

Forum:[Hack Forums](#)

Thread: [\[Network Reconnaissance\] Ping Computer to computer!](#)

Noobface80 - May 9, 2017, 7:15 pm

Hello my friends and foes; I am stuck with a dilemma! I'm trying to ping a machine.

Sounds simple enough right?

WRONG!

(Unless you're a wizard that is)

Getting to the point, I am trying to ping from computer A to computer B where both are under the network of a home router. I have tried research and came to a link here:

[Ping Different subnets using routing tables!](#)

Which showed me how to use routing tables in order to specify a route, but to no avail. I know firewall usually blocks icmp requests to pc's, but I know that my route table isn't successful because when I try to traceroute the gateway, which works beautifully, but then when trying to traceroute the internal hoping it takes the route of the gateway, it doesn't even leave the network. I figure I'm doing it wrong, but I'm just trying to get a proper path to the client computer on the network; that's all I need. I don't care about firewall blocked icmp request packets! Just help me get there (if you can!)

Gt403cyl - May 9, 2017, 7:32 pm

Ok I might have this completely wrong but.....

Sounds like you are trying to ping PC A from PC B while both are on the same network and are having problems.....

What command are you using?

Example:

From PC A use CMD- "ping 192.168.0.xx"

You need to use the LAN IP....

Armada - May 9, 2017, 7:58 pm

If both computers are on the same network it is as simple as pinging the internal IP# of the other machine. (Easily obtained from the connected devices table in router settings) If the machine still does not reply to pings, it means they have a software firewall which disables said replies.

Noobface80 - May 9, 2017, 8:30 pm

Sorry...I worded it wrong.

TLDR: I am trying to ping between 2 different computers on 2 different subnets and 2 different networks...

Armada - May 9, 2017, 8:42 pm

(May 9, 2017 08:30 PM)Noobface80 Wrote: [\[CITE\]](#) Sorry...I worded it wrong.

TLDR: I am trying to ping between 2 different computers on 2 different subnets and 2 different networks...

Ahhh yea, you need to add an IP table to connect a pipe between the 2 subnets.

Look into configuration of IP tables, you can likely do this straight from your router device too assuming it is a later model somewhere in advanced settings.

It is kind of odd you are running 2 subnets on a home network though. ?

Longdog - May 9, 2017, 8:43 pm

(May 9, 2017 08:30 PM)Noobface80 Wrote: [\[CITE\]](#) Sorry...I worded it wrong.

TLDR: I am trying to ping between 2 different computers on 2 different subnets and 2 different networks...

ping ExternalIPHere -t

if that doesn't work someone has ping disabled on their network.

Armada - May 9, 2017, 8:46 pm

(May 9, 2017 08:43 PM)Local Junkie Wrote: [\[CITE\]](#) ping ExternalIPHere -t

if that doesn't work someone has ping disabled on their network.

You have clearly missed the networking problem here.

He is running 2 separate subnets within the same LAN environment.

IE:

192.168.1.X

192.186.2.X

These by default do not communicate together, so he has to create a link or pipeline between the two to communicate.

Spoiler [\(Click to View\)](#)

Gt403cyl - May 9, 2017, 8:49 pm

(May 9, 2017 08:46 PM)Armada Wrote: [\[CITE\]](#) You have clearly missed the networking problem here.

He is running 2 separate subnets within the same LAN environment.

IE:

192.168.1.X

192.186.2.X

These by default do not communicate together, so he has to create a link or pipeline between the two to communicate.

Spoiler [\(Click to View\)](#)

They did also say on 2 different networks in their last reply....

So not sure...

Armada - May 9, 2017, 8:58 pm

(May 9, 2017 08:49 PM)Gt403cyl Wrote: [\[CITE\]](#) They did also say on 2 different networks in their last reply....

So not sure...

Shit did not notice that lol

Ignore IP tables and deal with proper port forwarding then ?

Asdethprime - May 9, 2017, 9:12 pm

(May 9, 2017 08:30 PM)Noobface80 Wrote: [\[CITE\]](#) I am trying to ping between 2 different computers on 2 different subnets and 2 different networks...

There are few things that has to be at play here:

- 1) The 2 different network need to have a LAN connection, with 2 routers/switches talking to each other.
- 2) You would need both the public IP and the internal IP of the router.

Only after that you will be able to ping a computer outside your network.

The reason you need a public IP is quite simple, computer on different networks have the same IP address.

The IP address of my switch is the same as yours. 192.168.0.1

This is the same IP address, anyone on a internal network would use to connect to their wifi box.

If you only give internal IP address the router will not be able to figure out where to send the packet.

Also could you type in the IP address of the 2 routers? Don't worry these are going to be internal IP. If the IP address of the 2 routers happen to be different then you will be able to follow the link you posted. If it's not you would need the public IP.

Noobface80 - May 9, 2017, 9:14 pm

I need to ping from PC A to PC B.

Thanks Fam!

Armada - May 9, 2017, 9:25 pm

(May 9, 2017 09:12 PM)Asdethprime Wrote: [\[CITE\]](#) There are few things that has to be at play here:

- 1) The 2 different network need to have a LAN connection, with 2 routers/switches talking to each other.
- 2) You would need both the public IP and the internal IP of the router.

Only after that you will be able to ping a computer outside your network.

The reason you need a public IP is quite simple, computer on different networks have the same IP address.

The IP address of my switch is the same as yours. 192.168.0.1

This is the same IP address, anyone on a internal network would use to connect to their wifi box.

If you only give internal IP address the router will not be able to figure out where to send the packet.

Also could you type in the IP address of the 2 routers? Don't worry these are going to be internal IP. If the IP address of the 2 routers happen to be different then you will be able to follow the link you posted. If it's not you would need the public IP.

Technically inaccurate.

Only the Client machine (Machine he is trying to ping) needs its proper ports forwarded to the internal subnet and internal IP# and then network communication is no problem.

Asdethprime - May 9, 2017, 10:17 pm

(May 9, 2017 09:25 PM)Armada Wrote: [\[CITE\]](#) Only the Client machine (Machine he is trying to ping) needs its proper ports forwarded to the internal subnet and internal IP# and then network communication is no problem.

How would that allow him, from a completely different network, to probe the client.

He can't reach the client directly what he is reaching is the switch/hub that runs the given subnet. Client forwarding port port to internal subnet would only allows a physically connected subnet to interact with him or once the packet reaches the switch to be forwarded to right direction. To reach the switch which will not be a different IP than the sending switch would need a public IP, no?

Remember, the attacker PC (lets just call him that) is on an entirely different network reachable only through the Internet. Without a public IP address how is port forwarding going to help?

Also you seem to be ignoring the fact that both the internal network will have same IP addresses. The IP address of your switch 192.168.0.1 is not unique outside your network. Since both client and attackers are on different network port forwarding won't work on its own.

(May 9, 2017 09:14 PM)Noobface80 Wrote: [\[CITE\]](#)

I need to ping from PC A to PC B.

Thanks Fam!

Ping the public IP address of switch.

Armada - May 9, 2017, 10:20 pm

(May 9, 2017 10:17 PM)Asdethprime Wrote: [\[CITE\]](#) How would that allow him, from a completely different network, to probe the client.

He can't reach the client directly what he is reaching is the switch/hub that runs the given subnet. Client forwarding port port to internal subnet would only allows a physically connected subnet to interact with him or once the packet reaches the switch to be forwarded to right direction. To reach the switch which will not be a different IP than the sending switch would need a public IP, no?

Remember, the attacker PC (lets just call him that) is on an entirely different network reachable only through the Internet. Without a public IP address how is port forwarding going to help?

Also you seem to be ignoring the fact that both the internal network will have same IP addresses. The IP address of your switch 192.168.0.1 is not unique outside your network. Since both client and attackers are on different network port forwarding won't work on its own.

Perhaps take some basic networking classes?
Re-read what I stated.

The Residing machine and network need to have the port forwarding enabled to allow outside traffic to be directed to the other machines internal IP#. ???

(May 9, 2017 09:14 PM)Noobface80 Wrote: [\[CITE\]](#)

I need to ping from PC A to PC B.
Thanks Fam!
Perfect example.

So Router Y needs to open ports and Forwards to PC B accordingly through the routers port forwarding settings. Voila ?

Edit: Quick testing of ports of PC B is easily done from canyouseeme.org as well :)

Asdethprime - May 9, 2017, 10:51 pm

(May 9, 2017 10:20 PM)Armada Wrote: [\[CITE\]](#) Perhaps take some basic networking classes?
Re-read what I stated.

The Residing machine and network need to have the port forwarding enabled to allow outside traffic to be directed to the other machines internal IP#.

Perfect example.

So Router Y needs to open ports and Forwards to PC B accordingly through the routers port forwarding settings. Voila ?

Edit: Quick testing of ports of PC B is easily done from canyouseeme.org as well :)
I am still confused to what you are talking about.

Router Y in this case need to open a port to reach PC B. If it does not do so all you would be pinging is Router Y and not PC B. That much I agree, never disagreed that.

Router Y however is in a completely different network that yours and as such you can't open a port from Router Y or anything. Because, Router Y is not a router you can control.

So again, you would need the public IP (which is what I have said) and the router Y router X needs to be talking.

You were the one who came in saying "technically inaccurate". I am just wondering can you actually show me anything in my post that is "technically inaccurate" rather than simply a ??? ?

Armada - May 9, 2017, 10:54 pm

(May 9, 2017 10:51 PM)Asdethprime Wrote: [\[CITE\]](#) I am still confused to what you are talking about.

Router Y in this case need to open a port to reach PC B. If it does not do so all you would be pinging is Router Y and not PC B. That much I agree, never disagreed that.

Router Y however is in a completely different network that yours and as such you can't open a port from Router Y or anything. Because, Router Y is not a router you can control.

So again, you would need the public IP (which is what I have said) and the router Y router X needs to be talking.

You were the one who came in saying "technically inaccurate". I am just wondering can you actually show me anything in my post that is "technically inaccurate" rather than simply a ??? ?
Correct.

You will be pinging Router Y's external IP#, which in return will forward the request to PC B's internal IP#.

This is how routing and networking works folks.

[BLANK] - May 9, 2017, 10:54 pm

OK the main problem here is you are trying to ping to internal IP address that doesn't exist on your network. This will never work, ever. The only method you could use is if the remote router has a port forward setup to the backend PC you are trying to connect to, but why would a router set that up for ICMP?

Here is the issue, when you try to ping the 172.16.x.x network, it is looking for that IP in YOUR network because it is a private IP. Even if you setup a client/server relationship between the two PC's what is happening is the external routers are opening sockets that forward traffic from that connection to the PCs but you can not arbitrarily do that for a ICMP command.

So if you have access to the external remote router you may be able to set up port forwarding and open the ports on the PC and router. This also requires that the ISP allows for the traffic you are sending.

Some basic reading:

<https://www.iplocation.net/public-vs-private-ip-address>

Armada - May 9, 2017, 10:57 pm

(May 9, 2017 10:54 PM)EasyGhost Wrote: [CITE](#) OK the main problem here is you are trying to ping to internal IP address that doesn't exist on your network. This will never work, ever. The only method you could use is if the remote router has a port forward setup to the backend PC you are trying to connect to, but why would a router set that up for ICMP?

Here is the issue, when you try to ping the 172.16.x.x network, it is looking for that IP in YOUR network because it is a private IP. Even if you setup a client/server relationship between the two PC's what is happening is the external routers are opening sockets that forward traffic from that connection to the PCs but you can not arbitrarily do that for a ICMP command.

So if you have access to the external remote router you may be able to set up port forwarding and open the ports on the PC and router. This also requires that the ISP allows for the traffic you are sending.

Some basic reading:

<https://www.iplocation.net/public-vs-private-ip-address>

If I have to whip Vlsio open to diagram this out to you all I swear Im a slap every one of you.

As Dude here stated, you can not ping another internal IP from your internal network if it resides on another network. That is why I have detailed port forwarding to you, THAT is your problem, and the fact you are pinging the wrong IP# likely.

PC B's EXTERNAL IP# is the IP you want to be pinging.

EXAMPLE:

OP has to open Ports on Firewall Y to allow and forward port communications to PC B's internal 172.16.1.x IP.

Then OP using PC A, pings Router Ys's External IP#.

Further info:

<https://kb.iu.edu/d/aopy>

Asdethprime - May 9, 2017, 11:10 pm

(May 9, 2017 10:54 PM)Armada Wrote: [\[CITE\]](#) Correct.

You will be pinging Router Y's external IP#, which in return will forward the request to PC B's internal IP#.

This is how routing and networking works folks.

And how is it different from what I said and how is my reply "technically incorrect", then?

Armada - May 9, 2017, 11:14 pm

(May 9, 2017 11:10 PM)Asdethprime Wrote: [\[CITE\]](#) And how is it different from what I said and how is my reply "technically incorrect", then?

Same explanation, different approaches it seems lol ?

Noobface80 - May 10, 2017, 12:09 pm

So long story short, unless I have access to both routers to enable port forwarding, the closest ill get in the network to being able to be in direct contact with the computer is me just pinging the router?

(That is...unless I can get them talking somehow?)

Armada - May 10, 2017, 12:56 pm

(May 10, 2017 12:09 PM)Noobface80 Wrote: [\[CITE\]](#) So long story short, unless I have access to both routers to enable port forwarding, the closest ill get in the network to being able to be in direct contact with the computer is me just pinging the router?

(That is...unless I can get them talking somehow?)

Only the destination network needs to have the ports opened to properly communicate.. The basic logic is, You can communicate outbound to the internet from behind the firewall without a problem, the firewalls in general inherently allow outbound connections, but block incoming communications.

So the machine trying to ping can be firewalled and locked down no problem, but the machine that is being attempted to ping will need to have the ports opened to communication.

Noobface80 - May 10, 2017, 2:36 pm

Last question. Is there any way to change the ports that you can send an ICMP request (ping) packet on? Thanks so much for your help thus far btw!

[BLANK] - May 10, 2017, 2:42 pm

You other option is to set up a virtual IPsec tunnel between the two routers and then set up DNAT

rules to handle address assignments. You will need to configure the routing tables on both ends to properly direct traffic across the bridge. If you have the right network devices this is actually fairly easy to do.

Noobface80 - May 10, 2017, 3:46 pm

What if you do not have access to both routers? The reason I am asking is because I need to know that I can send packets in between computers in 2 different networks and 2 different subnets. I have a few resources I can use for packet crafting, so as I stated in the past, ICMP requests being blocked by the firewall isn't a problem. ROUTING is my problem.

[BLANK] - May 10, 2017, 4:37 pm

(May 10, 2017 03:46 PM)Noobface80 Wrote: [\[CITE\]](#) What if you do not have access to both routers? The reason I am asking is because I need to know that I can send packets in between computers in 2 different networks and 2 different subnets. I have a few resources I can use for packet crafting, so as I stated in the past, ICMP requests being blocked by the firewall isn't a problem. ROUTING is my problem.

I am not sure you are understanding that private IP address ranges cannot be routed over the internet, at least not without setting up networking devices to establish a virtual tunnel as I mentioned in a prior post. I mentioned using a IPSec tunnel because that actually creates a layer 3 bridge between the routers and thus allows you to craft routes between different private subnets. But even then it has to be routed over the internet and thus is not a true layer 3 connection.

Here is the core issue, if you try to ping 172.16.22.4 where would the traffic go? Do you know how many 172.16.x.x networks exist in the world? A lot. You can't create a route for that directly.

I think you really need to study up on Public and Private IP ranges and routing limitations of using private IP ranges. Also you should study:

1. Difference between a LAN and WAN
2. How NAT works
3. Creating basic routing rules.

Simply put if you have no access or control over the remote network then you won't be able to ping the remote PC using their internal private IP address.