

### 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:

```
GigabitEthernet1 10.10.1 0.10 YES NVRAM up up
```

### TFTP config

```
copy tftp run
```

configure the router via TFTP (`copy tftp running-config`)

"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/tftp/ro ute rCo nfi gFile router Name  
-a udit01
```

copy the TFTP'd config file for <router> from TFTP server dir to current dir with name <routerName-audit01>

```
rat ./routerName-audit01
```

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)

<code>^Ctrl + Z</code>	disable	exit completely out	
<code>aaa new-model</code>	enable	of Config mode use new model for AAA: uses user IDs and passwords	access Enable mode, elevated priv
<code>area 0 authentication message-digest</code>	enable secret place order	configure <i>OSPF Area 0</i> to use message-digest authentication	set password on Enable mode with placeh ol der as password
<code>banner motd #Authorized access only!#</code>	exclude	set a "message of the day" banner	like <code>grep -v;</code> also <code>e</code>
<code>clock timezone utc 0</code>	exec-timeout 0 0	set clock to UTC timezone	disable timeout of Telnet sessions;
<code>configure replace tftp://10.10.10.5/ restore/route-name -ba se force</code>	exit	router config file on TFTP server; will apply all necessary additions & deletions	<b>insecure</b> only for class efficiency exit Line Config mode; (CTRL + Z to exit Config mode comple- tely)
<code>configure terminal</code>	hostname routerName	config router from terminal (current window); <i>can also be written conf t</i>	set hostname; prompt immedi- ately changes
<code>copy runnin g-c onfig startu p-c onfig</code>	include	copies current config from volatile RAM to non-vo- latile RAM (NVRAM); saves current config to	simple pattern searching, like <code>g rep</code> ; also <code>i</code>
<code>copy startu p-c onfig tftp</code>	int g1	default name; also copy run start	edit definition for interface Gigabi- tEthernet 1
<code>copy tftp runnin g-c onfig</code>	int gig 1	copy saved (startup) config to TFTP server	interface Gigabit 1
<code>crypto key generate rsa genera l-keys modulus 2048</code>	int gigabitEthernet 1	config router via TFTP; also copy tftp run	select first gigabitEthernet interface
	int loop 0	create public/pr- ivate asymmetric key pair to enable SSH connections	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)



Cisco IOS 16 router config cmds (cont)	Cisco IOS 16 router config cmds (cont)	
ip ospf message-digest-key 1 md5 somese cretkey	add MD5 digest key to OSPF packets - with passphrase "somesecretkey"	dis
ip ssh version 2	enforce SSHv2 only (v1 is subject to MITM attacks)	dis
line console 0	config the console rat ./< RAT aud itF ile Nam e>	dis
line vty 0 4	config network connections to virtual teletype terminal lines (ie Telnet)	dis
logging host <Windows Syslog Server ip>	send logs to syslog server	dis
logging source -interface gig 1	explicitly set source interface for syslog	dis
logging source g1	set interface GigabitEthernet 1 as logging source	dis
logging synchronous	prevent log msgs from interrupting cmd entry	dis
logging trap debug	log msgs at >= debug (severity debug or higher)	dis
login on-failure log	log failed logins	dis

login on-success log	log successful logins
network 10.10.10.0 0.0.0.255 area 0;network 10 .10.1.1.0 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



By **cheerio-cheeto**  
[cheatography.com/cheerio-cheeto/](http://cheatography.com/cheerio-cheeto/)

Not published yet.  
 Last updated 8th August, 2024.  
 Page 3 of 5.

Sponsored by **CrosswordCheats.com**  
 Learn to solve cryptic crosswords!  
<http://crosswordcheats.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 gigabitEthernet 1
```

```
ip address <router ip> 255.255.255.0
```

```
no shutdown
```

```
hostname routerName
```

```
ip domain-name DOMAIN.com
```

```
crypto key generate rsa general-keys modulus 2048
```

```
exit
```

```
configure replace tftp://<TFTP server IP>/restitute/routerName-base force
```

```
copy running-config startup-config
```

```
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>
```

```
<username>
```

```
<password>
```

```
enable
```

```
<enable password>
```

### show running config

```
show run
```

show router's running config

```
show run | include password
```

narrow search by piping output to include and look for 'password' (short for password)

```
show run | include password
```

same as above, can shorten include to i

```
show run | include 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 username@<router ip address>
```

**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 startup-config tftp
```

```
<TFTP Server IP>
```

