CCNA Master Cheat Sheet

Configure basic Networking

Command	Description
(config)# interface g1/0	Enter their interface config mode
(config-if)# description Link to Somehost	Human readable link description
(config-if)# ip address 10.23.42.5 255.255.0.0	Add IPv4 address to interface.
(config-if)# mac address 1234.5678.90AB	Overwrite MAC address.
(config-if)# no mac address	Remove MAC overwrite.
(config-if)# ipv6 address 2001:41d0:8:e115::ccc/64	Add IPv6 address to interface.
(config-if)# ipv6 address 2001:41d0:8:e115::/64 eui-64	Add IPv6 address based on MAC to interface.
(config-if)# ip address dhcp	Get IPv4 address via dhcp.
(config-if)# ipv6 address autoconfig [default]	Get IPv6 address [and default route] via autoconfig
(config-if)# ip dhcp client client-id asccii SW2	Set hostname transmitted as dhcp client to SW2
(config)# interface g1/0 - 2	Configure both interfaces at once.
(config-if)# [no] shutdown	En- or Disable interface. Often shutdown is the default.

Command	Description
(config)# ip default-gateway 10.23.42.1	Set 10.23.42.1 as the default gateway
(config)# ip route 10.20.30.0 255.255.255.0 {1.2.3.4,e0/0} [ad]	Add static route via next hop or interface
(config)# ipv6 route 2001:41d0:8:e115::/64 [g1/1] [next hop]	Next hop is required for Ethernet interface in IPv6
(config)# ip host the-space.agency 178.32.222.21	Create a static host entry on this device.
(config)# ipv6 unicast-routing	Globally enable ipv6 routing.

Troubleshoot basic Networking

Command	Description
# show interfaces [if-name]	Show interfaces mac, bandwidth, mtu, packet stats...
# show ip[v6] route [static]	Show routes and how they were learned.
# show ip[v6] interface [if-name]	Show interfaces ip/arp/icmp/nd... configuration
# show ip[v6] interface brief [if-name]	Only show ip, status and operational status
# show protocols [if-name]	Much like show ip int brief, w/ cidr, w/o ok/method
# show mac address-table	Show the mac address table of a switch.
# clear mac address-table [dynamic]	Clear the dynamically learned mac address table entries.

Command	Description
# show arp	Show {ip,ipx,appletalk}-mac bindings
# show ip arp [{ip, mac, if-name}]	Show ip-mac bindings
# clear [ip] arp 192.168.1.1	Remove arp entry for ip
# debug arp	Show debug messages when receiving/sending arp packets
# undebug all	Disable all previously enabled debugs
# show ipv6 neighbors	Show neighbor discovery table cache
# ping 1.2.3.4 [source g1/1]	
# traceroute 1.2.3.4 [source g1/1]	
# show control-plane host open-ports	netstat -tulpn on this cisco device, basically

Troubleshoot networks with SPAN

Command	Description
(config)# monitor session 23 source interface g1/1 {rx,tx,both}	Define SPAN #23 input as g1/1
(config)# monitor session 23 destination interface g1/2	Define SPAN #23 output as g1/2
# show monitor	Show all configured SPANs

Port Security

Command	Description
(config-if)# switchport mode {access, trunk}	
(config-if)# [no] switchport port-security	En/Disable port-security
(config-if)# switchport port-security maximum 1	Number of allowed MACs.
(config-if)# switchport port-security mac-address 1234.5678.9abc	Manually allow a MAC on this port.
(config-if)# switchport port-security mac-address sticky	Allow learning of connected macs until mac reached.
(config-if)# switchport port-security violation shutdown	Shutdown port when other device gets connected.
(config-if)# shutdown (config-if)# no shutdown	Reenable if after port-security violation.
(config)# errdisable recovery cause psecure-violation	Reenable if automatically after problem is fixed.
(config)# errdisable recovery interval 42	Recheck every 42 seconds. (min 30, default 300)

Port-security violation terms

Term	Definition
protect	Drops packets, no alert
restrict	Drops packets, increments security-violation count

Term	Definition
shutdown	Shuts down the port (default)

Troubleshooting Port Security

Command	Description
# show port-security [interface g1/1]	port status, violation mode, max/total MACs,...
# show port-security address	Secure MACs on ports.
# show errdisable recovery	Check if autorecovery is enabled. Disabled by default.

Configure vlans

Note: Even when a switch port is changed from access to trunk, its access vlan is maintained in the config. When automatic trunk negotiation fails (e.g. because I unplug a link between to switches and put it into my laptop) the configured access vlan becomes active once again and I might be able to reach network parts I'm not supposed to. Always disable DTP / trunk auto negotiation.

Layer2 Switch Vlan Config

Command	Description
(config)# [no] vlan 23	[delete vlan or] create vlan and enter config-vlan mode
(config-vlan)# name TelephoneSanitizer	Name this vlan TelephoneSanitizer

Command	Description
(config)# int g1/1	
(config-if)# switchport mode access	Make frames out this port untagged
(config-if)# switchport access vlan 23	
(config)# int g1/2	
(config-if)# switchport mode trunk	Make frames out this port tagged by default
(config-if)# switchport trunk encapsulation dot1q	Sometimes the default is ciscos old isl.
(config-if)# switchport trunk native vlan 256	Except for vlan 256, which is still untagged.
(config-if)# switchport nonegotiate	Disable DTP

Layer3 Switch Vlan Config

Command	Description
(config)# interface vlan 23	enter interface config mode
(config-if)# ip address 1.2.3.4 255.255.255.0	set device ip in vlan 23
(config-if)# no shutdown	virtual interfaces are disabled by default
(config-if)# int g	
(config)# no vlan 23	delete vlan 23

Router (on a Stick) Vlan Config

Command	Description
(config)# interface g1/1.10	Create subinterface g1/1.10 on g1/1
(config-subif)# encapsulation dot1q 10	enable ieee 802.1Q vlan tagging with vlan 10 on the subinterface
(config-subif)# ip address 10.0.10.1 255.255.255.0	
# show vlans	Show vlans and their trunk interfaces

Troubleshoot Vlans on a switch

Command	Description
# show vlan [{id 23, name TelephoneSanitizer}] [brief]	Show vlan settings for all switch ports
# show interfaces g1/1 switchport	Verify mode and vlan of g1/1
# show interfaces g1/1 trunk	Show trunk settings and state
# show run interface vlan 1	Quick way to search the running config.
# show interface status	Show trunk mode / access vlan
# show dtp interface g1/1	Show current DTP mode for g1/1

VTP

Command	Description
(config)# vtp mode [server, client, transparent]	
(config)# vtp domain	
(config)# vtp password	
(config)# vtp pruning	

Troubleshoot VTP

Command	Description
show vtp status	show vtp domain, pruning, mode and more
show vtp password	

STP

Spaning Tree Protocol (802.1D) blocks ports with redundant links to prevent layer 2 loops and broadcast storms.

Command	Description
(config)# spanning-tree vlan 1 root {primary, secondary}	Make this device the primary/secondary root bridge.
(config)# spanning-tree portfast bpduguard default	Enable bpdu guard for all portfast enable interfaces

Command	Description
(config)# spanning-tree portfast default	Enable portfast for all non-trunk interfaces
(config-if)# spanning-tree bpduguard enable	Enable gpduguard on this interface
(config-if)# spanning-tree portfast	Enable portfast on this interface
(config-if)# spanning-tree guard root	Enable root guard on this interface

Troubleshoot STP

Command	Description
# show spanning-tree [vlan 1]	Who's the root and how do I get there?
# show spanning-tree summary	Is global portfast/bpduguard configured?
# show running-config interface g1/1	Is portfast/bpduguard configured on this interface?
# show spanning-tree interface g1/1 portfast	Is portfast active on this interface?

RSTP

Rapid Spanning Tree Protocol (802.1w) reduces convergence time after a topology change compares to STP.

Command	Description
(config)# spanning-tree mode rapid-pvst	Change spanning-tree mode to RSTP

Etherchannel (Link Aggregation)

How to set LACP? TODO: Look at modes again

Command	Description
(config)# interface range g1/1 - 2	configure g1/1 and g1/2 at the same time
(config-if-range)# channel-group 1 mode {auto, desirable}	Add both interfaces to etherchannel 1 (PAgP)
(config-if-range)# channel-group 1 mode {active, passive}	Add both interfaces to etherchannel 1 (LACP)
(config-if-range)# channel-group 1 mode on	Add both interfaces to etherchannel 1 (Static)
(config)# interface port-channel 1	Configure virtual interface for etherchannel 1
(config-if)# switchport mode trunk	Put etherchannel 1 in trunk mode
(config-if)# switchport trunk allowed vlan 10,20,30	Add tagged vlans 10,20,30 on ethercahnnel 1

Troubleshoot Etherchannel (Link Aggregation)

Command	Description
# show interface port-channel 1	Has the combined bandwidth and members as extra info.
# show etherchannel summary	Show etherchannel protocols and members as a list

Command	Description
# show etherchannel port-channel 1	Show per member state and stats

Configure a Serial

Layer 1 link speed is dictated by a CSU/DSU, in a lab without an external CSU/DSU a DTE (Data Terminal Equipment) cable and DCE (Data Communications Equipment) cable are used.

Command	Description
(config)# interface serial 1/0	Configure interface serial 1/0
(config-if)# clock rate 128000	Set clock rate on DCE router side to 128 kbps
(config)# show controllers serial 1/0	Verify clock rate for serial interface 1/0

ACLs

#1-#99, #1300-#1999: Standard IPv4 ACL

#100-#199, #2000-#2699: Extended IPv4 ACL

Default mask for standard ACLs: 0.0.0.0

Command	Description
(config)# access-list 23 permit 1.2.3.4 [0.0.255.255]	Create ACL #23 or append a rule to ACL #23, allow 1.2.x.x
(config)# no access-list 23	Delete entire ACL #23

Command	Description
(config)# ip[v6] access-list resequence local_only 5 10	Renumber ACL Rules, put first on #5, increment by 10.
(config)# ip access-list {standard, extended} 23	Create ACL and/or enter config mode for ACL #23
(config)# ip access-list {standard, extended} local_only	Create ACL and/or enter config mode for ACL 'local_only'
(config-std-nac1)# permit 10.20.30.0 0.0.0.255	Append rule to standard ACL 'local_only'
(config-std-nac1)# 5 permit 10.20.30.0 0.0.0.255	Append rule to ACL at sequence number 5.
(config-std-nac1)# no <sequence#>	Remove rule with sequence# from ACL
(config-ext-nac1)# deny tcp any any	
(config-ext-nac1)# permit udp host 10.20.30.40 any lt 1024	
(config-ext-nac1)# permit udp host 10.20.30.40 any eq dns	
(config-ext-nac1)# deny udp host 10.20.30.40 any	
(config-ext-nac1)# permit ip any any	

Interface ACLs

Command	Description
(config)# inter g1/1	Enter if-config mode for g1/1
(config-if)# ip access-group 23 out	Apply ACL #23 to outgoing packets, not send by the router
(config-if)# ip access-group 42 in	Apply ACL #42 to incoming packets
(config-if)# ip access-group local_only in	Overwrite the used ACL, only one ACL per if + proto + direction!
(config-if)# ipv6 traffic-filter 23 out	The v6 syntax of course differs...
# show ip interface g1/1 | incl access list	Show ACLs on g1/1 (When none set shows not set for v4 and nothing for v6)

Troubleshooting ACLs

Command	Description
# show [ip[v6]] access-lists	Show all configured ACLs
# show access-list 10	Display all rules in ACL #10 and how often they matched.

NAT

Local addresses are any address as it appears inside the network. Global addresses are any address as it appears outside the network.

Term	Definition
inside local	IP address assigned to a host inside the network, non-routable
inside global	IP address assigned by Network Information Center or ISP, routable
outside local	IP address of a remote host as it appears inside the network, non-routable
outside global	IP address of a remote host assigned by the host owner, routable

Command	Description
(config)# int g1/1	Enter if-config mode for g1/1
(config-if)# ip address 1.2.3.4 255.255.255.240	configure 1.2.3.4/28 on g1/1
(config-if)# ip nat outside	Packets going out, need to change their src, incoming their dest ip.
(config)# int g1/2	Enter if-config mode for g1/2
(config-if)# ip address 10.10.23.1 255.255.255.0	configure 10.10.23.1/24 on g1/2
(config-if)# ip nat inside	Packets going out, need to change their dest, incoming their src ip.

SNAT

Command	Description
(config)# ip nat inside source static 10.10.23.2 1.2.3.5	SNAT - statically map an internal ip 1:1 to an external ip.

DNAT

Command	Description
(config)# access-list 42 permit 10.10.23.0 0.0.0.255	Create an ACL identifying 10.10.23/24
(config)# ip nat pool POOL 1.2.3.5 1.2.3.10 netmask 255.255.255.240	Create an IP Address Pool for NATing
(config)# ip nat inside source list 42 pool POOL	DNAT IPs matching ACL #42 1:1 with IPs from nat pool 'POOL'.

Note the missing overload.

PAT

The overload keyword means, that one or a couple of external IPs are to be used for multiple internal IPs. Higher level information like connection port numbers are used to identify the correct internal destination for incoming packets. Cisco calls this PAT, while this is what your average joes home router would call NAT.

Command	Description
(config)# access-list 10 permit 10.10.0.0 0.0.255.255	Create an ACL identifying 10.10/16
(config)# ip nat inside source list 10 interface g1/1 overload	PAT IPs matching ACL #10 many:1 with g1/1s public IP

Troubleshooting NAT

Command	Description
# show ip nat translations	Show nat table entries if any

Command	Description
# show ip nat statistics	Show translations are actually used and interfaces are marked in/out correctly.
# clear ip nat translation {ip, *}	Clear dynamic translations. Doesn't mess with SNAT!
# debug ip nat [detailed]	

Is the ACL correct? Is there a route to the address? Note: NAT Table entries are kept for 24h after the last use by default.

DHCP Server

Command	Description
(config)# ip dhcp excluded-address 10.30.4.1 10.30.4.100	Don't distribute these IPs in leases
(config)# ip dhcp pool PCs	Creat and/or enter dhcp config for pool 'PCs'
(dhcp-config)# network 10.30.4.0 /24	define pool addresses
(dhcp-config)# default-router 10.2.1.1	define default-gateway to be distributed in the leases
(dhcp-config)# dns-server 10.30.4.1	
(dhcp-config)# domain-name acme.com	
(dhcp-config)# lease	lease validity time

Command	Description
(config)# int g1/1	Enter interface config mode on client facing interface
(config-if)# ip helper-address 192.168.1.1	Relay DHCP Requests to this host

Troubleshooting DHCP

Command	Description
# debug ip dhcp server packet	
# show dhcp lease	Show dhcp lease information
# show ip dhcp pool	Show pool size and addresses in use
# show ip dhcp binding	Show which mac got which ip
# sh run | section dhcp	See if ip dhcp exclude-address / pool stuff is wrong.
# sh run int g1/1	See if ip helper-address is wrong.

HSRP

Command	Description
(config-if)# standby [group-number] ip	Join HSRP Group
(config-if)# standby [group-number] priority	(optional) Set prio of this router.

Command	Description
(config-if)# standby [group-number] preempt	(optional) Preempt other routers when this router becomes active
(config-if)# standby {1,2}	(optional) Set HSRP Version

Troubleshooting HSRP

Command	Description
# show standby	HSRP Groups, their VIPs, state, active router, standby router, preemption.

SLAs

Command	Description
(config)# ip sla 23	Create ip sla test #23 and enter its config mode.
(config-ip-sla)# icmp-echo 1.2.3.4	Define icmp-echo test.
(config-ip-sla)# frequency 42	frequency in seconds.
(config)# ip sla schedule 23 life {forever, seconds} start-time now	Start test #23 now and until manually stopped.

Troubleshooting SLAs

Command	Description
# show ip sla configuration	Show all configured ip sla configs

Command	Description
# show ip sla statistics	Show sla results

Device Management

Command	Description
(config)# hostname R1	Set hostname to R1
(config)# enable password	Set enable passwort.
(config)# enable secret	Same, but with hashing.
(config)# service password-encryption	Very weak encryption of passwords passwords.
# copy flash0: tftp:	Copy something from flash to tftp. Wizard asks for details. Works both ways.
# write	# copy running-config startup-config
# write erase	# erase startup-config
# reload	restart the device and load the startup-config
# copy running-config tftp:	copy running-config to an tftp server. (interactive)
# copy running-config	Merge source config into the running config.
# setup	initial configuration dialog

Command	Description
# show version	ios, bootloader and hardware infos, uptime, configuration register
# show {running,startup}-config	

Firmware Management

Note: flash: is the main flash memory on all iOS devices

Command	Description
(config)# boot system flash:filename.bin	Boot filename.bin from flash memory.
(config)# boot system tftp://10.20.30.40/filename.bin	Boot filename.bin from tftp.
(config)# boot system rom	Boot ROM monitor as a backup.
(config)# config-register 0x2342	Set the 16bit Configuration Register value used after reboot.
# show file systems	Lists available file systems
# show flash0:	List fs content and free space.

License Management

Command	**Description**
# license save flash:licenses.lic	Save a copy of all licenses.
# license install flash0:license.xml	Install a license.
(config)# license boot module technology-package	active a evaluation right-to-use license.
# reload	Reboot to activate the package and right to use license.
(config)# license boot module technology-package disable	deactive a technology-package.
# reload	Reboot without that technology-package.
# license clear	Remove license from the license storage.
(config)# no license boot module technology-package disable	Remove the no longer needed line from the config.
# reload	I don't even know why this is needed. Fu cisco.
# show license	active licenses

Command	**Description**
# show license feature	technology packe and feature licenses supported.
# show license udi	product id and serial number needed to order licenses

Reset Password

Command	**Description**
> confreq	Show the configuration register in rom monitor
> confreq 0x2142	Set the configuration register in rom monitor to not load startup-conf
> reset	Reboot in rom monitor
# copy startup running	
(config)# enable secret foobar	Overwrite forgotten password
(config)# config-register 0x2102	Do load startup-config after boot again.
# save	

Telnet / Console

Command	Description
(config)# banner login "Insert snarky banner."	Make sure to include legal terms to sound smart.
(config)# banner motd "Insert snarky banner."	Set Login Banner.
(config)# line vty 0 4	Enter config mode for vty 0 to 4 (up to 15 allowed).
(config)# line console 0	Enter config mode for the console port
(config-line)# login	Require login on telnet/console connection.
(config-line)# password	Enable Telnet and set vty login password.
(config-line)# access-class 10 in	Set ACL to limit inbound IPs allowed to access vty
(config-line)# access-class 42 in	Overwrite the used ACL, only one ACL per vty + direction!
(config-line)# exec-timeout 10	Autologout after 10 Minutes
(config-line)# login local	Require login on telnet/console connection via local users.
(config)# username h.acker secret C1sco123	Create local user with encrypted password.

SSH

Command	Description
(config)# hostname Foobar	Required to generate SSH keys.
(config)# ip domain-name example.com	Required to generate SSH keys.
(config)# crypto key generate rsa modulus 2048	Generate keys like it's 1995! Potentially takes forever.
(config)# ip ssh version 2	Force SSHv2
(config-line)# transport input ssh	Force ssh, disable telnet.
# show ip ssh	SSH version, timeout time, auth retries..
# show ssh	List of active connections

Clock

Command	Description
# show clock	Show time and date
(config)# clock set 23:50:42 10 Jan 2017	Update clock
(config)# clock timezone EST 0	Update timezone to EST
(config)# ntp server 10.20.30.40	Configure upstream ntp server.
(config)# ntp master [stratum]	Enable ntp server.

Command	Description
# show ntp associations	ntp connections.
# show ntp status	synchronized?, statum, ...

Disable unused services

Command	Description
# show control-plane host open-ports	Show open ports
(config)# no ip http server	Stop the http server (but not https).
(config)# no cdp enable	Stop CDP
# auto secure	

Radius

Command	Description
(config)# username password	Local backup user.
(config)# aaa new-model	Enable aaa services.
(config)# radius server	Add and define Radius conf.
(config-radius-server)# address ipv4 [auth-port]	Use this hostname/ip of server.
(config-radius-server)# key	Radius PSK

Command	Description
(config)# aaa group server radius	Create authentication group.
(config-sg-radius)# server name	Using the radius config.
(config)# aaa authentication login group local	Allow that group and local users in.

TACACS+

Command	Description
(config)# username password	Local backup user.
(config)# aaa new-model	Enable aaa services.
(config)# tacacs server	Add and define TACACS conf.
(config-server-tacacs)# address ipv4	
(config-server-tacacs)# [port]	
(config-server-tacacs)# key	
(config)# aaa group server tacacs+	Multiple possible.
(config-sg-tacacs+)# server name	
(config)# aaa authentication login group local	Allow that group and local users in.

Syslog

Command	Description
# logging 10.20.30.40	Log to this syslog server (name or ip)
# logging trap informational	Only log messages with min. informational sev.

service sequence-number | Needed for seqence number in syslog messages service time stamps log [datetime, log] | Needed for date and time in syslog messages

Command	Description
# show logging	syslog status, local logging buffer

SNMP

Command	Description
(config)# snmp-server contact admin@example.com	Contact email
(config)# snmp-server location RZ-Hamburg	Where is the device
(config)# snmp-server community [ro, rw]	Add community
(config)# snmp-server host 10.20.30.40	SNMP notifications recipient

Command	Description
# show snmp community	
# show snmp location	
# show snmp contact	

Command	Description
# show snmp host	

CDP - Cisco Discovery Protocol

Command	Description
# [no] cdp run	Enables cdp globaly and on all interfaces (default)
# (config-if)# [no] cdp enable	Enable cdp on an interface
# show cdp neighbors [detail]	List connected cisco devices (name, local/remote port, [ip] ..)
# show cdp entry *	

LLDP - Link Layer Discovery Protocol

Command	Description
# [no] lldp run	Enables lldp globaly and on all interfaces
(config-if)# [no] lldp transmit	Enable lldp packet transmission on interface
(config-if)# [no] lddp receive	Enable lldp packet reception on interace

PPP

Command	Description
(config)# username fnord password pass	Create users for pap auth.
(config)# inteface S0/0/0	
(config-if)# clock rate 125000	Baud rate. Only on DCE cable!
(config-if)# bandwidth 125	Logical speed used for routing cost calc, RSVP…
(config-if)# encapsulation ppp	Default is HDLC
(config-if)# ppp authentication pap	Require remote to authenticate via pap
(config-if)# ppp pap sent-username fnord password pass	Authenticate to remote pap
(config)# hostname routy1	Required for CHAP, used as chap client username
(config)# username routy2 password foobar	Create users for chap auth for routy2
(config)# inteface S0/0/0	
(config-if)# no ppp authentication pap	Remove in favor of chap
(config-if)# no ppp pap sent-username fnord password pass	Remove in favor of chap
(config-if)# ppp authentication chap	Require remote to authenticate via chap

Note: When routy1 connects to routy2 it looks in it's local user database for a user named routy2 and uses that users password. This means the passwords have to be the same on both sides and the usernames must be the other sides hostname.

Troubleshooting PPP

Command	Description
# show controllers S0/0/0	interface, connected type of cable, clock rate
# show interfaces	encapsulation, logical bandwidth
# show ppp all	session state, auth type, peer ip and name
# debug ppp authentication	

MLP

Command	Description
(config)# interface Multilink23	Create and configure virtual if
(config-if)# ip address 10.20.30.40 255.255.255.0	
(config-if)# ppp multilink	Enable mlp
(conifg-if)# ppp multilink group 23	Make phys ifs with mlp #23 join.
(config)# interface s0/0/0	Configure phys ifs
(config-if)# no ip address	Remove ip addrs.
(config-if)# encapsulation ppp	

Command	Description
(config-if)# ppp multilink	
(config-if)# ppp multilink group 23	Join mlp group #23.

Troubleshooting MLP

Command	Description
show ppp multilink	Physical IFs,

PPPoE

Command	Description
(config)# interface Dialer23	Create and configure virtual dialer interface.
(config-if)# ip address negotiated	Get IP via PPP/IPCP
(config-if)# encapsulation ppp	
(config-if)# dialer pool 23	The dialer interface is a member of one dialer pool…
(config)# interface s0/0/0	
(config-if)# no ip address	
(config-if)# pppoe-client dial-pool-number 23	… the pool is a group of one or more physical interfaces.

Troubleshooting PPPoE

Command	Description
# show ip interface brief	is the dialer if up? Does the dialer have an IP via IPCP?
# show pppoe session	Are PPPoE sessions established? Which ports.

GRE

Note: We can run OSPF and other routing protocols through this gre tunnel, as gre supports multicast.

Command	Description
(config)# interface tunnel23	
(config-if)# ip address 192.168.1.1 255.255.255.0	transit net
(config-if)# tunnel source 10.20.30.40	local, can be linklocal
(config-if)# tunnel destination 6.5.4.3	remote, can be linklocal

tunnel mode gre ip ip mtu

Troubleshooting GRE

Command	Description
# show ip interface brief tunnel23	Line hould be up, given a route to the destination.
# show inteface tunnel23	Tunnel source, dest, protocol
# show ip route	Should include the transit net as directly connected.

RIPv2

Command	Description
(config)# router rip	Enable RIP and enter it's config mode
(config-router)# version 2	Set RIPv2, which is Classless
(config-router)# network 192.168.0.0	Advertise connected networks which are within .
(config-router)# network 0.0.0.0	Advertise all connected networks.
(config-router)# timers basic	
(config-router)# no auto-summary	Don't summarize a smaller subnet route in a bigger one.
(config-router)# passive-interface g1/1	Don't send RIP updates out this interface
(config-router)# passive-interface default	Don't send RIP updates on any if by default
(config-router)# no passive-interface g1/2	Overwrite passive-interface default
(config-router)# default information originate	Advertise the default route.
(config-if)# no ip rip advertise 123	

Troubleshooting RIPv2

Command	Description
# show ip[v6] protocols	Show rip timers, interfaces, networks,
# show ip rip database	Routes learned by rip, used to combile the routing table
# show ip route	Show learned routes
# clear ip route *	Get rid of all routes

EIGRP

Note: The network command enables any interface with an ip in that net to send and receive EIGRP updates. Also it enables routes to this nets to start beeing advertised.

Command	Description
# show run &#124 section eigrp	Show EIGRP settings.
# show interfaces g1/1	Show configured/default bandwith and delay.
(config-if)# bandwidth	Overwrite bandwidth used for eigrp metric.
(config-if)# delay	Overwrite deplay used for eigrp metric.
(config)# router eigrp 23	Add and conf EIGRP AS#23
(config-router)# network 10.20.30.0 0.0.0.255	Announce routes to 10.20.30.0/24
(config-router)# no shutdown	On some iOS versions it's off by default.

Command	**Description**
(config-router)# [no] eigrp router-id	Defaults to highest loopback ip
(config-router)# [no] passive-interface g1/2	Disable EIGRP here. Ignore incoming pkgs.
(config-router)# [no] passive-interface default	Disable EIGRP on all ifs by default.
(config-router)# maximum-paths	Default 4, must match, number of loadbalanced paths.
(config-router)# variance 4	Default 1, Max 4:1 variance for unequal lb.
(config-router)# no auto-summary	Don't summarize a smaller subnet route in a big one.
# show ip[v6] eigrp neighbors	Neighbor addr, if, hold time, uptime, queued pkgs
# show ip[v6] eigrp interfaces [if-name]	If, Number of peers, pending routes, queued pkgs
# show ip[v6] route [eigrp]	Routes starting with D were learned via EIGRP
# show ip[v6] eigrp topology [all-links]	Topology table, as#, router-id

EIGRP with ipv6

Command	**Description**
(config)# ipv6 unicast-routing	Enable v6 routing on the router

Command	Description
(config)# ipv6 router eigrp 23	Configure eigrp as #23
(config-rtr)# no shutdown	Enable this eigrp routing process.
(config-if)# [no] ipv6 eigrp 23	Enable eigrp with ipv6 for as #23 on this if.

OSPF

cost = reference bandwidth / interface bandwidth

The default reference bandwith is 100Mbps. Everything faster has a cost of 1.

Command	Description
(config)# router ospf 1	1 is the pid, not the area.
(config-router)# router-id 1.2.3.4	Defaults to highest IPv4 on lo, then other ifs.
(config-router)# network 10.20.30.0 0.0.0.255 area 0	enable interfaces for ospf with matching IPs
(config-router)# (no) passive-interface g1/1	Stop in- and egress ospf hello packets.
(config-router)# passive-interface default	Mark all ifs passive by default.
(config-router)# default-information originate (always)	Advertise default routes into a normal area
(config-router)# auto-cost reference-bandwidth <refbw in Mb/s>	Change reference bandwidth speed

Command	Description
(config-if)# ip ospf cost 23	Overwrite interface cost to 23
(config-if)# bandwidth <bw in kb/s>	Change interface bandwidth

Router Types

Term	Definition
Internal Router	All OSPF interfaces in one area
Backbone Router	Has one or more OSPF interfaces in the backbone
Area Boundary Router (ABR)	Has at least one interface in the backbone area and at least one in another area
Autonomous System Boundary Router (ASBR)	Injects routes into OSPF via redistribution from other routing protocols

OSPF with ipv6 (OSPFv3)

Command	Description
(config)# ipv6 unicast-routing	
(config)# ipv6 router ospf	
(config-router)# router-id	Required if we don't have any v4 addrs configured.
(config-if)# ipv6 ospf area	Required for OSPFv3.

The networks command does not exist, non mentioned commands are the same.

Troubleshooting OSPF

Command	Description
# show run | sect ospf	
# show ip(v6) protocols	Other protocols with lower AD?
# show ipv6 ospf	reference bandwidth, router id, networks, interface per area
# show ip(v6) ospf neighbor	neighbor IDs, IPs and via interface.
# show ip(v6) ospf neighbor detail	dr, bdr, timers, ...
# show interface brief	admin down? link?
# show ip(v6) ospf interface brief	ospf enabled interfaces
# show ip(v6) ospf interface g1/1	ospf related infos for g1/1, passive?
# show ip(v6) route (ospf)	ospf routes are marked O, show route ad and cost

BGP

Note: In other routing protocols the network statement is used to determin the interfaces over which the protocol should talk to its neighbors. In BGP it indicates only which routes should be advertised to the BGP neighbors. The network needs to match an exact route in the routing table or it will still not be announced.

Command	Description
(config)# router bgp	Create routing process.
(config)# neighbor remote-as	BGP does not auto discover neighbors.
(config)# network [mask]	Advertise this network.

Command	Description
# show run | sect bgp	
# show ip bgp summary	neighbors IPs, ASs and session states, bgp version
# show ip bgp neighbors [peer-ip]	tcp sessions and timers, bgp parameters
# show ip bgp	routing infos received from all peers

CLI

Default Behavior

Here I'll collect crazy default behaviors and how to fix them, I guess..

Command	Description
(config)# no ip domain-lookup	Don't try to telnet unknown single word commands

Modes

Mode	Prompt	enter
User	>	N/A
Exec	#	> enable
Config	(config)#	# configure terminal
Interface	(config-if)#	(config)# interface g1/0
Line	(config-line)#	(config)# line vty 0 4
DHCP	(dhcp-config)#	(config)# ip dhcp pool Foobar

Filters

Name	Function
include hostname	find a line including 'hostname'
section interface	find a section including 'interface'
begin interface	Show remaining config starting with the first line containing 'interface'
exclude !	exclude all line containing ! (comments)

Navigation

Sequence	**Function**
Ctrl-Shfit-6	Kill many commands
Ctrl-Shift-6 x	Move telnet session to background
Esc-B	Ctrl-Left arrow
Esc-F	Ctrl-Right arrow
Ctrl-R	Redraw the current line
Ctrl-U	Erase line
Ctrl-W	Delete the word left of the cursor
Ctrl-C	Drop back to Exec, does *not* kill processes..
Ctrl-A	Move Cursor to the beginning of the line
Ctrl-E	Move Cursor to the end of the line
Tab	Autocompletion
?	Help, can be entered mostly everywhere

Packet Types

Ethernet Frame

Field	Field Length	Description
Preamble	8 bytes	Alternating 1s and 0s used to synchronize
Destination MAC (DA)	6 bytes	MAC of recipient
Source MAC (SA)	6 bytes	MAC of sender
802.1Q tag (optional)	4 bytes	Optional vlan tag. Starts with 0x8100 to mark 802.1Q mode in type location.
Type or Length	2 bytes	Layer three type OR length if smaler then 1536 bytes.
Data	46 - 1500 bytes	Payload
Frame check sequence (FCS)	4 bytes	32 bit CRC Checksum

IPv4 Header

Field	Field Length	Description
Version	4 bits	IP Version, always four
Internet Header Length (IHL)	4 bits	Length of the header
Service Type	8 bits	Desired QOS information (DSCP and ECN)

Field	Field Length	Description
Total Length	2 bytes	Packet length, including this header
Identification	2 bytes	A unique ID
Flag	3 bits	fragmentation behaviour
Fragment Offset	13 bits	
TTL	1 byte	TTL, decreased by every router by one.
Protocol	1 byte	Layer four type
Header Checksum	2 bytes	
Options (optional)	16 bytes	
Padding	max. 31 bits	Pad to the nearest 32 bit boundary

TCP Segment

Field	Field Length	Description
Source Port	2 bytes	
Destination Port	2 bytes	
Squence Number	4 bytes	Unique Number for this Segment
Acknowledgement Number	4 bytes	Next expected sequence number, acknowledge all prior Segments.

Field	Field Length	Description
Header Lenght	4 bits	Header size in multiples of 4 bytes, sometimes also called Data Offset.
Reserved	3 bits	N/A
Flags	9 bits	Control Flags like SYN, ACK, FIN, RST and Flags for congestion control.
Window size	2 bytes	bytes sender is currently willing to receive
Checksum	2 bytes	Header Checksum
Urgent Pointer	2 bytes	Points to the last 'urgent' byte in the Segment, used when URG flag is set.
Options	0 - 320 bits	The Size is determined by Header length. TODO:
Data	variable	

UDP Segment

Field	Field Length	Description
Source Port	2 bytes	
Destination Port	2 bytes	
Length	2 bytes	Length of the whole Segment
Checksum (optional)	2 bytes	Checksum of the whole Segment

Field	**Field Length**	**Description**
Data	variable	

To Sort and Misc

Command	**Description**
# telnet 1.2.3.4 23	Telnet to `1.2.3.4` using port `23`
# disconnect	Disconnect background telnet session
# ssh -l h.acker 1.2.3.4	SSH to `1.2.3.4` using `h.acker` user
(config-if)# duplex {full, auto}	Set duplex mode or set it to autonegotiation.
(config-if)# speed {100, auto}	Set speed or set it to autonegotiation.

The following additional guidelines are commands and their descriptions:

Configure Networking

The following includes basic configure networking commands and their descriptions:

Enter interface configuration mode: (config)# interface g1/0

Human-readable link description: (config-if)# description Link to Some host

Add IPv4 address to interface: (config-if)# ip address 10.23.42.5 255.255.0.0

Add IPv6 address to interface: (config-if)# ipv6 address 2001:41d0:8:e115::ccc/64

Overwrite MAC address: (config-if)# mac address 1234.5678.90AB

Remove MAC overwrite: (config-if)# no mac address

Add IPv6 address based on MAC to interface: (config-if)# ipv6 address 2001:41d0:8:e115::/64 eui-64

Get IPv4 address via dhcp: (config-if)# ip address dhcp

Get IPv6 address (and default route) via autoconfig: (config-if)# ipv6 address autoconfig [default]

Set hostname transmitted as dhcp client to SW2: (config-if)# ip dhcp client client-id asccii SW2

Configure both interfaces at once: (config)# interface g1/0 - 2

En- or Disable interface. Often shutdown is the default: (config-if)# [no] shutdown

Set 10.23.42.1 as the default gateway: (config)# ip default-gateway 10.23.42.1

Add static route via next hop or interface: (config)# ip route 10.20.30.0 255.255.255.0 {1.2.3.4,e0/0} [ad]

You can also set both: (config)# ipv6 route 2001:41d0:8:e115::/64 [g1/1] [next hop]

Create a static host entry on this device: (config)# ip host the-space.agency 178.32.222.21

Globally enable ipv6 routing: (config)# ipv6 unicast-routing

Basic Network Troubleshooting

Show interfaces mac, bandwidth, mtu, packet stats, etc.: # show interfaces [if-name]

Show routes and how they were learned: # show ip[v6] route [static]

Show interfaces ip/arp/icmp/nd... configuration: # show ip[v6] interface [if-name]

Only show ip, status, and operational status: # show ip[v6] interface brief [if-name]

Similar to show ip int brief, w/ cidr, w/o ok/method: # show protocols [if-name]

Show the MAC address table of a switch: # show mac-address-table

Clear the dynamically learned mac address table entries: # clear mac address-table [dynamic]

Show {ip,ipx,appletalk}-mac bindings: # show arp

Show ip-mac bindings: # show ip arp [{ip, mac, if-name}]

Remove arp entry for ip: # clear [ip] arp 192.168.1.1

Show debug messages when receiving/sending arp packets: # debug arp

Disable all previously enabled debugs: # undebug all

Show neighbor discovery table cache: # show ipv6 neighbors

Troubleshoot Networks with Span

Define SPAN #23 input as g1/1: (config)# monitor session 23 source interface g1/1 {rx,tx,both}

Define SPAN #23 output as g1/2: (config)# monitor session 23 destination interface g1/2

Show all configured SPANs: # show monitor

Port Security

En/Disable port-security: (config-if)# [no] switchport port-security

Number of allowed MACs: (config-if)# switchport port-security maximum 1

Manually allow a MAC on this port: (config-if)# switchport port-security mac-address 1234.5678.9abc

Allow learning of connected macs until mac reached: (config-if)# switchport port-security mac-address sticky

Shutdown port when another device gets connected: (config-if)# switchport port-security violation shutdown

Re-enable if after port-security violation: (config-if)# shutdown (config-if)# no shutdown

Re-enable if automatically after the problem is fixed: (config)# errdisable recovery cause psecure-violation

Re-check every 42 seconds (min 30, default 300): (config)# errdisable recovery interval 42

Port security terms of violation:

- Protect: drops packets, no alerts
- Restrict: drops packets, security violation count
- Shutdown: shuts down the port (default)

Troubleshooting Port Security

Port status, violation mode, max/total MACs and more: # show port-security [interface g1/1]

Secure MACs on ports: # show port-security address

Check if auto-recovery is enabled (disabled by default): # show errdisable recovery

Layer2 Switch Vlan Config

[delete vlan or] create vlan and enter config-vlan mode: (config)# [no] vlan 23

Name this vlan TelephoneSanitizer: (config-vlan)# name TelephoneSanitizer

Make frames out this port untagged: (config-if)# switchport mode access

Make frames out this port tagged by default: (config-if)# switchport mode trunk

Sometimes the default is ciscos old isl: (config-if)# switchport trunk encapsulation dot1q

Except for vlan 256, which remains untagged: (config-if)# switchport trunk native vlan 256

Layer3 Switch Vlan Config

Enter interface config mode: (config)# interface vlan 23

Set device ip in vlan 23: (config-if)# ip address 1.2.3.4 255.255.255.0

Virtual interfaces are disabled by default: (config-if)# no shutdown

Delete vlan 23: (config)# no vlan 23

Router (on a Stick) Vlan Config

Create subinterface g1/1.10 on g1/1: (config)# interface g1/1.10

Enable ieee 802.1Q vlan tagging with vlan 10 on the subinterface: (config-subif)# encapsulation dot1q 10

Show vlans and their trunk interfaces: # show vlans

Troubleshoot Vlans on a Switch

Show vlan settings for all switch ports: # show vlan [{id 23, name TelephoneSanitizer}] [brief]

Verify mode and vlan of g1/1: # show interfaces g1/1 switchport

Show trunk settings and state: # show interfaces g1/1 trunk

Quick way to search the running config: # show run interface vlan 1

Show trunk mode / access vlan: # show interface status

Show current DTP mode for g1/1: # show dtp interface g1/1

STP

Spanning Tree Protocol (STP) (802.1D) blocks ports that have repetitive links in order to prevent layer 2 loops and broadcast storms.

Make this device the primary/secondary root bridge: (config)# spanning-tree vlan 1 root {primary, secondary}

Enable bpdu guard for all portfast enable interfaces: (config)# spanning-tree portfast bpduguard default

Enable portfast for all non-trunk interfaces: (config)# spanning-tree portfast default

Enable gpduguard on this interface: (config-if)# spanning-tree bpduguard enable

Enable portfast on this interface: (config-if)# spanning-tree portfast

Enable root guard on this interface: (config-if)# spanning-tree guard root

Troubleshoot STP

Who's the root and how do I get there? # show spanning-tree [vlan 1]

Is global portfast/bpduguard configured? # show spanning-tree summary

Is portfast/bpduguard configured on this interface? # show running-config interface g1/1

Is portfast active on this interface? # show spanning-tree interface g1/1 portfast

Etherchannel (Link Aggregation)

Configure g1/1 and g1/2 at the same time: (config)# interface range g1/1 - 2

Add both interfaces to etherchannel 1 (PAgP): (config-if-range)# channel-group 1 mode {auto, desirable}

Add both interfaces to etherchannel 1 (LACP): (config-if-range)# channel-group 1 mode {active, passive}

Add both interfaces to etherchannel 1 (Static): (config-if-range)# channel-group 1 mode on

Configure virtual interface for etherchannel 1: (config)# interface port-channel 1

Put etherchannel 1 in trunk mode: (config-if)# switchport mode trunk

Add tagged vlans 10,20,30 on etherchannel 1: (config-if)# switchport trunk allowed vlan 10,20,30

Troubleshoot Etherchannel (Link Aggregation)

Includes the combined bandwidth and members as extra info: # show interface port-channel 1

Show etherchannel protocols and members as a list: # show etherchannel summary

Show per member state and stats: # show etherchannel port-channel 1

Configure a Serial

Layer 1 link speed is ordered by a CSU/DSU, in a lab without an external CSU/DSU and using a DTE (Data Termianl Equipment) cable and DCE (Data Communications Equipment) cable.

Configure interface serial 1/0: (config)# interface serial 1/0

Set clock rate on DCE router side to 128 kbps: (config-if)# clock rate 128000

Verify clock rate for serial interface 1/0: (config)# show controllers serial 1/0

ACLs

Create ACL #23 or append a rule to ACL #23, allow 1.2.x.x: (config)# access-list 23 permit 1.2.3.4 [0.0.255.255]

Delete entire ACL #23: (config)# no access-list 23

Renumber ACL Rules, put first on #5, increment by 10: (config)# ip[v6] access-list resequence local_only 5 10

Create ACL and/or enter config mode for ACL #23: (config)# ip access-list {standard, extended} 23

Create ACL and/or enter config mode for ACL 'local_only': (config)# ip access-list {standard, extended} local_only

Append rule to standard ACL 'local_only': (config-std-nac1)# permit 10.20.30.0 0.0.0.255

Append rule to ACL at sequence number 5: (config-std-nac1)# 5 permit 10.20.30.0 0.0.0.255

Remove rule with sequence# from ACL: (config-std-nac1)# no <sequence#>

Interface ACLs

Enter if-config mode for g1/1: (config)# inter g1/1

Apply ACL #23 to outgoing packets, not send by the router: (config-if)# ip access-group 23 out

Apply ACL #42 to incoming packets: (config-if)# ip access-group 42 in

Overwrite the used ACL, only one ACL per if + proto + direction!: (config-if)# ip access-group local_only in

The v6 syntax of course differs...: (config-if)# ipv6 traffic-filter 23 out

Show ACLs on g1/1 (When none set shows not set for v4 and nothing for v6): # show ip interface g1/1 | incl access list

Troubleshooting ACLs

Show all configured ACLs: # show [ip[v6]] access-lists

Display all rules in ACL #10 and how often they matched: # show access-list 10

NAT

Local addresses are inside the network. Global addresses are outside the network.

- Inside local: IP address assigned to a host inside the newtork, non-routable
- Inside global: IP address assigned by Network Information Center or ISP, routable
- Outside local: IP address of a remote host as it appears inside the network, non-routable
- Outside global: IP address of a remote host assigned by the host owner, routable

Enter if-config mode for g1/1: (config)# int g1/1

Configure 1.2.3.4/28 on g1/1: (config-if)# ip address 1.2.3.4 255.255.255.240

Packets going out, need to change their src, incoming their dest ip: (config-if)# ip nat outside

Enter if-config mode for g1/2: (config)# int g1/2

Configure 10.10.23.1/24 on g1/2: (config-if)# ip address 10.10.23.1 255.255.255.0

Packets going out, need to change their dest, incoming their src ip: (config-if)# ip nat inside

SNAT

SNAT - statically map an internal ip 1:1 to an external ip: (config)# ip nat inside source static 10.10.23.2 1.2.3.5

DNAT

Create an ACL identifying 10.10.23/24: (config)# access-list 42 permit 10.10.23.0 0.0.0.255

Create an IP Address Pool for NATing: (config)# ip nat pool POOL 1.2.3.5 1.2.3.10 netmask 255.255.255.240

DNAT IPs matching ACL #42 1:1 with IPs from nat pool 'POOL': (config)# ip nat inside source list 42 pool POOL

PAT

Create an ACL identifying 10.10/16: (config)# access-list 10 permit 10.10.0.0 0.0.255.255

PAT IPs matching ACL #10 many:1 with g1/1s public IP: (config)# ip nat inside source list 10 interface g1/1 overload

Troubleshooting NAT

Show nat table entries if any: # show ip nat translations

Show translations are actually used and interfaces are marked in/out correctly: # show ip nat statistics

Clear dynamic translations. Doesn't mess with SNAT!: # clear ip nat translation {ip, *}

DHCP Server

Don't distribute these IPs in leases: (config)# ip dhcp excluded-address 10.30.4.1 10.30.4.100

Create and/or enter dhcp config for pool 'PCs': (config)# ip dhcp pool PCs

Define pool addresses: (dhcp-config)# network 10.30.4.0 /24

Define default-gateway to be distributed in the leases: (dhcp-config)# default-router 10.2.1.1

Lease validity time: (dhcp-config)# lease

Enter interface config mode on client-facing interface: (config)# int g1/1

Relay DHCP Requests to this host: (config-if)# ip helper-address 192.168.1.1

Troubleshooting DHCP

Show dhcp lease information: # show dhcp lease

Show pool size and addresses in use: # show ip dhcp pool

Show which mac got which ip: # show ip dhcp binding

See if ip dhcp exclude-address / pool stuff is wrong: # sh run | section dhcp

See if ip helper-address is wrong: # sh run int g1/1

HSRP

Join HSRP Group: (config-if)# standby [group-number] ip (optional) Set prio of this router: (config-if)# standby [group-number] priority

(optional) Preempt other routers when this router becomes active: (config-if)# standby [group-number] preempt

(optional) Set HSRP Version: (config-if)# standby {1,2}

Troubleshooting HSRP

HSRP Groups, their VIPs, state, active router, standby router, preemption: # show standby

SLAs

Create ip sla test #23 and enter its config mode: (config)# ip sla 23

Define icmp-echo test: (config-ip-sla)# icmp-echo 1.2.3.4

Frequency in seconds: (config-ip-sla)# frequency 42

Start test #23 now and until manually stopped: (config)# ip sla schedule 23 life {forever, seconds} start-time now

Troubleshooting SLAs

Show all configured ip sla configs: # show ip sla configuration

Show sla results: # show ip sla statistics

Device Management

Set hostname to R1: (config)# hostname R1

Set enable password: (config)# enable password

Same but with hashing: (config)# enable secret

Very weak encryption of passwords: (config)# service password-encryption

Copy something from flash to tftp. Wizard asks for details. It works both ways: # copy flash0: tftp:

# copy running-config startup-config: # write

# erase startup-config: # write erase

Restart the device and load the startup-config: # reload

Copy running-config to a tftp server. (interactive): # copy running-config tftp:

Merge source config into the running config: # copy running-config

Initial configuration dialog: # setup

ios, bootloader and hardware infos, uptime, configuration register: # show version

- CEH Cheat Sheet
- C.I.S.S.P. Cheat Sheet
- CompTIA Security + Cheat Sheet
- CompTIA A+ Cheat Sheet

Firmware Management

Boot filename.bin from flash memory: (config)# boot system flash:filename.bin

Boot filename.bin from tftp: (config)# boot system tftp://10.20.30.40/filename.bin

Boot ROM monitor as a backup: (config)# boot system rom

Set the 16bit Configuration Register value used after reboot: (config)# config-register 0x2342

Lists available file systems: # show file systems

List fs content and free space: # show flash0:

License Management

Save a copy of all licenses: # license save flash:licenses.lic

Install a license: # license install flash0:license.xml

Activate evaluation right-to-use license: (config)# license boot module technology-package

Reboot to activate the package and right to use license: # reload

Deactivate a technology-package: (config)# license boot module technology-package disable

Reboot without that technology-package: # reload

Remove license from the license storage: # license clear

Remove the no longer needed line from the config: (config)# no license boot module technology-package disable

Active licenses: # show licenses

Technology pack and feature licenses supported: # show license feature

Product id and serial number needed to order licenses: # show license udi

Reset Password

Show the configuration register in rom monitor: > confreq

Set the configuration register in rom monitor to not load startup-conf: > confreq 0x2142

Reboot in rom monitor: > reset

Overwrite forgotten password: (config)# enable secret foobar

Do load startup-config after boot again: (config)# config-register 0x2102

Telnet / Console

Make sure to include legal terms to sound smart: (config)# banner login "Insert snarky banner."

Set Login Banner: (config)# banner motd "Insert snarky banner."

Enter config mode for vty 0 to 4 (up to 15 allowed): (config)# line vty 0 4

Enter config mode for the console port: (config)# line console 0

Require login on telnet/console connection: (config-line)# login

Enable Telnet and set vty login password: (config-line)# password

Set ACL to limit inbound IPs allowed to access vty: (config-line)# access-class 10 in

Overwrite the used ACL, only one ACL per vty + direction!: (config-line)# access-class 42 in

Autologout after 10 Minutes: (config-line)# exec-timeout 10

Require login on telnet/console connection via local users: (config-line)# login local

Create local user with encrypted password: (config)# username h.acker secret C1sco123

SSH

Required to generate SSH keys: (config)# hostname Fooba

Required to generate SSH keys: (config)# ip domain-name example.com

Generate keys like it's 1995! Potentially takes forever: (config)# crypto key generate rsa modulus 2048

Force SSHv2: (config)# ip ssh version 2

Force ssh, disable telnet: (config-line)# transport input ssh

SSH version, timeout time, auth retries: # show ip ssh

List of active connections: # show ssh

Clock

Show time and date: # show clock

Update clock: (config)# clock set 23:50:42 10 Jan 2017

Update timezone to EST: (config)# clock timezone EST 0

Configure upstream ntp server: (config)# ntp server 10.20.30.40

Enable ntp server: (config)# ntp master [stratum]

ntp connections: # show ntp associations

Disable Unused Services

Show open ports: # show control-plane host open-ports

Stop the http server (but not https): (config)# no ip http server

Stop CDP: (config)# no cdp enable

Radius

Local backup user: (config)# username password

Enable aaa services: (config)# aaa new-model

Add and define Radius conf: (config)# radius server

Use this hostname/ip of server: (config-radius-server)# address ipv4 [auth-port]

Radius PSK: (config-radius-server)# key

Create authentication group: (config)# aaa group server radius

Using the radius config: (config-sg-radius)# server name

Allow that group and local users in: (config)# aaa authentication login group local

TACACS+

Local backup user: (config)# username password

Enable aaa services: (config)# aaa new-model

Add and define TACACS conf: (config)# tacacs server

Multiple possible: (config)# aaa group server tacacs+

Allow that group and local users in: (config)# aaa authentication login group local

Syslog

Log to this syslog server (name or ip): # logging 10.20.30.40

Only log messages with min. informational sev: # logging trap informational

SNMP

Contact email: (config)# snmp-server contact admin@example.com

Where is the device: (config)# snmp-server location RZ-Hamburg

Add community: (config)# snmp-server community [ro, rw]

SNMP notifications recipient: (config)# snmp-server host 10.20.30.4

CDP - Cisco Discovery Protocol

Enables cdp globaly and on all interfaces (default): # [no] cdp run

Enable cdp on an interface: # (config-if)# [no] cdp enable

List connected cisco devices (name, local/remote port, [ip] ..): # show cdp neighbors [detail]

LLDP - Link Layer Discovery Protocol

Enables lldp globaly and on all interfaces: # [no] lldp run

Enable lldp packet transmission on interface: (config-if)# [no] lldp transmit

Enable lldp packet reception on interace: (config-if)# [no] lddp receive

PPP

Create users for pap auth: (config)# username fnord password pass

Baud rate. Only on DCE cable: (config-if)# clock rate 125000

Logical speed used for routing cost calc, RSVP: (config-if)# bandwidth 125

Default is HDLC: (config-if)# encapsulation ppp

Require remote to authenticate via pap: (config-if)# ppp authentication pap

Authenticate to remote pap: (config-if)# ppp pap sent-username fnord password pass

Required for CHAP, used as chap client username: (config)# hostname routy1

Create users for chap auth for routy2: (config)# username routy2 password foobar

Remove in favor of chap: (config-if)# no ppp authentication pap

Remove in favor of chap: (config-if)# no ppp pap sent-username fnord password pass

Require remote to authenticate via chap: (config-if)# ppp authentication chap

Disclaimer: All data and information provided on this site is for informational purposes only. This site makes no representations as to accuracy, completeness, correctness, suitability, or validity of any information on this site & will not be liable for any errors, omissions, or delays in this information or any losses, injuries, or damages arising from its display or use. All information is provided on an as-is basis.