Cisco Cheat Sheet

Basic Configuration

Initial Commands

Name the device:

```
Router# configure terminal
Router(config)# hostname [hostname]
```

Configure a banner:

```
R1(config)# banner motd $Autorized Access Only$
```

Save the Changes:

```
R1# copy running-config startup-config
```

Configure Interface IPv4:

```
R1(config)# interface gigabitethernet 0/0
R1(config-if)# description Link to LAN 1
R1(config-if)# ip address 192.168.10.1 255.255.255.0
R1(config-if)# no shutdown
```

-or-

```
R1(config)# interface serial 0/0/0
R1(config-if)# description Link to R2
R1(config-if)# ip address 209.165.200.225 255.255.255.252
R1(config-if)# clock rate 128000
R1(config-if)# no shutdown
```

Secure Management Access

```
R1(config)# enable secret class
R1(config)# line console 0
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# exit
R1(config)# line vty 0 4 ← depending on the number of VTYs!
R1(config-line)# password cisco
R1(config-line)# login
R1(config-exit)# exit
R1(config)# service password-encryption
```

VLAN

This chapter describes how to configure VLANs.

TODO

This subject needs some love, feel free to make a pull request via GitHub.

Access Control Lists

This chapter describes how to configure Access Control Lists (ACLs).

NOTE

Each ACL contains an implicit DENY at the end!

TODO

This subject needs some love, feel free to make a pull request via GitHub.

IPv6

This chapter describes how to configure IPv6.

IPv6 Autoconfiguration

NOTE

Autoconfiguration requires te least amount of configuration but makes it difficult to remember the IPv6 addresses. This method uses the MAC address of the device to create an IPv6 address with the `FE80::` prefix.

Begin by configuring the router. Enter the interface configuration mode and enable IPv6 on the interface.

```
R1(config)# ipv6 unicast-routing
R1(config)# interface FastEthernet0/0
R1(config-if)# ipv6 enable
```

Next, configure a link local address and a global unicast address on the interface. This example uses `eui-64` to reduce the configuration.

```
R1(config-if)# ipv6 address autoconfig
R1(config-if)# ipv6 add 2000::/64 eui-64
R1(config-if)# no shutdown
```

Verify the interface is *up* and has two IPv6 addresses.

```
R1>show ipv6 interface brief
```

IPv6 Static

Begin by configuring a static IPv6 address on the router

```
R1(config)# ipv6 unicast-routing
R1(config)# interface FastEthernet0/0
R1(config-if)# ipv6 enable
R1(config-if)# 2000::1/64
R1(config-if)# no shutdown
```

IPv6 Static Routing

Configuration commands for its static routing are similar to IPv4.

```
R1(config)# ipv6 unicast-routing
R1(config)# ipv6 route 2000:2::/64 2001::20
```

IPv6 Dynamic Routing

```
R1(config)# interface FastEthernet0/0
R1(config-if)# ipv6 address 2000:1::1/64
R1(config-if)# ipv6 rip Net1 enable
R1(config-if)# ipv6 enable
R1(config-if)# interface FastEthernet0/1
R1(config-if)# ipv6 address 2001::10/64
R1(config-if)# ipv6 rip Net1 enable
R1(config-if)# ipv6 enable
```

Spanning Tree

This chapter describes how to configure Spanning Tree.

Verify Spanning tree configuration

All:

```
S1# show spanning-tree
```

Per VLAN:

```
S1# show spanning-tree vlan 1
```

Discover layer 2 topology (*if cdp is enabled*):

```
S1# show cdp neighbours
```

Configure root bridge

Method 0: Do nothing and let the root bridge be determined by the lowest MAC address.
Method 1: Set specific switch as (secondary) root bridge.

```
S1(config)# spanning-tree VLAN 1 root primary
```

-or-

```
S1(config)# spanning-tree VLAN 1 root secondary
```

Method 2: Give priority numbers to all switches.
Lowest becomes root bridge (needs to be a multiple of 4096).

```
S1(config)# spanning-tree VLAN 1 priority 24576
```

Rapid spanning tree mode

Enable:

```
S1(config)# spanning-tree mode rapid-pvst
```

PortFast and BPDU guard for access ports

Method 1: Per interface:

```
S1(config)# interface f0/1
S1(config-if)# spanning-tree portfast
S1(config-if)# spanning-tree bpduguard enable
```

Method 2: Enable globally for nontrunking interfaces:

```
S1(config)#spanning-tree portfast default
Enable bpduguard on portfast enabled ports.
S1(config)#spanning-tree portfast bpduguard default
```

Link Aggregation

This chapter describes how to configure port channels and to apply and configure the Link Aggregation Control Protocol (LACP).

Configure Interfaces

```
S1(config)# interface range fe0/1-2
S1(config-if-range)# shutdown
S1(config-if-range)# channel-group 1 mode active
S1(config-if-range)# exit
S1(config)# interface port-channel 1
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk allowed vlan 1,2,20
```

Verify Link Aggregation

```
S1# show interface port-channel1
S1# show etherchannel summary
S1# show etherchannel port-channel
S1# show interfaces f0/1 etherchannel
```

More information about Link Aggregation Control Protocol (LACP) (802.3ad) for Gigabit Interfaces.

OSPF

This chapter describes how to configure OSPF.

Single-Area OSPF

```
R1(config)# interface GigabitEthernet0/0
R1(config-if)# bandwidth 1000000
R1(config-if)# exit
R1(config)# router ospf 10
R1(config-router)# router-id 1.1.1.1
R1(config-router)# auto-cost reference-bandwidth 1000
R1(config-router)# network 172.16.1.0 0.0.0.255 area 0
R1(config-router)# passive-interface g0/0
```

Single-Area OSPFv3

```
R1(config)# ipv6 router ospf 10
R1(config-router)# router-id 1.1.1.1
R1(config-router)# auto-cost reference-bandwidth 1000
R1(config-if)# interface GigabitEthernet 0/0
R1(config-if)# bandwidth 1000000
R1(config-if)# ipv6 ospf 10 area 0
```

Verifying Single-Area OSPF

NOTE

To verify Single-Area OSPFv3 please use the ipv6 command.

```
R1# show ip ospf neighbor
R1# show ip protocols
R1# show ip ospf
R1# show ip ospf interface
R1# show ip ospf interface brief
```

Multi-Area OSPF

NOTE

The same commands are used as for Single-Area OSPF, except there are more area's. Carefully look which device belong to which area.

Configure PPP

This chapter describes how to configure a PPP connection.

Basic PPP Configuration

```
R1(config)# interface Serial 0/0/0
R1(config-if)# encapsulation ppp
```

Basic PPP Compression

```
R1(config)# interface Serial 0/0/0
R1(config-if)# encapsulation ppp
R1(config-if)# compress predictor
```

Basic PPP Link Quality Control

```
R1(config)# interface Serial 0/0/0
R1(config-if)# encapsulation ppp
R1(config-if)# ppp quality 80
```

Basic PPP Link Quality Control

```
R1(config)# interface multilink 1
R1(config-if)# interface Serial 0/0/0
R1(config-if)# interface Serial 0/0/1
```

Basic PPP PAP Authentication

NOTE

The first command is the expected username and password which R3 will send!

```
R1(config)# username R3 secret class
R1(config)# interface s0/0/0
R1(config-if)# ppp authentication pap
R1(config-if)# ppp pap sent-username R1 password cisco
```

Basic PPP CHAP Authentication

NOTE

As opposed of PAP. CHAP passwords need to be identical

```
R1(config)# hostname Router1
Router1(config)# username Router 3 secret cisco
Router1(config)# interface s0/0/0
Router1(config-if)# ppp authentication chap
```

Troubleshoot PPP

```
R1# debug ppp packet R1# debug ppp negotiation
R1# debug ppp authentication R1# debug ppp error
```

Verifying PPP Connection

```
R1# show interface serial 0/0/0
R1# show ppp multilink
```

Security

This chapter explains how to secure devices

Commands to increase Acces Security

```
R1(config)# security paswords min-length 10
R1(config)# service password-encryption
R1(config)# line vty 0 4
R1(config)# exec-timeout 3 30
R1(config)# line console 0
R1(config)# exec-timeout 3 30
```

Enable Stronger Password Encryption

NOTE

There are two methods. With the first method you use the already encrypted passwords hash. algoritm-type does not work in Packet Tracer

```
First Methode
R1(config)# enable secret 9 HZWdzLHwhPtZ3UD9OlUDSGvBy.m8Tf9vCGDJRcY

Second Method
R1(config)# enable algorithm-type scrypt secret cisco
```

Password Encryption for username secret

```
R1(config)# username Bob algorithm-type scrypt secret cisco
```

Configure Secure Line Acces

```
R1(config)# username Bob algorithm-type scrypt secret cisco
R1(config)# line console 0
R1(config-line)# login local
R1(config-line)# exit
R1(config)# line aux 0
R1(config-line)# login local
R1(config-line)# exit
R1(config)# vty 0 4
R1(config-line)# login local
R1(config-line)# transport input ssh
```

Enhance Login

NOTE

PERMIT-ADMIN is an ACL-class. These enhancement only work on virtual connections like SSH

```
R1(config)# login block-for 10 attempts 3 within 30
R1(config)# login quiet-mode acces-class PERMIT-ADMIN
R1(config)# login delay 5
R1(config)# login on-succes log
R1(config)# login on-failure log
```

Verify login

```
R1# show login
R1# show login failures
```

Configure SSH

NOTE

To SSH from router-to-router use SSH -l username ip

```
R1(config)# ip domain-name example.com
R1(config)# crypto key generate rsa general-keys modulus 2048
R1(config)# ip ssh version 2
R1(config)# username Bob algorithm-type scrypt secret cisco
R1(config)# line vty 0 4
R1(conifg-line)# login local
R1(config-line)# transport input ssh
R1(config-line)# end
```

You can also modify SSH parameters

```
R1(config)#ip ssh time-out 60
R1(config)#ip ssh authentication-retries 3
```

Verify SSH

```
R1# show ip ssh
R1# show crypto key mypubkey rsa
```

Limit Command Availibilty

This chapter explains how to limit commands within Cisco IoS.
When there is a global command please use ? for the correct syntax

Configure Privilege level

```
R1(config)# privilege mode (level leven) | reset command
```

AAA

This chapter describes how to configure AAAA.

SSH

After the default SSH configuration:

```
R1(config)#ip domain-name ccnasecurity.com
R1(config)#crypto key generate rsa
R1(config)#ip ssh version 2
```

RADIUS

```
R1(config)# aaa new-model
R1(config)# radius-server host 192.168.3.2
R1(config)# radius-server key radiuspa55
R1(config)# aaa authentication login default group radius loca
```

NOTE

With the last command the router/switch first looks at the RADIUS server. If the RADIUS server is not available he uses the local login database.

Console via RADIUS:

```
R1(config)# line console 0
R1(config-line)# login authentication default
```

SSH via RADIUS:

```
R1(config)# line vty 0 15
R1(config-line)# login authentication default
R1(config-line)# transport mode ssh
```

Configure SNMPv3

This chapter explains how to configure SNMPv3 securely

Configure SNMPv3 Security

```
R1(config)# ip acces-list standard PERMIT-ADMIN
R1(config-nacl)# permit 192.168.1.0 0.0.0.255
R1(config-nacl)# exit
R1(config)# snmp-server view SNMP-RO iso included
R1(config)# snmp-server group ADMIN v3 priv
read SNMP-RO acces PERMIT-ADMIN
R1(config#) snmp-server user BOB ADMIN v3 auth sha
cisco12345 priv aes 128 cisco54321
R1(config)# end
```

Syslog

This chapter describes how to configure Syslog.

```
R1(config)# logging 192.168.1.3
R1(config)# logging trap 4
R1(config)# logging source-interface g0/0
R1(config)# service timestamps log datetime msec
```

NTP

This chapter describes how to configure NTP.

```
R1(config)# ntp server 64.103.224.2
R1(config)# service timestamps log datetime msec
```

Additional Resources

Additional resources for more information about Cisco configuration.

Cisco DocWiki `http://docwiki.cisco.com/wiki/Main_Page`

---

https://github.com/roaldnefs/cisco-cheatsheet