**How to block ICMP Ping on Cisco Routers**

This tutorial explains how to block ICMP ping messages on Cisco routers. Learn how to create and implement an extended access list to block ICMP echo messages on Cisco routers.

ICMP is a network management protocol. By default, this protocol is enabled on all IP devices. A device uses the ICMP protocol to notify another device about an error and receive information from another device. It allows devices to send and receive errors and messages.

An adversary can use the ICMP protocol to reveal information about your network or to launch a DoS attack on a device in your network. For example, the **'tracert'** command and the **'ping'** command use the ICMP protocol to function. An adversary can use the **'tracert'** command to locate your network resources or can use the **'ping'** command to launch a DoS attack on your servers.

To prevent an adversary from abusing the ICMP protocol, you can use extended access lists. An extended access list allows you to control ICMP errors and messages that devices can send and receive.

**Creating extended access lists for ICMP messages**

The following global configuration mode command is used to create an extended access list for ICMP messages.

Router(config)# access-list 100-199|2000-2699 permit|deny icmp

source\_address source\_wildcard\_mask

destination\_address destination\_wildcard\_mask

[icmp\_message] [log]

Let’s discuss the above command.

**100-199|2000-2699**: - Two number ranges: 100-199 and 2000-2699 are reserved for extended access lists. To create an extended access list, we have to select a number from these ranges.

**permit|deny**: - This is the action that the ACL will perform if the defined criteria meet.

**icmp**: - This option specifies that we are creating a statement for the ICMP protocol.

**source\_address source\_wildcard\_mask**: - define the source IP address that we want to match.

**destination\_address destination\_wildcard\_mask**: - define the destination IP address that we want to match.

**icmp\_message**: - This is the type of ICMP message that we want to filter.

The following table lists some most common types of messages that you can filter.

|  |  |
| --- | --- |
| Message | Description |
| echo | The ping command sends this message to test connectivity from the remote host. |
| echo-reply | The remote host sends this message in response to the echo message. |
| traceroute | This message contains information that the traceroute command uses to map the devices on the path. |
| administratively-prohibited | This message indicates that the packet has been filtered by a security device or an application. |
| host-unreachable | This message indicates that the subnet is reachable, but the host is not reachable. |
| net-unreachable | This message indicates that the subnet or the network is not reachable. |

**log**:- Display a log message when this statement hits.

To learn more about the options, arguments, and parameters of the access-list command or learn how to create an extended access list, you can check the previous parts of this tutorial.

An access list does nothing until you apply it to an interface. To apply an access list, enter interface configuration mode and run the following command.

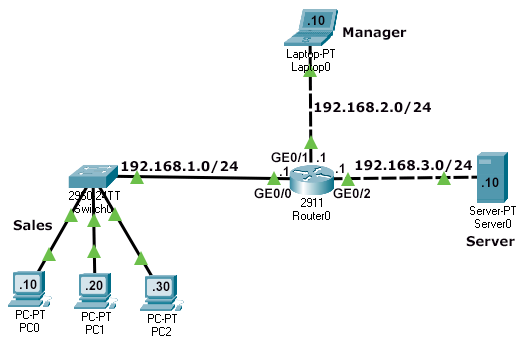
Router(config-if)#ip access-group ACL\_# in|out

Replace the **ACL\_#** with the ACL number or name. To apply the ACL in the outward direction, use the **'out'** option. To apply the ACL in the inward direction, use the **'in'** option.

Let's take an example to understand how to create and apply an ACL to filter ICMP messages.

Either create a packet tracer lab as shown in the following image or download the following pre-created lab and load it on Packet Tracer.

[Download Packet Tracer Lab with Initial Configuration](https://www.computernetworkingnotes.org/download/cisco/ccna-study-guide/pklab/csg106-01-with-ip-configuration-without-acl.pkt)

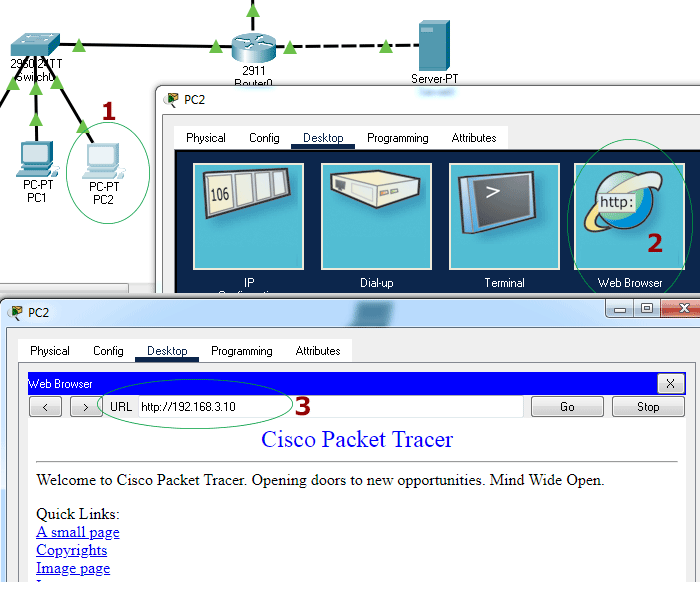


Currently in this network:-

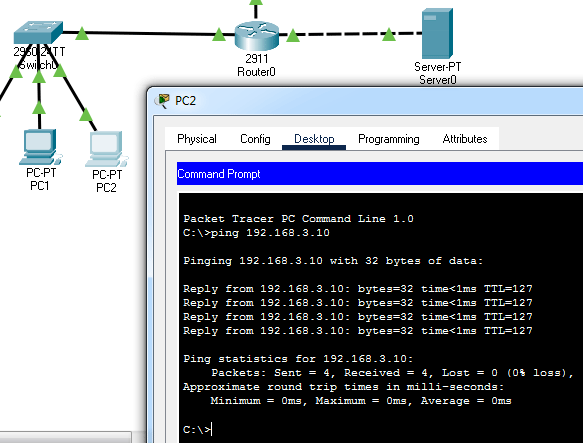
* All sections can access each other.
* HTTP, HTTPs, FTP, TFTP, EMAIL, DHCP, and NTP services are running on the Server.
* The Sales section and Manager section can access services running on the Server.
* The sales section can also send ping requests to the Server.

To verify the setup, access the web service running on the Server from PC2 and send ping requests from PC0 to the Server.

The following image verifies that the Sales section (PC2) can access the web service.



The following image verifies that the Sales section (PC0) can send ping requests to the Server.



**Requirements**

Suppose, we want to block the Sales section from sending ping requests to the Server. But at the same time, we don't want to interrupt or disturb any other service or feature of the network. For this, we will create an extended access list on the Router.

**Creating an extended access list to block ICMP echo messages**

Access the CLI prompt of the Router and enter the following commands.

Router>enable

Router#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#access-list 101 deny icmp 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255 echo

Router(config)#access-list 101 permit ip any any

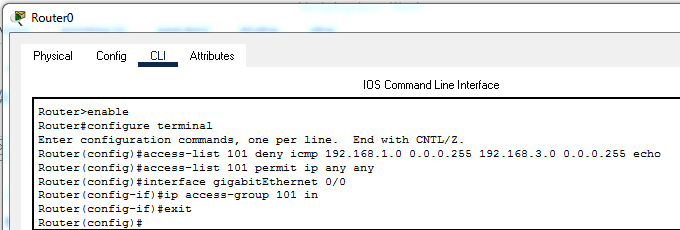
Router(config)#interface gigabitEthernet 0/0

Router(config-if)#ip access-group 101 in

Router(config-if)#exit

Router(config)#

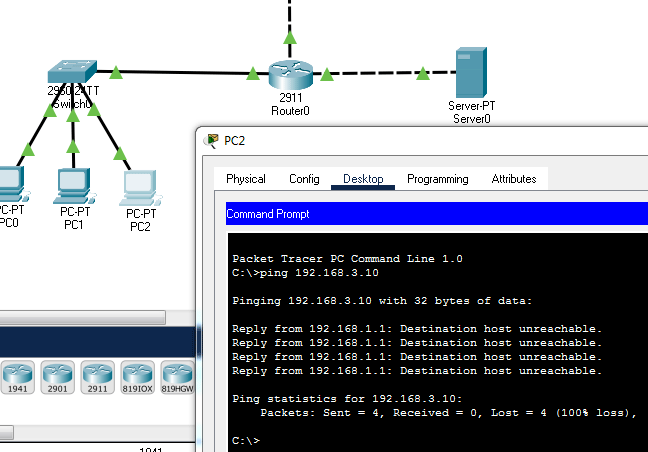
The following image shows how to enter the above commands on the Router.



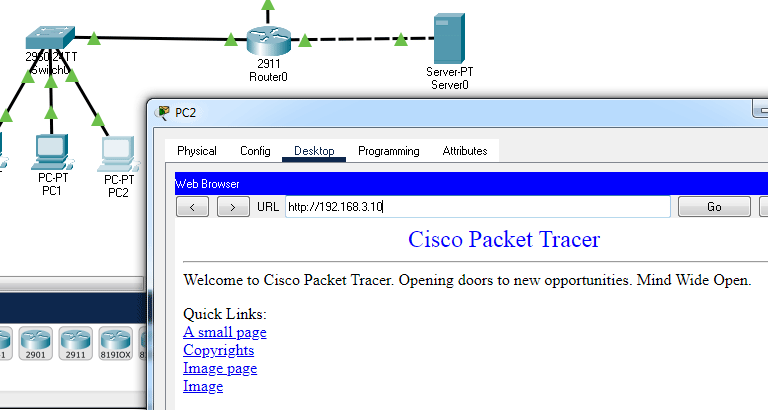
**Verifying the ACL implementation**

We have created and implemented the ACL to block echo requests from the Sales section without blocking the data flow of any other service or breaking the connectivity between Sections.

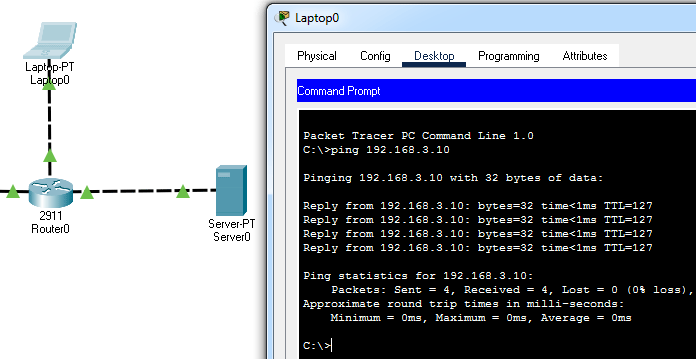
To verify this, send ping requests from PC2 to Server0. If ping requests are blocked, it verifies that the ACL is correctly implemented to block ICMP echo requests. The following image shows this testing.



This ACL must not block any other features and services of the network. To verify this, access the web service again from PC2. If PC2 can access a web page from the webserver running on the Server0, it verifies that the ACL is not blocking and interrupting any other service apart from the echo messages. The following image shows this testing.



This ACL must not block echo requests from the Manager section. To verify this, send a ping request from the Manager section. If the Manager section can ping the Server section, it verifies that the ACL is not blocking echo requests from other sections. The following image shows this testing.



**Configured Packet Tracer Lab**

The following link provides the configured packet tracer lab of the above example.

[Download Packet Tracer Lab with ACL Configuration](https://www.computernetworkingnotes.org/download/cisco/ccna-study-guide/pklab/csg106-02-with-access-list-configured.pkt)

That's all for this tutorial. If you like this tutorial, please share it through your favorite social networking site and subscribe to our YouTube channel.