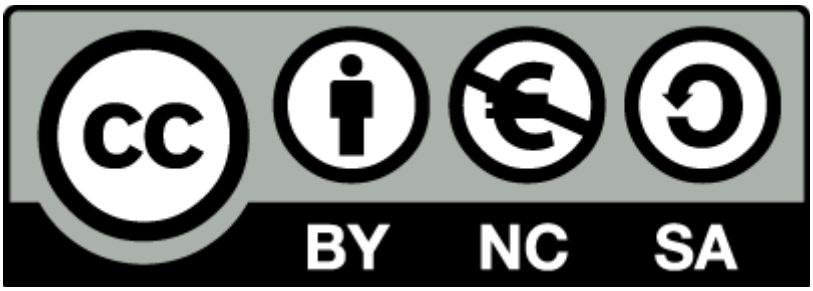
1 Intro

Hi. I am Panteleimon Sarantos (You can call me Pantelis) and I made this list of commands for the Cisco Routers and Switches.

2 License

This work is licensed under the Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-sa/4.0/ or send a letter to Creative Commons, PO Box 1866, Mountain View, CA 94042, USA.



3 Table of Contents

1 Intro....1
2 License....1
3 Table of Contents....1
4 Save Progress....3
5 Router....3
5.1 Security....3
5.1.1 Management Security....3
5.1.1.1 Enable CLI Password....3
5.1.1.2 Enable Password after enable – EXEC – Global Configuration....3
5.1.1.3 Enable Telnet Password....3
5.1.1.4 SSH....4
5.1.1.4.1 SSH Configuration....4
5.1.1.4.2 More SSH Settings....4
5.1.2 Access Lists Security....4
5.1.2.1 Standard ACLs....4
5.1.2.1.1 Numbered Standard ACLs....4
5.1.2.1.2 Named Standard ACLs....4
5.1.2.1.3 Modify Named ACLs....5
5.1.2.2 Extended ACLs....5
5.1.2.2.1 Numbered Extended ACLs....5
5.1.2.2.2 Named Extended ACLs....5

5.1.2.2.3 Modify Numbered Extended ACLs....5
5.1.2.2.4 Modify Named Extended ACLs....6
5.1.2.3 Access Lists Info....6
5.1.2.3.1 More SSH Settings....6
5.2 IP....6
5.2.1 Assign IP to Interface....6
5.2.1.1 IPv4....6
5.2.1.2 IPv6....6
5.3 Routing....6
5.3.1 OSPF....6
5.3.2 EIGRP....7
5.3.3 RIPv2....7
5.4 InterVLAN Routing....7
5.5 DHCP....7
5.6 NAT....8
5.6.1 Static NAT....8
5.6.1.1 Configuration....8
5.6.1.2 Assign NAT to Interfaces....8
5.6.2 Dynamic NAT....8
5.6.2.1 Configuration....8
5.6.3 PAT....8
5.6.4 General....8
5.6.4.1 Verify Configuration....8
5.6.4.2 Clear Static NAT....8
5.6.4.3 Clear Dynamic NAT....9
5.6.4.4 Remove the public NAT pool....9
5.6.4.5 Remove the NAT translation from inside source list to outside pool....9
5.7 General Settings....9
5.7.1 Date and Time Settings....9
5.7.2 Prevent unwanted DNS Lookups....9
6 Switch....9
6.1 Security....9
6.1.1 Management Security....9
6.1.1.1 Enable CLI Password....9
6.1.1.2 Enable Encrypted Password after enable – EXEC – Global Configuration 10
6.1.1.3 Enable Telnet Password....10
6.1.1.3.1 SSH....10
6.1.1.3.1.1 SSH Configuration....10
6.1.1.3.1.2 More SSH Settings....10
6.1.2 Port Security....10
6.1.2.1 Close unused physical ports....10
6.1.2.2 Configure Basic Port Security....11
6.2 VLAN....11

6.2.1 Create a VLAN....11
6.2.2 Assign Physical Access Ports to VLAN....11
6.2.3 Set Physical Ports to Trunk....11
6.2.4 Set Physical Ports to Native Trunking....11
6.2.5 Assign IP to VLAN....11
6.2.6 Verify VLAN....12
6.3 IP....12
6.3.1 Prevent unwanted DNS Lookups....12
6.3.2 Default Gateway....12
6.4 General Settings....12
6.4.1 Date and Time Settings....12
6.4.2 Log In Banner Message....12

4 Save Progress

To save the following commands to the startup-config run:
en
conf t
wr

#or
do wr

5 Router

5.1 Security

5.1.1 Management Security

5.1.1.1 Enable CLI Password

en
conf t
line con 0
password conpass

5.1.1.2 Enable Password after enable – EXEC – Global Configuration

en
conf t
enable secret password

5.1.1.3 Enable Telnet Password

en
conf t
line vty 0 15

password telnetpass
login

5.1.1.4 SSH

5.1.1.4.1 SSH Configuration

en
conf t
ip domain-name isp.gr
username admin privilege 15 secret sshpass
line vty 0 15
transport input ssh
login local
exit
crypto key generate rsa
end
show ip ssh

5.1.1.4.2 More SSH Settings

en
conf t
ip ssh time-out 75
ip ssh authentication-retries 2

5.1.2 Access Lists Security

5.1.2.1 Standard ACLs

5.1.2.1.1 Numbered Standard ACLs

en
conf t
access-list 1 remark Allow R1 LANs Access
access-list 1 permit 192.168.10.0 0.0.0.255
access-list 1 permit 192.168.20.0 0.0.0.255
access-list 1 deny any

en
conf t
interface g0/1
ip access-group 1 out

5.1.2.1.2 Named Standard ACLs

en
conf t
ip access-list standard BRANCH-OFFICE-POLICY
permit host 192.168.30.3

```
permit 192.168.40.0 0.0.0.255
end

en
conf t
int g0/1
ip access-group BRANCH-OFFICE-POLICY out
```

5.1.2.1.3 Modify Named ACLs

```
en
conf t
ip access-list standard BRANCH-OFFICE-POLICY
30 permit 209.165.200.224 0.0.0.31
40 deny any
end
```

5.1.2.2 Extended ACLs

5.1.2.2.1 Numbered Extended ACLs

```
en
conf t
access-list 100 remark Allow Web & SSH Access
access-list 100 permit tcp host 192.168.10.3 host 10.2.2.1 eq 22
access-list 100 permit tcp any any eq 80

en
conf t
interface g0/1
ip access-group 100 out
```

5.1.2.2.2 Named Extended ACLs

```
en
conf t
ip access-list extended WEB-POLICY
permit tcp 192.168.30.0 0.0.0.255 host 10.1.1.1 eq 80
permit tcp 192.168.30.0 0.0.0.255 209.165.200.224 0.0.0.31 eq 80

en
conf t
interface S0/0/1
ip access-group WEB-POLICY out
```

5.1.2.2.3 Modify Numbered Extended ACLs

```
en
conf t
ip access-list extended 100
```

```
30 permit ip 192.168.10.0 0.0.0.255 192.168.30.0 0.0.0.255
end
```

5.1.2.2.4 Modify Named Extended ACLs

```
en
conf t
ip access-list extended WEB-POLICY
30 permit ip 192.168.30.0 0.0.0.255 192.168.10.0 0.0.0.255
end
```

5.1.2.3 Access Lists Info

```
en
show access-lists
```

5.1.2.3.1 More SSH Settings

```
en
conf t
ip ssh time-out 75
ip ssh authentication-retries 2
```

5.2 IP

5.2.1 Assign IP to Interface

5.2.1.1 IPv4

```
En
conf t
int g0/0
ip add 192.168.1.1 255.255.255.0
no shut
```

5.2.1.2 IPv6

```
en
conf t
ipv6 unicast-routing
int g0/0
ipv6 add 2001:db8:1:1::1/64
ipv6 add fe80::1 link-local
no shut
```

5.3 Routing

5.3.1 OSPF

```
en
conf t
```

```
router ospf 1
network 192.168.1.0 0.0.0.255 area 0
network 10.0.0.0 0.0.0.3 area 0
network 10.1.1.0 0.0.0.3 area 0
```

5.3.2 EIGRP

```
en
conf t
router eigrp 1
network 200.200.200.0 0.0.0.3
network 100.100.100.0 0.0.0.255
auto-summary
```

5.3.3 RIPv2

```
en
conf t
router rip
version 2
network 192.168.10.0
network 192.168.20.0
network 192.168.30.0
no auto-summary
```

5.4 InterVLAN Routing

```
interface g0/1.1
encapsulation dot1Q 1
ip add 192.168.1.1 255.255.255.0
interface g0/1.10
encapsulation dot1Q 10
ip add 192.168.10.1 255.255.255.0
interface g0/1.20
encapsulation dot1Q 20
ip add 192.168.20.1 255.255.255.0
exit
interface g0/1
no shut
```

5.5 DHCP

```
en
conf t
ip dhcp excluded-address 100.100.100.1
ip dhcp pool KATOSTARI
```

network 100.100.100.0 255.255.255.0
default-router 100.100.100.1

5.6 NAT

5.6.1 Static NAT

5.6.1.1 Configuration

en
conf t
ip nat inside source static <Private Address> <Public Address>
ip nat inside source static 192.168.1.20 209.169.200.225

5.6.1.2 Assign NAT to Interfaces

en
conf t
int g0/1
ip nat inside
int s0/0/1
ip nat outside

5.6.2 Dynamic NAT

5.6.2.1 Configuration

en
conf t
access-list 1 permit 192.168.1.1 0.0.0.255
ip nat pool public_access 209.169.200.242 209.169.200.254 netmask 255.255.255.224
ip nat inside source list 1 pool public_access

5.6.3 PAT

en
conf t
access-list 1 permit 192.168.1.1 0.0.0.255
ip nat inside source list 1 interface serial 0/0/1 overload

5.6.4 General

5.6.4.1 Verify Configuration

en
show ip nat translations
show ip nat statistics

5.6.4.2 Clear Static NAT

en

```
conf t
no ip nat inside source static 192.168.1.20 209.169.200.225
```

5.6.4.3 Clear Dynamic NAT

```
en
clear ip nat translation *
clear ip nat statistics
```

5.6.4.4 Remove the public NAT pool

```
en
conf t
no ip nat pool public_access 209.169.200.225 209.169.200.230 netmask
255.255.255.248
```

5.6.4.5 Remove the NAT translation from inside source list to outside pool

```
en
conf t
no ip nat inside source list 1 pool public_access overload
```

5.7 VPN

5.7.1 Site to Site VPN

5.7.1.1 Activate securityk9 module.

```
en
conf t
license boot module c1900 technology-package securityk9
end
wr
reload
```

5.7.2 Configure IPsec Parameters on R1

5.7.2.1 ACL

```
en
conf t
access-list 110 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
```

5.7.2.2 ISAKMP Phase 1

```
en
conf t
crypto isakmp policy 10
encryption aes
authentication pre-share
```

group 2
exit
isakmp key cisco address 10.2.2.2

5.7.2.3 ISAKMP Phase 2

en
conf t
crypto ipsec transform-set VPN-SET esp-3des esp-sha-hmac
crypto map VPN-MAP 10 ipsec-isakmp
description VPN connection to R3
set peer 10.2.2.2
set transform-set VPN-SET
match address 110
exit

5.7.2.4 Configure the crypto map on the outgoing interface.

en
conf t
interface S0/0/0
crypto map VPN-MAP

5.7.3 Configure IPsec Parameters on R3

5.7.3.1 ACL

en
conf t
access-list 110 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255

5.7.3.2 ISAKMP Phase 1

en
conf t
Crypto isakmp policy 10
encryption aes
authentication pre-share
group 2
exit
isakmp key cisco address 10.1.1.2

5.7.3.3 ISAKMP Phase 2

en
conf t
crypto ipsec transform-set VPN-SET esp-3des esp-sha-hmac
crypto map VPN-MAP 10 ipsec-isakmp
description VPN connection to R1
set peer 10.1.1.2

```
set transform-set VPN-SET
match address 110
exit
```

5.7.3.4 Configure the crypto map on the outgoing interface

```
en
conf t
interface S0/0/1
crypto map VPN-MAP
```

5.7.4 Verify the IPsec VPN

```
en
show crypto ipsec sa
```

5.8 General Settings

5.8.1 Date and Time Settings

```
en
clock set 16:45:00 Dec 8 2016
show clock
```

5.8.2 Prevent unwanted DNS Lookups

```
en
conf t
no ip domain-lookup
```

6 Switch

6.1 Security

6.1.1 Management Security

6.1.1.1 Enable CLI Password

```
en
conf t
line con 0
password conpass
login
logging synchronous
```

6.1.1.2 Enable Encrypted Password after enable – EXEC – Global Configuration

```
en
```

conf t
service password-encryption
enable secret pass

6.1.1.3 Enable Telnet Password

en
conf t
line vty 0 15
password telnetpass
login

6.1.1.3.1 SSH

6.1.1.3.1.1 SSH Configuration

en
conf t
ip domain-name isp.gr
username admin privilege 15 secret sshpass
line vty 0 15
transport input ssh
login local
exit
crypto key generate rsa
2048
ip ssh version 2
end
show ip ssh

6.1.1.3.1.2 More SSH Settings

en
conf t
ip ssh time-out 75
ip ssh authentication-retries 2

6.1.2 Port Security

6.1.2.1 Close unused physical ports

en
conf t
int f0/0 | int range f0/0 – 4
shut
do sh ip interface brief

6.1.2.2 Configure Basic Port Security

en

conf t
int f0/5
shut
switchport mode access
switchport port-security
switchport port-security mac-address xxxx.xxxx.xxxx
(switchport port-security maximum 2)
(switchport port-security mac-address sticky)
no shut
end
sh port-security int f0/5

6.1.3 Configure Basic Port Security Violation

en
conf t
int f0/5
switchport port-security violation [value]
[shutdown | restrict | protect]

6.2 VLAN

6.2.1 Create a VLAN

en
conf t
vlan 10
name Students
exit

6.2.2 Assign Physical Access Ports to VLAN

en
conf t
int range f0/1 – 24, g0/1 – 2
switchport access vlan 10

6.2.3 Set Physical Ports to Trunk

en
conf t
int g0/1
switchport mode trunk

6.2.4 Set Physical Ports to Native Trunking

en
conf t
int g0/1

switchport mode trunk
switchport trunk native vlan 99

6.2.5 Assign IP to VLAN

int vlan99
ip add 192.168.1.2 255.255.255.0
no shut

6.2.6 Verify VLAN

en
sh vlan brief

6.3 IP

6.3.1 Prevent unwanted DNS Lookups

en
conf t
no ip domain-lookup

6.3.2 Default Gateway

en
conf t
ip default-gateway 192.168.1.1

6.4 General Settings

6.4.1 Date and Time Settings

show clock detail
clock set 16:30:00 Mar 27 2017
do wr

6.4.2 Log In Banner Message

en
conf t
banner motd #
Some message #