Forum aux questions sur le routeur

Objectif

Ce document vise à répondre à des questions courantes sur les fonctionnalités et les fonctionnalités d'un routeur Cisco, ainsi que sur la manière et le moment de les utiliser. Si vous êtes intéressé par le contenu vidéo, consultez notre liste de lecture vidéo en cliquant ici.

Périphériques pertinents

- Gamme RV100
- Gamme RV200
- Gamme RV300

Table des matières

1. Qu'est-ce que les règles d'accès ?

Les règles de contrôle d’accès sont des règles qui imposent l’envoi de trafic spécifique à certains utilisateurs d’un réseau. Les règles d'accès peuvent être configurées pour être en vigueur à tout moment ou en fonction d'un planning défini. Bien qu'une règle d'accès puisse être configurée sur un routeur ou un commutateur, elle est configurée en fonction de différents critères afin d'autoriser ou de refuser l'accès à certaines ou à toutes les ressources du réseau.

2. Quelles sont les options 66, 67 et 150 pour le serveur TFTP ?

Un serveur TFTP permet à un administrateur de stocker, de récupérer et de télécharger des fichiers de configuration pour les périphériques d'un réseau. Un serveur DHCP (Dynamic Host Configuration Protocol) loue et distribue des adresses IP aux périphériques du réseau. Lorsqu'un périphérique démarre et qu'une adresse IPv4 ou IPv6 et une adresse IP de serveur TFTP ne sont pas préconfigurées, le périphérique envoie une requête au serveur DHCP avec les options 66, 67 et 150. Ces options sont des requêtes adressées au serveur DHCP pour obtenir des informations sur le serveur TFTP.

- DHCP Option 150 est propriétaire de Cisco. Il fournit les adresses IP dans une liste de serveurs TFTP. L'équivalent standard de l'IEEE (Institute of Electrical and Electronics Engineers) est l'option 66.
- DHCP Option 66 donne l'adresse IP ou le nom d'hôte d'un seul serveur TFTP.
- DHCP Option 67 fournit le nom du fichier de démarrage du serveur TFTP.

3. Quelles sont les différences entre le mode routeur et le mode passerelle ?

Il existe deux modes dans lesquels votre routeur peut fonctionner : le mode routeur et le mode passerelle. Le mode routeur est le mode de fonctionnement qui désactive la traduction d’adresses de réseau (NAT) sur le périphérique et est utilisé pour connecter plusieurs routeurs et plusieurs réseaux. Il est le mieux utilisé dans les environnements de réseau étendu.

Le mode Passerelle est recommandé si le routeur héberge une connexion réseau directement à Internet. La fonction NAT s'exécute lorsque le mode passerelle est activé, ce qui signifie qu'elle ne prend qu'une seule adresse IP WAN et qu'elle possède un bloc entier d'adresses IP LAN.

4. Que sont les journaux système ?

Les journaux système (Syslog) sont des enregistrements d'événements réseau. En cas de dysfonctionnement du système, vous pouvez récupérer les journaux pour diagnostiquer le problème système. Les journaux sont des outils importants qui permettent de comprendre comment un réseau fonctionne pour exécuter le système en douceur et éviter les pannes. Ils sont utiles pour la gestion, le dépannage et la surveillance du réseau.

5. Que sont les modes DHCP ?

Le protocole DHCP (Dynamic Host Configuration Protocol) comporte deux modes : Serveur DHCP et relais DHCP Un serveur DHCP attribue automatiquement les adresses IP disponibles à un client ou hôte DHCP sur le réseau. Le serveur DHCP et le client DHCP doivent être connectés à la même liaison réseau. Dans les réseaux plus importants où les clients et les serveurs ne se trouvent pas sur le même sous-réseau physique, chaque liaison réseau contient un ou plusieurs agents de relais DHCP. Un agent de relais DHCP peut être un routeur. Lorsqu'un client envoie au routeur une requête DHCP, le routeur la transmet ensuite au serveur DHCP lui demandant de fournir une adresse IP pour le client. Le serveur DHCP envoie sa réponse au routeur, puis le routeur la transmet au client. Le routeur et le serveur DHCP n'ont pas besoin d'être sur le même sous-réseau pour fonctionner. Le routeur sert de liaison entre le client et le serveur DHCP.

6. Qu'est-ce que la 3G/4G ?

Il s'agit du type de technologie pour le haut débit mobile ou l'Internet sans fil qui est accessible via des téléphones portables ou des modems portables. La lettre G représente la génération. La technologie 4G est l'une des plus récentes et des plus rapides aujourd'hui après Long Term Evolution (LTE). Certains routeurs VPN Cisco vous permettent de partager la connexion Internet à partir de dongles USB 3G/4G pris en charge qui peuvent y être connectés pour servir de basculement en cas de panne ou de ralentissement du principal fournisseur d'accès Internet (FAI).

7. Qu'est-ce qu'un générateur de certificats et quand l'utiliserais-je ?

Un certificat numérique certifie la propriété d'une clé publique par l'objet nommé du certificat. Cela permet aux parties de confiance de dépendre des signatures ou des assertions faites par la clé privée qui correspond à la clé publique qui est certifiée. Un routeur peut générer un certificat auto-signé, un certificat créé par l'administrateur réseau. Il peut également envoyer des demandes aux autorités de certification (AC) pour demander un certificat d'identité numérique. Il est important d'avoir des certificats légitimes provenant de demandes tierces.

8. Qu'est-ce qu'un pare-feu et quand en utiliser un ?

L'objectif principal d'un pare-feu est de contrôler le trafic réseau entrant et sortant en analysant les paquets de données et en déterminant s'il doit être autorisé à traverser ou non, sur la base d'un ensemble de règles prédéfini. Un routeur est considéré comme un pare-feu matériel puissant en raison de fonctions permettant le filtrage des données entrantes. Un pare-feu de réseau crée un pont entre un réseau interne supposé être sécurisé et fiable et un autre réseau, généralement un interréseau externe tel qu'Internet, supposé ne pas être sécurisé et non fiable.

9. Qu'est-ce qu'un certificat IPSec approuvé ?

IPSec (Internet Protocol Security) génère des communications sécurisées, authentifiées et fiables sur les réseaux IP. Il est utilisé dans l'échange de données de génération et d'authentification de clé, le protocole d'établissement de clé, l'algorithme de chiffrement ou le mécanisme d'authentification pour l'authentification sécurisée et la validation des transactions en ligne avec des certificats SSL (Secure Socket Layer). Sur le routeur RV320, vous pouvez ajouter un maximum de 50 certificats qui sont auto-signés ou autorisés par une autorité de certification tierce. Ces certificats peuvent être exportés vers un ordinateur ou un périphérique USB et importés pour être utilisés par un client ou un administrateur.

10. Qu'est-ce qu'un certificat SSL approuvé ?

Les certificats sont utilisés pour vérifier l'identité de l'utilisateur sur un ordinateur ou sur Internet et pour améliorer une conversation privée ou sécurisée. Secure Sockets Layer (SSL) est la technologie de sécurité standard permettant de créer une liaison chiffrée entre un serveur Web et un navigateur. Ces certificats peuvent être exportés vers un ordinateur ou un périphérique USB et importés pour être utilisés par un client ou un administrateur.

11. Qu'est-ce que le VPN client-à-passerelle ?

Réseau privé virtuel (VPN) client-passerelle : un utilisateur peut connecter à distance différentes branches de votre entreprise situées dans différentes zones géographiques pour transmettre et recevoir les données entre les zones de manière plus sécurisée. Un utilisateur dispose généralement d'un logiciel client VPN tel que le client Cisco AnyConnect Secure Mobility installé sur un ordinateur, se connecte avec les informations d'identification nécessaires et se connecte à un routeur ou à une passerelle distants.

Note: Des mises à jour ont été effectuées sur les exigences de licence pour la gamme RV340 à partir de la version 1.0.3.15. Pour plus de détails, cliquez ici.

12. Qu'est-ce que le filtrage de contenu ?

Le filtrage de contenu est une fonctionnalité qui permet à un administrateur de bloquer des sites Web désignés indésirables. Le filtrage de contenu peut bloquer les listes et autoriser l'accès aux sites Web en fonction des mots clés et des URL (Uniform Resource Locators). Un administrateur peut appliquer une planification au filtrage de contenu en fonction du moment où il doit être actif.

Pour plus d'informations, reportez-vous au glossaire.

13. Qu'est-ce que la CoS ?

La classe de service (CoS) est un moyen de gérer le trafic sur un réseau en attribuant une priorité à d'autres types de trafic. Il est utilisé pour attribuer des niveaux de priorité aux en-têtes de trame Ethernet du trafic réseau et ne s'applique qu'aux liaisons agrégées. En différenciant le trafic, la CoS permet de contrôler et de hiérarchiser les paquets de données préférés en cas de problèmes de congestion ou de retard sur le réseau. Vous pouvez mapper les paramètres de priorité CoS à la file d'attente de transfert du trafic sur un routeur.

14. Qu'est-ce que DHCP Option 82 ?

Le relais DHCP est une fonctionnalité incluse dans le routeur qui permet la communication DHCP entre les hôtes et les serveurs DHCP distants qui ne sont pas sur le même réseau. L'option 82 est une option d'informations d'agent de relais DHCP qui permet à un agent de relais DHCP d'inclure des informations sur lui-même lors du transfert de paquets DHCP provenant du client vers un serveur DHCP. Le serveur DHCP peut utiliser ces informations pour implémenter l'adressage IP ou d'autres stratégies d'attribution de paramètres. Son identification approfondie de la connexion ajoute de la sécurité au processus DHCP.

15. Qu'est-ce que DHCP ?

Le protocole DHCP (Dynamic Host Configuration Protocol) est un protocole de configuration réseau qui configure automatiquement les adresses IP des périphériques sur un réseau afin qu'ils puissent se connecter les uns aux autres au lieu d'attribuer manuellement une adresse IP à un périphérique.

16. Qu'est-ce que la DMZ et quand dois-je l'utiliser ?

Une zone démilitarisée (DMZ) est un sous-réseau ouvert au public mais situé derrière le pare-feu. Une zone démilitarisée (DMZ) vous permet de rediriger les paquets entrant dans votre port WAN vers une adresse IP spécifique de votre réseau local. Vous pouvez configurer des règles de pare-feu pour autoriser l'accès à des services et ports spécifiques dans la zone DMZ à partir du LAN ou du WAN. En cas d'attaque sur l'un des noeuds DMZ, le réseau local n'est pas nécessairement vulnérable. Il est recommandé de placer les hôtes qui doivent être exposés au WAN (tels que les serveurs Web ou de messagerie) dans le réseau DMZ.

17. Qu'est-ce que le DSCP ?

Le DSCP (Differentiated Services Code Point) est utilisé pour classer le trafic réseau et attribuer différents niveaux de service aux paquets en les marquant avec des codes DSCP dans le champ d'en-tête IP. Les paramètres DSCP dictent la manière dont les valeurs DSCP sont mappées à la qualité de service (QoS), qui est une méthode de gestion des niveaux de priorité du trafic sur un réseau. C'est par l'intermédiaire du DSCP que le routeur peut utiliser les bits de priorité de l'octet ToS (Type of Service) pour hiérarchiser le trafic par rapport à la QoS de la couche 3.

18. Qu'est-ce que le DNS dynamique ?

Dynamic Domain Name System (DNS) est une méthode de mise à jour automatique d'un serveur de noms dans le DNS, souvent en temps réel, avec la configuration DDNS active de ses noms d'hôte, adresses ou autres informations configurés. Ce service attribue un nom de domaine fixe à une adresse IP WAN dynamique, afin que vous puissiez héberger votre propre site Web, FTP ou un autre type de serveur TCP/IP sur votre LAN. Le routeur utilise DDNS via un compte DDNS Web. Si l'adresse IP WAN du routeur change, la fonction DDNS informe le serveur DDNS de la modification. Le serveur DDNS met ensuite à jour la configuration pour inclure la nouvelle adresse IP WAN. Cela est utile si l'adresse IP WAN du routeur change souvent. Un compte DDNS doit être créé sur l'un des sites Web fournis pour utiliser la fonctionnalité DDNS sur le routeur.

19. Qu'est-ce que le VPN passerelle à passerelle ? Quand l'utiliseriez-vous ?

Une connexion VPN passerelle à passerelle permet à deux routeurs de se connecter de manière sécurisée et à un client d'une extrémité de s'afficher de manière logique comme s'ils faisaient partie du réseau de l'autre extrémité. Cela permet de partager plus facilement et en toute sécurité les données et les ressources sur Internet. La configuration doit être effectuée sur les deux routeurs pour activer un VPN passerelle à passerelle.

20. Qu'est-ce que la liaison IP et MAC ? Quand l'utiliserais-je ?

La liaison d'adresses IP et MAC est un processus qui relie une adresse IP à une adresse MAC et vice versa. Si le routeur reçoit des paquets avec la même adresse IP mais une adresse MAC différente, il abandonne les paquets. Elle permet d'empêcher l'usurpation d'adresse IP et d'améliorer la sécurité du réseau, car elle ne permet pas à un utilisateur de modifier les adresses IP des périphériques. L'adresse IP de l'hôte source et l'adresse MAC du trafic doivent toujours correspondre pour que l'accès au réseau soit autorisé. Si le routeur reçoit des paquets avec la même adresse IP mais une adresse MAC différente, il abandonne les paquets.

21. Qu'est-ce que l'équilibrage de charge et quand l'utiliserais-je ?

L'équilibrage de charge permet à un routeur de tirer parti de plusieurs meilleurs chemins vers une

destination donnée. Il est inhérent au processus de transfert dans le routeur et est automatiquement activé si la table de routage a plusieurs chemins vers une destination. La configuration de l'équilibrage de charge dans le routeur permet d'optimiser l'utilisation des ressources, le débit, le temps de réponse et surtout d'éviter la surcharge lors de la distribution de la charge de travail sur plusieurs ordinateurs, liaisons réseau et autres ressources.

22. Qu'est-ce que le clone d'adresse MAC et quand dois-je l'utiliser ?

Le clone d'adresse MAC est le moyen le plus simple de dupliquer la copie exacte de l'adresse MAC d'un périphérique vers un autre, tel qu'un routeur. Parfois, les FAI vous demandent d'enregistrer une adresse MAC de votre routeur pour authentifier le périphérique. Une adresse MAC est un code hexadécimal à 12 chiffres donné à chaque élément matériel afin de pouvoir l'identifier de manière unique. Si vous avez déjà enregistré une autre adresse MAC auprès de votre FAI, un clone d'adresse MAC peut être utilisé pour cloner cette adresse sur votre nouveau routeur. De cette manière, vous n'avez pas à contacter le FAI pour modifier l'adresse MAC précédemment enregistrée, ce qui réduit les coûts et le temps de maintenance.

23. Qu'est-ce que la fonction NAT un-à-un et quand dois-je l'utiliser ?

La traduction d'adresses de réseau (NAT) un-à-un crée une relation qui mappe une adresse IP WAN valide aux adresses IP LAN qui sont masquées du WAN (Internet) par la NAT. Cela protège les périphériques LAN contre la détection et les attaques. Sur le routeur, vous pouvez mapper une seule adresse IP privée (adresse IP LAN) à une seule adresse IP publique (adresse IP WAN), ou une plage d'adresses IP privées à une plage d'adresses IP publiques.

24. Qu'est-ce que la complexité des mots de passe et pourquoi est-ce bénéfique pour moi ?

La complexité des mots de passe est une caractéristique d'un périphérique réseau qui impose une complexité minimale des mots de passe pour les modifications de mot de passe. Cela est bénéfique pour tous les types de réseaux. Les mots de passe complexes peuvent être définis pour expirer après un délai spécifié.

25. Qu'est-ce que la traduction d'adresses de port (PAT) et quand dois-je l'utiliser ?

Cette fonction permet de mapper plusieurs périphériques d'un réseau privé ou local à une adresse IP publique unique. La fonction PAT permet de conserver les adresses IP. Il s'agit d'une extension de traduction d'adresses de réseau (NAT). La fonction PAT est également appelée port, surcharge de ports, NAT multiplexée au niveau des ports et NAT à adresse unique.

26. Qu'est-ce que le transfert de port et quand dois-je l'utiliser ?

Port Forwarding est une fonction utilisée pour transmettre des données à un périphérique spécifique au sein d'un réseau local privé. Il le fait en mappant le trafic des ports choisis sur votre périphérique aux ports correspondants sur le réseau. Le routeur prend en charge cette fonctionnalité qui permet à votre ordinateur de diriger efficacement le trafic là où il est nécessaire afin d'améliorer les performances et les caractéristiques d'équilibrage du réseau. Le transfert de port ne doit être utilisé que lorsque cela est nécessaire, car cela pose un risque de sécurité en raison de l'ouverture permanente d'un port configuré.

27. Qu'est-ce que la mise en miroir des ports ?

La mise en miroir des ports est une méthode utilisée pour surveiller le trafic réseau. Avec la mise en miroir des ports, des copies des paquets entrants et sortants aux ports (ports source) d'un périphérique réseau sont transmises à un autre port (port cible) où les paquets sont étudiés.

28. Qu'est-ce que le déclenchement de port et quand dois-je l'utiliser ?

Le déclenchement de port est similaire au transfert de port, sauf qu'il est plus sécurisé car les ports entrants ne sont pas ouverts en permanence. Les ports restent fermés jusqu'à ce qu'ils soient déclenchés, ce qui limite la possibilité d'un accès aux ports non souhaité. Le déclenchement de port est une méthode de transfert de port dynamique. Lorsqu'un hôte connecté au routeur ouvre un port de déclenchement configuré dans une règle de déclenchement de plage de ports, le routeur transfère les ports configurés à l'hôte. Une fois que l'hôte ferme le port déclenché, le routeur ferme les ports transférés. Tout ordinateur d'un réseau peut utiliser la configuration de déclenchement de port car il ne nécessite pas d'adresse IP interne pour transférer les ports entrants, contrairement à la configuration de transfert de port.

29. Qu'est-ce que le serveur PPTP ? Quand l'utiliseriez-vous ? Comment le mettriez-vous en place ?

Le protocole PPTP (Point-to-Point Tunneling Protocol) est un protocole réseau utilisé pour mettre en oeuvre des tunnels VPN entre des réseaux publics. Les serveurs PPTP sont également appelés serveurs VPDN (Virtual Private Dialup Network). PPTP utilise un canal de contrôle sur le protocole TCP (Transmission Control Protocol) et un tunnel GRE (Generic Routing Encapsulation) pour encapsuler les paquets PPP. Jusqu'à 25 tunnels VPN PPTP peuvent être activés pour les utilisateurs qui exécutent un logiciel client PPTP. La mise en oeuvre PPTP la plus courante concerne les gammes de produits Microsoft Windows et met en oeuvre différents niveaux d'authentification et de chiffrement nativement en tant que fonctionnalités standard de la pile PPTP Windows. Le protocole PPTP est préféré aux autres protocoles car il est plus rapide et peut fonctionner sur des périphériques mobiles. Cliquez ici pour savoir comment le configurer.

30. Qu'est-ce que la QoS ?

La qualité de service (QoS) est principalement utilisée pour améliorer les performances du réseau et pour fournir les services souhaités aux utilisateurs. Il donne la priorité au flux de trafic en fonction du type de trafic. La qualité de service peut être appliquée au trafic prioritaire pour les applications sensibles à la latence (voix ou vidéo, par exemple) et pour contrôler l'impact du trafic non sensible à la latence (transferts de données en masse, par exemple).

31. Qu'est-ce que RIPv1 ? RIPv2 ?

Le protocole RIP (Routing Information Protocol) est un protocole à vecteur de distance utilisé par les routeurs pour échanger des informations de routage. Le protocole RIP utilise le nombre de sauts comme métrique de routage. Le protocole RIP empêche les boucles de routage de se poursuivre indéfiniment en implémentant une limite sur le nombre de sauts autorisés dans un chemin entre la source et la destination. Le nombre maximal de sauts pour le protocole RIP est de 15, ce qui limite la taille du réseau qu'il peut prendre en charge. C'est pourquoi le protocole RIPv2 a été développé. Contrairement à RIPv1 par classe, RIPv2 est un protocole de routage sans classe qui inclut les masques de sous-réseau lorsqu'il envoie ses mises à jour de routage.

La récapitulation des routes dans RIPv2 améliore l'évolutivité et l'efficacité des grands réseaux. La récapitulation des adresses IP signifie qu'il n'y a aucune entrée pour les routes enfant (routes créées pour toute combinaison d'adresses IP individuelles contenues dans une adresse

récapitulative) dans la table de routage RIP, réduisant ainsi la taille de la table et permettant au routeur de gérer davantage de routes.

32. Qu'est-ce que Smart Link Backup ?

Smart Link Backup est une fonctionnalité qui permet à l'utilisateur de configurer un second WAN en cas de défaillance de la première liaison ou de la liaison principale. Cette fonction permet de garantir que la communication entre le WAN et le périphérique est toujours continue. Cette fonctionnalité est présente dans les routeurs dotés de deux connexions WAN.

33. Qu'est-ce que le VPN SSL ? Quand l'utiliseriez-vous ?

Un VPN SSL (Secure Sockets Layer Virtual Private Network), également appelé WebVPN, est une technologie qui fournit une fonctionnalité VPN d'accès à distance à l'aide de la fonction SSL intégrée à un navigateur Web moderne. Cela ne nécessite pas l'installation d'un client VPN sur le périphérique du client. Le VPN SSL permet aux utilisateurs de n'importe quel site Internet de lancer un navigateur Web pour établir des connexions VPN d'accès à distance, promouvant ainsi des améliorations de productivité et une meilleure disponibilité, ainsi que de nouvelles réductions de coûts informatiques pour le logiciel client VPN et la prise en charge.

34. Qu'est-ce que le Passthrough VPN ?

VPN Passthrough (Passthrough VPN) permet de connecter deux réseaux sécurisés via Internet. Ceci est utilisé pour permettre au trafic VPN généré par les clients VPN connectés au routeur de passer à Internet et permettre à la connexion VPN de réussir.

35. Qu'est-ce que le VPN ?

Un réseau privé virtuel (VPN) est une connexion sécurisée établie au sein d’un réseau ou entre des réseaux par la création d’un tunnel. Les VPN servent à isoler le trafic entre les hôtes et les réseaux spécifiés du trafic des hôtes et des réseaux non autorisés. Les VPN sont bénéfiques pour les entreprises de telle manière qu'ils soient hautement évolutifs, qu'ils simplifient la topologie du réseau et qu'ils améliorent la productivité en réduisant le temps de déplacement et les coûts pour les utilisateurs distants.

36. Pourquoi modifier les valeurs du masque de sous-réseau ?

Un sous-réseau est une partie d’un réseau qui partage une adresse de sous-réseau à particules. Un masque de sous-réseau est une combinaison de 32 bits utilisée pour décrire quelle partie d’une adresse réseau fait référence au sous-réseau et quelle partie fait référence à l’hôte. Un administrateur peut vouloir modifier les valeurs de masque de sous-réseau dans le cas où un hôte ne peut pas communiquer avec le réseau. Les masques de sous-réseau peuvent également être modifiés si un administrateur souhaite augmenter le nombre d’hôtes sur un sous-réseau sans devoir effectuer de modifications physiques.