Domande frequenti sui router

Obiettivo

Questo documento ha lo scopo di rispondere a domande frequenti sulle funzionalità e le funzionalità di un router Cisco, nonché su come e quando utilizzarle. Se siete interessati al contenuto video, consultate la nostra playlist video facendo clic qui.

Dispositivi interessati

- Serie RV100
- Serie RV200
- Serie RV300

Sommario

1. Che cosa sono le regole di accesso?

Le regole di controllo di accesso sono regole che impongono l'invio di traffico specifico da e verso determinati utenti di una rete. È possibile configurare le regole di accesso in modo che siano sempre attive o basate su una pianificazione definita. Una regola di accesso può essere configurata su un router o uno switch, ma viene configurata in base a vari criteri in modo da consentire o negare l'accesso ad alcune o a tutte le risorse della rete.

2. Quali sono le opzioni 66, 67 e 150 per il server TFTP?

Un server TFTP consente a un amministratore di memorizzare, recuperare e scaricare i file di configurazione dei dispositivi su una rete. Un server DHCP (Dynamic Host Configuration Protocol) concede in lease e distribuisce gli indirizzi IP ai dispositivi della rete. Quando un dispositivo viene avviato e un indirizzo IPv4 o IPv6 e un indirizzo IP del server TFTP non sono preconfigurati, il dispositivo invierà una richiesta al server DHCP con le opzioni 66, 67 e 150. Queste opzioni sono richieste al server DHCP per ottenere informazioni sul server TFTP.

- L'opzione DHCP 150 è proprietaria di Cisco. Fornisce gli indirizzi IP in un elenco di server TFTP. L'equivalente standard IEEE (Institute of Electrical and Electronics Engineers) è l'opzione 66.
- L'opzione DHCP 66 fornisce l'indirizzo IP o il nome host di un singolo server TFTP.
- L'opzione DHCP 67 fornisce il nome del file di avvio per il server TFTP.

3. Quali sono le differenze tra l'esecuzione in modalità router e in modalità gateway?

Il router può funzionare in due modalità, la modalità router e la modalità gateway. La modalità router è la modalità operativa che disabilita Network Address Translation (NAT) sul dispositivo e viene utilizzata per connettere più router e più reti. Questa funzionalità è ideale per gli ambienti di rete WAN.

La modalità gateway è la modalità consigliata se il router ospita una connessione di rete direttamente a Internet. NAT è in esecuzione quando la modalità gateway è abilitata, ossia accetta un singolo indirizzo IP WAN e ha un intero blocco di indirizzi IP LAN.

4. Che cosa sono i registri di sistema?

I registri di sistema (Syslog) sono record di eventi di rete. In caso di malfunzionamento del sistema, è possibile recuperare i registri per diagnosticare il problema. I registri sono strumenti importanti che vengono utilizzati per comprendere il funzionamento di una rete per eseguire il sistema senza problemi e prevenire errori. Sono utili per la gestione della rete, la risoluzione dei problemi e il monitoraggio.

5. Che cosa sono le modalità DHCP?

Il protocollo DHCP (Dynamic Host Configuration Protocol) può funzionare in due modalità: Server DHCP e inoltro DHCP. Un server DHCP assegna automaticamente gli indirizzi IP disponibili a un client o host DHCP della rete. Il server DHCP e il client DHCP devono essere connessi allo stesso collegamento di rete. Nelle reti più grandi in cui i client e i server non si trovano nella stessa subnet fisica, ogni collegamento di rete contiene uno o più agenti di inoltro DHCP. Un agente di inoltro DHCP può essere un router. Quando un client invia al router una richiesta DHCP, il router la inoltra al server DHCP richiedendo di fornire un indirizzo IP per il client. Il server DHCP invia la sua risposta al router, che la inoltrerà al client. Affinché il router e il server DHCP funzionino, non è necessario che si trovino nella stessa subnet. Il router funge da collegamento tra il client e il server DHCP.

6. Cos'è 3G/4G?

Èil tipo di tecnologia per banda larga mobile o Internet wireless a cui è possibile accedere tramite telefoni cellulari o modem portatili. La lettera G rappresenta la generazione. La tecnologia 4G è una delle più recenti e più rapide oggi dopo Long Term Evolution (LTE). Alcuni router VPN Cisco consentono di condividere la connessione Internet da dongle USB 3G/4G supportati che possono essere collegati a esso per fungere da failover in caso di arresto o rallentamento del principale provider di servizi Internet (ISP).

7. Che cos'è un generatore di certificati e quando utilizzarlo?

Un certificato digitale certifica la proprietà di una chiave pubblica da parte del soggetto specificato del certificato. In questo modo le relying party possono dipendere da firme o asserzioni effettuate dalla chiave privata corrispondente alla chiave pubblica certificata. Un router può generare un certificato autofirmato, ovvero un certificato creato dall'amministratore di rete. Può inoltre inviare richieste alle Autorità di certificazione (CA) per richiedere un certificato di identità digitale. È importante disporre di certificati legittimi provenienti da applicazioni di terze parti.

8. Che cos'è un firewall e quando utilizzarne uno?

L'obiettivo principale di un firewall è controllare il traffico di rete in entrata e in uscita analizzando i pacchetti di dati e determinando se consentirne il passaggio o meno, in base a un set di regole predeterminato. Un router è considerato un potente firewall hardware a causa di funzioni che consentono di filtrare i dati in ingresso. Un firewall di rete crea un bridge tra una rete interna considerata sicura e attendibile e un'altra rete, in genere una rete interna esterna come Internet che si presume non sia sicura e non attendibile.

9. Che cos'è un certificato IPSec attendibile?

IPSec (Internet Protocol Security) genera comunicazioni protette, autenticate e affidabili sulle reti IP. Viene utilizzato per lo scambio di dati di generazione e autenticazione di chiavi, protocolli di definizione delle chiavi, algoritmi di crittografia o meccanismi di autenticazione per l'autenticazione e la convalida sicure delle transazioni online con certificati SSL (Secure Sockets Layer). RV320 consente di aggiungere un massimo di 50 certificati autofirmati o autorizzati da un'autorità di certificazione di terze parti. Questi certificati possono essere esportati in un computer o dispositivo USB e importati per essere utilizzati da un client o un amministratore.

10. Che cos'è un certificato SSL attendibile?

I certificati vengono utilizzati per verificare l'identità dell'utente su un computer o su Internet e per migliorare una conversazione privata o protetta. SSL (Secure Sockets Layer) è la tecnologia di

protezione standard per la creazione di un collegamento crittografato tra un server Web e un browser. Questi certificati possono essere esportati in un computer o dispositivo USB e importati per essere utilizzati da un client o un amministratore.

11. Che cos'è la VPN da client a gateway?

Rete privata virtuale (VPN) da client a gateway: un utente può connettere in remoto diverse filiali della società situate in aree geografiche diverse per trasmettere e ricevere i dati tra le aree in modo più sicuro. In genere, un utente dispone di un software client VPN, ad esempio Cisco AnyConnect Secure Mobility Client, installato su un computer, può accedere con le credenziali necessarie e connettersi a un router o gateway remoto.

Nota: Sono disponibili aggiornamenti sui requisiti di licenza per la serie RV340 a partire dalla versione 1.0.3.15. Per ulteriori informazioni, fare clic qui.

12. Che cos'è il filtro contenuti?

Il filtro dei contenuti è una funzione che consente a un amministratore di bloccare siti Web designati e indesiderati. Il filtro contenuti può bloccare l'elenco e consentire l'accesso a siti Web in base a parole chiave e URL (Uniform Resource Locator). Un amministratore può applicare una pianificazione al filtro del contenuto in base al momento in cui deve essere attivo.

Per ulteriori informazioni, consultare il glossario.

13. Cos'è il CoS?

Il servizio CoS (Class of Service) consente di gestire il traffico in una rete assegnando una priorità rispetto ad altri tipi di traffico. Viene utilizzato per assegnare livelli di priorità alle intestazioni frame Ethernet del traffico di rete ed è applicabile solo ai collegamenti trunked. Differenziando il traffico, il CoS permette di sorvegliare i pacchetti di dati preferiti e di assegnare loro una priorità per la trasmissione nel caso in cui la rete subisca problemi di congestione o ritardo. È possibile mappare le impostazioni di priorità CoS alla coda di inoltro del traffico su un router.

14. Cos'è l'opzione DHCP 82?

L'inoltro DHCP è una funzionalità inclusa nel router che consente la comunicazione DHCP tra gli host e i server DHCP remoti non inclusi nella stessa rete. L'opzione 82 è un'opzione delle informazioni dell'agente di inoltro DHCP e consente a un agente di inoltro DHCP di includere informazioni su se stesso quando inoltra pacchetti DHCP originati dal client a un server DHCP. Il server DHCP può utilizzare queste informazioni per implementare indirizzi IP o altri criteri di assegnazione dei parametri. L'identificazione completa della connessione aggiunge sicurezza al processo DHCP.

15. Informazioni su DHCP

Il protocollo DHCP (Dynamic Host Configuration Protocol) è un protocollo di configurazione di rete che configura automaticamente gli indirizzi IP dei dispositivi in rete in modo che possano connettersi tra loro anziché assegnare manualmente un indirizzo IP a un dispositivo.

16. Che cos'è DMZ e quando è necessario utilizzarlo?

Una zona demilitarizzata (DMZ) è una sottorete aperta al pubblico ma situata dietro il firewall. Una DMZ consente di reindirizzare i pacchetti in entrata nella porta WAN a un indirizzo IP specifico

nella LAN. È possibile configurare le regole del firewall per consentire l'accesso a servizi e porte specifici nella DMZ sia dalla LAN che dalla WAN. In caso di attacco a uno dei nodi DMZ, la LAN non è necessariamente vulnerabile. Si consiglia di collocare gli host che devono essere esposti alla WAN (ad esempio server Web o di posta elettronica) nella rete DMZ.

17. Che cos'è DSCP?

Il DSCP (Differentiated Services Code Point) viene usato per classificare il traffico di rete e assegnare diversi livelli di servizio ai pacchetti contrassegnandoli con codici DSCP nel campo dell'intestazione IP. Le impostazioni DSCP determinano il modo in cui i valori DSCP vengono mappati a QoS (Quality of Service), che è un metodo per gestire i livelli di priorità del traffico in una rete. Tramite DSCP il router può utilizzare i bit di priorità nell'ottetto Type of Service (ToS) per assegnare la priorità al traffico rispetto al QoS nel layer 3.

18. Che cos'è il DNS dinamico?

Il DNS (Dynamic Domain Name System) è un metodo per aggiornare automaticamente un server dei nomi nel DNS, spesso in tempo reale, con la configurazione DNS attiva dei nomi host, degli indirizzi o di altre informazioni configurate. Questo servizio assegna un nome di dominio fisso a un indirizzo IP WAN dinamico, in modo da poter ospitare il proprio server Web, FTP o un altro tipo di server TCP/IP sulla LAN. Il router usa il DNS con un account DNS basato sul Web. Se l'indirizzo IP WAN del router cambia, la funzione DNS notificherà la modifica al server DNS. Il server DNS aggiornerà quindi la configurazione per includere il nuovo indirizzo IP WAN. Questa opzione è utile se l'indirizzo IP WAN del router cambia spesso. Per utilizzare la funzionalità DNS sul router, è necessario creare un account DNS su uno dei siti Web forniti.

19. Che cos'è la VPN da gateway a gateway? Quando lo utilizzereste?

Una connessione VPN da gateway a gateway consente a due router di connettersi in modo sicuro tra loro e al client di un'estremità di apparire logicamente come se facessero parte della rete dell'altra estremità. In questo modo è possibile condividere dati e risorse su Internet in modo più semplice e sicuro. Per abilitare una VPN da gateway a gateway, la configurazione deve essere eseguita su entrambi i router.

20. Che cosa sono i binding IP e MAC? Quando lo utilizzerei?

Il binding degli indirizzi IP e MAC è un processo che collega un indirizzo IP a un indirizzo MAC e viceversa. Se il router riceve pacchetti con lo stesso indirizzo IP ma un indirizzo MAC diverso, scarta i pacchetti. Aiuta a prevenire lo spoofing IP e migliora la sicurezza della rete, in quanto non consente a un utente di modificare gli indirizzi IP dei dispositivi. L'indirizzo IP dell'host di origine e l'indirizzo MAC del traffico devono sempre corrispondere per poter accedere alla rete. Se il router riceve pacchetti con lo stesso indirizzo IP ma un indirizzo MAC diverso, scarta i pacchetti.

21. Che cos'è il bilanciamento del carico e quando è necessario utilizzarlo?

Il bilanciamento del carico consente a un router di sfruttare più percorsi ottimali per una determinata destinazione. È inerente al processo di inoltro nel router e viene attivata automaticamente se la tabella di routing ha più percorsi per raggiungere una destinazione. Configurare il bilanciamento del carico nel router consente di ottenere un utilizzo corretto delle risorse, massimizzare il throughput, il tempo di risposta ed evitare principalmente il sovraccarico in quanto distribuisce il carico di lavoro su più computer, collegamenti di rete e altre risorse.

22. Che cos'è il clone dell'indirizzo MAC e quando è necessario utilizzarlo?

Il clone dell'indirizzo MAC è il modo più semplice per duplicare la copia esatta dell'indirizzo MAC di un dispositivo su un altro dispositivo, ad esempio un router. A volte gli ISP richiedono di registrare un indirizzo MAC del router per autenticare il dispositivo. Un indirizzo MAC è un codice esadecimale a 12 cifre assegnato a ogni componente hardware in modo che possa essere identificato in modo univoco. Se è già stato registrato un altro indirizzo MAC con l'ISP, è possibile utilizzare un clone di indirizzi MAC per clonare tale indirizzo sul nuovo router. In questo modo non è necessario contattare l'ISP per modificare l'indirizzo MAC registrato in precedenza, riducendo i costi e i tempi di manutenzione.

23. Che cos'è un NAT uno a uno e quando è necessario utilizzarlo?

NAT (One-to-one Network Address Translation) crea una relazione che mappa un indirizzo IP WAN valido agli indirizzi IP LAN nascosti dalla WAN (Internet) da NAT. Ciò protegge i dispositivi LAN da rilevamento e attacchi. Sul router, è possibile mappare un singolo indirizzo IP privato (indirizzo IP LAN) a un singolo indirizzo IP pubblico (indirizzo IP WAN) o un intervallo di indirizzi IP privati a un intervallo di indirizzi IP pubblici.

24. Che cos'è la complessità della password e perché è utile per me?

La complessità della password è una funzione di un dispositivo di rete che applica un requisito minimo di complessità della password per la modifica della password. Questa funzione è utile per tutti i tipi di rete. Le password complesse possono essere impostate in modo da scadere dopo un periodo di tempo specificato.

25. Che cos'è Port Address Translation (PAT) e quando è necessario utilizzarlo?

Èuna funzione che consente di mappare più dispositivi all'interno di una rete privata o locale a un singolo indirizzo IP pubblico. PAT viene utilizzato per conservare gli indirizzi IP. È un'estensione di Network Address Translation (NAT). Il PAT è anche noto come porting, sovraccarico porta, NAT multiplexato a livello porta e NAT a indirizzo singolo.

26. Che cos'è Port Forwarding e quando è necessario utilizzarlo?

L'inoltro porte è una funzione utilizzata per passare dati a un dispositivo specifico all'interno di una LAN privata. A tale scopo, esegue il mapping del traffico dalle porte scelte sul dispositivo alle porte corrispondenti sulla rete. Il router supporta questa funzionalità che consente al computer di indirizzare in modo efficiente il traffico dove è necessario per migliorare le prestazioni e le caratteristiche di bilanciamento della rete. È consigliabile utilizzare l'inoltro porte solo quando necessario, in quanto ciò comporta un rischio per la sicurezza dovuto al fatto che una porta configurata è sempre aperta.

27. Che cos'è il mirroring delle porte?

Il mirroring delle porte è un metodo utilizzato per monitorare il traffico di rete. Con il mirroring delle porte, le copie dei pacchetti in entrata e in uscita sulle porte (porte di origine) di un dispositivo di rete vengono inoltrate a un'altra porta (porta di destinazione) dove i pacchetti vengono analizzati.

28. Che cos'è Port Triggering e quando è necessario utilizzarlo?

L'attivazione delle porte è simile all'inoltro delle porte, con la differenza che è più sicura in quanto

le porte in ingresso non sono sempre aperte. Le porte restano chiuse fino a quando non vengono attivate, limitando la possibilità di accessi indesiderati. L'attivazione delle porte è un metodo di inoltro dinamico delle porte. Quando un host connesso al router apre una porta trigger configurata in una regola di attivazione per gli intervalli di porte, il router inoltra le porte configurate all'host. Quando l'host chiude la porta attivata, il router chiude le porte inoltrate. Tutti i computer della rete possono utilizzare la porta che attiva l'installazione, poiché non è necessario un indirizzo IP interno per inoltrare le porte in ingresso, a differenza di quanto avviene in Port Forwarding.

29. Che cos'è il server PPTP? Quando lo utilizzereste? Come si configura?

Il protocollo PPTP (Point-to-Point Tunneling Protocol) è un protocollo di rete utilizzato per implementare i tunnel VPN tra le reti pubbliche. I server PPTP sono anche noti come server VPDN (Virtual Private Dialup Network). Il PPTP utilizza un canale di controllo sul protocollo TCP (Transmission Control Protocol) e un tunnel GRE (Generic Routing Encapsulation) che operano per incapsulare i pacchetti PPP. È possibile abilitare fino a 25 tunnel VPN PPTP per gli utenti che eseguono un software client PPTP. L'implementazione PPTP più comune fa parte delle famiglie di prodotti Microsoft Windows e implementa diversi livelli di autenticazione e crittografia in modo nativo come funzionalità standard dello stack PPTP di Windows. Il protocollo PPTP è preferito ad altri protocolli perché è più veloce e può funzionare sui dispositivi mobili. Fare clic qui come riferimento per ottenere informazioni su come configurarlo.

30. Che cos'è QoS?

QoS (Quality of Service) viene utilizzato principalmente per migliorare le prestazioni della rete e per fornire i servizi desiderati agli utenti. Assegna la priorità al flusso del traffico in base al tipo di traffico. QoS può essere applicato al traffico con priorità per le applicazioni sensibili alla latenza (come voce o video) e per controllare l'impatto del traffico non sensibile alla latenza (come i trasferimenti di grandi quantità di dati).

31. Che cos'è RIPv1? RIPv2?

RIP (Routing Information Protocol) è un protocollo vettore di distanza utilizzato dai router per scambiare informazioni di routing. RIP utilizza il conteggio hop come metrica di routing. RIP impedisce ai loop di routing di continuare all'infinito implementando un limite al numero di hop consentiti in un percorso dall'origine alla destinazione. Il numero massimo di hop per RIP è 15, che limita le dimensioni della rete supportate. Per questo motivo è stato sviluppato il RIPv2. A differenza del RIPv1 classful, RIPv2 è un protocollo di routing senza classi che include le subnet mask quando invia gli aggiornamenti del routing.

Il riepilogo delle route in RIPv2 migliora la scalabilità e l'efficienza nelle reti di grandi dimensioni. Il riepilogo degli indirizzi IP significa che non esiste alcuna voce per le route figlio (route create per qualsiasi combinazione di singoli indirizzi IP contenuti in un indirizzo di riepilogo) nella tabella di routing RIP, riducendo le dimensioni della tabella e consentendo al router di gestire più route.

32. Che cos'è il backup Smart Link?

Smart Link Backup è una funzione che consente all'utente di configurare una seconda WAN in caso di guasto del primo o del collegamento principale. Questa funzione viene utilizzata per garantire che la comunicazione tra la WAN e il dispositivo sia sempre continua. Questa funzione è disponibile nei router con connessioni WAN doppie.

3. Che cos'è SSL VPN? Quando lo utilizzereste?

Una VPN SSL (Secure Sockets Layer Virtual Private Network), nota anche come WebVPN, è una tecnologia che fornisce funzionalità VPN di accesso remoto utilizzando la funzione SSL integrata in un moderno browser Web. Non è necessario installare un client VPN nel dispositivo del client. SSL VPN consente agli utenti di qualsiasi postazione abilitata per Internet di avviare un browser Web per stabilire connessioni VPN ad accesso remoto, promettendo in tal modo miglioramenti della produttività e maggiore disponibilità, nonché un'ulteriore riduzione dei costi IT per il software e il supporto dei client VPN.

34. Che cos'è VPN Passthrough?

Il VPN Passthrough è un modo per connettere due reti protette su Internet. Questa opzione viene utilizzata per consentire il passaggio a Internet del traffico VPN generato dai client VPN connessi al router e la riuscita della connessione VPN.

35. Che cos'è VPN?

Una VPN (Virtual Private Network) è una connessione protetta stabilita all'interno di una rete o tra reti tramite la creazione di un tunnel. Le VPN consentono di isolare il traffico tra host e reti specificati dal traffico di host e reti non autorizzati. Le VPN sono vantaggiose per le aziende in quanto sono altamente scalabili, semplificano la topologia di rete e migliorano la produttività riducendo i tempi e i costi di viaggio per gli utenti remoti.

36. Perché è necessario modificare i valori della subnet mask?

Una subnet è una parte di una rete che condivide un particolare indirizzo di subnet. Una subnet mask è una combinazione a 32 bit utilizzata per descrivere quale parte di un indirizzo di rete si riferisce alla subnet e quale parte all'host. Un amministratore può modificare i valori della subnet mask nel caso in cui un host non sia in grado di comunicare con la rete. Le subnet mask possono essere modificate anche nel caso in cui un amministratore desideri aumentare il numero di host su una sottorete senza dover apportare modifiche fisiche.