Router Frequently Asked Questions

Objective

This document aims to answer common questions about the capabilities and features found in a Cisco router, as well as how and when to use them. If you are interested in video content, see our video playlist by clicking here.

Applicable Devices

- RV100 Series
- RV200 Series
- RV300 Series

Table of Contents

31. What is RIPv1? RIPv2?
32. What is Smart Link Backup?
33. What is SSL VPN? When would you use it?
34. What is VPN Passthrough?
35. What is VPN?
36. Why would I change the subnet mask values?

1. What are Access Rules?

Access Control Rules are rules that mandate specific traffic from being sent to and from certain users on a network. Access Rules can be configured to be in effect all the time or based on a defined schedule. While an access rule can be configured on a router or a switch, it is configured based on various criteria in order to allow or deny access to some or all resources in the network.

2. What are options 66, 67, and 150 for TFTP server?

A TFTP server allows an admin to store, retrieve, and download configuration files for devices on a network. A Dynamic Host Configuration Protocol (DHCP) Server leases and distributes IP addresses to devices on the network. When a device boots, and an IPv4 or IPv6 address and TFTP server IP address are not preconfigured, the device will send out a request to the DHCP server with Options 66, 67, and 150. These options are requests to the DHCP server to obtain information about the TFTP server.

- DHCP Option 150 is Cisco proprietary. It provides the IP addresses in a list of TFTP servers. The Institute of Electrical and Electronics Engineers (IEEE) standard equivalent is Option 66.
- DHCP Option 66 gives the IP address or the hostname of a single TFTP server.
- DHCP Option 67 provides the boot file name for the TFTP server.

3. What are the differences between running in router mode vs. gateway mode?

There are two modes in which your router can operate, the router mode and the gateway mode. The router mode is the operating mode that disables Network Address Translation (NAT) on the device and is used to connect more than one router and multiple networks. This is best used in wide area network environments.

Gateway mode is the recommended mode if the router is hosting a network connection directly to the Internet. NAT is running when Gateway mode is enabled, meaning that it will take a single WAN IP address and have an entire block of LAN IP addresses.

4. What are systems logs?

System logs (Syslog) are records of network events. In the event of system malfunction, you can retrieve the logs to diagnose the system problem. Logs are important tools that are used to understand how a network operates to run the system smoothly and prevent failures. They are useful for network management, troubleshooting, and monitoring.

5. What are DHCP Modes?

Dynamic Host Configuration Protocol (DHCP) has two modes: DHCP Server and DHCP Relay. A DHCP server automatically assigns available IP addresses to a DHCP client or host on the

network. The DHCP server and DHCP client must be connected to the same network link. In larger networks where the clients and the servers are not on the same physical subnet, each network link contains one or more DHCP relay agents. A DHCP relay agent can be a router. When a client sends the router a DHCP request, the router will then forward it to the DHCP server asking to provide an IP address for the client. The DHCP server sends its reply to the router and then the router will forward it to the client. The router and the DHCP server do not need to be on the same subnet to function. The router acts as a liaison between the client and the DHCP server.

6. What is 3G/4G?

It is the type of technology for mobile broadband or wireless Internet that can be accessed through mobile phones or through portable modems. The letter G stands for the generation. The 4G technology is one of the latest and one of the fastest today after Long Term Evolution (LTE). Some Cisco VPN Routers allow you to share the Internet connection from supported 3G/4G USB dongles that can be attached to it to serve as a failover in case the main Internet Service Provider (ISP) goes down or slows down.

7. What is a certificate generator and when would I use it?

A digital certificate certifies the ownership of a public key by the named subject of the certificate. This allows relying parties to depend upon signatures or assertions made by the private key that corresponds to the public key that is certified. A router can generate a self-signed certificate, a certificate created by the network administrator. It can also send out requests to Certificate Authorities (CA) to apply for a digital identity certificate. It is important to have legitimate certificates from third party applications.

8. What is a firewall and when would I use one?

The primary objective of a firewall is to control the incoming and outgoing network traffic by analyzing the data packets and determining whether it should be allowed through or not, based on a predetermined rule set. A router is considered to be a strong hardware firewall due to functions that allow filtering of inbound data. A network firewall builds a bridge between an internal network that is assumed to be secure and trusted and another network, usually an external internetwork such as the Internet that is assumed not to be secure and untrusted.

9. What is a trusted IPSec Certificate?

Internet Protocol Security (IPSec) generates secure, authenticated, and reliable communication over IP networks. It is used in the exchange of key generation and authentication data, key establishment protocol, encryption algorithm, or authentication mechanism of secure authentication and validation of online transactions with Secure Socket Layer (SSL) certificates. On the RV320, you can add a maximum of 50 certificates that are either self-signed or authorized by third party CA. These certificates can be exported to a computer or USB device and be imported to be used by a client or administrator.

10. What is a trusted SSL certificate?

Certificates are used to verify the user identity on a computer or Internet and to enhance a private or secured conversation. Secure Sockets Layer (SSL) is the standard security technology for creating an encrypted link between a web server and a browser. These certificates can be exported to a computer or USB device and be imported to be used by a client or administrator.

11. What is Client-To-Gateway VPN?

Client-to-Gateway Virtual Private Network (VPN) means a user can remotely connect different branches of your company located at different geographical areas to transmit and receive the data among the areas more securely. A user would typically have a VPN client software such as the Cisco AnyConnect Secure Mobility Client installed on a computer, log in with the necessary credentials and connect to a remote router or gateway.

Note: There have been updates on licensing requirements for RV340 series starting with version 1.0.3.15 moving forward. For details about this, click here.

12. What is Content Filtering?

Content filtering is a feature that allows an administrator to block designated, unwanted websites. Content filtering can block list and allow list access to websites according to keywords and Uniform Resource Locators (URLs). An administrator may apply a schedule to content filtering according to when it should be active.

See glossary for additional information.

13. What is CoS?

Class of Service (CoS) is a way of managing traffic over a network by assigning a priority over other kinds of traffic. It is used to assign priority levels to Ethernet frame headers of network traffic, and is only applicable to trunked links. By differentiating traffic, CoS allows preferred data packets to be policed and prioritized for transmission in the event that the network experiences issues such as congestion or delay. You can map CoS priority settings to the traffic forwarding queue on a router.

14. What is DHCP Option 82?

The DHCP relay is a feature included in the router that allows DHCP communication between hosts and remote DHCP servers that are not on the same network. Option 82 is a DHCP relay agent information option allows a DHCP relay agent to include information about itself when forwarding client-originated DHCP packets to a DHCP server. The DHCP server can use this information to implement IP addressing or other parameter-assignment policies. Its thorough identification of the connection adds security to the DHCP process.

15. What is DHCP?

Dynamic Host Configuration Protocol (DHCP) is a network configuration protocol that automatically configures the IP addresses of devices on a network so that they can connect to one another instead of manually assigning an IP address to a device.

16. What is DMZ and when should I use it?

A Demilitarized Zone (DMZ) is a sub-network that is open to the public but behind the firewall. A DMZ allows you to redirect packets coming into your WAN port to a specific IP address in your LAN. You can configure firewall rules to allow access to specific services and ports in the DMZ from both the LAN or WAN. In the event of an attack on any of the DMZ nodes, the LAN is not necessarily vulnerable. It is recommended that you place hosts that must be exposed to the WAN (such as web or e-mail servers) in the DMZ network.

17. What is DSCP?

Differentiated Services Code Point (DSCP) is used to classify network traffic and assign different levels of service to packets by marking them with DSCP codes in the IP header field. The DSCP settings will dictate how DSCP values map to Quality of Service (QoS), which is a method of managing priority levels of traffic on a network. It is through DSCP that the router can use the priority bits in the Type of Service (ToS) octet to prioritize traffic over QoS in layer 3.

18. What is Dynamic DNS?

Dynamic Domain Name System (DNS) is a method of automatically updating a name server in the DNS, often in real time, with the active DDNS configuration of its configured hostnames, addresses or other information. This service assigns a fixed domain name to a dynamic WAN IP address, so you can host your own web, FTP, or another type of TCP/IP server on your LAN. The router uses DDNS through a web-based DDNS account. If the WAN IP address of the router changes, the DDNS feature will notify the DDNS server of the change. The DDNS server will then update the configuration to include the new WAN IP address. This is useful if the WAN IP address of the router often changes. A DDNS account must be created on one of the provided websites to utilize the DDNS feature on the router.

19. What is Gateway-To-Gateway VPN? When would you use it?

A gateway-to-gateway VPN connection allows for two routers to securely connect to each other and for a client on one end to logically appear as if they are a part of the network on the other end. This enables data and resources to be shared more easily and securely over the Internet. The configuration must be done on both routers to enable a gateway-to-gateway VPN.

20. What are IP and MAC Binding? When would I use it?

IP and MAC address binding is a process which links an IP address to a MAC address and vice versa. If the router receives packets with the same IP address but a different MAC address, it drops the packets. It helps to prevent IP spoofing and enhances network security, as it does not allow a user to change IP addresses of devices. The source host IP address and MAC address of the traffic need to always match to be allowed access to the network. If the router receives packets with the same IP address but a different MAC address, it drops the packets.

21. What is Load Balancing and when would I use it?

Load balancing allows a router to take advantage of multiple best paths to a given destination. It is inherent to the forwarding process in the router and is automatically activated if the routing table has multiple paths to a destination. Configuring load balancing in the router helps to achieve proper resource utilization, maximize throughput, response time, and mainly avoid the overload as it distributes the workload across multiple computers, network links and other various resources.

22. What is MAC address clone and when would I need to use it?

MAC address clone is the simplest way to duplicate the exact copy of the MAC address of one device to another device such as a router. Sometimes, ISPs ask you to register a MAC address of your router to authenticate the device. A MAC address is a 12-digit hexadecimal code given to every piece of hardware so it can be uniquely identified. If you already have registered another MAC address with your ISP, a MAC address clone can be used to clone that address to your new router. This way you do not have to contact the ISP to change the previously registered MAC

address which reduces cost and time of maintenance.

23. What is One-to-One NAT and when would I need to use it?

One-to-one Network Address Translation (NAT) creates a relationship that maps a valid WAN IP address to LAN IP addresses that are hidden from the WAN (Internet) by NAT. This protects the LAN devices from discovery and attack. On the router, you can map a single private IP address (LAN IP address) to a single public IP address (WAN IP address), or a range of private IP addresses to a range of public IP addresses.

24. What is password complexity and why is it beneficial to me?

Password complexity is a feature of a networking device that enforces a minimum password complexity requirement for password changes. This is beneficial for all types of networks. Passwords with complexity can be set to expire after a specified time.

25. What is Port Address Translation (PAT) and when would I need to use it?

It is a function that allows multiple devices within a private or local network to be mapped to a single public IP address. PAT is used to conserve IP addresses. It is an extension of Network Address Translation (NAT). PAT is also known as porting, port overloading, port-level multiplexed NAT, and single address NAT.

26. What is Port Forwarding and when would I need to use it?

Port Forwarding is a feature that is used to pass data to a specific device within a private LAN. It does so by mapping traffic from chosen ports on your device to corresponding ports on the network. The router supports this feature that allows your computer to efficiently direct traffic where it is needed in order to improve performance and network balancing characteristics. Port forwarding should be used only when necessary as this poses a security risk due to a configured port always being open.

27. What is Port Mirroring?

Port Mirroring is a method used to monitor network traffic. With Port Mirroring, copies of incoming and outgoing packets at the ports (Source Ports) of a network device are forwarded to another port (Target Port) where the packets are studied.

28. What is Port Triggering and when would I need to use it?

Port Triggering is similar to port forwarding except that it is more secure because the incoming ports are not open all the time. The ports remain closed until they are triggered thereby, limiting the possibility of unwanted port access. Port triggering is a method of dynamic port forwarding. When a host that is connected to the router opens a trigger port that is configured in a port range triggering rule, the router forwards the configured ports to the host. Once the host closes the triggered port, the router closes the forwarded ports. Any computer on a network can use the port triggering setup since it does not require an internal IP address to forward the incoming ports unlike in Port Forwarding.

29. What is PPTP Server? When would you use it? How would you set it up?

The Point-to-Point Tunneling Protocol (PPTP) is a network protocol used to implement VPN

tunnels between public networks. PPTP servers are also known as Virtual Private Dialup Network (VPDN) servers. PPTP uses a control channel over Transmission Control Protocol (TCP) and a Generic Routing Encapsulation (GRE) tunnel operating to encapsulate PPP packets. Up to 25 PPTP VPN tunnels can be enabled for users who are running a PPTP client software. The most common PPTP implementation is with the Microsoft Windows product families and implements different levels of authentication and encryption natively as standard features of the Windows PPTP stack. PPTP is preferred over other protocols because it is faster and has the ability to work on mobile devices. As a reference, click here to get an idea on how to set it up.

30. What is QoS?

Quality of Service (QoS) is mainly used to improve the network performance and is used to provide desired services for the users. It prioritizes the traffic flow based on the type of traffic. QoS can be applied to prioritized traffic for latency-sensitive applications (such as voice or video) and to control the impact of latency-insensitive traffic (such as bulk data transfers).

31. What is RIPv1? RIPv2?

Routing Information Protocol (RIP) is a distance-vector protocol used by routers to exchange routing information. RIP uses hop count as its routing metric. RIP prevents routing loops from continuing indefinitely by implementing a limit on the number of hops allowed in a path from the source to a destination. The maximum hop count for RIP is 15 which limits the network size that it can support. This is why the RIPv2 was developed. Unlike the classful RIPv1, RIPv2 is a classless routing protocol that includes the subnet masks when it sends out its routing updates.

Summarizing routes in RIPv2 improves scalability and efficiency in large networks. Summarizing IP addresses means that there is no entry for child routes (routes that are created for any combination of the individual IP addresses contained within a summary address) in the RIP routing table, reducing the size of the table and allowing the router to handle more routes.

32. What is Smart Link Backup?

Smart Link Backup is a feature that allows the user to set up a second WAN in case the first one or the primary link fails. This feature is used to assure that the communication between the WAN and the device is always continuous. This feature is found in routers with dual WAN connections.

33. What is SSL VPN? When would you use it?

A Secure Sockets Layer Virtual Private Network (SSL VPN), also known as WebVPN, is a technology that provides remote access VPN capability using the SSL function that is built into a modern web browser. This does not require you to install a VPN client on the device of the client. SSL VPN allows users from any Internet-enabled location to launch a web browser to establish remote-access VPN connections, thus promising productivity enhancements and improved availability, as well as further IT cost reduction for VPN client software and support.

34. What is VPN Passthrough?

VPN Passthrough is a way to connect two secured networks over the Internet. This is used to allow VPN traffic generated from VPN clients connected to the router to pass through to the Internet and allow the VPN connection to succeed.

35. What is VPN?

A Virtual Private Network (VPN) is a secure connection established within a network or between networks by creating a tunnel. VPNs serve to isolate traffic between specified hosts and networks from the traffic of unauthorized hosts and networks. VPNs are beneficial to companies in such a way that it is highly scalable, simplifies network topology, and improves productivity by reducing travel time and cost for remote users.

36. Why would I change the subnet mask values?

A subnet is a portion of a network that shares a particulate subnet address. A subnet mask is a 32-bit combination used to describe which portion of a network address refers to the subnet and which part refers to the host. An administrator may want to change the subnet mask values in case a host cannot communicate to the network. Subnet masks may also be changed in case an administrator wants to increase the number of hosts on a subnetwork without having to make any physical changes.