RAW SOCKET

mohamed hamam | SPL training 2024

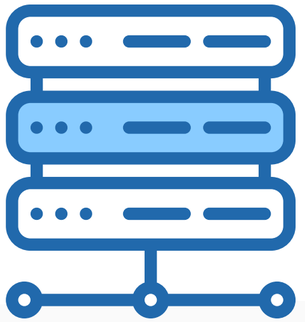
What is a Raw Socket?

- Imagine you have two toy walkie-talkies. Normally, you just press a button and talk, and the walkie-talkie handles everything else. But what if you wanted to change the walkie-talkie's inner parts to make it do something special? That’s kind of what a raw socket does. Instead of using a pre-built way to talk (like using the walkie-talkie as it is), raw sockets let you control the "inside" of the communication.

- So, a raw socket gives you more control over how data (messages) is sent between two computers.

Creating a Raw Socket

- When we create a raw socket, it’s like we’re making our own custom walkie-talkie. Normally, the walkie-talkie decides how to send the message, but with a raw socket, we decide what the message looks like, including things that the walkie-talkie usually takes care of for us.



- **In computers, we use a special command called socket() to make this custom walkie-talkie (raw socket). Here’s how:**

- **Domain**: Think of this as the type of message we want to send, like “Hey, I want to send it to a computer!” So, we use something called AF_INET for talking over the internet.

- **Type**: We say, "I want a special type of walkie-talkie that gives me full control." This is called SOCK_RAW.

- **Protocol**: Now, we tell the computer what kind of message we want to send. For example, using IPPROTO_ICMP means we are sending a "ping" message to check if another computer is awake.

Parts of a Message in Raw Sockets

Let’s imagine you are sending a letter:

- **IP Header**: This is like the address on an envelope. It tells the postman (or computer) where to send the letter (or message). When using raw sockets, we can even write the address ourselves.

- **Protocol Header**: Inside the envelope, there’s another small paper that says, "This is a ping message" or "This is a custom message I made up."

- **Payload**: This is the actual message you want to send. It’s like the note inside the envelope that says, "Hello!"

Socket Options

Sometimes, we want to tell the computer to let us do extra things with our raw socket (like adding a sticker to our letter). These are called socket options.

- **IP_HDRINCL**: Normally, the computer writes the envelope (address) for you. But with this option, you can say, "No, I want to write the address myself!" So, now you can fully control the envelope.

- **SO_BINDTODEVICE**: Let’s say you have more than one mailbox (or network interface, like Wi-Fi and Ethernet). You can say, "I want my message to go through this specific mailbox!" This option lets you pick which path the message should take.

Why Raw Sockets Can Be Dangerous?

- Remember how raw sockets give you full control? Well, that can be fun, but it can also be risky. Imagine if someone took control of your toy and sent fake messages pretending to be you! That’s why computers often require you to be a special user (like sudo) to use raw sockets, to keep bad people from doing sneaky things.

How We Use Raw Sockets

- **Ping**: If you send a message saying "Are you awake?" to another computer and it replies "Yes!", that's called a ping. It uses a raw socket to send a message called an ICMP Echo Request.

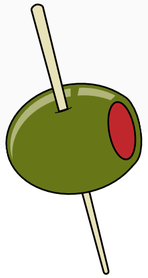
- **Traceroute**: When you send a message to a computer far away, the message might bounce between many computers. A program called traceroute can use raw sockets to figure out which computers the message bounces through, like a map of the message's path.

- **Packet Sniffers**: These are like super-spies that use raw sockets to listen in on all the messages being sent. They don’t change anything, they just watch!

Example Code

- Let’s imagine you want to say "Hi!" to a computer far away (using an ICMP Echo Request). You can write a little program to do this with raw sockets. It’s like building a toy walkie-talkie from scratch and then using it to send a message.

- But remember, only people who know how to build the toy should try this because it’s tricky and could break if not done carefully!



ELZATONA ^_^

- **Raw sockets** are like a build-your-own-walkie-talkie kit. They give you control over how messages are sent between computers, letting you play with all the parts that are usually hidden. This gives you power, but with power comes responsibility. Raw sockets can be used for good (like checking if a computer is working) or for bad (like sending fake messages).

References:

- Stevens, W. Richard. UNIX Network Programming, Volume 1.
- Linux Man Pages, Socket(7).
- RFC 791 - Internet Protocol, IETF.