Ccnp troubleshooting commands pdf

Fixing problems are three big things: predicting what might happen, identifying anomalies, and investigating the causes of those anomalies. Many network administrators break down network infrastructure problems by analyzing the path of Layer 3 through the network, jumping on hops, in both directions. This process helps them isolate the problem; Once they determine which jump in the path of the layer fails, they can look further in detail. There are various tools that can help you fix problems on your network. Let's take a look at them and see what questions they can help you explore. Cisco Discovery Protocol (CDP) Cisco Discovery Protocol (CDP) detects basic information about neighboring routers and switches without having to know the passwords for these Cisco network devices. This is possible because Cisco routers and switches regularly send CDP messages that announce information about themselves. Thus, Cisco's CDP-enabled hardware can learn about other devices by listening to these messages. CDP detects several useful details from neighboring Cisco devices: Device ID: Host address list: Network and link data address Port ID: Interface on a remote device that sent a list of CDP advertising capabilities: Device type (e.g. router or switch) Platform: iOS version works on the deviceIn the device To see this information, use the command cdp:show cdp neighbors This team lists each neighboring device One at a time. Each line provides the most important topological information about the neighbor: its host name (device ID), the interface of the local device and its interface (under the title Port). This interface command also lists the platform by identifying a specific model of a nearby router or switch. To get more information, such as the full name of the Switch model and the IP address configured on a nearby device, add the detail option as follows: show cdp neighbors detailOf course, being able to discover a lot of information about neighboring devices is exposure network security. Cisco recommends disabling CDP on any IP interface that doesn't need it. To switch it to a specific interface, use non-CDP to turn on and cdp to include the subcommand interface. The VersionYou show can use the Cisco iOS team show in privileged exec mode to test the Cisco iOS version and release iOS software numbers running on Cisco devices. It displays the following information: Cisco iOS software version - The name and number of the Cisco software version Running time - The length of time since the device was last downloaded switch platform - Equipment platform information, including revision and the amount of RAM processor board ID - serial number of the devicePing the main goal for ping is is for availability, travel time (RTT) and package loss. To trouble the device for these properties, we must use the device's IP address - for example, ping 172.17.4.6. This command sends an Internet Control Message Protocol (ICMP) echo request and displays one of the following:! - The ICMP Echo Response Package was received during the timeout period (2 seconds by default). - No reply was received during the time-out period. You can ping from a specific interface by adding the original interface name parameter at the end of the command - for example, ping 172.17.4.6 source Ethernet 0/0.TracerouteTraceroute is a feature that tracks the path from one network to another, so it can help diagnose the source of many problems. Traceroute works by sending a remote host a sequence of three UDP datagrams with TTL 1 in the IP header; this results in a timeout datagram when it hits the first router on the way, causing the router to respond with the ICMP being exceeded by the message. The traceroute then sends a set of three UDP datagrams to TTL 2, so they time out when they hit the second router, causing it to respond with a timeout message. This process continues until the package reaches its final destination and receives an unattainable ICMP port. Thus, you can trace the way in which the packages decided to move to their destination. You can also use an extended tracing command to check your connection from a specified source - for example, tracing 10.10.60.6 Source Loopback0.Telnet When you use Telnet to connect to a remote device, it uses the default port (23). You can use any port number from 1 to 65535 to check whether a remote device is listening to a particular port, such as telnet 172.17.5.74 8080.Show Interfaces Command and Interface Status CodesCisco Switches use two different sets of interface status codes. Both sets of state codes can determine if the interface is working. Show interfaces and show description of interfaces - These commands list line status and protocol status. They usually indicate whether Layer 1 (line status) is working and whether layer 2 (protocol status) is working. For LAN switch interfaces, both codes tend to have the same value, either up or down. This single status code corresponds to different combinations of line status and protocol status, as shown in the table below. For example, the state of the connected interface corresponds to an up/up state for two other states. Here's a list of status codes and problems they can specify: Line StatusProtocol StatusInterface StatusInterface StatusPossible Root CauseAdministratively downDisDownabledInterface is disabled due to a shutdown command. DownDownNot connectedNoty physical connection, inappropriate device turned off, bug error connectedAnd interface is not expected on physical interfaces. The DownDown error disabled. UpUpConnected Interface works. Cisco Shutdown CommandWhen first set up the interface in terminal setting mode, you must administratively enable the interface before the router can use it to transfer or receive packages. Use the Cisco no shutdown command to allow iOS software to use the interface. Later, you can disable a specific interface to perform hardware maintenance on it or in the network segment. You can also disable the interface if a problem exists in a particular segment of the network, and you should isolate that segment from the rest of the network. The shutdown team administratively allows the interface. To restart the interface, use the command without turning it off. IP RouteMost routing tables contain a combination of static routes and dynamic routes. However, before using any static or dynamic routing, the routing table must contain directly connected networks that are used to access remote networks. To test static routes in the routing table, use the show ip route command, specifying a network address, subnet mask, and IP address of the next hop router or exit interface. These interfaces can be configured using a certain speed using a speed (10 x 100 x 1000) subcommande interface, as well as using a specific duplex using a duplex (half) sub-team interface. If both are configured for the interface, the switch or router disables the IEEE-standard automatic alignment process on this interface. The show's interfaces and interface status commands show speed and duplex settings on the interface, but only the show's state interface team shows how the switch determined speed and duplex settings; It lists all automatic settings with a-set-up. For example, a-full means a full duplex as automatic alignment, while full means full duplex, but as manually configured. While automatic negotiations work well, defaults allow for a possibility problem called a duplex mismatch in which the devices believe that the link has been up, but one side will use a semi-duplex and the other side will use a full duplex. The number of input errors and the number of CRC errors are only two counters in the output of the show's interface team. The challenge is to decide which counters you see which ones show that the problem is happening and which ones are normal and have nothing to do with it. Here's a list of counters to help you begin to understand which ones point to problems and which are just counting normal events that aren't problems: Runts: Footage did not meet the minimum frame size requirements (64 bytes, including 18-bytes MAC, original MAC and type). The handles can be caused by collisions. Giants: Frames exceeding the maximum need for frame size (1518 bytes, including 18-byte MAC destination, original MAC and type). Input errors: Total counters, including hicps, giants, no buffer, CRC, frame, overruns and ignored calculations. CRC: Footage that did not pass FCS mathematics has been received; they can be caused by collisions. Frame: Received footage that has an illegal format (for example, ending in a partial way); they can be caused by collisions. Package output: Total number of packages (frames) of forward interfaces. Conclusion errors: The total number of packages (frames) that the switch port tried to transmit, but for which there was some problem. Clashes: Countering all collisions that occurred during the transmission of the frame interface. Late clashes: A subset of all collisions that occur after the 64th Frame Stakes has been transferred. In a well-functioning Ethernet network, collisions must occur within the first 64 bytes; Late collisions today often indicate a duplex mismatch. Predicting the contents of the MAC Address TableSwitches to find out the MAC address and then use the entries in the MAC address table to make an overheating/filtering solution for each frame. To know exactly how the particular switch will rewind the Ethernet frame, you need to examine the TABLE of MAC addresses on the Cisco switch. The mac-table address-table command displays the contents of the switch's MAC address table. This team lists all THE addresses known as the Switch. The output includes some static overhead MAC addresses used by the switch, and any static-minded MAC addresses, such as those configured with port security. The team also lists all the dynamically studied MAC addresses. If you only want to see dynamically studied MAC address table entries, just use the dynamic exec address-table command. When predicting THE mac table records, you need to submit a frame sent by the device to another device on the other side of the network, and then determine which switch ports will enter the frame when it moves through LAN. Port security and filtering, when tracking the path that frame passes through LAN switches, remember that different types of filters can drop frames even if all interfaces are up. For example, LAN switches can use filters called Access Control Lists (ACL) that filter based on the MAC's source address and purpose, discarding some frames. In addition, routers can filter IP packages using IP addresses. In some it is easy to say that the port security service took action because it closed the interface. In other cases, however, port security leaves the interface up and simply discards traffic for violators. From Ot Perspective, a port security configuration that leaves the interface up but still discards frames, requires the network engineer to keep a close eye on port security rather than just looking at the interfaces and address table MAC. Port security allows for three violations (off, protection, and restriction), but only the default shutdown setting causes the switch to fail by disabling the interface. To find evidence that port security is running, you need to run the show's port-security interface team. In addition, the MAC address table gives some clues as to what port security can be enabled. Because port security controls MAC addresses, any MAC addresses associated with the port that includes port security will be kneaded as static MAC addresses. As a result, the dynamic show mac address-table command does not list the mac addresses of interfaces that include port security. However, show the Mac address-table and show the Mac address-table static commands do a list of these static MAC addresses. Ensuring that the correct access interfaces are in the right VLANsTo to ensure that each access interface is assigned to the correct VLAN, engineers simply need to determine which Switch interfaces are access interfaces instead of barrel interfaces, identify assigned VLANs access on each interface, and compare information with documentation. If possible, start by using the vlan show and show the vlan short commands, because they list the commands of all known VLANs and access interfaces assigned to each VLAN. Keep in mind, however, that these two commands do not list operational barrels. The output makes a list of all the other interfaces (those that are not currently trunk), regardless of whether the interface is in working or inoperable. If the vlan and show switchport interface commands are not available, the show mac address desk command can also help determine VLAN access. This command lists the MAC address table with each entry, including the MAC address, interface, and VLAN ID. If the interface is not assigned to the wrong VLAN, use the switchport vlan vlan-id sub-comment interface to assign the correct VLAN ID. Access to VLANs Not Being DefinedSwitches does not override frames for VLANs that are not configured or configured, but are disabled (off). The vlan show team always lists all VLANs known to the switch, but the show's launch team doesn't. Switches configured as VTP servers and customers do not list vlan commands in the current running configuration or start-up configuration file; On these switches, you have to use the vlan show command. Switches configured to use transparent VTP mode or switched off VTP list vlan configuration in configuration files. (Use the show vtp state command to find out the current VTP switch mode.) Once determining that VLAN does not exist, the problem may be that VLAN VLAN must be determined. Access to VLANs being a disabledAnother step into troubleshooting to make sure that every VLAN is active. The vlan show team lists one of two states: active or active/lshut. The latter means that VLAN is closed. Turning off VLAN disables VLAN only on this switch, so the switch won't forward the frames in that VLAN. Cisco iOS gives you two similar configuration methods that can be used to disable (off) and enable (non-stop) VLAN. Check the permitted VLAN list at both ends of the trunk If the permitted VLAN lists at the ends of the trunk are incompatible, the trunk cannot pass traffic for this VLAN. The output of the team barrel show interfaces on each side will look perfectly normal; You can detect the problem only by comparing the permitted lists at both ends of the barrel. Mismatched backbone operating statesIf the highway is configured correctly, both switch forward frames for the same set of VLANs. If the trunks are incorrectly configured, there may be several different results. In some cases, both switches come to the conclusion that their interfaces are not barrel. In other cases, one switch thinks its interface is the right trunk and the other switch isn't. The most common incorrect configuration - which results in both switches not being profiable - uses a dynamic automatic switch mode command on both switches on the link. The word auto makes us think that the link will barrel automatically, in fact both switches wait for another device on the link to start negotiations. To detect this incorrect configuration, use the show's switchport interface command to check whether both switches have an administrative auto condition and that both work as static port access. ConclusionSday you know the main troubleshooting commands to investigate the problems that network administrators face every day. You can also download the Cisco Team Cheat sheet for a quick help list of troubleshooting commands and their descriptions at hand. Hand. ccnp troubleshooting commands pdf