

Should ChatGPT configure a router?

Neil Fenemor

No.

Can ChatGPT help me operate a network?

Neil Fenemor

Who am I?

- Been doing this internet thing since '97
- Part of the core team who built the third inter-regional fibre network in New Zealand
- Currently helping solve technology and business problems
- Been doing a lot with OpenLI recently, so I apologise for any OpenLI / OpenAI confusion!
- This is my first PacNOG, so thanks for having me!

What is ChatGPT then?

- A product offered by OpenAI with two different models available (GPT 3.5, GPT 4.0)
- A form of Generative AI called a Large Language Model
- Publicly useable and has Enterprise and API options
- Microsoft has cumulatively invested \$13bn into OpenAI

What is a Large Language Model?

- A large language model (LLM) is a type of language model notable for its ability to achieve general-purpose language understanding and generation.
- LLMs acquire these abilities by using massive amounts of data to learn billions of parameters during training and consuming large computational resources during their training and operation.
- LLMs are artificial neural networks (mainly transformers) and are (pre-)trained using self-supervised learning and semi-supervised learning.
- As autoregressive language models, they work by taking an input text and repeatedly predicting the next token or word.

Where are LLMs used?

- Microsoft Copilot suite of products
- Github Copilot
- Search engines (Bing Chat)
- Chat bots
- Many industry specific tools
 - Security products analysing log messages
 - Legal summary generation

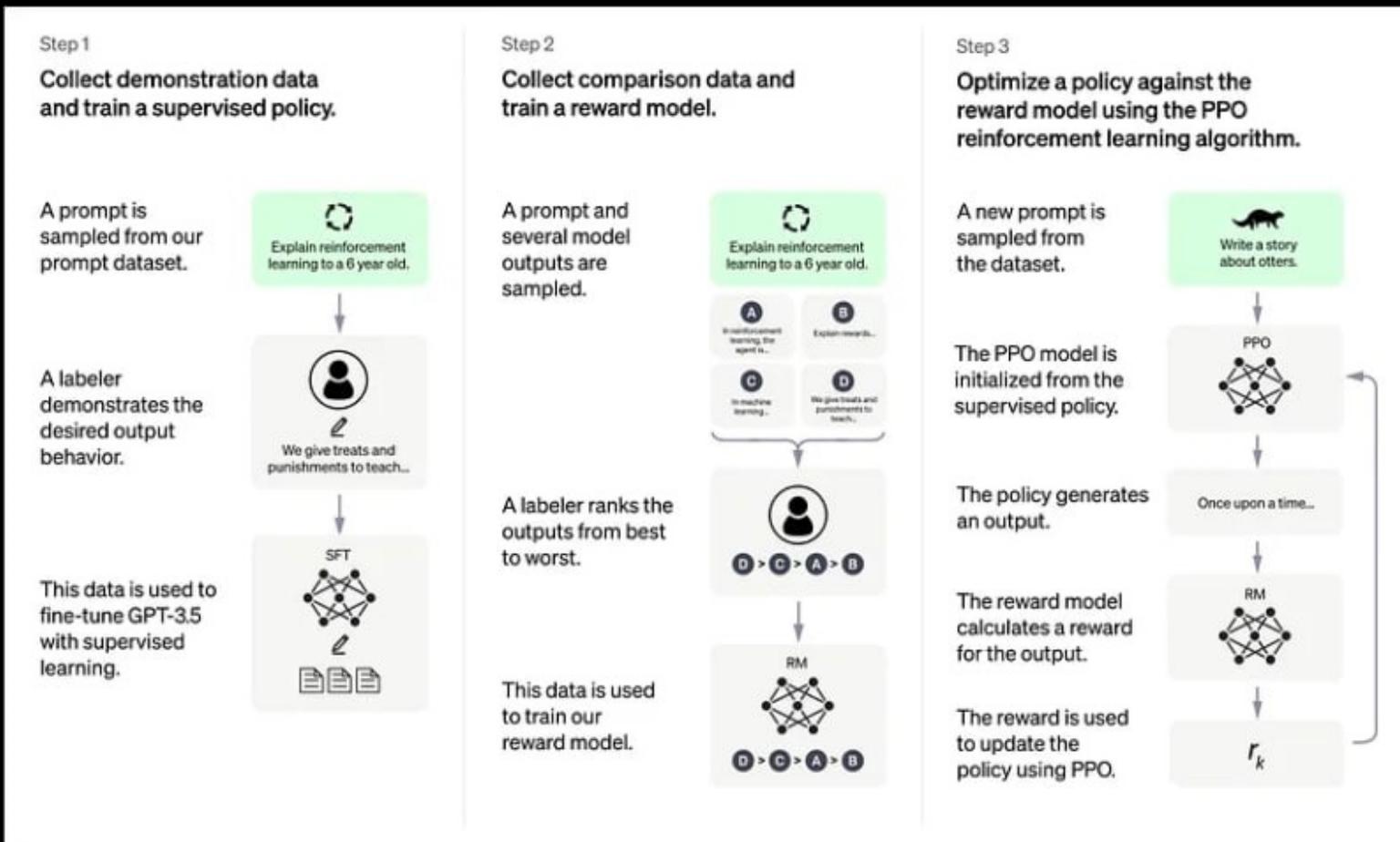
Training a Generative AI

- Training sets are important
- Any biases or errors in the training sets will naturally be carried through to the output
- Many LLMs (including ChatGPT) allow for fine tuning and introduction of your own data sets

What sources of data are used for training OpenAI models?

OpenAI uses data from different places including public sources, licensed third-party data, and information created by human reviewers. We also use data from versions of ChatGPT and DALL-E for individuals. Data from ChatGPT Enterprise and the API Platform (after March 1, 2023) isn't used for training our models.

Training a Generative AI



Training a Generative AI

- The models are continually evolving and changing - sometimes they work better, but sometimes they do not.
- You can provide your own data set for additional training - remember previously the online default is trained off of publicly available sources, licensed third party information, etc.

How could you use an LLM in network administration

- Building router configuration
- Intent based networking...based on natural language?
- Script generation (provisioning, debugging)
- General debugging

Building router config

- Can build a base config based on your prompt.

You
I need a base configuration for a Cisco IOS-XE device

ChatGPT
Certainly! Configuring a Cisco IOS-XE device involves several steps, and the specific configuration depends on your network requirements. Below is a basic configuration template that you can use as a starting point. You can customize it based on your specific needs.

```
bash Copy code

# Enter global configuration mode
enable
configure terminal

# Set the hostname
hostname YourDeviceName

# Configure interface GigabitEthernet0/0 (replace with your interface)
interface GigabitEthernet0/0
  description LAN Interface
  ip address 192.168.1.1 255.255.255.0
  no shutdown

# Configure interface GigabitEthernet0/1 (replace with your interface)
interface GigabitEthernet0/1
  description WAN Interface
  ip address dhcp
  no shutdown

# Configure default gateway
ip route 0.0.0.0 0.0.0.0 192.168.1.254

# Set the enable secret password
enable secret YourEnableSecretPassword

# Set the console and VTY (SSH) passwords
line console 0
  password YourConsolePassword
  login
line vty 0 4
  password YourVTYPassword
  login
```

Building router config

Why prompts matter...

- Similar to the previous base config, however now that we've asked for a NIST aligned config, we have a lot more safeguards built in.
- But do we have them all?
- Does this include all best practice?
- Could we have included others like CIS Workbench?

You

I need a secure base configuration for a Cisco ASR1000 running IOS-XE, please include the NIST standards for device hardening.

ChatGPT

Configuring a Cisco ASR1000 router running IOS-XE to meet NIST (National Institute of Standards and Technology) standards for device hardening is an important step in ensuring the security of your network. Here is a basic outline of steps you can take to harden the device:

1. Access Control:

- Implement strong authentication (e.g., TACACS+ or RADIUS) for accessing the device.
- Use strong, unique passwords for local accounts.
- Disable any unnecessary services and interfaces.

2. SSH Configuration:

- Use SSH version 2 for secure remote access.
- Disable SSH version 1.
- Enable strong encryption and authentication algorithms.

```
arduino Copy code  
  
crypto key generate rsa general-keys modulus 2048  
ip ssh version 2  
line vty 0 15  
  transport input ssh
```

3. Console Access:

- Implement console access restrictions using login banners and access control lists (ACLs).

```
lua Copy code  
  
line console 0  
  exec-timeout 5 0  
  logging synchronous  
  login local  
  transport output ssh
```

4. AAA (Authentication, Authorization, and Accounting):

- Set up AAA to control user access and privilege levels.
- Use TACACS+ or RADIUS for centralized authentication and authorization.

```
sql Copy code  
  
aaa new-model  
aaa authentication login default group tacacs+ local  
aaa authorization exec default group tacacs+ local  
aaa accounting exec default start-stop group tacacs+
```

Building router config

Why prompts matter...

NIST (cont)

9. Unnecessary Services:

- Disable any unnecessary services (e.g., CDP, HTTP, SNMP) that are not required for operation.

```
perl Copy code  
  
no cdp run  
no ip http server  
no ip http secure-server  
no snmp-server community <community-string> R0
```

10. File System Security:

- Encrypt sensitive files and directories using technologies like Cisco Type 7 or AES.

```
Copy code  
  
service password-encryption
```

-
- The same...but different...

 You

I need a secure Cisco IOS-XE base config

 ChatGPT

Configuring a Cisco router with a secure base configuration is essential for network security. Below is a basic template for a Cisco IOS-XE router. Keep in mind that this is a starting point and you should customize it based on your specific network requirements and security policies.

```
# Configure secure management protocols (optional)  
ip http secure-server  
crypto pki trustpoint TP-self-signed  
  enrollment selfsigned  
  subject-name cn=IOS-Self-Signed-Certificate  
  revocation-check none  
  rsa-key-pair TP-self-signed 2048  
!
```


Prompt engineering

- Strategies for getting better results:
 - Write clear instructions
 - Provide reference text
 - Split complex tasks into simpler subtasks
 - Give the model time to think

Script generation

- Using plain English, I can describe an event script that I want created
- I can review the code and confirm whether this is achieving what I want it to.

 **You**

I need an event script for a JunOS device that checks the optical receive level of an optic that has gone down, and disables / enables the interface that has gone down.

 **ChatGPT**

Creating an event script for Juniper JunOS involves using the Junos operational mode command-line interface (CLI) and scripting language, which is based on the Python programming language. Below is an example of an event script that monitors the optical receive level of an interface and takes action if it goes down:

```
python Copy code

#!/usr/bin/python

from junos import Junos_Context
from junos import Junos_Trigger_Event

def main():
    # Get the current event
    event = Junos_Trigger_Event()

    # Check if the event is an interface change event
    if event.xpath('//interface-event') is not None:
        # Get the interface name
        interface_name = event.xpath('//interface-name')[0].text

        # Check if the interface is operational
        if event.xpath('//interface-status')[0].text != 'up':
            # Interface is down, check optical receive level
            optical_receive_level = get_optical_receive_level(interface_name)

            # Define the threshold for optical receive level
            threshold = -15 # Change this value as needed

            # Take action if optical receive level is below the threshold
            if optical_receive_level < threshold:
                disable_interface(interface_name)
                print(f"Interface {interface_name} disabled due to low optical receive level")
            else:
                print(f"Optical receive level for {interface_name} is below threshold")
        else:
            print(f"Interface {interface_name} is up.")
```

Script generation

- In this case, it was not as I asked for the interface to be enabled and disabled.
- Ask a follow up question for simple adjustments.
- Not perfect, but this is a good start to build from.

 You

I need the script to reenable the interface after it has been disabled.

 ChatGPT

Certainly! To enable the interface again after it has been disabled, you can modify the script to include a function for enabling the interface. Here's the updated script:

```
python Copy code

#!/usr/bin/python

from junos import Junos_Context
from junos import Junos_Trigger_Event

def main():
    # Get the current event
    event = Junos_Trigger_Event()

def disable_interface(interface_name):
    # Use Junos operational mode command to disable the interface
    command = f'set interfaces {interface_name} disable'
    Junos_Context.run_op_cli(command)

def enable_interface(interface_name):
    # Use Junos operational mode command to enable the interface
    command = f'set interfaces {interface_name} enable'
    Junos_Context.run_op_cli(command)
```

Debugging

 You

What does this error mean?

```
500 Nov 23 15:41:17.126 Up
499 Nov 23 15:41:17.125 Self-ping started
498 Nov 23 15:41:17.125 Self-ping enqueued
497 Nov 23 15:41:17.125 Record Route: 192.0.2.52(flag=0x20) 192.0.2.92(Label=333098)
192.0.2.102(flag=0x20) 192.0.2.96(Label=908695) 192.0.2.114(flag=0x20)
192.0.2.122(Label=534414) 192.0.2.64(flag=0x20) 192.0.2.98(Label=377191) 192.0.2.135(flag=0x20)
192.0.2.79(Label=29120) 192.0.2.190(flag=0x20) 192.0.2.69(Label=67029) 192.0.2.228(flag=0x20)
192.0.2.66(Label=79962) 192.0.2.224(flag=0x20) 192.0.2.177(Label=3)
496 Nov 23 15:41:16.056 Originate Call
495 Nov 23 15:41:16.056 CSPF: computation result accepted 192.0.2.92 192.0.2.96 192.0.2.122
192.0.2.98 192.0.2.79 192.0.2.69 192.0.2.66 192.0.2.177
494 Nov 23 15:40:46.218 CSPF failed: no route toward 192.0.2.224[88 times, first Nov 23
14:58:44.164]
493 Nov 23 14:58:44.162 CSPF: link down/deleted: 192.0.2.68(192.0.2.135:82)
(device1.00/192.0.2.135)->0.0.0.0(0.0.0.0:0)(device2.03/0.0.0.0)
492 Nov 23 14:58:42.989 CSPF failed: no route toward 192.0.2.224
491 Nov 23 14:58:42.988 Clear Call: CSPF computation failed
490 Nov 23 14:58:42.984 192.0.2.79: Tunnel local repaired
489 Nov 23 14:58:42.966 Link-protection Down
```



 ChatGPT

The error messages you've posted appear to be log entries from some networking or routing system. Let's break down some of the information:

- CSPF (Constrained Shortest Path First) Failed:**
 - Entries like "CSPF failed: no route toward 192.0.2.224" indicate that the CSPF algorithm, which is used in routing protocols to find a constrained path, failed to find a valid route toward the specified IP address (192.0.2.224).
- Link-protection Down:**
 - The log entry "Link-protection Down" suggests that a link protection mechanism, likely in a network, is no longer active.
- Tunnel local repaired:**
 - The log entry "192.0.2.79: Tunnel local repaired" indicates that a tunnel to IP address 192.0.2.79 has been repaired locally.
- Clear Call: CSPF computation failed:**
 - "Clear Call: CSPF computation failed" suggests that a call was cleared due to the failure of the CSPF computation.

Without more context or the specific system/application generating these logs, it's challenging to provide a precise solution. However, these messages generally indicate issues with routing, path computation, or link failures in a network environment. You may want to check the configuration, status of links, and the CSPF algorithm implementation in your networking equipment or software. If there are specific error codes or messages associated with these log entries, those would be helpful for a more detailed analysis. Additionally, consulting the documentation of the system generating these logs may provide insights into the meaning of these messages in the context of your specific setup.



**Sounds great! So what can go
wrong??**

Hallucinations

- Where information is presented as true, but has been generated artificially.
- Basically it just makes things up.

In August, MSN featured a story on its homepage that falsely claimed President Joe Biden had fallen asleep during a moment of silence for victims of the catastrophic Maui wildfire.

The next month, Microsoft republished a story about Brandon Hunter, a former NBA player who died unexpectedly at the age of 42, under the headline, “Brandon Hunter useless at 42.”

Then, in October, Microsoft republished an article that claimed that San Francisco Supervisor Dean Preston had resigned from his position after criticism from Elon Musk.

The story was entirely false.

<https://edition.cnn.com/2023/11/02/tech/microsoft-ai-news/index.html>

Two US lawyers fined for submitting fake court citations from ChatGPT

Law firm also penalised after chatbot invented six legal cases that were then used in an aviation injury claim



▣ The judge said one of the fake decisions had 'some traits that are superficially consistent with actual judicial decisions' but other portions contained 'gibberish' and were 'nonsensical'.

Photograph: Richard Drew/AP

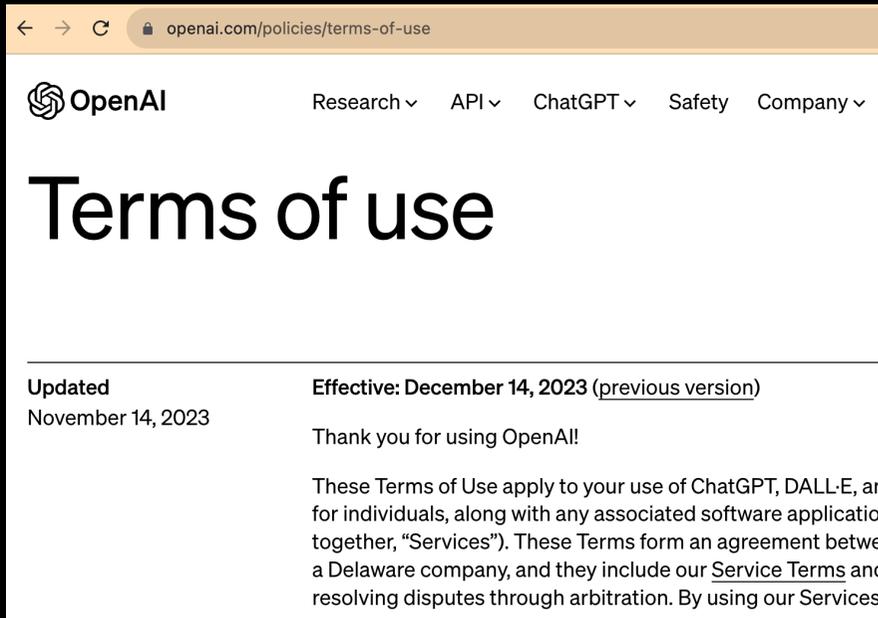
A US judge has fined two lawyers and a law firm \$5,000 (£3,935) after fake citations generated by ChatGPT were submitted in a court filing.

<https://www.theguardian.com/technology/2023/jun/23/two-us-lawyers-fined-submitting-fake-court-citations-chatgpt>

Not creative

- Being a statistical model, an LLM is *not* creative
- It does not have the context and insight that a person can hold
- Prompts matter, and your results will vary wildly

Ownership of your content



The screenshot shows the OpenAI website's Terms of Use page. The browser address bar displays 'openai.com/policies/terms-of-use'. The page features the OpenAI logo and a navigation menu with links for Research, API, ChatGPT, Safety, and Company. The main heading is 'Terms of use'. Below this, there is a section with two columns: 'Updated November 14, 2023' and 'Effective: December 14, 2023 (previous version)'. The text begins with 'Thank you for using OpenAI!' and continues with 'These Terms of Use apply to your use of ChatGPT, DALL-E, and...'.

Our Use of Content. We may use Content to provide, maintain, develop, and improve our Services, comply with applicable law, enforce our terms and policies, and keep our Services safe.

Ownership of your content

Our commitments

Ownership: You own and control your data

- ✓ We do *not* train on your data from ChatGPT Enterprise or our API Platform
- ✓ You own your inputs and outputs (where allowed by law)
- ✓ You control how long your data is retained (ChatGPT Enterprise)

3.2 *Our Obligations for Customer Content.* We will process and store Customer Content in accordance with our Enterprise privacy commitments. We will only use Customer Content as necessary to provide you with the Services, comply with applicable law, and enforce OpenAI Policies. We will not use Customer Content to develop or improve the Services.

Summary

- ChatGPT (and other LLMs) can be a great tool
- You need a human in the middle to validate everything
- A LLM does not replace skilled workers, but can be used to support them
- Make sure you know your organisations privacy and information handling policies before using any LLM

Questions?

