i dettagli della backbone area

c) Genera LSA di tipo 5 per descrivere destinazioni esterne al dominio di routing.

d) Inoltra, mediante il meccanismo del flooding, tutti gli LSA che riceve da un'area a tutte le altre su cui si affaccia

51. Un LSA Router Link del protocollo OSPF descrive:

a) Un link che connette l'advertising router con uno dei router ad esso adiacenti

b) Un riassunto delle reti raggiungibili

c) La lista dei router connessi in una LAN

d) Il valore corrente dei parametri (carico della CPU, carico sul link, uptime, etc.) relativi ad un link tra due router

52. Nel protocollo OSPF, gli LSA di tipo *Network Link* presenti nel Link State Database di un router contengono:

a) Le adiacenze di ogni router con le reti IP configurate sulle proprie interfacce

b) Le reti IP presenti nel dominio OSPF ma in aree differenti dall'area nella quale è situato il router

c) Le adiacenze con le reti di transito presenti nel dominio OSPF

d) Le adiacenze con le reti di transito presenti nell'area in esame

53. In OSPF, un pacchetto di "Database Description":

a) Viene utilizzato da due router adiacenti per scambiarsi le rispettive copie del database OSPF

b) Viene utilizzato da due router adiacenti per scambiarsi le rispettive copie della routing table

c) Permette ad un router che ha rilevato una nuova adiacenza con un altro router OSPF di conoscere gli LSA a lui mancanti

d) Permette ad un router appena acceso di conoscere gli LSA a lui mancanti

54. In OSPF, un pacchetto di "Database Description":
    a) Viene utilizzato durante la fase di "Neighbor Discovery"
    b) Viene utilizzato durante la fase di riallineamento delle adiacenze
    c) Viene sempre inviato cifrato per evitare problemi di sicurezza
    d) Viene sempre inviato cifrato per problemi di privacy

55. In OSPF, un pacchetto di "Link State Update":
    a) Viene utilizzato anche nella procedura di *Exchange* per lo scambio di tutti gli LSA posseduti dai router, e trasporta ogni LSA in forma completa
    b) Trasporta le informazioni principali relative ad un Link State Advertisement
    c) È utilizzato per aggiornare lo stato dell'adiacenza con un router vicino e trasporta solamente le informazioni relative a quel cambiamento
    d) Viene inviato per in condizioni di rete a regime, quando il transitorio è ormai esaurito

7.4 BGP

56. Il protocollo di routing BGP:
    a) Utilizza regole (policy) su informazioni aggiuntive a metriche di costo per identificare il percorso "migliore" per raggiungere una destinazione
    b) È utilizzato esclusivamente per scambi di informazioni tra router di autonomous system differenti
    c) È utilizzato esclusivamente per scambi di informazioni tra router dello stesso autonomous system
    d) È il protocollo che andrà a sostituire OSPF

57. La tecnica "Path Vector" impiegata dal BGP:
    a) Memorizza nei Path Vectors l'elenco degli Autonomous Systems da attraversare per raggiungere una data rete di destinazione
    b) Memorizza nei Path Vectors l'elenco di routers da attraversare per raggiungere una data rete di destinazione
    c) Memorizza nei Path Vectors il prossimo Autonomous System da attraversare per raggiungere una data rete di destinazione
    d) Memorizza nei Path Vectors il prossimo router da attraversare per raggiungere una data rete di destinazione

58. Nel protocollo di routing BGP:
    a) Le informazioni di topologia hanno sempre la precedenza sull'applicazione delle politiche di instradamento ("policy")
    b) L'applicazione delle politiche di instradamento ("policy") ha sempre la precedenza rispetto alle informazioni di topologia

c) Viene scelto sempre il percorso a costo inferiore verso ogni destinazione

d) Viene scelto sempre il percorso a costo inferiore verso ogni destinazione, a meno di limitazioni intrinseche al funzionamento del routing gerarchico

8 Algoritmi di routing multicast

59. L'algoritmo di instradamento Reverse Path Multicasting limita il traffico multicast:
    a) Non inoltrando il traffico multicast sulle reti
    b) Inoltrando il traffico multicast solo sulle reti dove sono presenti degli host ricevitori per quel gruppo multicast
    c) Non inoltrando il traffico multicast sulle reti "foglia"
    d) Non inoltrando il traffico multicast sulle reti "foglia" se su esse non sono presenti degli host ricevitori per quel gruppo multicast

60. Nell'algoritmo di instradamento Reverse Path Multicasting:
    a) Si possono verificare delle tempeste di multicast periodico sulle reti "foglia"
    b) Si possono verificare delle tempeste di multicast periodico sul backbone della rete, ma non sulle reti "foglia"
    c) Le reti "foglia" sono quelle che non hanno ricevitori per quel gruppo multicast
    d) Le reti "foglia" sono quelle che non vengono utilizzate da nessun router nel percorso verso i ricevitori di quel gruppo multicast

61. Se M rappresenta il numero di gruppi multicast attivi in un dominio di multicast basato sull'algoritmo link-state, e N rappresenta il numero di host attivi in ogni gruppo, il numero di alberi di distribuzione presenti all'interno della rete è:
    a) Uno
    b) N
    c) M
    d) N*M

62. Se M rappresenta il numero di gruppi multicast attivi in un dominio di multicast basato sull'algoritmo Core-Based Tree, e N rappresenta il numero di host attivi in ogni gruppo, il numero di alberi di distribuzione presenti all'interno della rete è:
    a) Uno
    b) N
    c) M
    d) N*M

9 Protocolli di routing multicast

63. Nell'ambito del routing multicast, il protocollo DVMRP:
    a) È di tipo Distance Vector e deve essere installato in reti con protocolli di routing unicast di tipo Distance Vector

b) È di tipo Path Vector ed è indipendente dal protocollo di routing unicast operante sulla rete

c) Si calcola i suoi Distance Vector, che possono differire da quelli calcolati dal protocollo di routing unicast

d) È in grado di gestire anche il routing unicast, e può tranquillamente essere l'unico protocollo di routing che opera sulla rete

64. Si consideri una rete non particolarmente estesa (es. un campus universitario), in cui sia prevista l'esistenza di numerosi gruppi multicast. Le statistiche dicono che in ogni area della rete è possibile trovare, in media, almeno un utente che sia interessato all'ascolto di ciascun gruppo multicast presente. Quale protocollo di routing sarebbe opportuno abilitare in uno scenario di questo tipo?
    a) PIM-SM (Sparse Mode)
    b) PIM-DM (Dense Mode)
    c) DVMRP (versione 1)
    d) MOSPF

10 Algoritmi e applicazioni peer-to-peer

65. In una DHT (Distributed Hash Table):
    a) Ogni nodo è posizionato in una ben precisa posizione della struttura logica dell'overlay
    b) Ogni nodo ha una posizione arbitraria dell'overlay, che può cambiare con il tempo
    c) Ogni nodo ha una posizione arbitraria dell'overlay, ma una volta inserito non si può spostare in un'altra posizione
    d) Ogni nodo fa capo ad un server centralizzato che rappresenta una sorta di "centro stella" dell'overlay

66. Una rete P2P non strutturata:
    a) È caratterizzata dal fatto che una ricerca per una risorsa (es. un file) presente nella rete ha sempre esito positivo
    b) È caratterizzata dal fatto che una ricerca per una risorsa (es. un file) presente nella rete potrebbe non avere esito positivo
    c) È basata sul concetto di Distributed Hash Table
    d) Rende difficoltosa la ricerca di risorse tramite wilcard (es. "*pippo*.txt*")

67. In una rete P2P strutturata:
    a) Le ricerche fatte su parole chiave (es. *pippo**) sono particolarmente ottimizzate
    b) Le operazioni di connessione/sconnessione di nodi alla rete non causano particolari problemi di funzionamento a livello globale
    c) Gli identificativi dei nodi e quelli delle chiavi appartengono sempre allo stesso spazio di valori
    d) Nessuna delle risposte precedenti

68. In una rete P2P non strutturata:

a) Si basa su un nodo centrale (opportunamente ridondato) per garantire il corretto funzionamento della rete

b) Le query di localizzazione di una risorsa vengono mediamente inviate a una piccola percentuale dei nodi dell'overlay

c) Le query di localizzazione di una risorsa vengono inviate al server centrale

d) La probabilità di trovare una risorsa è indipendente dalla sua "popolarità" (numero di nodi che dispongono della risorsa)

69. La rete P2P Bittorrent:

a) È progettata per permettere un meccanismo efficiente per il lookup delle risorse

b) Nella sua versione iniziale, rappresenta il tipico caso di rete P2P strutturata

c) È in grado di trasferire contemporaneamente più segmenti (*chunk*) della stessa risorsa

d) È in grado di funzionare correttamente senza l'ausilio di nessuna entità centralizzata

70. Si consideri una rete P2P Chord, in cui le chiavi sono lunghe 3 bit. I nodi attualmente connessi alla rete hanno ID 0, 1, 2, 5, 7. All'interno della rete è presente una risorsa la cui chiave è 4. Quale nodo è responsabile dell'indicizzazione della risorsa?

a) I nodi 2 e 5

b) Il nodo 0

c) Il nodo 5

d) Nessun nodo, in quanto il nodo 4 non è attualmente connesso alla rete

11 Packet filters

71. Il packet filter di tipo BPF:

a) Definisce una macchina virtuale decisamente potente, capace di effettuare elaborazioni arbitrarie sul pacchetto

b) Definisce una macchina virtuale limitata, nella quale alcune operazioni molto comuni non sono possibili

c) Definisce delle primitive estremamente efficienti per la composizione di filtri (es. Redundant Predicate Elimination)

d) È stato sostanzialmente rimpiazzato dal BPF+ nei sistemi operativi moderni

72. Il packet filter "PathFinder" è caratterizzato da:

a) Un'implementazione basata su JIT

b) Una virtual-machine register-based

c) Un modello di esecuzione basato sul concetto di cella per confrontare un campo con un set di valori

d) Una complessità lineare nel numero di filtri nel caso di esecuzione di filtri composti

73. Il concetto di "Virtual Machine" nel caso di packet filters:

a) È l'unico modo per garantire la safety del codice in esecuzione

b) È un modo semplice per garantire la safety del codice in esecuzione

c) È stato introdotto per rendere il codice portabile sulle varie piattaforme

d) Serve per garantire che del codice malevolo contenuto in un pacchetto di rete possa infettare l'host destinazione

74. In un packet filter, il tempo di update di un filtro:

a) È sempre molto importante

b) Non è un parametro importante

c) L'importanza o meno dipende dall'applicativo

d) È importante nell'analisi di flussi in tempo reale (*live*), mentre non lo è nelle analisi offline

75. In un packet filter di tipo CSPF:

a) Le prestazioni sono basse a causa in quanto il processamento di un pacchetto richiede obbligatoriamente un context-switch per il suo trasferimento da kernel a user-space

b) Le istruzioni del packet filter sono eseguite tramite uno strato software intermedio che funge da virtual machine per l'esecuzione

c) Il processamento utilizza un modello basato sul Control-Flow Graph

d) È molto semplice effettuare la composizione di filtri (es. `filtro1 AND filtro2`)

76. Su un sistema che utilizza un packet filter di tipo BPF (Berkeley Packet Filter) viene lanciato un analizzatore di rete configurato con il filtro "tcp and port 80". In questo contesto, quale componente è responsabile della traduzione del filtro in codice interpretabile dalla macchina virtuale?

a) L'analizzatore di rete

b) La libreria `libpcap`

c) Non è necessaria alcuna traduzione, in quanto la macchina virtuale *pcap* è in grado di interpretare direttamente l'espressione di "alto livello" del filtro

d) La situazione sopra esposta non può mai verificarsi, in quanto il packet filter BPF risiede a livello kernel del sistema operativo e pertanto non può ricevere comandi da un'applicazione residente in user space

77. Su un analizzatore di rete vengono configurati due filtri: "tcp and port 80" e "tcp and port 8080". Quale packet filter software permette di eseguire contemporaneamente questi filtri, ottenendo nel complesso prestazioni migliori rispetto alla loro esecuzione lineare:

a) CSPF

b) BPF

c) BPF+

d) Swift

78. In un sistema che implementa una tecnologia di "early demultiplexing":

a) La sequenza degli header contenuti in un pacchetto viene considerata come un'unica struttura dati, ed è processata in un unico step

b) La sequenza degli header contenuti in un pacchetto viene considerata come un set di N strutture dati annidate, ed è processata in N step distinti

c) L'elaborazione è caratterizzata da una alta flessibilità, data la modularità dell'approccio

d) L'elaborazione è tipicamente sequenziale: il livello N deve attendere che il livello N-1 termini prima di poter elaborare il pacchetto

12 Implementazioni software di packet filters

79. In un packet filter realizzato per un sistema operativo standard, in software, i costi maggiori:
    a) Sono imputabili alla parte di filtraggio del pacchetto
    b) Sono imputabili al costo delle copie del pacchetto dalla memoria gestita dal NIC driver a quella gestita dal kernel, e poi da qui a user-level
    c) Sono imputabili a funzionalità accessorie quali il timestamping
    d) Sono imputabili alle operazioni svolte dal NIC e dal sistema operativo

80. Il fenomeno del Livelock:
    a) È un blocco (crash) dell'intero sistema
    b) Fa sì che il pacchetto non riesca ad essere trasferito dalla NIC al sistema operativo
    c) Fa sì che il sistema funzioni al 100% del carico, ma il pacchetto non riesca ad essere elaborato dall'applicazione
    d) È un fenomeno che compare nel momento in cui gran parte dell'elaborazione viene fatta in hardware su una scheda dedicata

81. Quale caratteristica NON è tipica del componente software libpcap:
    a) Lavora in user space
    b) È in grado di interagire direttamente con il driver della scheda di rete, se quest'ultimo supporta questa funzionalità
    c) Permette di aumentare le prestazioni offrendo meccanismi di batch-processing dei pacchetti
    d) Controlla il comportamento del BPF (BSD Packet Filter) iniettando le istruzioni che verranno eseguite dalla macchina virtuale

82. In un packet filter software in grado di eseguire il codice generato con la tecnologia "JIT" (Just-In-Time), le istruzioni eseguite dal filtro sono:
    a) Istruzioni di alto livello, eseguite in un ambiente virtualizzato per garantire la massima sicurezza possibile
    b) Istruzioni native per la piattaforma sulla quale è caricato il sistema, per aumentare le prestazioni
    c) Istruzioni di alto livello o native a seconda della modalità con la quale viene configurato (per privilegiare sicurezza o prestazioni)
    d) Il packet filter non esegue istruzioni, in quanto la tecnologia JIT si riferisce alla capacità della scheda di rete di trasferire immediatamente i dati al packet filter stesso in modo da diminuire la latenza.

83. Durante la cattura di pacchetti effettuata su un host connesso ad una rete ad alta velocità, può verificarsi il fenomeno del *Livelock*, in cui la maggior parte del tempo di CPU viene speso:
    a) Dalla trasferimento dei dati dalla scheda di rete (NIC) ai buffer a livello kernel gestiti dal sistema operativo

b) All'interno del NIC driver, che, operando ad un livello di privilegio molto alto, si trova a dover servire in continuazione nuovi interrupt provenienti dall'hardware

c) Dal capture driver, che deve filtrare i pacchetti

d) Dall'applicazione che ha iniziato la cattura, che non riesce a reggere il carico di processamento in ingresso

84. L'implementazione di un meccanismo di packet filtering disgiunto dallo stack di rete:

a) Permette alla scheda di rete in esame di interagire con il sistema operativo normalmente, ma richiede l'implementazione di un driver dedicato

b) Sfrutta una tecnologia basata sul principio dell' "Interrupt mitigation", che permette di diminuire la mole di interrupt inviati dalla scheda al sistema operativo

c) Non consente di raggiungere prestazioni particolarmente buone a causa della necessità di duplicare, nel driver della scheda di rete, funzioni e strutture già presenti nel sistema operativo

d) Permette alla scheda di rete in esame di gestire in maniera estremamente efficace la cattura di traffico, al prezzo di non essere più pilotabile dal sistema operativo

13 Bloom filters

85. Un Bloom Filter:

a) Ha un tempo di update (es. aggiunta di un nuovo item da filtrare) molto elevato

b) Permette la cancellazione di un elemento in un tempo estremamente ridotto

c) È adatto nel caso in cui si cerchi la risposta alla domanda "*l'elemento E appartiene ad un certo set S?*"

d) È adatto nel caso in cui si cerchi la risposta alla domanda "*l'elemento E non appartiene ad un certo set S?*"

86. Un Bloom Filter:

a) Garantisce una risposta esente da errori

b) Può avere falsi positivi

c) Può avere falsi negativi

d) Può avere sia falsi positivi che falsi negativi

87. Si consideri un set di indirizzi IP (`192.168.0.1`, `192.168.0.2`, `192.168.0.3`). Attraverso un Bloom Filter, si esegue un lookup dell'indirizzo IP `192.168.0.4`, e la funzione ritorna `TRUE`. Quale conclusione si può dedurre osservando questo risultato?

a) La funzione di lookup dice con certezza che l'indirizzo IP non appartiene al set

b) La funzione di lookup dice con certezza che l'indirizzo IP appartiene al set

c) La funzione di lookup dice che l'indirizzo IP potrebbe appartenere al set, ma è necessario eseguire controlli aggiuntivi (e indipendenti dal Bloom Filter) per averne la certezza

d) L'implementazione del Bloom Filter non è corretta, in quanto la funzione di lookup deve restituire FALSE in questo specifico caso

88. Un Bloom Filter:

a) È particolarmente efficiente quando la cardinalità del set di valori da testare è dell'ordine del numero di valori ammissibile per quel test

b) È solitamente basato sull'utilizzo di una sola funzione di hash per il mapping dei valori nella struttura interna del filtro

c) Non è consigliabile quando le specifiche di progetto impongono l'utilizzo di un ammontare di memoria limitato

d) Permette la rimozione di un valore da un insieme solamente nella sua implementazione con i contatori (Counting Bloom Filter)

14 Lookup e classificazione ad alte prestazioni

89. Si supponga di voler realizzare uno switch Ethernet con una memoria in grado di implementare una tecnica di Exact Lookup per effettuare il forwarding delle trame a livello 2. La dimensione della memoria sarà ragionevolmente pari a:

    a) 256 Kilobytes

    b) 256 Megabytes

    c) 256 Gigabytes

    d) 256 Terabytes

90. Si supponga di voler realizzare uno switch Ethernet con una memoria di tipo CAM (Content Addressable Memory) per effettuare il forwarding delle trame a livello 2. La dimensione della memoria sarà ragionevolmente pari a:

    a) 64 entries

    b) 64K entries

    c) 64M entries

    d) 64G entries

91. Nell'ambito delle funzioni di lookup utilizzate negli apparati di rete, le memorie TCAM (Ternary CAM) possono essere utilizzate:

    a) Per effettuare il forwarding a livello 2 (switch)

    b) Per effettuare il forwarding a livello 3 (router)

    c) Negli apparati che presentano problemi di eccessivo consumo energetico

    d) Negli apparati a basso costo

92. Nel campo del networking, le memorie CAM sono particolarmente adatte per:

    a) Effettuare il lookup nella tabella di instradamento di livello 2 (*filtering database*)

    b) Effettuare il lookup nella routing table

    c) Mantenere il Link State Database in un router OSPF

    d) Realizzare il modulo di Content Inspection in un firewall

15 Classificazione di traffico

93. Un moderno sistema di classificazione di traffico "payload-based" ("Deep Packet Inspection") a livello applicativo:
    a) Richiede necessariamente il riassemblaggio delle sessioni
    b) Può essere implementato in modalità completamente stateless
    c) Può essere implementato in modalità "packet-based", con un sistema aggiuntivo di session-tracking
    d) È decisamente complesso in quanto richiede l'emulazione della macchina a stati del protocollo rilevato (es. HTTP)

94. Un sistema per la classificazione di traffico applicativo basato su tecnologia Deep Packet Inspection ("payload-based"):
    a) Può classificare la maggior parte del traffico, anche se questo è cifrato
    b) Non ritorna mai risultati che sono "falsi positivi"
    c) Necessita delle "signature" relative ai protocolli che si intende classificare
    d) Gestisce facilmente i casi di tunnelling di un protocollo in un altro, ma non gestisce i protocolli criptati

95. Un classificatore di traffico di tipo statistico:
    a) Prevede l'inserimento manuale delle signature dei protocolli applicativi che si intendono classificare
    b) Può essere ragionevolmente efficace anche con protocolli criptati e/o tunnellati
    c) Necessita di esaminare i primi bytes dell'intestazione TCP/IP
    d) Sfrutta come principio di base l'idea di associare ad un set di porte TCP/UDP un determinato insieme di servizi

16 Architettura degli apparati di rete

96. Il concetto di "Slow path" nei routers:
    a) È caratteristico degli apparati di prima generazione, realizzati interamente in software
    b) Negli apparati che prevedono gran parte dl processing fatto in hardware, individua il percorso dei pacchetti trattati in software dalla CPU general-purpose dell'apparato
    c) Individua i pacchetti di management, che devono essere elaborati localmente dalla CPU del router
    d) È un concetto non più presente negli apparati di nuova generazione, dove tutti i pacchetti sono elaborati in hardware

97. In un router di prima generazione, il collo di bottiglia è:
    a) Nei circuiti ASICs presenti sulle linecard, che non sono particolarmente veloci
    b) Nel fatto per cui l'elaborazione sulle varie linecard viene fatto da CPU non ottimizzate per il packet processing
    c) Nella switching fabric, di tipo bloccante

d) Nell'architettura generale, simile a quella del PC, e nel processamento software

98. Considerando l'offerta commerciale di un generico costruttore di apparati di livello 3 (router):
    a) Gli apparati delle serie *high-end* offrono tipicamente una configurazione fissa
    b) La commutazione di pacchetti a livello 4-7 è effettuata in hardware
    c) Tra le varie serie di apparati vi sono nette differenze a livello si features software supportate
    d) Gli apparati condividono normalmente la gran parte delle feature, anche se differiscono nelle prestazioni garantite delle stesse

99. Nel progetto dell'architettura di un router è stato deciso l'utilizzo di una switching fabric a "basse" prestazioni (*speedup* unitario). Quali dei seguenti modelli di buffering NON è possibile adottare, considerando che il router avrà N linecard:
    a) Output queuing
    b) Input queuing
    c) Virtual output queuing
    d) Buffered fabric

100. In un router basato su una architettura di seconda generazione:
    a) Ogni pacchetto transita tipicamente due volte sul bus
    b) Ogni pacchetto transita tipicamente una volta sulla switching fabric
    c) Ogni pacchetto transita tipicamente una volta sul bus
    d) Ogni pacchetto transita direttamente dalla linecard sorgente a quella di destinazione

101. In un router dotato di linecard intelligenti (es. architettura di seconda generazione):
    a) Le routing table presenti sulle varie linecard sono un duplicato della routing table contenuta nella memoria centrale
    b) I pacchetti vengono tipicamente processati dall'unità di elaborazione centrale
    c) La memoria presente sulle linecard è sempre di tipo CAM (Content Addressable Memory)
    d) Le funzionalità di forwarding sono facilmente aggiornabili da una nuova release software del sistema operativo

17 Processori per elaborazione di traffico

102. Un processore di tipo sistolico:
    a) È utilizzabile solo se il codice da eseguire non ha branch e loop
    b) È utilizzabile solo se il codice da eseguire non ha loop
    c) È utilizzabile solo se il codice da eseguire ha loop facilmente "srotolabili"
    d) Ha le caratteristiche di un processore general-purpose, ma gestisce il parallelismo in maniera estremamente efficiente

103. I processori per packet processing di tipo "massive multicore":
    a) Non saranno mai la soluzione al problema del packet processing a livello applicativo perchè non gestiscono bene i cicli ("loop") nel codice

b) Sono molto facili da programmare perché gestiscono il parallelismo in maniera automatica

c) Sono molto facili da programmare perché, avendo lo stesso set di istruzioni delle CPU general-purpose, consentono il riutilizzo degli ambienti di sviluppo disponibili per le CPU classiche (es. `gcc`) senza alcuna modifica

d) Sono molto difficili da programmare in maniera efficiente per il problema di gestire la concorrenza nei programmi applicativi

104. Un router nel quale i componenti principali di processamento sono fatti in tecnologia ASIC:

a) Consente di aggiornare facilmente le sue funzionalità in futuro

b) Ha dei tempi di progettazione relativamente brevi

c) Permette il riutilizzo del software fatto per altre piattaforme

d) È normalmente estremamente performante

105. Un processore per packet processing di tipo "massive multicore":

a) Normalmente definisce un set di istruzioni dedicato per il processamento di pacchetti

b) Utilizza un modello di processamento control-flow-based

c) Utilizza un modello di processamento data-flow-based

d) Tipicamente non contiene moduli hardware dedicati per eseguire particolari funzionalità comuni nel campo del networking

106. Uno dei vantaggi derivanti dall'utilizzo di processori RISC per funzionalità di packet processing è:

a) La possibilità di riutilizzare tool di sviluppo già esistenti e testati

b) L'alta capacità di I/O

c) L'efficienza che si ottiene durante l'esecuzione di programmi di lunga durata, come i tipici algoritmi di elaborazione pacchetti

d) L'estrema velocità di questi processori anche quando vengono utilizzati in modalità single-core

107. Si consideri un processore sistolico avente una pipeline di 100 PE (Processing Engine):

a) Il throughput dipende dal traffico in input (più corti sono i pacchetti, maggiore è il throughput)

b) Il throughput del processore è dipendente dalla lunghezza della pipeline

c) Permette l'esecuzione di programmi in cui il numero di istruzioni è multiplo di 100

d) Permette l'esecuzione di programmi con al massimo 100 istruzioni