Tecnologia e Servizi di Rete

Nell'algoritmo del secchiello a gettoni:

A. La capacità del secchiello è legata alla velocità media sul lungo periodo.

B. La capacità del secchiello è legata al massimo burst size.

C. La capacità del secchiello ha relazione diretta con la banda.

D. Serve per implementare il weighted fair queuing.

Le così dette soluzioni VPN (virtual private network) di accesso o virtual dial-up VPN

attualmente più diffuse sono basate su:

A. Connessioni dial-up.

B. Tunnelling attraverso una rete IP.

C. Utilizzo di un'infrastruttura di cablaggio esistente per fornire servizi di accesso a larga

banda

D. Nuovi protocolli di linea (livello data-link).

Le soluzioni per la realizzazione di VPN (virtual private network) di livello 3 attraverso una

dorsale MPLS sono caratterizzate da

A. Livelli particolarmente alti di sicurezza.

B. Elevata scalabilità

C. A differenza di tutte le altre soluzioni proposte, non richiedono l'utilizzo di funzionalità di

NAT (network address translator) quando si abbia a che fare con indirizzi privati.

D. La fornitura di un servizio a qualità garantita al traffico che attraversa la VPN.

In un pacchetto che viaggia su un tunnel GRE quante intestazioni possono essere presenti?

A. Una sola, altrimenti l'indirizzamento è ambiguo.

B. Due intestazioni, ma quella interna può solo contenere indirizzi privati.

C. Due intestazioni, senza particolari limitazioni.

D. Due intestazioni, ma quella esterna può solo contenere indirizzi privati.

In un pacchetto che viaggia su una rete MPLS, è possibile avere più label contemporaneamente?

A. No, non è previsto.

B. Sì, ma non più di 2.

C. Sì, ma non più di 20.

D. Sì, ma solo nei tunnel MPLS usati per le VPN.

Quale è la funzione dello “scope” associato agli indirizzi IPv6?

A. Serve a risolvere, in casi particolari, l'ambiguità riguardo il mittente.

B. Non esiste uno scope associato agli indirizzi IPv6.

C. Serve per poter utilizzare gli indirizzi globali.

D. Serve per poter utilizzare gli indirizzi anycast.

L'autoconfigurazione stateless di IPv6 presenta problemi di riservatezza?

A. Non vi sono particolari problemi.

B. Non permette la cifratura del carico.

C. E' possibile individuare la stessa interfaccia, se si collega a internet da vari provider.

D. Non permette l'uso delle intestazioni di sicurezza (tipo IPsec).

In che modo MPLS può essere utilizzato per realizzare una VPN?

A. Per realizzare una VPN di accesso.

B. MPLS non può essere usato per realizzare VPN.

C. Può fornire tutto il meccanismo di instradamento in reti overlay o dei collegamenti punto-a-punto in reti peer.

D. Può fornire collegamenti punto-a-punto in reti overlay o tutto il meccanismo di instradamento in reti peer.

L'architettura MPLS (multi-protocol label switching) è caratterizzato da

A. Un diverso meccanismo (rispetto all'IP puro) per decidere l'interfaccia di uscita verso cui un pacchetto debba essere inoltrato.

B. Un supporto particolarmente evoluto per fornire servizi a qualità garantita.

C. Protocolli di routing particolarmente veloci ad aggiornare le tabelle di routing in seguito

a cambiamenti topologici in modo da recuperare velocemente i guasti.

D. Terminali di rete intelligenti in grado di personalizzare i servizi ricevuti dalla rete.

Il protocollo PPTP viene utilizzato di solito per:

A. Permettere di creare un tunnel in una VPN di accesso.

B. Permettere di creare un tunnel in una VPN site-to-site di tipo overlay.

C. Permettere di creare un tunnel in una VPN site-to-site di tipo peer.

D. Permettere di creare un tunnel in una VPN di livello 4.

DiffServ si differenzia da IntServ perché:

A. DiffServ tende a fornire una garanzia su QoS che IntServ non dà.

B. DiffServ introduce nuovi protocolli per permettere la prenotazione di risorse allo scopo di ottenere una data QoS.

C. IntServ tende a fornire una garanzia su QoS che DiffServ non dà.

D. DiffServ tende a garantire un tempo massimo di attraversamento, mentre IntServ tende a

fornire una banda minima garantita.

Qual è l'uso dei meccanismi di policing?

A. Servono all'utente per concordare con il fornitore il livello di QoS da ottenere.

B. Servono al fornitore di servizi per verificare che il traffico immesso dal cliente sia conforme agli accordi presi.

C. Servono all'utente per verificare che il traffico in arrivo dal fornitore sia conforme agli accordi presi.

D. Sono usati nei vari router per garantire un tempo massimo di attraversamento per ciascuno di essi.

A differenza della versione 4 dell'IP, la versione 6:

A. Non ha intestazione di lunghezza variabile.

B. Non permette di scoprire l'indirizzo MAC di un'altra stazione, conoscendone l'indirizzo

IP.

C. Non ha un equivalente del TTL (time-to-live).

D. Non permette l'uso di IPsec.

Nel meccanismo del secchiello a gettoni si riesce a controllare:

A. Il tempo di attraversamento massimo di un router.

B. La gestione interna delle code con WFQ.

C. La velocità minima di immissione dei dati.

D. Il burst size massimo e la velocità media di immissione dei dati.

Gli LSP (label switched path) nell’architettura MPLS (multi-protocol label switching)

A. Sono ottenuti riservando risorse nei nodi di rete in modo da garantire opportuna qualità del servizio alle applicazioni che li hanno creati.

B. Costituiscono il percorso più breve verso una destinazione.

C. Vengono creati (set up) dalle applicazioni per il trasporto di pacchetti appartenenti ad una classe di equivalenza di inoltro (forwarding equivalence class, FEC).

D. Vengono creati dai nodi di rete che si accordano sulle etichette da utilizzare per i pacchetti appartenenti ad una classe di equivalenza di inoltro (forwarding equivalence class,

FEC).

Le soluzioni di VPN (virtual private network) di livello 3 attraverso una dorsale MPLS sono

caratterizzate da

A. Livelli particolarmente alti di sicurezza grazie all'utilizzo di tecniche crittografiche.

B. Buon livello di automatizzazione e integrazione tra la dorsale pubblica e le reti private.

C. Meccanismi di tunneling di livello 3, ovvero all'interno di pacchetti IP.

D. Gestione diretta da parte dell'utente, senza intervento dell'operatore.

Il protocollo GRE serve per:

A. Incapsulare i pacchetti in altre intestazioni IP, in modo da poterle inviare su un tunnel.

B. Garantire la riservatezza delle comunicazioni.

C. Garantire l'autenticità dei pacchetti.

D. Riservare della banda per la comunicazione.

La caratteristica di una VPN di accesso centralizzata è che

A. Il traffico non diretto alla VPN viene fatto passare comunque attraverso il VPN gateway.

B. L'autenticazione dell'utente per l'accesso alla VPN viene delegato all'ISP.

C. Il traffico non diretto alla VPN non è costretto a passare attraverso il VPN gateway.

D. L'autenticazione dell'utente non viene fatta dal VPN gateway.

Nel protocollo IPv6:

A. I protocolli di routing (ad esempio il formato dei pacchetti) non cambiano rispetto ad IPv4.

B. Il protocollo ARP viene inglobato in ICMPv6, ma mantiene esattamente lo schema di funzionamento (richiesta broadcast, risposta unicast) precedente.

C. Esiste la possibilità, per una stazione su un segmento di rete, di autoconfigurarsi attraverso l'ascolto di messaggi di Router Advertisement.

D. Come IPv4, IPv6 non prevede meccanismi di riconfigurazione dei router.

Nel IPv6 cosa sparisce dalle intestazioni, rispetto a IPv4?

A. Il tempo di vita del pacchetto.

B. Gli indirizzi mittente e destinatario.

C. L'indicazione su quale sia l'intestazione successiva.

D. Il checksum dell'intestazione.

Lo schema di indirizzamento IPv6:

A. Prevede esclusivamente indirizzi assegnati in modo univoco da un ente preposto.

B. Prevede che ogni entità (es. azienda) si faccia assegnare globalmente un insieme di indirizzi, che diventano di sua proprietà a tempo illimitato.

C. Prevede che i primi 64 bit di un indirizzo siano normalmente identificati come il prefisso di rete, almeno sulle LAN.

D. Non prevede l'esistenza di indirizzi di multicast.

Gli indirizzi link-local

A. Sono validi all'interno di una organizzazione che li può utilizzare per assegnare indirizzi alle macchine nelle varie sottoreti della propria intranet (sono gli omologhi degli indirizzi privati di IPv4).

B. Non possono essere assegnati ai router.

C. Sono normalmente costruiti automaticamente dalla stazione a partire dall'indirizzo MAC della propria scheda, a cui si pre-pende un prefisso predefinito.

D. Vengono utilizzati per identificare macchine che svolgono un certo servizio (ad esempio

server DNS).

Per realizzare una VPN usando MPLS, al livello 3 secondo il modello peer, è possibile:

A. Utilizzare una versione opportunamente modificata del BGP.

B. Utilizzare una versione opportunamente modificata del TCP.

C. Utilizzare una versione opportunamente modificata del RIP.

D. Utilizzare una versione opportunamente modificata del RTP.

Gli algoritmi di scheduling vengono utilizzati:

A. Nei router di accesso, per assicurarsi che il traffico generato da un utente sia conforme al profilo di traffico contrattato con il proprio service provider.

B. Nei firewall, per ritardare i pacchetti che entrano in una rete aziendale provenendo dalla rete Internet con lo scopo di impedire alcuni tipi di attacchi alla sicurezza.

C. Nei router, per decidere quale sia l'ordine con cui debbano essere trasmessi i pacchetti in attesa ad una interfaccia.

D. Nei router, per schedulare opportunamente l'elenco dei comandi di configurazione impartiti dall'utente in modo da minimizzare il disservizio causato dal tempo necessario per l'applicazione delle modifiche.

Gli LSP (label switched path) nell'architettura MPLS (multi-protocol label switching)

A. Rappresentano percorsi alternativi mantenuti nella tabella di un router per l'inoltro di pacchetti verso una destinazione.

B. Vengono scambiati dai router per costruire una mappa della rete.

C. Costituiscono il percorso più breve verso una destinazione.

D. Vengono creati (set up) per il trasporto di pacchetti appartenenti ad una classe di equivalenza di inoltro (forwarding equivalence class, FEC).

Il protocollo GRE ha lo scopo di:

A. Proteggere i pacchetti contro le intercettazioni.

B. Gestire l'incapsulamento di pacchetti da trasportare attraverso un tunnel.

C. Autenticare il mittente dei pacchetti.

D. Verificare l'integrità dei pacchetti in arrivo.

L'autoconfigurazione stateless in IPv6 richiede:

A. Un server DHCPv6 (Dinamic Host Configuration Protocol version 6).

B. Un server presente sulla rete locale.

C. Un server presente sulla rete aziendale (intranet).

D. È possibile anche se non si è in presenza di server o router.

In quale situazione è possibile che un pacchetto abbia due intestazioni IP?

A. Il pacchetto ha attraversato un firewall in ingresso.

B. Il pacchetto è nella rete pubblica, dopo aver attraversato in uscita un NAT.

C. Il pacchetto è nella rete pubblica, dopo aver attraversato in uscita un firewall.

D. Il pacchetto è nella rete pubblica in transito su un tunnel IP che collega due segmenti di una VPN basata su IP.

In una stazione utente collegata ad una VPN con accesso centralizzato, i messaggi diretti a stazioni esterne alla VPN passano attraverso:

A. Il sito della VPN a cui la macchina utente è collegata.

B. Non è possibile raggiungere stazioni esterne alla VPN.

C. Un router specializzato per questi pacchetti.

D. Vengono inviati direttamente dalla stazione utente al destinatario esterno.

A differenza della versione 4 dell'IP, la versione 6:

A. Non ha una versione dell'ICMP associata.

B. Non permette di scoprire l'indirizzo MAC di un'altra stazione, conoscendone l'indirizzo IP.

C. Non ha indirizzi broadcast.

D. Non ha un equivalente del campo TTL (time-to-live).

Utilizzando l'algoritmo del secchiello a gettoni (o secchio bucato) di capacità B token e velocità di riempimento r token/s si riesce a controllare:

A. Che il tempo di attraversamento non superi rB secondi.

B. Il numero di pacchetti al secondo immessi non superi r, ed il massimo burst non superi B.

C. Il numero di pacchetti al secondo immessi non superi B, ed il massimo burst non superi r.

D. Il jitter non superi B/r.

Lo standard IPsec viene utilizzato nelle VPN (virtual private network) per

A. Verificare le informazioni di autenticazione fornite da utenti remoti tramite uno scambio di informazione con un server di autenticazione.

B. Consentire l'invio di informazioni di autenticazione (per esempio username e password o tramite meccanismi di sfida) da parte degli utenti di una VPN di accesso.

C. La realizzazione di tunnel attraverso una rete IP pubblica sul tramite i quali sia possibile trasportare pacchetti IP provenienti da o destinati ad una rete privata indipendentemente dal piano di indirizzamento utilizzato su tale rete privata (purchè i piani di indirizzamento delle due reti private non siano sovrapposti).

D. La creazione automatica di collegamenti cifrati tra le sedi di un'azienda attraverso una rete pubblica, sulla quale la comunicazione è quindi intrinsecamente non sicura.

L'architettura DiffServ è caratterizzata da:

A. Un meccanismo per separare il traffico in classi ognuna delle quali può ricevere un servizio specifico in ogni nodo attraversato

B. Protocolli di segnalazione sofisticati per la prenotazione delle risorse

C. La capacità di fornire servizio a qualità garantita alle applicazioni o flussi che nefacciano esplicita richiesta alla rete

D. Protocolli di routing sofisticati per scegliere il percorso di ogni singolo pacchetto in modo da assicurare che esso riceva il servizio di cui necessita

In che modo si può usare L2TP per realizzare una VPN:

Per realizzare una VPN d'accesso.

Quali operazioni possono essere effettuate sui label in un router MPLS:

Modificare, aggiungere, eliminare il label più esterno.

I meccanismi di transizione in IPV6:

Su meccanismi di tunnel più o meno sofisticati (IPV6 in IPV4)

L'importanza di MPLS (multi-protocol label switching) nelle reti odierne e future deriva dalla possibilità di

A. Trasportare efficientemente pacchetti IP sulle reti ATM

B. Collegare ad alta velocità i server ai loro dischi

C. Realizzare facilmente ed efficacemente ingegnerizzazione del traffico (traffic engineering)

D. Realizzare apparati in grado di operare senza bisogno di configurazione

Le reti ottiche si basano sull'utilizzo di

A. Collegamenti in fibra ottica tra commutatori di pacchetto ad elevate prestazioni

B. Router IP in grado di inoltrare i pacchetti in base al loro indirizzo destinazione realizzando il look-up nella tabella di routing con tecniche ottiche.

C. Apparati in grado di commutare un segnale elettromagnetico ad una certa frequenza portante nel campo dell'ottica da una porta di ingresso ad una porta di uscita

Le reti private virtuali (virtual private network, VPN) vengono utilizzate per

A. Trasportare traffico privato su una infrastruttura condivisa ricreando le stesse condizioni che si avrebbero tramite l'utilizzo di una infrastruttura privata

B. Suddividere una rete locale aziendale in una serie di sottoreti separate per le diverse funzioni aziendali (vendite, acquisti, engineering, marketing)

C. Partizionare una rete privata (per esempio quella di un'azienda madre con un certo numero di aziende sussidiare) in varie reti virtualmente separate

Le soluzioni di VPN (virtual private network) basate su SSL (secure socket layer) consentono

A. Di distribuire in modo sicuro su diversi server applicazioni basate sul web

B. Di creare cluster di server privati

C. Ad un'azienda di rendere disponibili in modo sicuro ai propri dipendenti fuori sede specifiche applicazioni aziendali.

D. La realizzazione di un backbone sul quale un fornitore di servizi (service provider) può facilmente ed efficientemente fornire servizi di connettività ai suoi clienti

Il protocollo IPv6 prevede che l'intestazione dei pacchetti IP:

A. Sia sempre autenticata tramite oppurtuni algoritmi di cifratura per aumentare la sicurezza delle transmissioni

B. Sia di dimensioni inferiori rispetto a quella dei pacchetti IPv4 in modo da aumentare l'efficienza nell'uso della banda trasmissiva riducendo l'overhead protocollare

C. Sia costituita solo da campi di lunghezza fissa che portano informazioni necessarie in ogni pacchetto

D. Comprenda alcuni campi, prima disponibili solamente come opzioni di IPv4, per funzionalità che si sono rivelate di largo uso nel corso del tempo.

L'inoltro di pacchetti Ipv6 su una LAN:

• Non fa uso di meccanismi di neighbor discovery in quanto esiste una regola per mappare un qualunque indirizzo IPv6 in un indirizzo MAC.

• Non fa uso di meccanismo di neighbor discovery per quanto riguarda l'inoltro di pacchetti IPv6 multicast e broadcast in quanto esiste una regola per mappare questi indirizzi IPv6 in un indirizzo MAC.

• Fa uso di meccanismi di neighbor discovery per tutte le tipologie di indirizzi IPv6.

• Non fa uso di meccanismi di neighbor discovery per quanto riguarda l'inoltro di pacchetti IPv6 multicast in quanto esiste una regola per mappare questi indirizzi IPv6 in un indirizzo MAC.

Un host IPv6 al reboot, acquisirà il seguente indirizzo:

• Non è possibile sapere con precisione l'indirizzo stesso, dal momento che l'indirizzo IPv6 viene ogni volta rigenerato con un numero casuale per quanto riguarda la parte riservata all'Interface ID.

• Un indirizzo FE80::/32

• Per quanto riguarda l'indirizzo link-local, assumera' lo stesso indirizzo IPv6 che possedeva prima del reboot.

• L'indirizzo dipende interamente dalla configurazione che acquisirà dal suo default router.

Un indirizzo link-local:

• E' utilizzabile per permettere la comunicazione tra stazioni su link locali (es. una LAN) in mancanza di altri indirizzi IPv6.

• Serve per collegare fisicamente due stazioni su un link locale.

• E' l'indirizzo utilizzato dalle stazioni su una LAN per scambiarsi i dati.

• E' utilizzato in tutte le comunicazioni tra stazioni locali.

Gli indirizzi Ipv6

• Permettono la comunicazione di stazioni IPv6 con stazioni IPv4 senza nessun particolare meccanismo aggiuntivo.

• Mantengono la stessa suddivisione flessibile tra una parte network e una parte host già presente in IPv4.

• Sono rigidamente partizionati in una parte network, subnetwork e host.

• Sono rigidamente partizionati in una parte network e una parte host.

La combinazione di meccanismi di secchiello dei token (o secchio bucato) e Weighted Fair Queueing (WFQ) serve a garantire:

• Un tempo di attraversamento massimo di un router.

• Un tempo di attraversamento massimo di un NAT.

• Una banda massima per ogni flusso di pacchetti.

• Un burst massimo di pacchetti consecutivi, per ciascun flusso.

What is the typical role of IPSec in VPNs?

A. To distribute in a secure way the key required by other protocols to open a tunnel

B. To allow the transmission of authentication information (e.g. username and password) by users of access VPN

C. To open a managed secure tunnel across the public internet

D. To verify the user identity to allow other protocols to open tunnels only with authorized parties.

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

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

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

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

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

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

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

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.

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")

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

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 attraversare per raggiungere quella destinazione

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

E’ possibile l'instaurazione di un loop in una rete che utilizza un routing di tipo Link State?

a) Si

b) No, perché ogni router ha una visione completa della topologia della rete

c) No, perché gli aggiornamenti del Link State vengono inviati in flooding

d) No, perché viene usato un Hold-Down timer

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)

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

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

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

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

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

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

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

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)

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

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

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

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

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

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

Il protocollo di routing BGP:

a) Utilizza regole (policy) su informazioni aggiuntive a metriche di costo per identificare il “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

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

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