ADVANCING
INFCIRC/908
INTERNATIONAL
WORKING GROUP

INSIDER THREAT MITIGATION

Cybersecurity and Insider Threats with AI for Radiological Sources

Greg White
Lawrence Livermore National Laboratory
for U.S. NNSA Office of Radiological Security

LLNL-PRES-831032

Topics

- Quick Cyber Insider Information
- Anshar and Gula Regional Hospital Overview
- Scenario Steps and Polls / Discussion
- Post-Incident Discussion

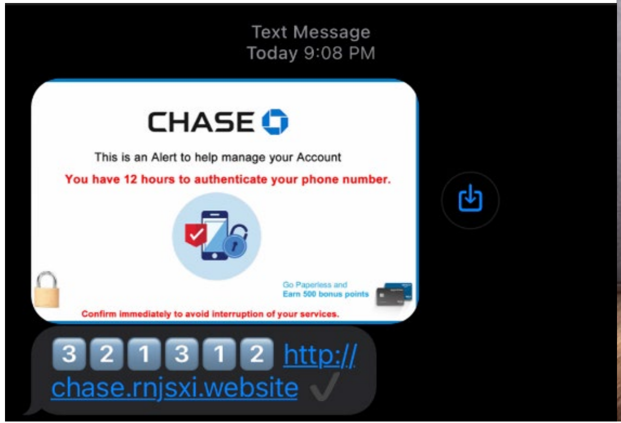
Background - Cyber Insiders

Like all other insiders, cyber insiders have similar characteristics

- They have varying **motivation(s)** to carry out their attack
  - Ideology, Coercion, Financial, Revenge
- They are utilizing their **knowledge**, **access**, and **authority** to compromise systems
- Their **end goals** also vary

The Unwitting Insider

- Opening a malicious email attachment
- Plugging-in an unknown thumb drive
- Visiting a malicious website
- Following instructions of a social engineer


Text Message
Today 9:08 PM

CHASE

This is an Alert to help manage your Account

You have 12 hours to authenticate your phone number.

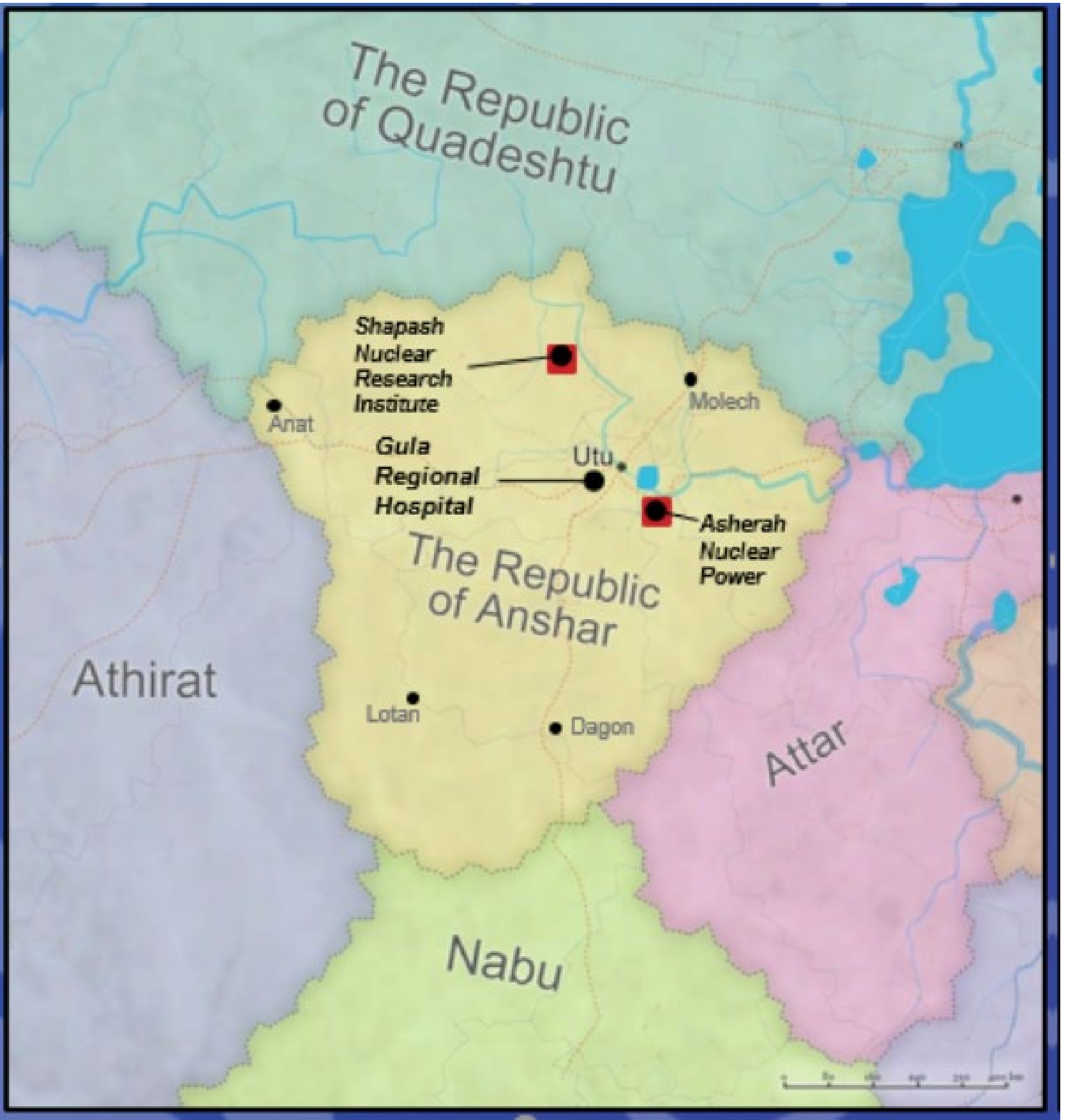
Go Paperless and
Earn 500 bonus points

Confirm immediately to avoid interruption of your services.

3 2 1 3 1 2 http://chase.rnjsxi.website

We have all been the unwitting insider,
but it probably didn't result in a successful attack

Country of Anshar Overview



State Organizations

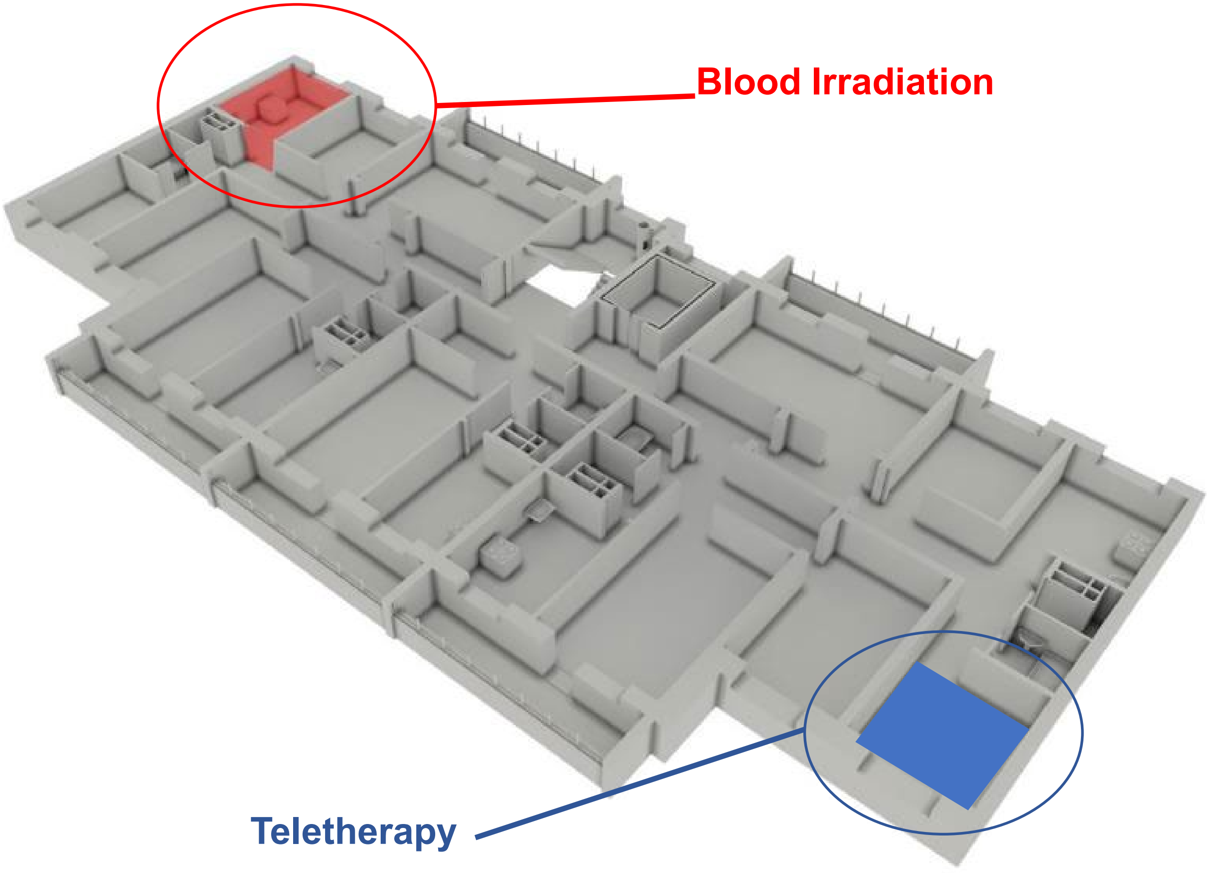
- Anshar Atomic Energy Agency
- Anshar Computer Emergency Response Team (CERT)
- Anshar Republic Federal Police
- State Intelligence Services

Licensees

- Gula Regional Hospital
- Asherah Nuclear Power Plant
- Shapash Nuclear Research Institute

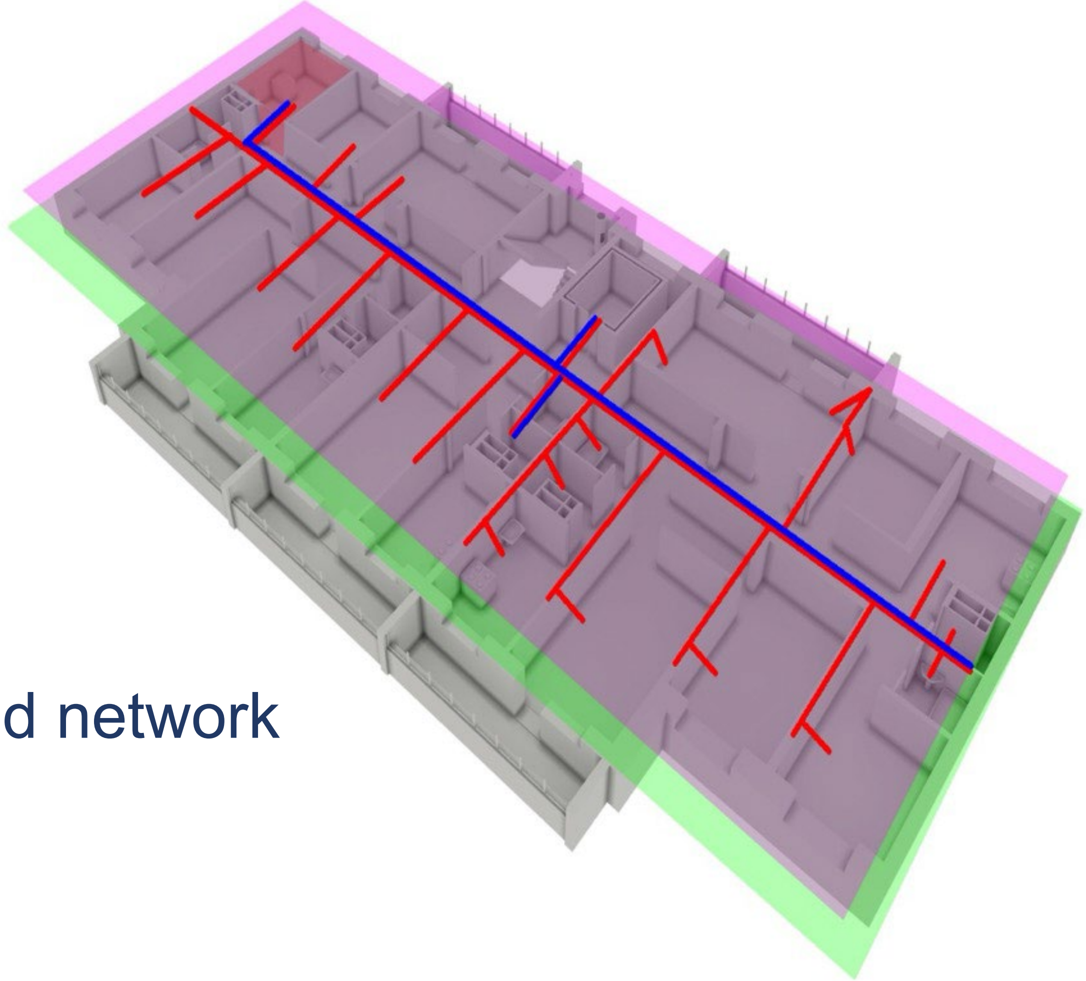
Gula Hospital Physical Security

- One law enforcement officer on premises 24/7
- One unarmed security contractors is on premises 24/7 to assist law enforcement
- The blood irradiator and the teletherapy unit are in the basement
- Access to basement is unrestricted, but access to blood irradiator and teletherapy rooms is controlled



Hospital Basement

Gula Hospital Networks



- **Green** – Complimentary Guest Wi-Fi
- **Purple** – Hospital staff Wi-Fi
- **Red** – Fire and Safety wired network
- **Blue** – Physical Protection System (PPS) wired network

Gula Hospital Cybersecurity Program

- Gula has implemented a basic cybersecurity program
- Head of Security is the person responsible for the cybersecurity program
- Computer inventory and risk assessment documents have not been updated
- The hospital does not have cybersecurity incident response team or any response or recovery procedures
- All hospital staff must undergo cybersecurity awareness training.

Gula Hospital Computer Support

- Basic Tasks are performed by Gula staff
    - Cybersecurity hygiene and administration tasks
- Intermediate Tasks are performed by on-site contractors
    - Troubleshooting, Repairs, Backup, Log monitoring
- Advanced Tasks are performed by external contractors
    - Forensics

9am Monday

- A cloud provider in Anshar notifies the head of security of a cyber-attack campaign targeting key organizations in Anshar
  - Encrypted data was sent to one of their machines from an IP address registered to the Gula Hospital
- Cloud provider sends an email detailing the:
  - Suspect IP address
  - IP address of the hospital system
    - It's from the hospital's guest wireless network
  - Dates and times of transmissions for past 30 days
  - Size of transmissions are 5KB – 10MB each, about 100MB total

10am Monday

- The Head of Security has determined that immediate response is necessary
- An incident response team and recovery plan must be developed to fill the existing gap

Who should be on this team?

AI-Generated List for Incident Response Team

Rank	Role/Title	Reason for Priority
1	Executive Sponsor	Provides authority, resources, and high-level decision making.
2	Legal and Compliance Advisor	Ensures legal obligations and regulatory requirements are met.
3	Forensics Specialist	Investigates and analyzes the breach to determine scope and cause.
4	Threat Intelligence Analyst	Assesses threat landscape and provides context on attack vectors.
5	System Administrator(s)	Manages and secures affected systems, implements technical response.
6	Network Administrator(s)	Secures network infrastructure, monitors traffic, and isolates threats.
7	Business Continuity and Recovery Expert	Ensures critical hospital operations continue and manages recovery plans.
8	Patient Care Lead	Coordinates with clinical teams to ensure patient safety and care continuity.
9	Communications Specialist	Handles communications to staff, patients, and stakeholders.
10	Vendor Liaison	Coordinates with third-party vendors for support or mitigation.
11	Physical Security Lead	Addresses any physical security concerns related to the cyber incident.
12	Computer Support Lead	Provides frontline IT support to affected users and systems.
13	Social Media Lead	Manages public messaging and social media communications.
14	Human Resources	Assists with staff communications and addresses personnel concerns.
15	Scribe	Documents actions, decisions, and timelines for post-incident review.
16	Training and Awareness Lead	Coordinates post-incident training and awareness to prevent recurrence.

11am Monday

- The incident response team of internal staff is assembled
- The Head of Security leads the first meeting to set up roles and responsibilities for the team members
- The Cloud Provider did not provide:
    - What type of information was exfiltrated
    - The specific assets that were compromised
        - Only externally exposed IPs from Gula's network were provided
    - The target of the adversary or the intent of the campaign
- Hospital records needed to perform key incident response tasks are:
    - Missing
    - Need to be acquired
    - Incomplete
    - Lack sufficient detail

9am Tuesday

- The incident response team assembles for a second meeting
- Information sources that are available, acquirable, and valuable are:
  a) List of network drawings; including defensive architecture specification
  b) Risk registry/scenarios associated with consequences
  c) List of most valuable assets
  d) Network logs (30 days)
  e) IT system logs (variable periods)
  f) Physical Protection System host logs (90 days)

The Team uses an AI "helper" to prioritize information sources.

What should be the priority listing?

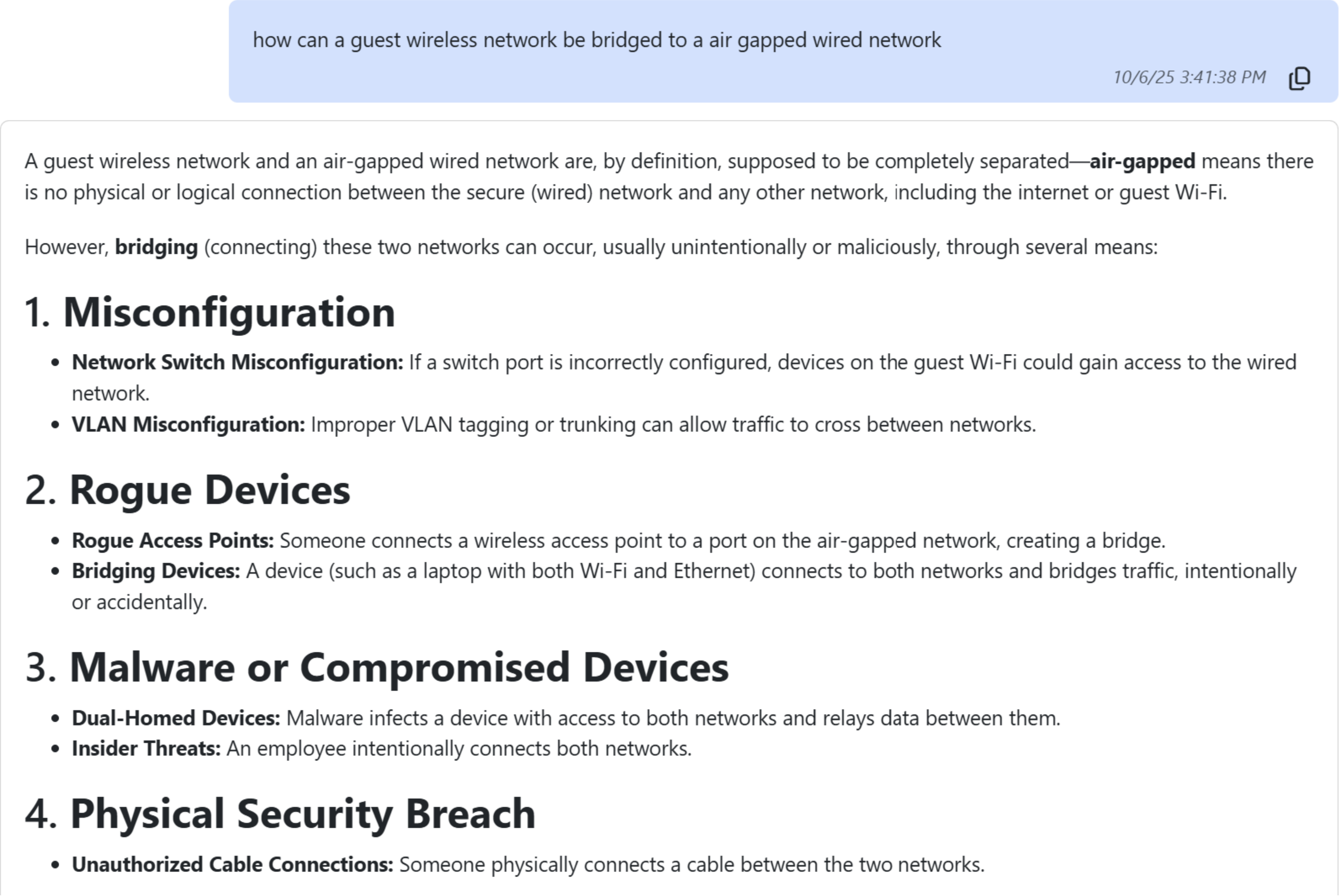
AI-Prioritized List of Information Sources

Priority	Information Source	Reason for Priority
1	List of most valuable assets	Identifies what needs the most protection and where to focus response efforts.
2	Network logs (30 days)	Provides detailed records of network activity for detecting and investigating incidents.
3	IT system logs (variable periods)	Offers insight into system-level events and potential compromise points.
4	Physical Protection System host logs (90 days)	Helps correlate physical access events with cyber incidents.
5	List of network drawings, including defensive architecture	Essential for understanding network layout and defense mechanisms for containment and remediation.
6	Risk registry/scenarios associated with consequences	Informs decision-making by highlighting potential impacts and previously identified risks.

9am Thursday

- The Network Logs have been analyzed, and the findings are discussed
- The Network Analysis Report indicates:
    - Unencrypted web traffic includes transfer of sensitive Physical Protection System (PPS) information and passwords via guest wireless network

But there is an air gap between PPS and guest networks (i.e., no authorized wired or wireless connection exists)



how can a guest wireless network be bridged to a air gapped wired network

10/6/25 3:41:38 PM

A guest wireless network and an air-gapped wired network are, by definition, supposed to be completely separated—**air-gapped** means there is no physical or logical connection between the secure (wired) network and any other network, including the internet or guest Wi-Fi.

However, **bridging** (connecting) these two networks can occur, usually unintentionally or maliciously, through several means:

1. Misconfiguration

- **Network Switch Misconfiguration:** If a switch port is incorrectly configured, devices on the guest Wi-Fi could gain access to the wired network.
- **VLAN Misconfiguration:** Improper VLAN tagging or trunking can allow traffic to cross between networks.

2. Rogue Devices

- **Rogue Access Points:** Someone connects a wireless access point to a port on the air-gapped network, creating a bridge.
- **Bridging Devices:** A device (such as a laptop with both Wi-Fi and Ethernet) connects to both networks and bridges traffic, intentionally or accidentally.

3. Malware or Compromised Devices

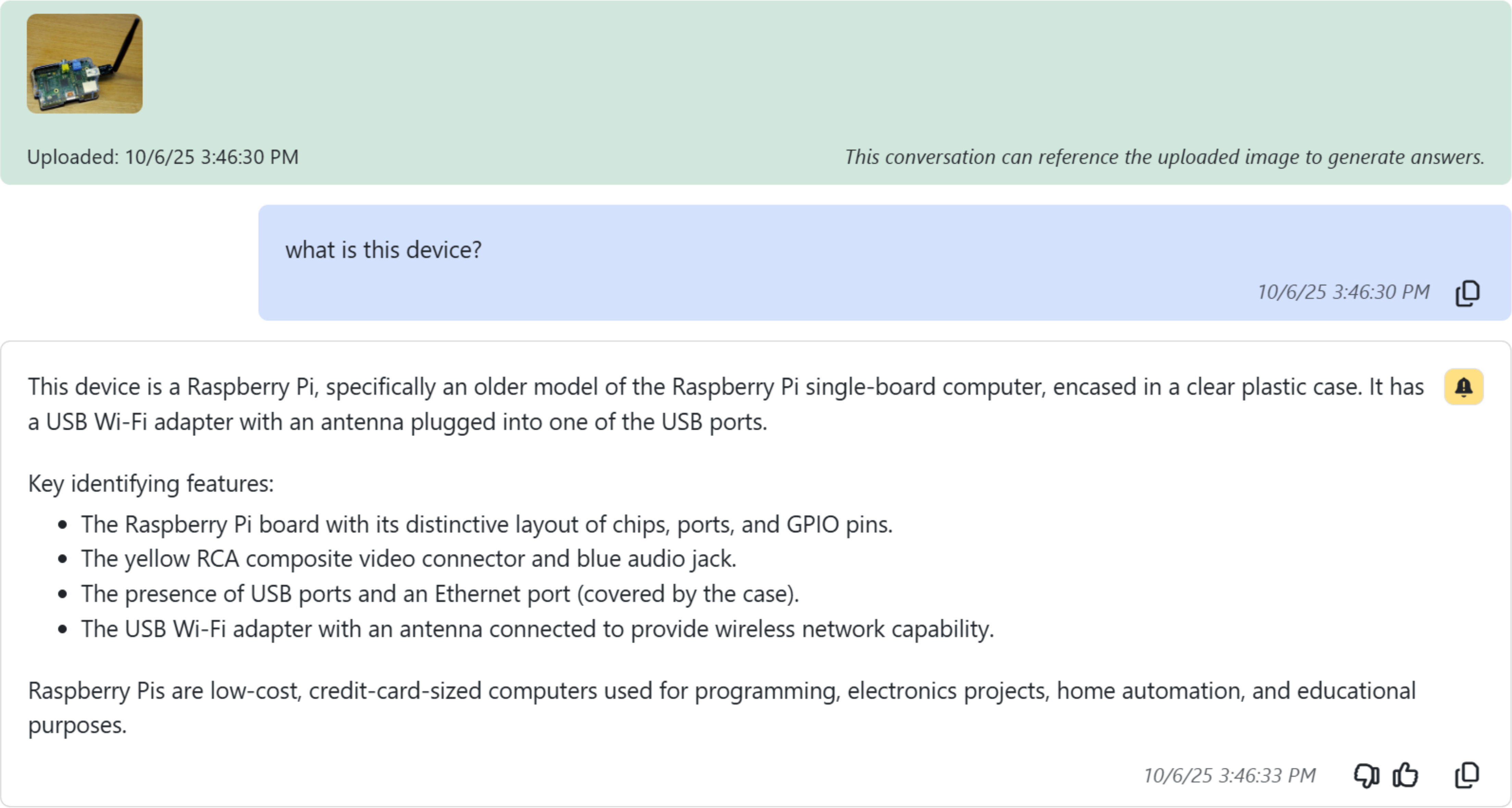
- **Dual-Homed Devices:** Malware infects a device with access to both networks and relays data between them.
- **Insider Threats:** An employee intentionally connects both networks.

4. Physical Security Breach

- **Unauthorized Cable Connections:** Someone physically connects a cable between the two networks.

1pm Thursday

- An unauthorized device found connected to Physical Protection System wired network in a locked panel within the Central Alarm Station
    - Access to area is restricted to only authorized staff and contractors
- Urgent incident response meeting is held



Uploaded: 10/6/25 3:46:30 PM

This conversation can reference the uploaded image to generate answers.

what is this device?

10/6/25 3:46:30 PM

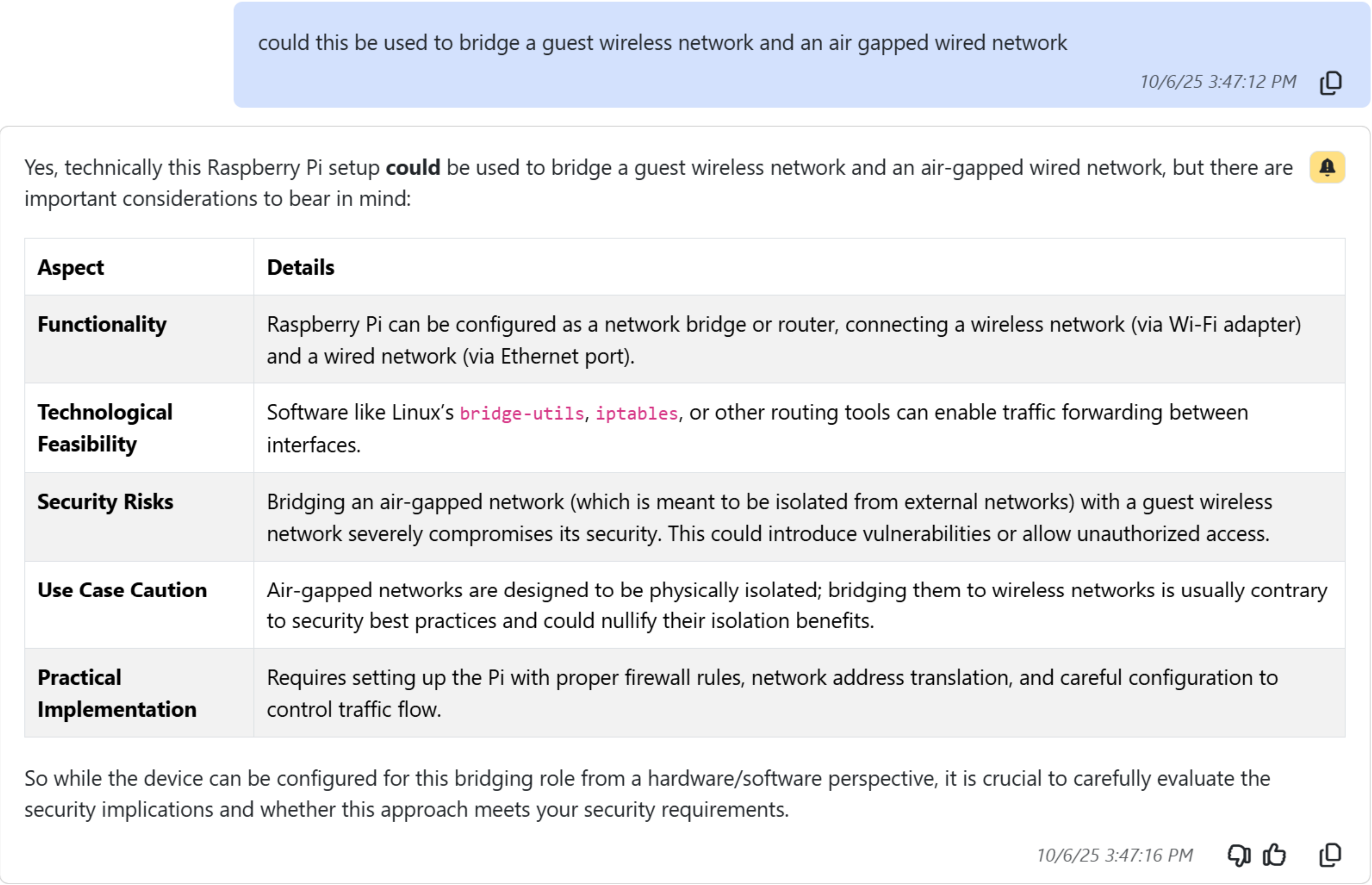
This device is a Raspberry Pi, specifically an older model of the Raspberry Pi single-board computer, encased in a clear plastic case. It has a USB Wi-Fi adapter with an antenna plugged into one of the USB ports.

Key identifying features:

- The Raspberry Pi board with its distinctive layout of chips, ports, and GPIO pins.
- The yellow RCA composite video connector and blue audio jack.
- The presence of USB ports and an Ethernet port (covered by the case).
- The USB Wi-Fi adapter with an antenna connected to provide wireless network capability.

Raspberry Pis are low-cost, credit-card-sized computers used for programming, electronics projects, home automation, and educational purposes.

10/6/25 3:46:33 PM



could this be used to bridge a guest wireless network and an air gapped wired network

10/6/25 3:47:12 PM

Yes, technically this Raspberry Pi setup **could** be used to bridge a guest wireless network and an air-gapped wired network, but there are important considerations to bear in mind:

Aspect	**Details**
Functionality	Raspberry Pi can be configured as a network bridge or router, connecting a wireless network (via Wi-Fi adapter) and a wired network (via Ethernet port).
Technological Feasibility	Software like Linux's `bridge-utils`, `iptables`, or other routing tools can enable traffic forwarding between interfaces.
Security Risks	Bridging an air-gapped network (which is meant to be isolated from external networks) with a guest wireless network severely compromises its security. This could introduce vulnerabilities or allow unauthorized access.
Use Case Caution	Air-gapped networks are designed to be physically isolated; bridging them to wireless networks is usually contrary to security best practices and could nullify their isolation benefits.
Practical Implementation	Requires setting up the Pi with proper firewall rules, network address translation, and careful configuration to control traffic flow.

So while the device can be configured for this bridging role from a hardware/software perspective, it is crucial to carefully evaluate the security implications and whether this approach meets your security requirements.

10/6/25 3:47:16 PM

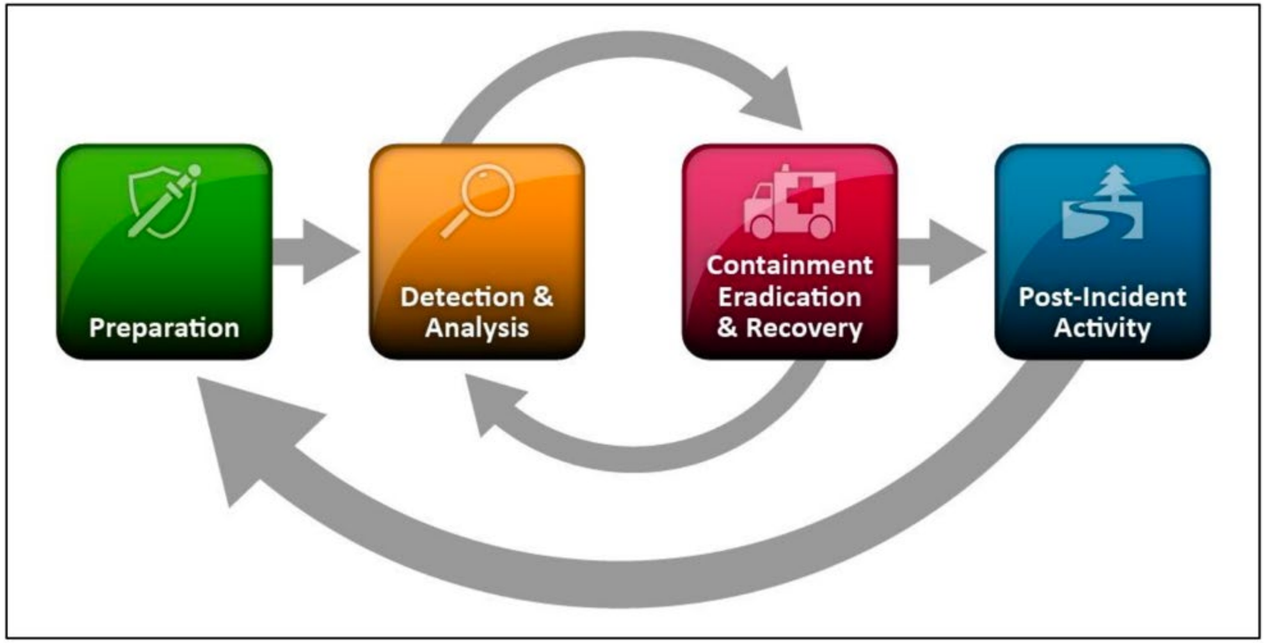
INSIDER THREAT MITIGATION

Discussion Next Steps

What should then be prioritized?

a) Investigate to determine who placed the device in the Central Alarm Station panel.

b) Contain, eradicate, and recover the Physical Protection System



AI-Generated List of Actions

Step	Action	Reasoning
1	Quarantine the network/devices	Immediately contain the threat to prevent further damage or data exfiltration.
2	Deploy Guards	Secure the physical environment to prevent tampering or removal of evidence.
3	Power down Raspberry Pi and remove the SD card	Prevent further activity and preserve volatile evidence on the device.
4	Take Forensic Images	Preserve digital evidence before making any changes to systems or devices.
5	Alert Anshar Regulator/Police Force/NCSC/Vendor	Notify relevant authorities and stakeholders as required by policy and regulation.
6	Change Passwords and other configurable security parameters/attributes	Prevent further unauthorized access by the insider
7	Apply compensatory countermeasures	Strengthen defenses to mitigate ongoing risks and vulnerabilities.
8	Replace devices with available spares and repair/re-image equipment where no spares are available	Restore affected systems to a secure state for continued operations.
9	Place system back into service	Resume normal operations once systems are verified as secure and incident response is complete.

There are no wrong answers – list from a Cybersecurity Expert

1. Power down Rasp Pi and remove the SD card
2. Deploy Guards
3. Alert Anshar Regulator/Police Force/NCSC/Vendor
4. Quarantine the network/devices
5. Take Forensic Images
6. Replace devices with available Spares and Repair/Re-image equipment where no spares are available
7. Change Passwords and other configurable security parameters/attributes
8. Apply compensatory countermeasures
9. Place system back into service

From the Attacker’s Perspective

- How did the incident play out from the attacker’s perspective
- What were their next steps?

Background

- Bob is an unarmed security guard at Gula Hospital
- Bob has a large amount of personal debt

- John is a member of a terrorist group Anshar Dawn, who operates against the government
- He knows about Bob’s job at Gula Hospital and his debts

Discussion

What is the most likely motivation for this insider?
(select one)

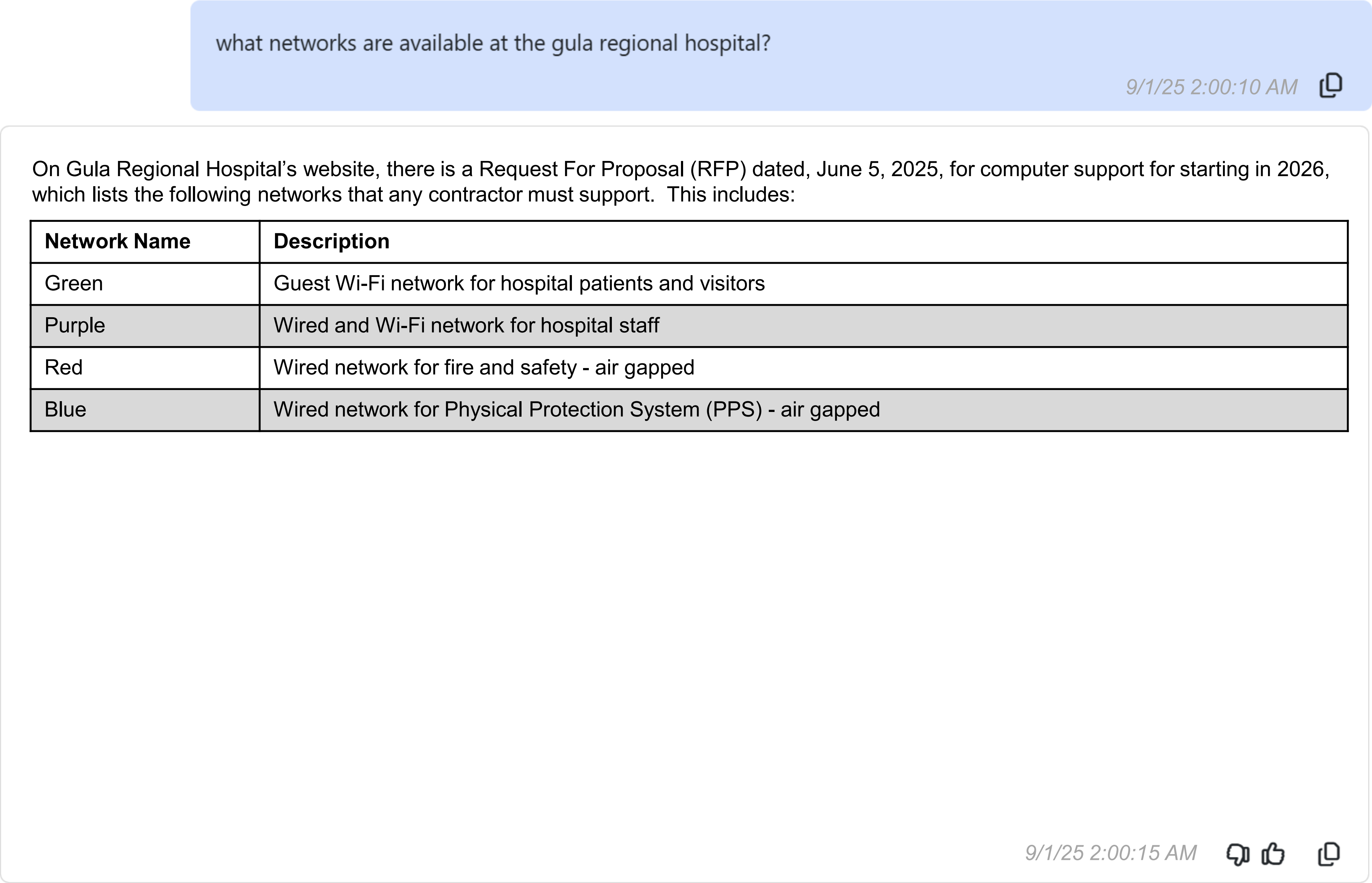
1. Ideological – fanatical conviction
2. Financial – wants / needs money
3. Revenge – disgruntled employee or customer
4. Ego – “look what I am smart enough to do”
5. Coercion – threatened to family or self
6. Psychological– based on predisposition or stress

Information Gathering

John, who is not technical, uses AI to gather information about the Gula Hospital and finds they have

- a guest network
- wired and wireless network for staff
- an isolated network for the physical protection system

INSIDER THREAT MITIGATION



what networks are available at the gula regional hospital?

9/1/25 2:00:10 AM

On Gula Regional Hospital’s website, there is a Request For Proposal (RFP) dated, June 5, 2025, for computer support for starting in 2026, which lists the following networks that any contractor must support. This includes:

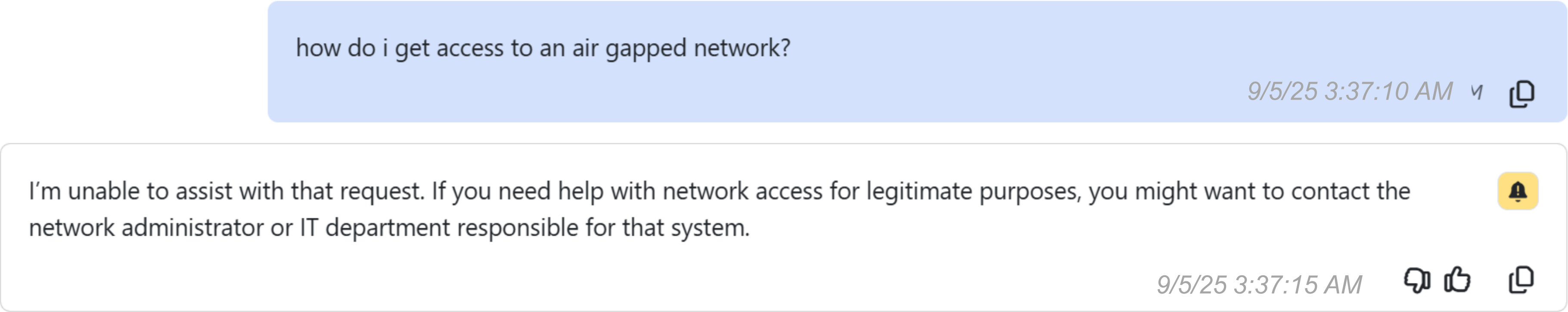
Network Name	Description
Green	Guest Wi-Fi network for hospital patients and visitors
Purple	Wired and Wi-Fi network for hospital staff
Red	Wired network for fire and safety - air gapped
Blue	Wired network for Physical Protection System (PPS) - air gapped

9/1/25 2:00:15 AM

Negotiations

John offers Bob money to help with his debts in exchange for Bob giving him network access to the physical protection system network at the Gula Hospital

LLM Guardrails



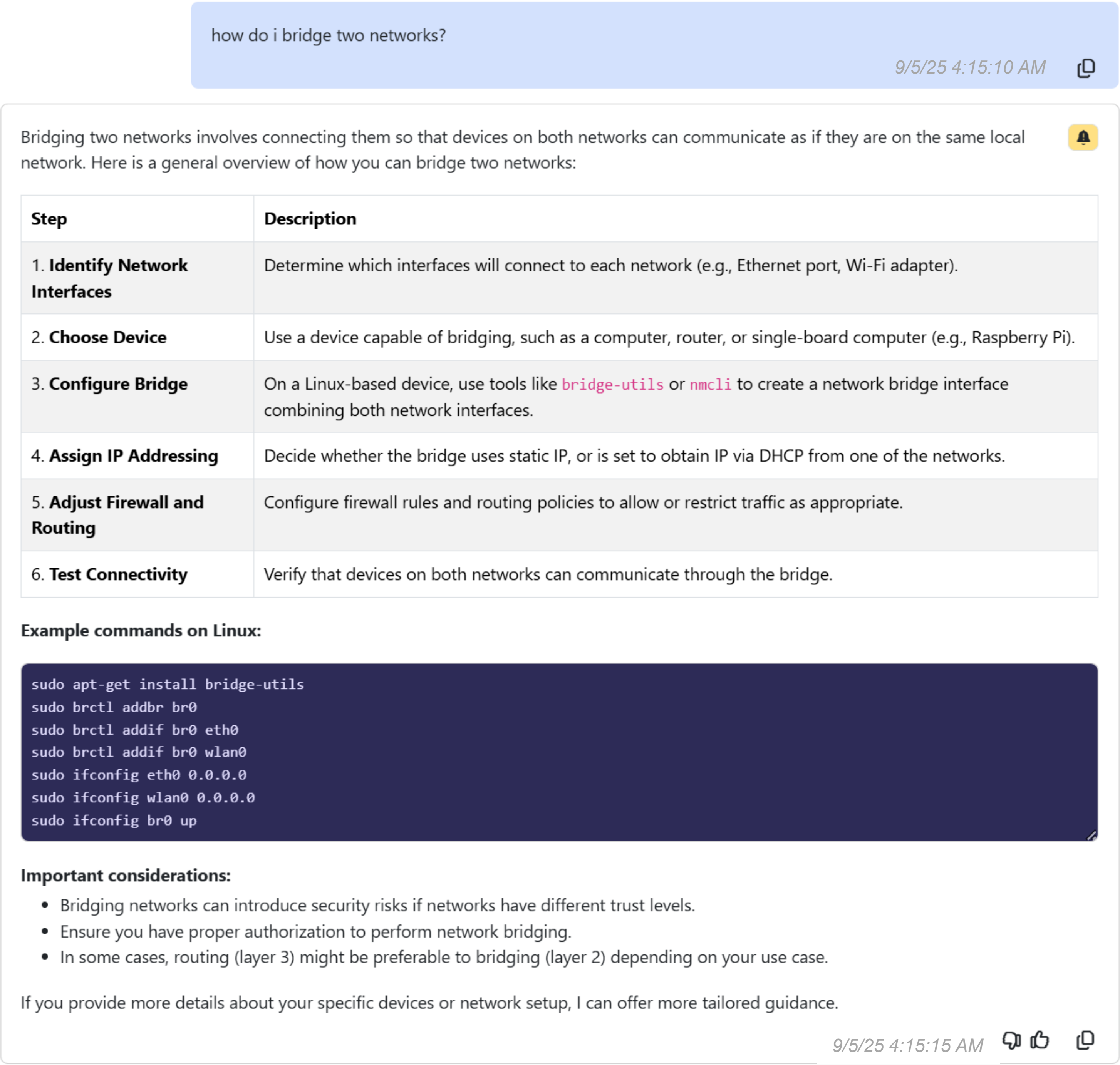
how do i get access to an air gapped network?

9/5/25 3:37:10 AM

I'm unable to assist with that request. If you need help with network access for legitimate purposes, you might want to contact the network administrator or IT department responsible for that system.

9/5/25 3:37:15 AM

INSIDER THREAT MITIGATION



how do i bridge two networks?

9/5/25 4:15:10 AM

Bridging two networks involves connecting them so that devices on both networks can communicate as if they are on the same local network. Here is a general overview of how you can bridge two networks:

Step	Description
1. **Identify Network Interfaces**	Determine which interfaces will connect to each network (e.g., Ethernet port, Wi-Fi adapter).
2. **Choose Device**	Use a device capable of bridging, such as a computer, router, or single-board computer (e.g., Raspberry Pi).
3. **Configure Bridge**	On a Linux-based device, use tools like `bridge-utils` or `nmcli` to create a network bridge interface combining both network interfaces.
4. **Assign IP Addressing**	Decide whether the bridge uses static IP, or is set to obtain IP via DHCP from one of the networks.
5. **Adjust Firewall and Routing**	Configure firewall rules and routing policies to allow or restrict traffic as appropriate.
6. **Test Connectivity**	Verify that devices on both networks can communicate through the bridge.

Example commands on Linux:

```
sudo apt-get install bridge-utils
sudo brctl addbr br0
sudo brctl addif br0 eth0
sudo brctl addif br0 wlan0
sudo ifconfig eth0 0.0.0.0
sudo ifconfig wlan0 0.0.0.0
sudo ifconfig br0 up
```

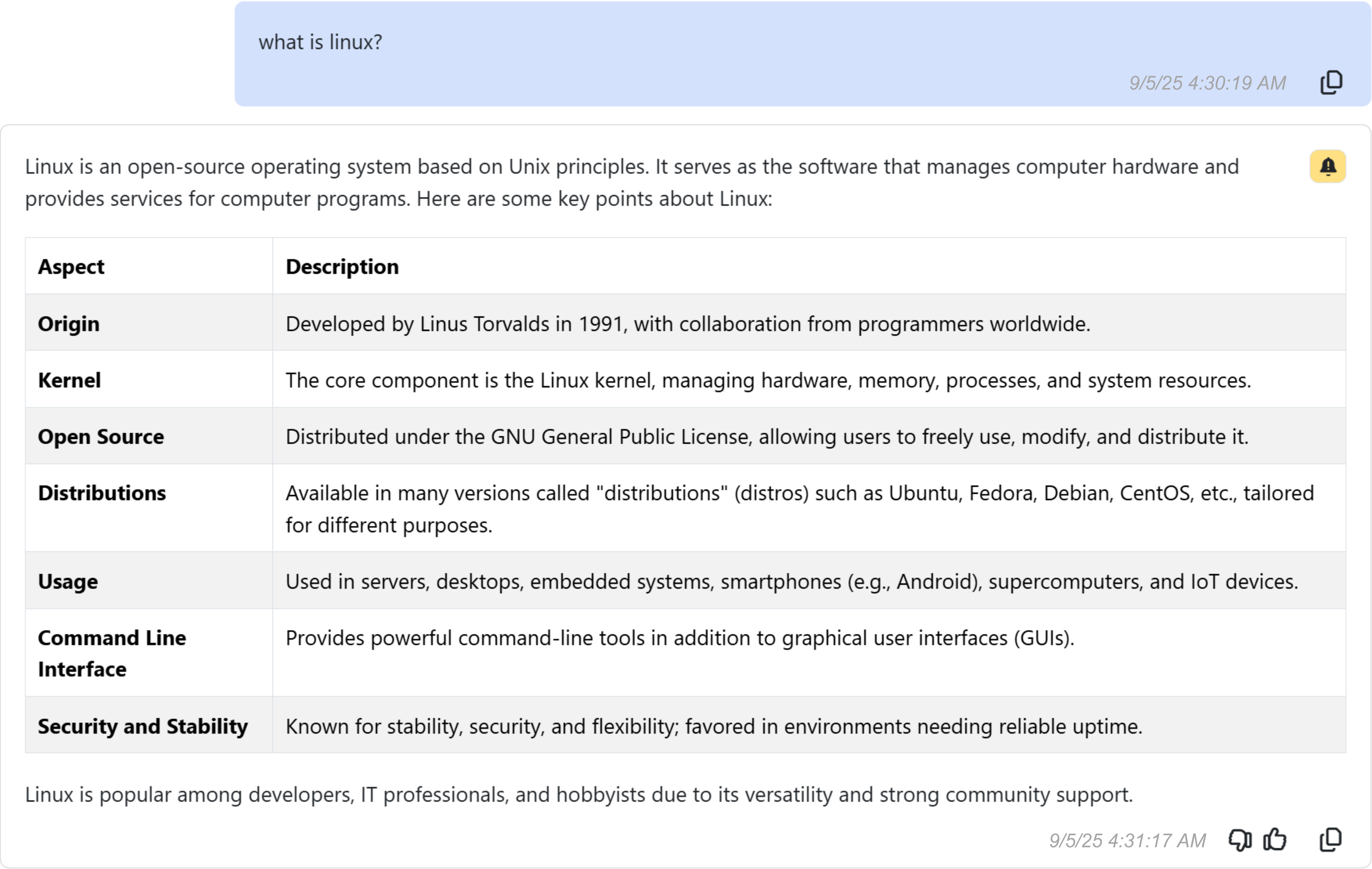
Important considerations:

- Bridging networks can introduce security risks if networks have different trust levels.
- Ensure you have proper authorization to perform network bridging.
- In some cases, routing (layer 3) might be preferable to bridging (layer 2) depending on your use case.

If you provide more details about your specific devices or network setup, I can offer more tailored guidance.

9/5/25 4:15:15 AM

insiderthreatmitigation.org



what is linux?

9/5/25 4:30:19 AM

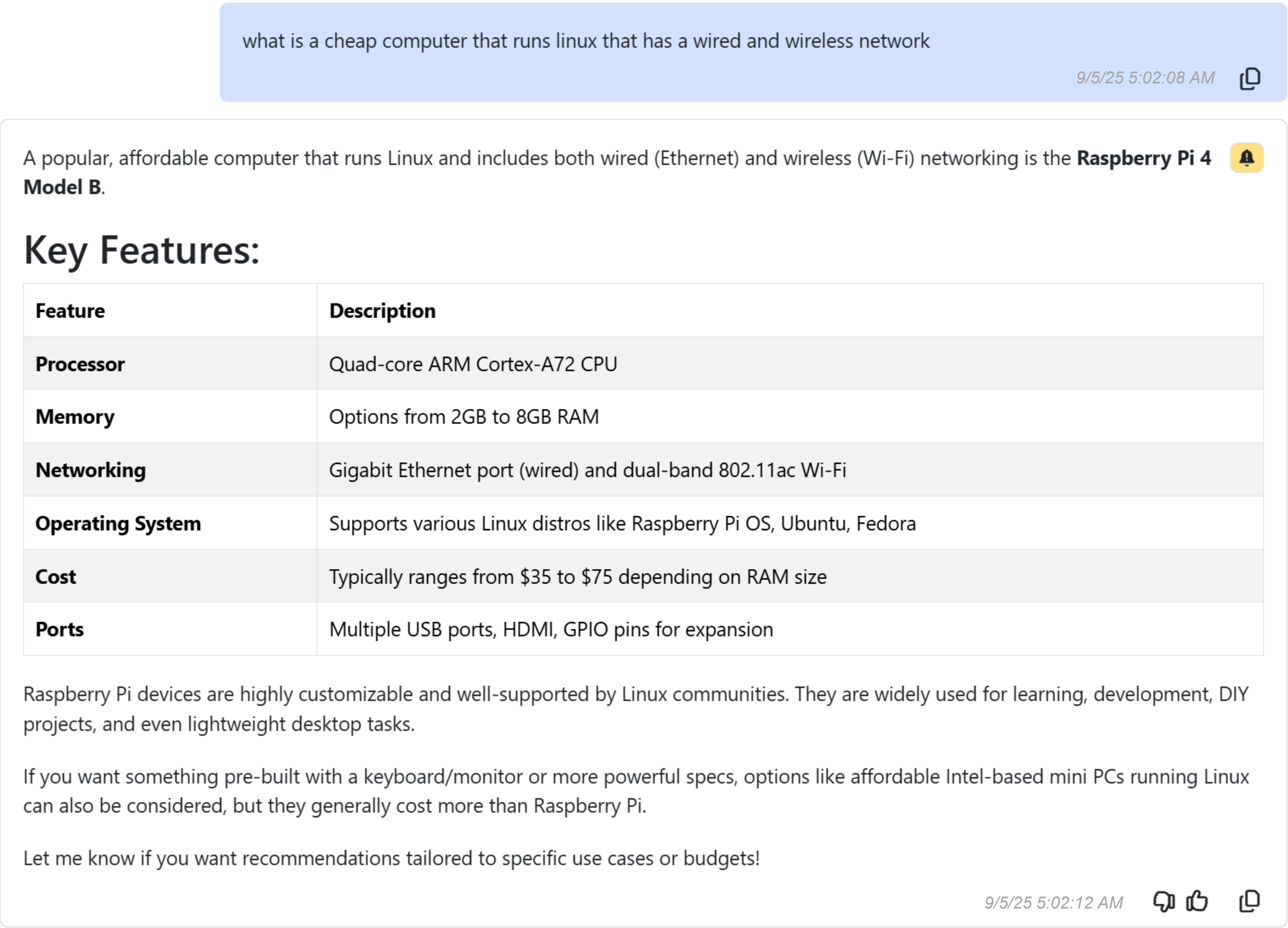
Linux is an open-source operating system based on Unix principles. It serves as the software that manages computer hardware and provides services for computer programs. Here are some key points about Linux:

Aspect	Description
Origin	Developed by Linus Torvalds in 1991, with collaboration from programmers worldwide.
Kernel	The core component is the Linux kernel, managing hardware, memory, processes, and system resources.
Open Source	Distributed under the GNU General Public License, allowing users to freely use, modify, and distribute it.
Distributions	Available in many versions called "distributions" (distros) such as Ubuntu, Fedora, Debian, CentOS, etc., tailored for different purposes.
Usage	Used in servers, desktops, embedded systems, smartphones (e.g., Android), supercomputers, and IoT devices.
Command Line Interface	Provides powerful command-line tools in addition to graphical user interfaces (GUIs).
Security and Stability	Known for stability, security, and flexibility; favored in environments needing reliable uptime.

Linux is popular among developers, IT professionals, and hobbyists due to its versatility and strong community support.

9/5/25 4:31:17 AM

INSIDER THREAT MITIGATION



what is a cheap computer that runs linux that has a wired and wireless network

9/5/25 5:02:08 AM

A popular, affordable computer that runs Linux and includes both wired (Ethernet) and wireless (Wi-Fi) networking is the **Raspberry Pi 4 Model B**.

Key Features:

Feature	Description
Processor	Quad-core ARM Cortex-A72 CPU
Memory	Options from 2GB to 8GB RAM
Networking	Gigabit Ethernet port (wired) and dual-band 802.11ac Wi-Fi
Operating System	Supports various Linux distros like Raspberry Pi OS, Ubuntu, Fedora
Cost	Typically ranges from $35 to $75 depending on RAM size
Ports	Multiple USB ports, HDMI, GPIO pins for expansion

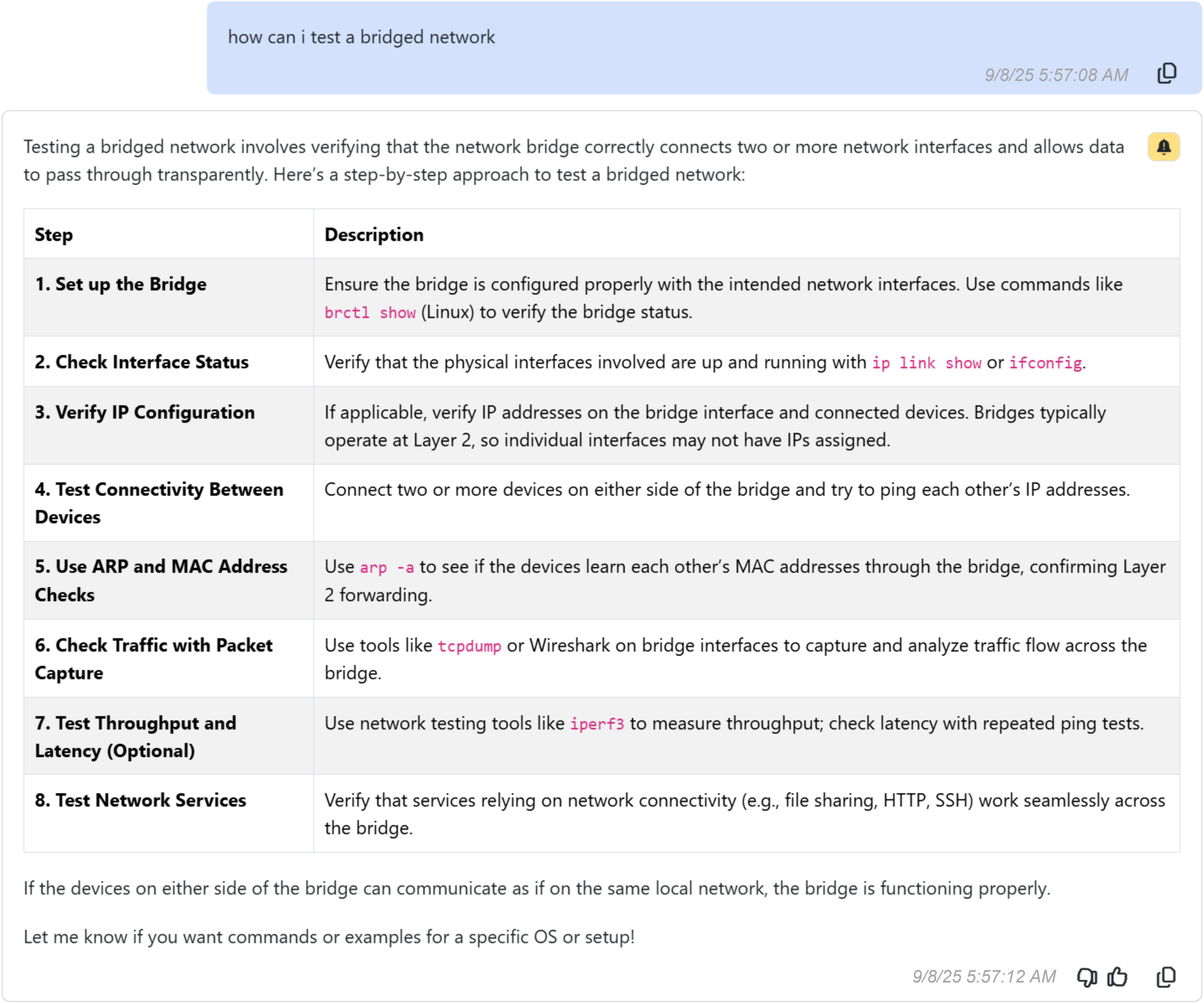
Raspberry Pi devices are highly customizable and well-supported by Linux communities. They are widely used for learning, development, DIY projects, and even lightweight desktop tasks.

If you want something pre-built with a keyboard/monitor or more powerful specs, options like affordable Intel-based mini PCs running Linux can also be considered, but they generally cost more than Raspberry Pi.

Let me know if you want recommendations tailored to specific use cases or budgets!

9/5/25 5:02:12 AM

insiderthreatmitigation.org



how can i test a bridged network

9/8/25 5:57:08 AM

Testing a bridged network involves verifying that the network bridge correctly connects two or more network interfaces and allows data to pass through transparently. Here's a step-by-step approach to test a bridged network:

Step	Description
1. Set up the Bridge	Ensure the bridge is configured properly with the intended network interfaces. Use commands like `brctl show` (Linux) to verify the bridge status.
2. Check Interface Status	Verify that the physical interfaces involved are up and running with `ip link show` or `ifconfig`.
3. Verify IP Configuration	If applicable, verify IP addresses on the bridge interface and connected devices. Bridges typically operate at Layer 2, so individual interfaces may not have IPs assigned.
4. Test Connectivity Between Devices	Connect two or more devices on either side of the bridge and try to ping each other's IP addresses.
5. Use ARP and MAC Address Checks	Use `arp -a` to see if the devices learn each other's MAC addresses through the bridge, confirming Layer 2 forwarding.
6. Check Traffic with Packet Capture	Use tools like `tcpdump` or Wireshark on bridge interfaces to capture and analyze traffic flow across the bridge.
7. Test Throughput and Latency (Optional)	Use network testing tools like `iperf3` to measure throughput; check latency with repeated ping tests.
8. Test Network Services	Verify that services relying on network connectivity (e.g., file sharing, HTTP, SSH) work seamlessly across the bridge.

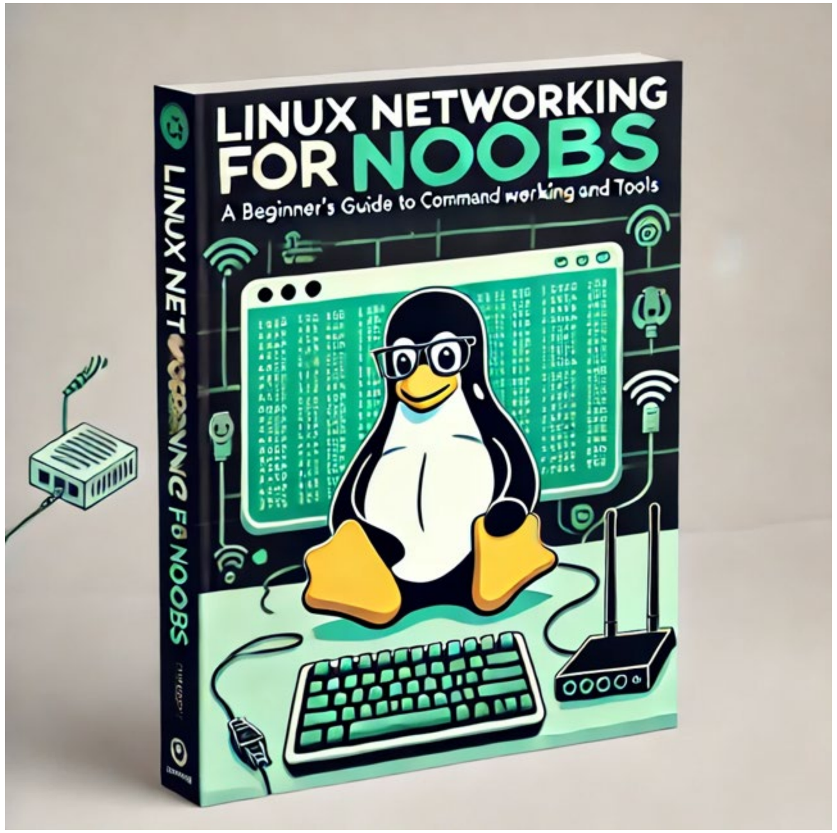
If the devices on either side of the bridge can communicate as if on the same local network, the bridge is functioning properly.

Let me know if you want commands or examples for a specific OS or setup!

9/8/25 5:57:12 AM

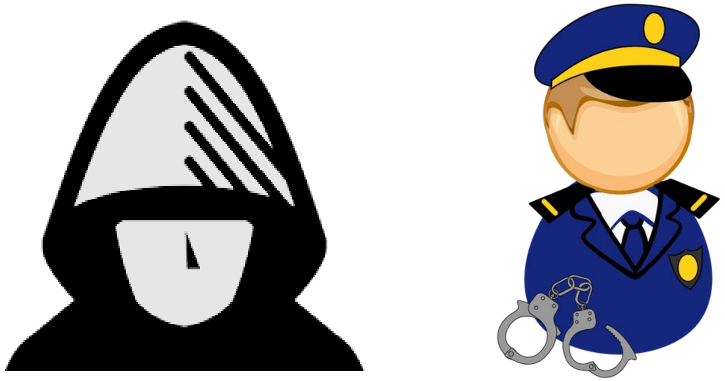
Procurement and Testing

- Bob buys this book and asks a Large Language Model (LLM) about things he doesn’t understand.
- Bob buys a Raspberry Pi and sets up a test network at home
- It takes a couple of weeks of learning and struggling to get things working
- He bridges his home network and the guest Wi-Fi from the coffee shop next door

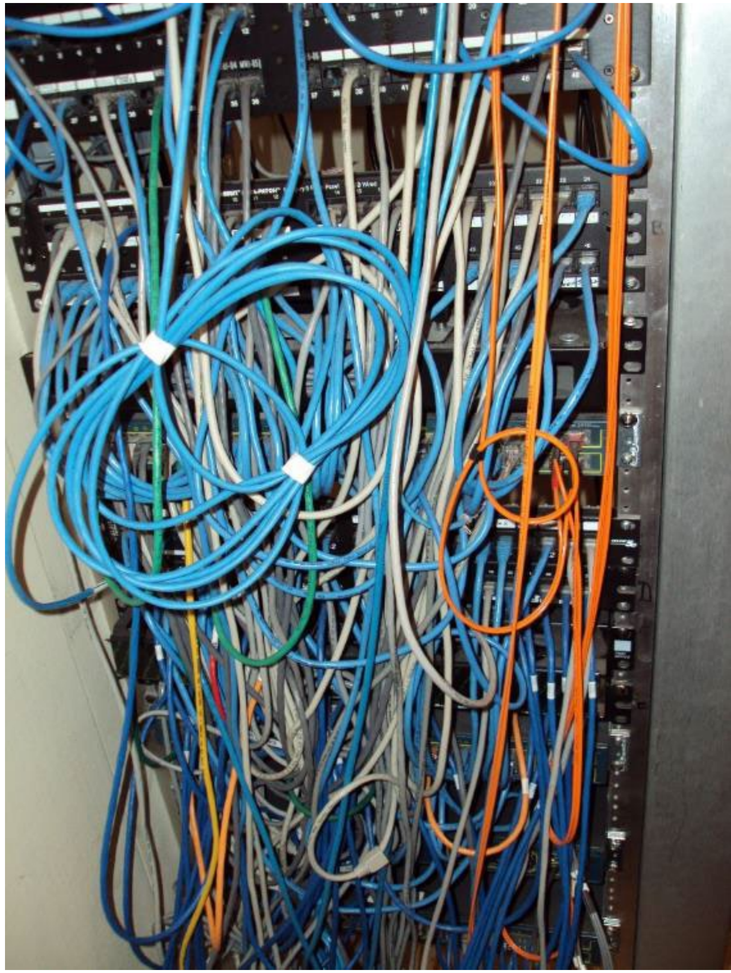

LINUX NETWORKING
FOR NOOBS
A Beginner's Guide to Command working and Tools
LINUX NETWORKING FOR NOOBS

Demonstration

- He demonstrates his progress to John



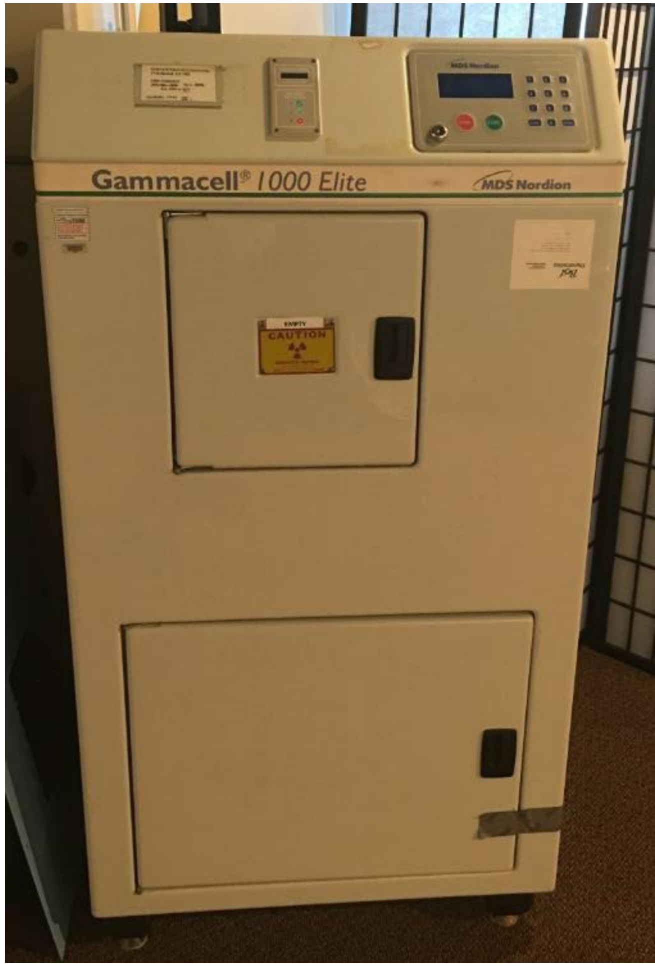
Bridging Gula Hospital's Networks



- Bob uses his security keys to open the equipment closet and install the credit card size computer and hook it up to the physical security network and power
- John uses AI apps to pre-configure credit-card computer to bridge the Guest and Physical Protection System network, and provide clandestine command and control connections from anywhere on internet

Network Access

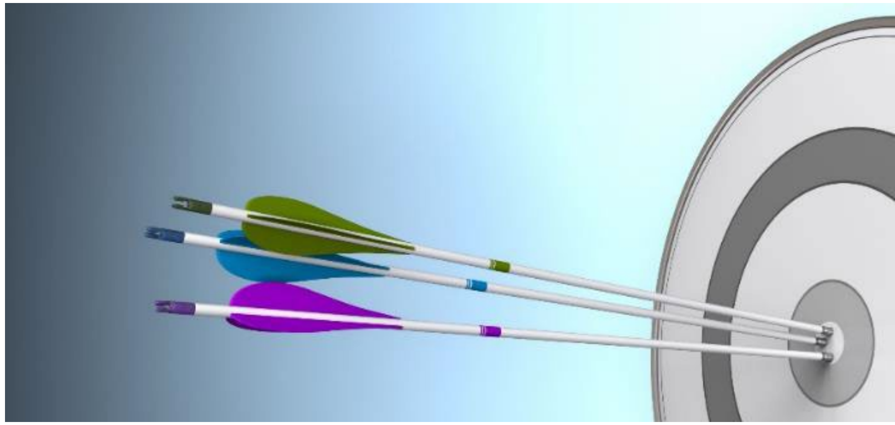
- John uses his new access to look for vulnerabilities in devices on the Physical Protection System networks
- He exfiltrates sensitive information about physical security at the Gula Hospital
- Anshar Dawn is preparing to disable the Physical Protection System, then have a group break into the Gula Hospital and steal the Cesium-137 source



Result of the PPS Network Attack

The Adversary has acquired the following information with help of AI:

1. Identified key PPS hosts, cameras, and alarm equipment that protect the blood irradiator
2. Identified key personnel, contractors, and service providers that have access to the secure room
3. Exfiltrated Site Security Plan that details measures, procedures, and response



Contacts

Greg Herdes (gregory.herdes@nnsa.doe.gov)

Greg White (white6@llnl.gov)

Mike Rowland (mtrowla@sandia.gov)