Cheatography

Cisco IOS 16 Router Config Cheat Sheet

by cheerio-cheeto via cheatography.com/206203/cs/44052/

brief overview of interface settings

`show ip interface brief`	can also be typed as `sh ip int br`

interface, ip address, OK?, Method, Status, Protocol

example:

```
Gigabi tEt hernet1 10.10.1 0.10 YES NVRAM up up
```

TFTP config

`copy tftp run`	configure the router via TFTP (`copy tftp runnin g-c onfig`)
"address or name of remote host []?"	input ip address of remote host
"source filename []?"	name of file of TFTP server
"destination filename [running-config]?"	hit `Enter`; overwrite running config

Reinstalling config to router from remote IP address using Trivial File Transfer Protocol (TFTP);

remember to `copy run start` to maintain config across reboots!;

Note: *TFTP is an insecure protocol (no authentication, no encryption of data in transit)*; use **SCP (Secure File Copy) in production envs instead, which uses SSH (Secure Shell) protocol**

Audit Router Config

`cd`	change to home dir
`mkdir -p rtaudit.1`	make sub-dir for this lab (`-p` = no errors if it already exists
`cd rtaudit.1`	change to that sub-dir
`cp /srv/t ftp /ro ute rCo nfi gFile router Nam e -a udit01`	copy the TFTP'd config file for <router> from TFTP server dir to current dir with name `<ro ute rNa me- aud it0 1>`
`rat ./rout erN ame -au dit01`	run `rat` against that file

Auditing our initial config using CIS Router Assessment Tool (RAT).

Note: RAT is deprecated, but sufficient for this exercise. CIS now has CIS-CAT Pro which requires membership fee.

Other audit tools such as `Tenable's Nessus` can also perform CIS assessments against router configs.

Cisco IOS 16 router config cmds

Cisco IOS 16 router config cmds (cont)

^Ctrl + Z	
aaa new-model	
area 0 authen tic ation messag e-d igest	
banner motd #Autho rized access onlyl!#	
clock timezone utc 0	
configure replace tftp:/ /10.10.10.5/ res tor e/r out erN ame -ba se force	
configure terminal	
copy runnin g-c onfig startu p-c onfig	
copy startu p-c onfig tftp	
copy tftp runnin g-c onfig	
crypto key generate rsa genera l-keys modulus 2048	

disable	exit completely out of Config mode
enable	access Enable mode, elevated priv
enable secret placeh older	set password on `Enable` mode with `placeh older` as password
exclude	like `grep -v`; also `e`
exec-t imeout 0 0	disable timeout of Telnet sessions; **insecure** only for class effeciency
exit	exit Line Config mode; (`CTRL` + `Z` to exit Config mode completely)
hostname routerName	set hostname; prompt immediately changes
include	simple pattern searching, like `grep`; also `i`
int g1	edit definition for interface GigabitEthernet 1
int gig 1	interface Gigabit 1
int gigabi tEt hernet 1	select first gigabitEthernet interface
int loop 0	config interface loopback 0
int loopback 0	create loopback interface
ip address 10.10.1 0.13 255.25 5.255 .0	assign ip and specific subnet mask
ip domain -name DOMAIN.com	config router's domain name (prereq for creating crypto keys)

By **cheerio-cheeto** cheatography.com/cheerio-cheeto/	Not published yet. Last updated 8th August, 2024. Page 2 of 5.	Sponsored by **Readable.com** Measure your website readability! https://readable.com

Cheatography

Cisco IOS 16 Router Config Cheat Sheet

by cheerio-cheeto via cheatography.com/206203/cs/44052/

Cisco IOS 16 router config cmds (cont)

`ip ospf messag e-d ige st-key 1 md5 somese cre tkey`	add MD5 digest key to OSPF packets - with passphrase "somese-cretkey"
`ip ssh version 2`	enforce SSHv2 only (v1 is subject to MITM attacks)
`line console 0`	config the console
`line vty 0 4`	config network connec-tions to *virtual teletype/-terminal lines* (ie Telnet)
`logging host <Wi ndows Syslog Server ip>`	send logs to syslog server
`logging source -in terface gig 1`	explicitly set source interface for syslog
`logging source g1`	set interface GigabitEt-hernet 1 as logging source
`logging synchr onous`	prevent log msgs from interrupting cmd entry
`logging trap debug`	log msgs at >= debug (severity debug or higher)
`login on-failure log`	log failed logins

Cisco IOS 16 router config cmds (cont)

`no ip proxy-arp`	dis
`no ip redirects`	dis cti
`no ip source -route`	dis ro
`no shutdown`	sta (by no
`no user admin`	re ac pa
`ntp source gig 1`	ex so NT
`rat ./< RAT aud itF ile Nam e>`	CI As (R
`router ospf 1`	cre *ro*
`show crypto key mypubkey rsa`	vie ke
`show ip interface brief`	int als br
`show run`	sh ru
`show run | i pas`	na inc *pa* ow
`show run | i enable`	se
`snmp-s erver trap-s ource gig1`	ex so SN
`stand 1 ip <ip addres s>`	se *ac*
`stand 1 priority 120`	se
`standby 1 authen tic ation md5 key-string PASSWO RD`	se ati PA

`login on-success log`	log successful logins
`network 10.10.10.0 0.0.0.255 area 0;network 10.10.1.0 0.0.0.255 area 0`	add network to routing process in area 0
`no ip direct ed- bro adcast`	disable directed broadcasts
`no ip domain lookup`	disable IP domain (ie DNS) lookups - else every typo will be read as hostname and router will try to Telnet

Sponsored by **Readable.com**
Measure your website readability!
https://readable.com

Cisco IOS 16 router config cmds (cont)

`standby 1 name CONFIGname`	name standby config `CONFIGname` (case-sensitive)
`standby 1 preempt`	after an outage, device configured as primary will "-preempt" ctrl required to regain desired state
`username user privilege 15 password pass`	create new user `user`, with password `pass`

initial config

```
enable
configure terminal
int gigabi tEt hernet 1
ip address <router ip> 255.25 5.255.0
no shutdown
hostname routerName
ip domain -name DOMAIN.com
crypto key generate rsa genera l-keys modulus 2048
exit
configure replace tftp:/ /<TFTP server IP> /re sto re/ rou ter Nam e-ba se force
copy runnin g-c onfig startu p-c onfig
disable
```

tasks:
- assign hostname
- enable over-network access, which requires:
1. login username and password
2. password for `enable` cmd
3. public/private key pair (to identify router to remote host for SSH)

remote connect TO router via TELNET

```
telnet <router ip>
<us ern ame>
<user passwo rd>
enable
<enable passwo rd>
```

show running config

`show run`	show router's running config
`show run | include pas`	narrow search by piping output to `include` and look for 'pas' (short for *password*)
`show run | i pas`	same as above, can shorten `include` to `i`
`show run | i enable`	searching for `enable`

- `include` command (`i`) does simple pattern matching, like `grep`
- Cisco IOS requires space before and after pipe `|`
- there is also `exclude`, similar to `grep -v` and can be shortened to `e`

remote connect TO router via SSH

```
ssh userna me@ <router ip addres s>
```

SSH is only available when RSA crypto keys have been previously generated; *keys CANNOT be imported via TFTP*

view RSA public keys generated

```
show crypto key mypubkey rsa
```

copy saved (startup) config to TFTP server

```
copy startu p-c onfig tftp
<TFTP Server IP>
```


Sponsored by **Readable.com**
Measure your website readability!
https://readable.com