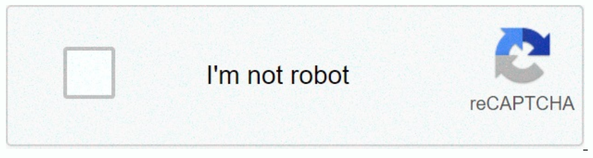

Continue

Cisco switch commands cheat sheet pdf

Cheatografi LevelModePrompt1User EXECDevice>2Privileged EXECDevice # 3Global ConfigDevice (config)#4aInterface Config Moute ArrowAutomatly re-kalit #4bLine e komandmanCtrl + Shift + 6Oh krap, sispann! (Anile tou sa li ap fe kounye a) Ctrl + CExits konfigirasyon modeCtrl + ZApplies aktyel lod & retounen nan prive. EXEC modeCtrl + UErases anyen sou line aktyel lineTabCompletes abreje komandman Paret vesyon pipiti de youn, memwa kapasite, elatriye montre mac adres-tableMAC tableMAC ip routerouting tablo entefas g0 / 0status, MAC, IP, elatriye. pou Gigabit Ethernet 0 / 0show ip koodone briefname, IP, estati, elatriye (tout interfaces) KomandFrom ModeFunctionsm pre doub deflob konfigirasyon si chanje pa pral pran adres IPv6 Adres ShortCommandComplete CommandFunctionenuser EXEC > prive. EXECconf tconfig terminalpriv. EXEC > mondyal konfigirasyon konfigirasyon mondyal konfigirasyon > kfigligal konfigirasyon > liy konfigirasyon kouri-configshow aktyel configcop r scopy kouri-config demaraj-configsaves aktyel konfigirasyon mwen dopm lono ip domen-Lookuppeps routeur soti nan ap eseye li cmds move kom zetwal non lame [Tab] efase demaraj-konfigirasyonGMUST itilize apre laboratwa reyajiste routeute konfigirasyon!del vlan.datedelete vlan.dateMUST itilize apre laboratwa yo Reyajiste konfigirasyon routeute! CommandFrom ModeWhat It Doeshostname xyzglobal configsets hostname to xyzenable secret xyzglobal configsets encrypted password for priv. EXEC to xyzservice password-encryptglobal configencrypts all passwordsline console 0global configenters line config mode for consoleline vty 0 15global configenters line config mode for 16 vty linespassword xyzline configsets line password to xyzloginline configenables users to loginint vlan 1global configenters interface config mode for vlan1ip address [IP] [subnet]interface configsets IP addressno shutinterface configturns on interfacebanner motd #Text Here#global configsets motd banner CommandFrom ModeFunctioninterface g0/1global configenters interface config for Gigabit Ethernet 0/1ip address IP/prefixinterface configsets interface's IPv4 addressno shutinterface configturns on the interfacedescription description textinterface configused to document info about the interfaceipv6 address IP/prefixinterface configsets interface's IPv6 addressipv6 address IP/prefix link-localinterface configsets interface's IPv6 link-local addressipv6 unicast-routingglobal configenables IPv6 routing commands beginner intermediate cisco networking ios cli We offset our carbon usage with Ecologi.

Klike sou lyen ki anba a pou ede nou! ;> 2 Paj Your download will start automatically in 5 Seconds.Close these are some quick notes I have to refresh my memory on Cisco switch setup. Feel free to send me any comments or suggestions. Password Recovery Quick-Links Cisco 2900XL Series Switch - tried this on a 2912XL, and instructions did not properly work. In Flash: Contains files named words, which need to be either renamed or deleted as well for the password recovery at work. Also I used no secret permits and there is no allowed password as well. This did not apply to the 2950XL switches. Adding an IP address of a changed type allows to enter privileged type mode type configuration attribute vlan 1 type ip address 192.168.1.4 255.255.255.0 type there is no shutdown – required to activate address the management address type from default ip type-gate 192.168.1.1 Remove an IP address from a change type allowed to enter privileged mode to configure interface type vlan 1 type has no ip address Configuring Interfaces and port types allow to enter privileged type configuration type interface type fastethernet0/{port #} - the port # is essential or anything an 'Incomplete Command' will result type of auto dud – auto-detect duplex /half duplex type auto speed – auto detect 10/100/1000 speed type spaning-tree port - speed up (a lot) time it takes for the port to get into forwarding mode. Note: Using only if a server/work station is connected to this port, causes it could prevent the Spaning-Tree protocol from detecting and disabling loop through the network. Configuring multiple ports at the same time Turns out there is no way to specify a range of IP addresses for my old IOS switch. However a quick script can quickly generate commands for me copying/pasting to the terminal. >i = 1; while [$i-lt 25]; iron echo ai fast0/$i; echoing auto speeds; echoing duplex auto; echoing portfas span; let i += 1; born; From: can I put the speed and duplex on all skin katalyst switches together or do I need to configure each port individually? This depends on the switch platform that you're referring to. If you are working with a Cisco switch that runs the OS chat, then you can. You can both configure ports that are sequence and not sequences all at the same time. Here are a few examples to do so. set duplex ports 2/1-20, 2/22 full port set speed 2/2-12, 2/15-16 100 If you are working with a Cisco switch that runs the IOS, then you must be a little creative. You don't have the same CLI options to configure multiple ports along with a Cisco switch running the IOS. You have several options though. The easiest way to do this type of configuration is to create a text file, for example in VI or Notepad. After creating the statements in your text editor, simply copy and paste the lines to the CLI. Here is a text example that can be copied CLI. Configure the terminal fastethernet interface 1/1 speed 100 duplex full interface full fastethernet 1/2 speed 100 duplex interface full fastether 1/3 speed 100% full... end omitted text! To return to privileged mode shows run-config! To verify your configuration Newer IOS-based switch allows multiple ports to be configured at the same time. Fix the command interface running on all platforms that support Cisco IOS Release 12.0 (7) XE, Release 12.1E, and Release 12.1(5)T. In Interface range configuration mode, you can configure multiple interfaces with the same configuration parameters. Once you enter the interface-range configuration mode, all command parameters you enter are attributed to all interfaces in that range until you exit the interface-row configuration mode. Tracking is an example of using the command. Please note that the space before the dash is required. routeji (setup)# interface range fastethernet 5/1 – 5, gigabitethernet 1/1 – 2 router (config-if) # speed 100 router (config-if) # duplex router (setup-if) # no shutdown You can also use SNMP and the GUI to change completes this setup. Even if I believe the easiest path is to create a text file. Provides ports of a VLAN over 2900 switch from Cisco Documentation to configure terminal interface {name} switchport access switchport access vlan {num} show run-con Settings a telenet password enabling SNMP allow privilege mode to configure terminal snmp-server community {password} RO - sets a community string and Read only privileges only. or no community snmp-server {password} - remove a community string. Get MAC address discovery for each port on a Cisco WS-X2948 display cam Dynamic Saving Setup on 2948 Port Switch copy flash configuration should ask if flashdevice is bootflash, hit Enter Ask if name for copying in is: myswitch.cfg, Set Y set boot auto-config botflash: myswitch.cfg May have warnings such as: nvram configuration may be lost during next botup, and re-configured using the file(s) specified. These can be ignored. By Edward Tetz To create and configure a Cisco network, you need to know about routers and switch to develop and manage Cisco system security. Come to understand with Cisco network devices and code lists; and find out how to manage static routes and view routing information. While you may not use the OSI model every day, you should be familiar with it, especially when working with Cisco Switch and routers (which operate in Layer 2 and Layer 3, respectively). Here are some of the items that operate at each level of the AS template: Layer Example Description 7. Applications responsible for the initiative or request service. SMTP, DNS, HTTP, and Telnet 6. Presentation Formats the information so that it is understood by the recipient system. Compression and encryption depend on the 5 application. Sessions responsible for manage, and terminate the session.NetBIOS 4. Transport information Breaks in segments and is responsible for connections and communications without connection. TCP and UDP 3. Network responsible for logical address and routing IP, ICMP, ARP, RIP, IGRP, and routers 2. Data Link is responsible for physical addresses, error editing, and preparing the information for the MAC media address, CSMA/CD, change, and bridge 1. Physical deals with the electric signal. Cables, connectors, hub, and echo like all networks, a Cisco network needs to be properly configured. To do this, you need to know the configuration modes to use when configuring your network. You also should know how to configure a headrn, configure a switch management client, and configure a headquarn to use DHCP for your Cisco network. Configuring mode for Cisco networks when you're moving around in the Cisco IOS, you'll see many prompts. These prompts changes as you move from one configuration mode to another. Here is a summary of the major configuration modes: User EXEC mode: When you connect to a Cisco device to setup mode is runtime user mode. With user runtime mode you can view the settings on the device, but don't make any changes. You know you are in EXEC user mode because the IOS prompt displays a >. PRIVILEGED MODE EXEC: In order to make changes to the device you must navigate to Privileged EXEC mode where you may be required to enter a password. Privileged mode EXEC is shown with a C# at the prompt. Global configuration mode: Global configuration mode is where you go to make global changes in the router like the hostname. navigate to Global Configuration mode from Privileged EXEC mode you type to configure terminal or configuration t where you will put in (config)# prompt. Sub prompt: There are a number of different sub invitations from Global configuration mode you can navigate to such as the invitation invitations to modify settings on a specific kentre, or prompts to edit the different ports on the device. Configure a headquarter for Cisco networks when working with particular routers, but also when facing the management interface on switch, you will often need to configure network interface that will either match physical ports or virtual interfaces in the form of a LAN virtual (VLAN) interface (when dealing with switch). For your router interface the following example will set speed, duplex and IP configuration information for the FastEthernet 0/0 interface notice as slot/port). In the case of the router, the kides is allowed using the command to no lock in the final step; interfaces on switches are enabled by default. Router1>able Router1 # configure terminal Router1 (config)#interface FastEthernet0/0 Router1 (config-if)#description Private LAN 100 Router1 (config-if)#duplex full Router1 (config-if) #ip address 192.168.1.1 255.255.255.0 Router1 (config-if)#no Call Configure a switch management client for Cisco network for your switch, to enable an IP address on your management client, you will use something similar to the following example. In this example, management is held on VLAN 1 – the default VLAN. Switch1>enable Switch1 # configure terminal Switch1 #interface VLAN 1 Switch1 (config-if) #ip address 192.168.1.241 255.255.255.25 5.0 Configure an Inter Interface to use DHCP for Cisco Network if you want to configure either a router or switch to retrieve its IP configuration information from a Dynamic Network Host Configuration Protocol (DHCP) server, then you can order like the following example. Router1>enable Router1 # configure terminal Router1 (config)#interface FastEthernet0/0 Router1 (config-if)#ip dhcp When working with your Cisco network, you may want to separate users from different streaming domains for security or traffic reductions. You can do this by applying VLANs. The following example will create VLAN (VLAN2) and set the ports on a switch (from 1-12) to VLAN2. Switch1>enable Switch1 # configure terminal Switch1 (config)#interface vlan 2 Switch1 (config-if))#description Finance VLAN Switch1 (config-if) #exit Switch1 (config)#interface Fix FastEthernet 0/1, FastEther Net 0/12 Switch1 (config-if-range) #switchport Switch1 access mode (config-if-range) #switchport access vlan 2 If you're connecting two switches simultaneously, then you'll want to allow all VLANs configured to pass between the two switches. This is accomplished by applying a skin trunk. To configure port 24 on your changes to be a trunk port, you will use the following code: Switch1>able Switch1 # configure terminal Switch1 (config) > #interface FastEthernet 0/24 Switch1 (config-if-range) #switchport trunk no need to pair to use EtherChannel on your Cisco network. EtherChannel allows you to take up to eight skins on your switch and treat them as a major link. This can be used to connect servers with four multiple networks that are linked (or team) to a switch, or connect multiple switch simultaneously. There are two main negotiation protocols, the Aggregation Protocol Port (PAgP) which is a cisco protocol protocol and Link Aggation Control Protocol (LACP) which is an open standard protocol. To set EtherChannel to use and in the protocols you will configure it to support one of these modes. Auto: Sets headline in responding to PAgP negotiation package, but the headquarn will begin negotiations on its own. Desirable: Sets the cornea actively attempting to negotiate a PAgP connection. On: Force the connection to bring all links up without using a negotiated connection protocol. This mode can only connect to another device that is also set to On. When using this mode, change by bargain the link using either PAgP or LACP. Active: Set kurone in actively try to negotiate connection with other LACP devices. passive: Setting the address to respond to LACP data if it receives negotiation requests from other systems. The following example will configure EtherChannel to use port groups 11 and 12 on the switch simultaneously using PAgP as the protocol. The same type in order should be used on the change that change1 is connected. Switch1 > enable Switch1 # configure the terminal Switch1 (config)# keyboard range FastEthernet0/11-12 Switch (config-if-range) # mode switchport access Switch1 (config-range) # switchport access vlan 10 Switt (config-if-range) # channel-group 5 desirable mode Spain Tree Protocol (STP) allows you to create redundant loop on your Cisco network for strong tolerance, and prevent inadvertent loop that can be created on your network from bringing the network to its knees. The following code will enable Cisco's proprietary schemes per VLAN Spaning Tree Protocol (PVST) on the open standard of several Tree Spaning protocols (MSTP). In addition to configuring STP on the switch, you will also configure port 2 on the switch for portfast, allowing the port to immediately transition to Send mode. Switch1 > Enable Switch1 # configure the terminal switch1 (config)#spanning-footer mode quick-pvst switch1 (config)#interface Fast Swiss 0/2 Switch1 (config-if) #spanning-foot port warning logs: portfast should only be allowed on ports that are connected to a single host. Connecting hub, concentrateurs, switching, bridges, etc... in this cornea when portfast is enabled, may cause temporary loop bridges to temporary. Use with Portfast CAUTION will be configured at kine 10 due to the row order, but will only have effects when the interfaces are in a non-confusing mode. When working with your routers on your Cisco network, it's highly likely that you'll want to have your routers data routers. The first step in having your router data pass from one headrn to another edge is to enable routing; just use these commands. Router1>enable Router1 # Configure terminal Router1 (setup)#ip if you don't choose to use a dynamic route protocol route, you can add static routes to your router. The following will add a static route of Router1 to send data to the 192.168.5.0/24 network using the router with the IP address of 192.168.3.2. Router1>enable Router1 # configure terminal Router1 (config)#ip router1(config)#ip Router192.168.5.0 255.255.255.0 192 1 68.3.2 Managing route protocol information for Cisco Network Route Information Protocol (RIP) is widely used, and version 2 allowing you to use Variable Length Subnet Masks (VLSM) across your network. The following code will enable routing, enable RIP, set RIP to version 2, disable summary routes, define the distributed network in this kom 192.168.5.0 / 24, ak olye ke wout difize, li pral voye RIP done direkteman nan 192.168.1.1. Routeur2>enable Routeur2 # configured teminal Routeur2 (config)#ip routeur2 (konfigirasyon) #router rip Routeur2 (config-routeute) #version 2 Routeuter2 (config-routeus)#no oto-rezime Route1 (config-router)#network 192 168.5.0 Routeur2 (config-routeur)#neighbor 192.168.1.1 Managing ranfose potay enteye pwotokol pou Cisco rezo amelyore Enterye Gateway Routing Pwotokol (EIGRP) se vesyon an mete ajou nan IGRP. Kod ki anba la a pral pemet EIGRP le li sevi avek yon autonomous-sistem (AS) nimewo nan 100, distribye de rezo ak enfim rezime oto. Routeur2>enable Routeur2 #configured teminal Routeur2 (config)#ip routeur Routeur2 (config)#router égiepteur 100 Routeur2 (config-routeur)#network 192.168.1.Router2 (config-config-routeur) #network 192.168.1.Router2 (config-config-routeur) #network 192.168.1.Router2 (config-config-routeur) #network 192.168.1.Router2 (config-config-routeur) #network 192.168.1.Router2 (config-config-routeur) #network 192.168.1.Router2 (config-config-routeur)#network 192.168.routeur)#network 192.168.5.0 Routeur2 (config-routeur)#no oto-rezime Managing chemen ouve pi kout premye pou rezo Cisco rezo Open kout Path Premye (OSPF) se yon pwotokol eta lyen ki se lajman itilize. OSPF itilize adres la nan kone nan loopback kom idantifyan an OSPF, Se konsa, egzanp sa a pral mete adres la nan kone nan loopback, Le sa a, pemet OSPF ak yon pwosesis ID nan 100, ak distribye yon rezo nan 192.168.255.254 ak yon rezo nan 192.168. 5.0 / 24 Routeur2>enable Routeur2 #configured teminal Routeur2 (config)#interface loopback 0 Router2 (config-si) #ip adres 192.168.255.254 255.255.255.0 Router2 (config-si)#exit Route2 (config)#router ospf 100 Router2 (config-route #network 192.168.255.254 0.0.0.0 zon 0 Router2 (config-routeuter)#network #network 192.168.5.0.0.0.0.255 zon 0 Apre mete kanpe nenpot pwotokol routing ke ou vle aplike - RIP, OSPF, OSPF, oswa EIGRP - ou ka we tout enfomasyon ou wout nan lod la wout ip. Sa ki anba la a se yon egzanp nan pwodiksyon an nan lod sa a. Pwodiksyon an gen ladan yon lejand ki montre kod yo pou chak pwotokol wout, ak wout yo espesifik yo idantifye pa pwotokol la sous. Router2>enable Password: Router2#show ip route Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 ia - IS-IS inter area, * - candidate default, U - per-user static route o - ODR, P - periodic downloaded static route Gateway of last resort is not set D 192.168.10.0/24 [90/284160] via 192.168.1.1, 00:04:19, FastEthernet0/0 O 192.168.10.0/24 [110/11] via 192.168.1.1, 00:01:01, FastEthernet0/0 R [120/1] via 192.168.1.1, 00:00:07, FastEthernet0/0 C 192.168.5.0/24 is directly connected, FastEthernet0/1 C 192.168.1.0/24 is directly connected, FastEthernet0/0 S 192.168.3.0/24 [1/0] across 192.168.1.1 Security is still a concern, and your Cisco network needs to be quite well In the following sections, you see how to secure your Cisco network by configuring NAT, by configuring an ACL, and when you implement that ACL. Keep your Cisco network by configuring nat the following commands to use to configure NAT service overload on a router called Router1. In this example, a source address list is created in access list #1, which is then used as the source list inside. The fastEthernet 0/0 port is the public address port excessively loading that all addresses inside get translated into. Router1>enable Router1 # configure terminal Router1 (config)#access -list 1 allow 10.0.0.0.0.255.2 55.255 Router1 (setup)#ip nat inside list 1 Interface FastEthernet 0/0 overload Router1 (1 config)#interface FastEthernet0/0 Router1 (config-if)#ip nat out router1 (config-if)#interface FastEthernet0/1 Router1 (config-if)#ip #interface nat inside your Cisco Network Tightly by configuring an Access Control List (ACL) ACLs to use to control traffic flow. They can be used to allow or deny flows of traffic. The two main types of ACLs are: Standard ACLs, which have fewer options for classifying data and controlling traffic flow than extended ACLs. They are only able to manage traffic based on the source IP address. These ACLs are numbered at 1–99 and from 1300–1999. Extended ACLs, which offer the ability to filter or control traffic based on a variety of criteria such as source or destination IP addresses, as well as protocol types such as, ICMP, TCP, UDP, or IP. These ACLs are numbered at 100–199 and from 2000–2699. To create an ACL Standard, you can use the following example that will create an ACL that allows traffic for the 192.168.8.0/24 network. Switch1>enable Switch1 # configure terminal Switch1 (config)#access-list 50 allow 192.168.8.8 0.0.0.255 to create an extended ACL you can use the following example that will create an ACL that allows traffic and addresses in 192. 168.8.0/24 network with tcp port of either 80 (http) or 443 (https): Router1>enable Router1 # configure terminal Router1 (config)#access-list 101 Note This ACL is to monitor the round round traffic. Router1 (config)#access-list 101 allow tcp 192.168.8.0.0.0.0.255 any eq 80 Router1 (config)#access-list 1011 allow tcp 192.1 68.168.8.0.0.0.255 Any eq 443 Save your Cisco network by applying an Access Control List after you have created an Access Control List (ACL), such as ACL 101 created above, you can apply ACL to a connection. In this example, this ACL is set to restrict traffic from FastEthernet0/1. Router1>enable Router1 # configure terminal Router1 (config)#interface FastEthernet0/1 Router1 (config-if) #ip Access-Cluster 101 exit