



**Networkforyou**

Subscribe to our  
**You Tube Channel**



**Networkforyou**



**Welcome**

**To**

**Network for you**

**Tshoot Common Commands**



Email us:  
[networkforyou4@gmail.com](mailto:networkforyou4@gmail.com)

1 of 13

WhatsApp Us : +918143809578



## Troubleshooting Commands:

- In Cisco Router, Switch and Firewall all show commands help in trouble shooting.
- Mostly, all the Show commands can be filtered by using the | pipe character.
- Show commands combine it with the, begin, section, include or exclude parameters.

Show option	Description
show interfaces	Displays information of all interfaces
show interfaces switchport	Displays the status of a switching (non routing) port
show interfaces trunk	Displays information on the interface-trunk
show ip interface	Displays statuses of all IPv4 interfaces, add brief to get a summary
show ipv6 interface	Displays statuses of all IPv6 interfaces, add brief to get a summary
show ip traffic	Displays statistics on IP traffic
show ip route	Displays the IPv4 routing table of the router
show ipv6 route	Displays the IPv6 routing table of the router
show controllers	Displays clock rate and connected cable type for interface
show clock	Displays the system clock of the router
show users	Displays all users connected to the router
show file systems	Lists available file systems
show disk:	Displays file system information for the disk
show processes detailed	Displays detailed information about all current processes or a specified process
show processes cpu	Displays all processes and their CPU utilization
show processes memory	Displays the amount of memory used by each system process or a specified process
show history	Displays command line history
show flash	Displays information about Flash memory
show version	Displays information about loaded Cisco IOS software
show mac-address table	Displays the MAC address table
show arp	ARP table of the router address to MAC address mappings
show protocols	Displays status of configured Layer 3 protocols
show logging	Displays the state of syslog and system logging buffer.

**Email us:**  
**networkforYou4@gmail.com**

2 of 13

**WhatsApp Us : +918143809578**



show startup-config	Displays configuration saved in NVRAM
show running-config	Displays configuration currently running in RAM
show spanning-tree	Displays information about the spanning tree state
show vlan	Displays Virtual Local Area Network (VLAN) information
show cdp neighbors	Displays information of connected routers found

### Show & Troubleshooting Command:

```
show ip int brief | include administratively
show run | section vty
show run | begin router eigrp
show ip interface brief | exclude up
show interface gi1/1
ping 192.168.2.2 source loopback 0
telnet 192.168.2.2 80
telnet 192.168.2.1 22
telnet 192.168.2.1 22 /source-interface loopback 0
show ip protocols
show ip route rip
show ip rip database
show run interface FastEthernet 0/0
show ip eigrp neighbors
show run | section eigrp
show ip ospf neighbor
show run | section ospf
show ip interface brief
show interfaces f1/1
show ip interface brief
show interfaces status err-disabled
show port-security interface f1/1
show port-security interface f1/1 address
show port-security
show vlan
show interfaces fa0/2 switchport
show vlan id 100
show interfaces trunk
show spanning-tree vlan 10
show etherchannel 2 detail
```

**Email us:**  
[networkforyou4@gmail.com](mailto:networkforyou4@gmail.com)

3 of 13

**WhatsApp Us : +918143809578**



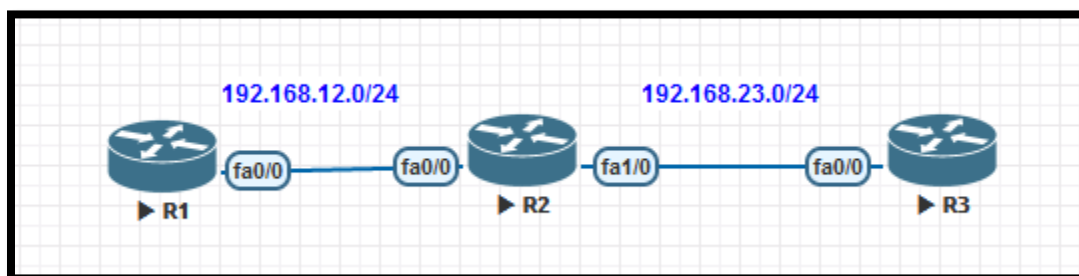
## Debug and Conditional Debug:

- Debugs are useful tools when troubleshooting specific issues.
- Debug commands help to show the real time information on device.
- Debug facility used to keep track in case of events or protocol errors.
- Debug facility used to keep track the internal messages taking place.
- Conditional debug is very useful to filter out some of the debug information.
- Conditionally debugging generates debugging messages matching given condition.
- Such as conditionally debugging messages for one interface or sub-interface.
- Turn on debugging for all interfaces that meet specified conditions.
- Debugs can produce a huge amount of information, which overload the router.
- Use conditional debug to limit information based on specific interface, or protocol.
- Using no debug all or undebug all does not remove the condition debugging.

Debugging and Condition Debugging	
R1# debug ip icmp	R1# debug condition ?
R1# debug ip packet	R1#debug condition interface f0/0
R1# debug interface	R1#undebug condition interface f0/0
R1# debug eigrp packets hello	R1#show debugging
R1#show debug condition	R1#no debug all

Lab time:

let do a Basic OSPF lab and use Debug and Conditional Debug:



Email us:  
networkforYou4@gmail.com

4 of 13

WhatsApp Us : +918143809578



R1 Configuration	R2 Configuration	R3 Configuration
en config t hostname R1  int f0/0 ip add 192.168.12.1 255.255.255.0 no sh  router ospf 1 int f0/0 ip ospf 1 area 0	en config t hostname R2  int f0/0 ip add 192.168.12.2 255.255.255.0 no sh  int f1/0 ip add 192.168.23.1 255.255.255.0 no sh  router ospf 1 int f0/0 ip ospf 1 area 0  int f1/0 ip ospf 1 area 0	en config t hostname R3  int f0/0 ip add 192.168.23.2 255.255.255.0 no sh  router ospf 1 int f0/0 ip ospf 1 area 0

When Enable OSPF debugging on R2. Showing OSPF debug information from both interfaces

```
R2#debug ip ospf packet
OSPF packet debugging is on
R2#
*Apr 29 19:46:00.055: OSPF: rcv. v:2 t:1 l:48 rid:192.168.23.2
aid:0.0.0.0 chk:8DF1 aut:0 auk: from FastEthernet1/0
*Apr 29 19:46:05.815: OSPF: rcv. v:2 t:1 l:48 rid:192.168.12.1
aid:0.0.0.0 chk:AEF2 aut:0 auk: from FastEthernet0/0
```

If only, want to see the debug information from one interface then use a debug condition.

Email us:  
networkforYou4@gmail.com

WhatsApp Us : +918143809578



Using debug condition only can see OSPF debug information from the FastEthernet 0/0 interface.

```
R2#debug condition int fastEthernet 0/0
Condition 1 set
R2#debug ip os
R2#debug ip ospf pac
R2#debug ip ospf packet
OSPF packet debugging is on
R2#
*Apr 29 19:49:18.423: OSPF: rcv. v:2 t:1 l:48 rid:192.168.12.1
aid:0.0.0.0 chk:AEF2 aut:0 auk: from FastEthernet0/0
*Apr 29 19:49:28.107: OSPF: rcv. v:2 t:1 l:48 rid:192.168.12.1
aid:0.0.0.0 chk:AEF2 aut:0 auk: from FastEthernet0/0
*Apr 29 19:49:37.791: OSPF: rcv. v:2 t:1 l:48 rid:192.168.12.1
aid:0.0.0.0 chk:AEF2 aut:0 auk: from FastEthernet0/0
```

To remove condition debug put no in the begging of the command and type yes.

```
R2#no debug condition interface fastEthernet 0/0
This condition is the last interface condition set.
Removing all conditions may cause a flood of debugging
messages to result, unless specific debugging flags
are first removed.

Proceed with removal? [yes/no]: yes
Condition 1 has been removed
```

### Ping Command:

- Ping stand for Packet Internet groper.
- The ping command is a very common method for troubleshooting the accessibility of devices.
- It uses two Internet Control Message Protocol (ICMP) query messages, ICMP echo requests and ICMP echo replies, to determine whether a remote host is active.
- The ping command also measures the amount of time it takes to receive the echo reply.
- The ping command first sends an echo request packet to an address, and then it waits for a reply.
- The ping is successful only if the echo request gets to the destination, and the destination is able to get an echo reply back to the source of the ping.

Email us:  
networkforYou4@gmail.com

6 of 13

WhatsApp Us : +918143809578



Character	Meaning
!	Successful receipt of a reply.
.	Device timed out while waiting for a reply.
U	A destination unreachable error protocol data unit (PDU) was received.
Q	Source quench (destination too busy).
M	Could not fragment.
?	Unknown packet type.
&	Packet lifetime exceeded.

### Extended Ping Command:

- When a normal ping command is sent from a router, the source address of the ping is the IP address of the interface that the packet uses to exit the router.
- If an extended ping command is used, the source IP address can be changed to any IP address on the router.

```
R2#ping
Protocol [ip]:
Target IP address: 10.0.0.2
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: yes
Source address or interface: 192.168.5.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.2, timeout is 2 seconds:
Packet sent with a source address of 192.168.5.1
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
```

Email us:  
networkforyou4@gmail.com

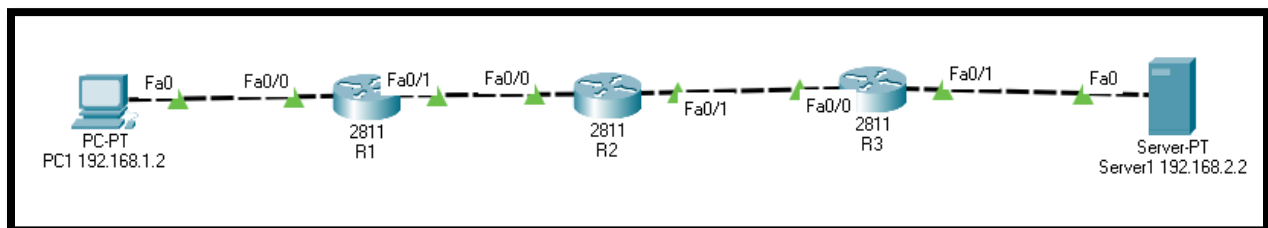
7 of 13

WhatsApp Us : +918143809578



## Traceroute Command:

- Traceroute, like the ping command can be used to isolate problems in our network. The ping command is a bit limited sometimes.
- The traceroute command can be used to discover the routes packets take to a remote destination, as well as where routing breaks down.
- The device executing the traceroute command sends out a sequence of User Datagram Protocol (UDP) datagrams, each with incrementing Time-To-Live (TTL) values, to an invalid port address at the remote host.
- The purpose behind the traceroute command is to record the source of each ICMP "time exceeded" message to provide a trace of the path the packet took to reach the destination.



- When we send a ping from PC1 (192.168.1.2) to Server1 (192.168.2.2) and this ping doesn't work, what does it mean? We'll know something is not working but we don't know whether the problem is in between PC1-R1, R1-R2, R2-R3 or R3-Server1.
- If you know the IP addresses of all routers in the path then you could ping all of these routers one by one. What if you have no idea how many routers are in between? Or if you don't know their IP addresses?

The traceroute command will help us with that. Let see for above example:

```
C:\>tracert 192.168.2.2

Tracing route to 192.168.2.2 over a maximum of 30 hops:

  1  0 ms    0 ms    0 ms    192.168.1.1
  2  0 ms    0 ms    0 ms    192.168.12.2
  3  0 ms    0 ms    0 ms    192.168.23.2
  4  *        0 ms    6 ms    192.168.2.2

Trace complete.
```

Email us:  
[networkforyou4@gmail.com](mailto:networkforyou4@gmail.com)

WhatsApp Us : +918143809578



Above used the tracert (traceroute) command on a Windows computer to trace the path from my computer to Server1. You can see all the IP addresses and hostnames of the routers in between my computer and the server that responds to 192.168.2.2. The response times that you see is the round trip time from my computer to the router. For each router, traceroute sends three probes.

So, how does traceroute work?

Traceroute uses the TTL (Time to Live) field in the IP packet header. Normally, TTL is used to prevent packets from being forwarded forever when there is a routing loop. Whenever an IP packet is forwarded by a router, the TTL is decreased by one. When the TTL is zero, the IP packet will be discarded.

```
R1#Traceroute 192.168.2.1
Type escape sequence to abort.
Tracing the route to 192.168.2.1

 1  192.168.12.2      8 msec    0 msec    0 msec
 2  192.168.23.2     0 msec    0 msec    0 msec
```

Email us:  
[networkforyou4@gmail.com](mailto:networkforyou4@gmail.com)

9 of 13

WhatsApp Us : +918143809578



```
C:\>tracert 192.168.2.2
```

```
Tracing route to 192.168.2.2 over a maximum of 30 hops:
```

```
 1  0 ms      0 ms      0 ms      192.168.1.1
 2  0 ms      0 ms      0 ms      192.168.12.2
 3  0 ms      0 ms      0 ms      192.168.23.2
 4  *          *          *          Request timed out.
 5  *          *          *          Request timed out.
 6  *          *          *          Request timed out.
 7  *          *          *          Request timed out.
 8  *          *          *          Request timed out.
 9  *          *          *          Request timed out.
10  *          *          *          Request timed out.
11  *          *          *          Request timed out.
12  *          *          *          Request timed out.
13  *          *          *          Request timed out.
14  *          *          *          Request timed out.
15  *          *          *          Request timed out.
```

If you see above picture with this you can say till R3 is ok after that some issues so this way we can trace issues.

Email us:  
[networkforyou4@gmail.com](mailto:networkforyou4@gmail.com)

10 of 13

WhatsApp Us : +918143809578



## Extended Traceroute Command:

- The extended traceroute command is a variation of the traceroute command.
- An extended traceroute command can be used to see what path packets are taking to get to a destination, and the command can be used to check routing at the same time.
- This is helpful for troubleshooting routing loops, or for determining where packets are getting lost.

```
R1#traceroute
Protocol [ip]:
Target IP address: 192.168.1.103
Source address:
Numeric display [n]:
Timeout in seconds [3]:
Probe count [3]:
Minimum Time to Live [1]:
Maximum Time to Live [30]:
Port Number [33434]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Type escape sequence to abort.
Tracing the route to 192.168.1.103

 1 192.168.1.103 4 msec 12 msec *
```

## Command-Line Tools:

- On Windows PCs, the command prompt can be accessed by searching for it in the start menu or by typing “cmd” into the Run window. On a Linux system, you can press Ctrl + Alt + T to open the command line. The following commands can be entered into the command prompt one at a time to reveal specific information about the network status:

### Ping:

- A TCP/IP utility that transmits a datagram to another host, specified in the command. If the network is functioning properly, the receiving host returns the datagram.

Email us:  
networkforYou4@gmail.com

11 of 13

WhatsApp Us : +918143809578



### tracert/traceroute:

- A TCP/IP utility that determines the route data takes to get to a particular destination. This tool can help you to determine where you are losing packets in the network, helping to identify problems.

### Nslookup:

- A DNS utility that displays the IP address of a hostname or vice versa. This tool is useful for identifying problems involving DNS name resolution.

### Ipconfig:

- A Windows TCP/IP utility that verifies network settings and connections. It can tell you a host's IP address, subnet mask and default gateway, alongside other important network information.

### Ifconfig:

- A Linux or UNIX TCP/IP utility that displays the current network interface configuration and enables you to assign an IP address to a network interface. Like ipconfig on Windows, this command will tell you vital information about the network and its status.

### ARP:

- Utility that supports the Address Resolution Protocol (ARP) service of the TCP/IP protocol suite. It lets the network admin view the ARP cache and add or delete cache entries. It can be used to address problems having to do with specific connections between a workstation and a host.

### Telnet:

- When you use Telnet to connect to a remote device, it uses the default port (23).
- We can use any port number from 1 to 65535 to test whether a remote device is listening to the specific port, for example, telnet 192.168.1.1 443.
- Telnet is still valuable as a troubleshooting tool. we can use telnet to test TCP connections to a remote server on any port.
- Once telnet establishes a connection, you can send raw commands to do additional testing. Linux and Macintosh OS X include the telnet client by default.
- Windows 10 includes telnet as part of the Windows Subsystem for Linux.



**NetworkforYou**

Subscribe to our  
**You Tube Channel**

**CDP:**

- Provides a degree of reachability information of directly connected Cisco devices.
- This is an extremely useful tool to determine the operational status of the physical and data link layer.
- Cisco Discovery Protocol (CDP) is a proprietary data link layer protocol.
- Use Cisco Discovery Protocol to gather useful information about neighbor devices and map out a network.
- By using CDP, Network Engineers can gather information about neighboring network devices, determining the type of hardware or equipment, software version, active interfaces the device is using (whether physical or VLAN), how they are configured, and other useful information.
- That is quite a bit of information, and this is useful for troubleshooting and documenting the network.

NetworkforYou

**Email us:**  
**networkforYou4@gmail.com**

13 of 13

**WhatsApp Us : +918143809578**