

# Beth Isreal Lahey Health (CareGroup)

Network Administration

TEAM MEMBERS



Team 8 - Network Admin.

Daniel Thach  
Christian Najera  
Angel Contreras

CIS 4900, Dr. Howell

---

# Meet the team

Christian Najera - Team Lead

Angel Contreras – Project Coordinator

Daniel Thach – Technical Coordinator

Team Lead:

- Guides delegation of meetings
- Ensures deliverables are produced
- Responsible for final submission

Project Coordinator:

- Leads project timeframes
- Guides delegation of deliverables

Technical Coordinator:

- Leads feedback review
- Ensures consistency of reports
- Guides technical review

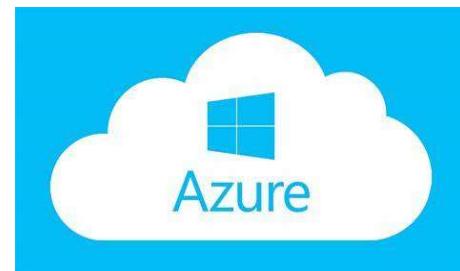
## CareGroup/BILH

- 100+ year old medical network
- State-of-the art inpatient/outpatient facilities
- Manages over 39,000 employees
- Committed to excellence in healthcare
- Notorious for IT collapse of 2002



# **Virtualization - A comprehensive solution**

- An inarguable need
- Tailored to accessibility
- Tailored to scalability
- Virtualization on Microsoft Azure Platform

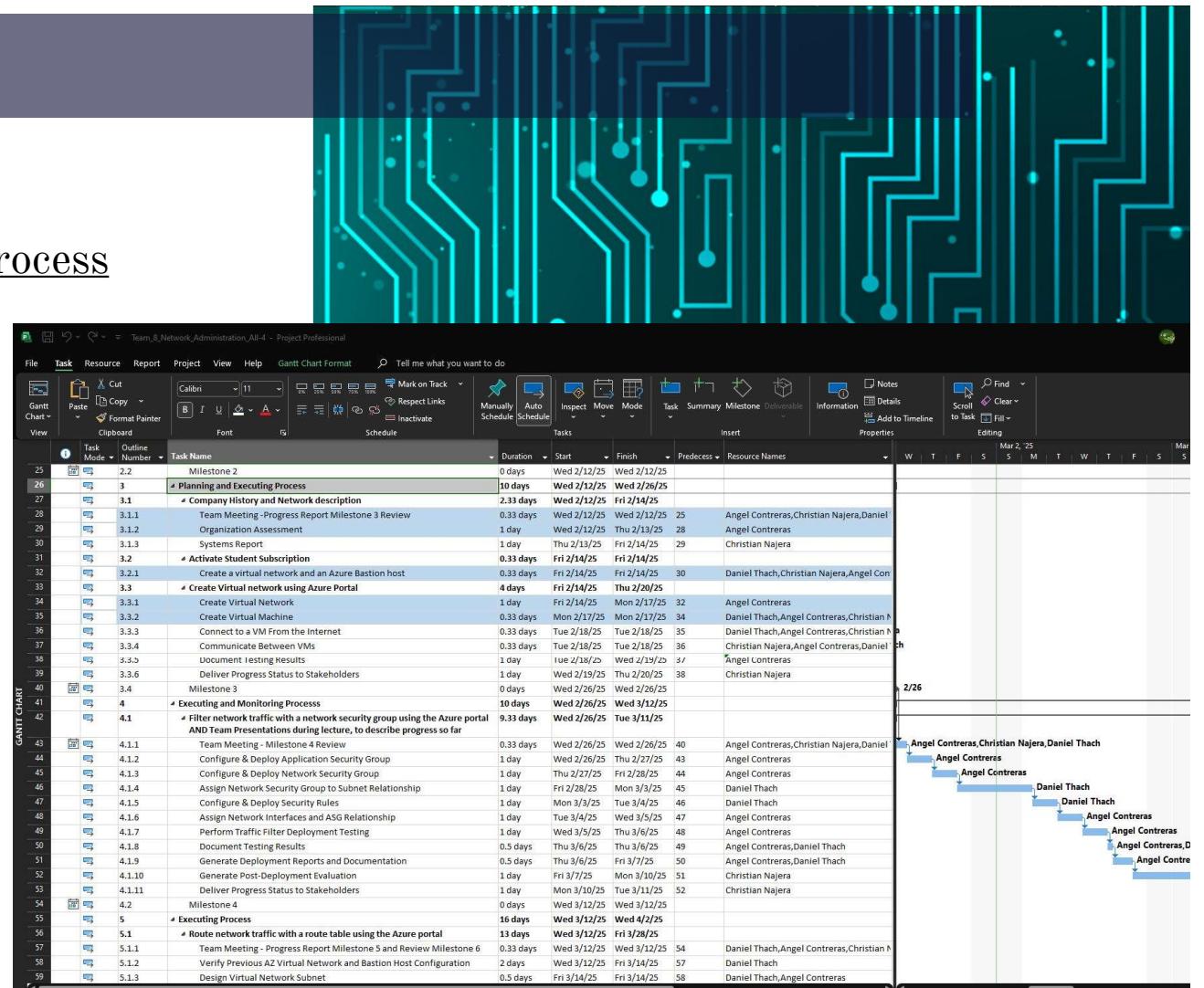


# Milestone 3

## Planning and Executing Process

- Project Scope
- Roles & Responsibilities
- Virtual Network for Beth

Isreal Lahey Health

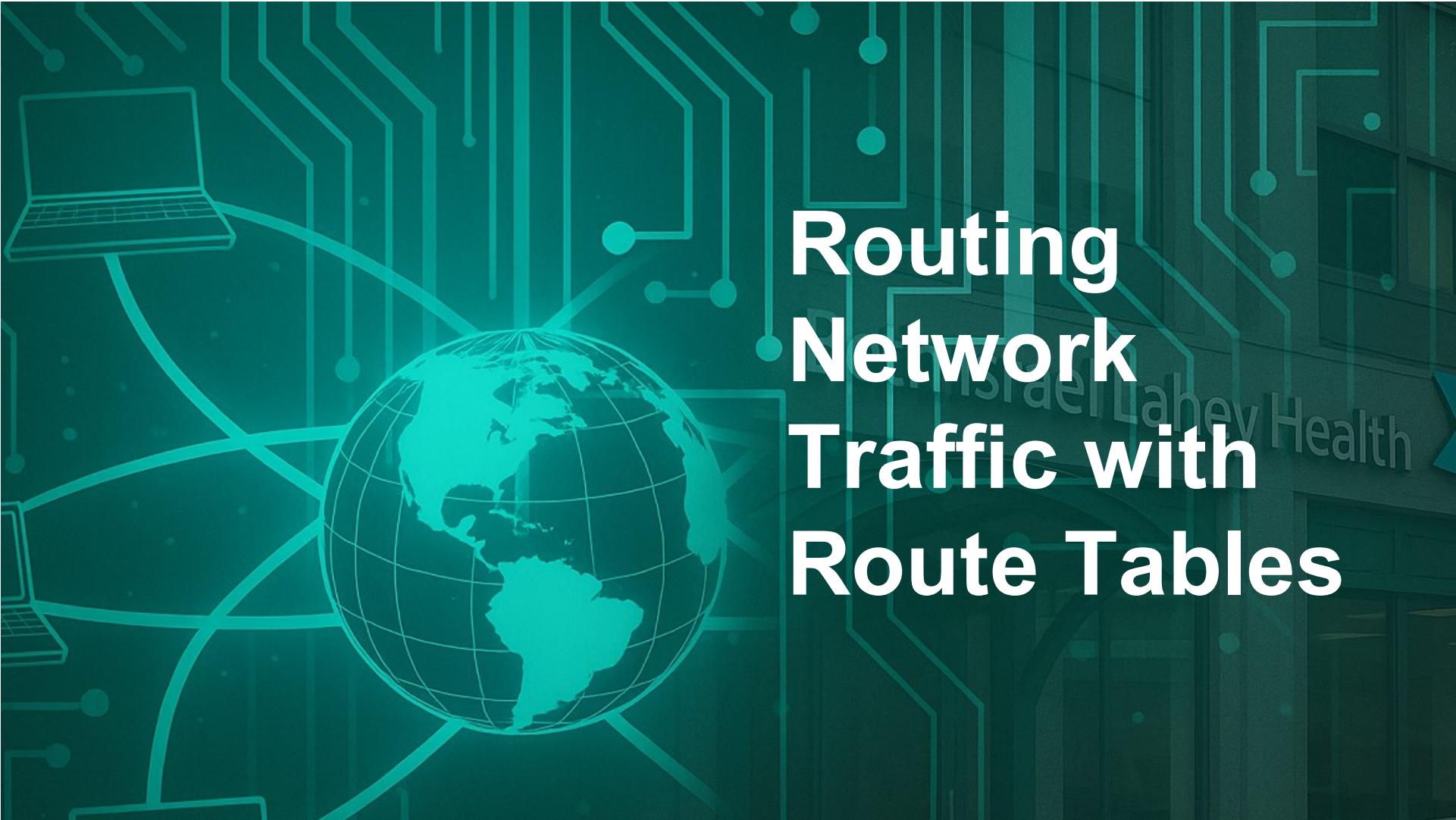


# Milestone 4

## Executing and Monitoring Process

- PowerPoint Outline
- Networking Lab Guides
- Tested Traffic Filters





# Routing Network Traffic with Route Tables

# Routing Network Traffic with Route Tables

- Creating a NVA
- Creating a Route Table
- Creating a route
- Configuring IP forwarding
- Protocol Mapping



# Creating a Network Virtual Appliance

The screenshot shows the Microsoft Azure portal interface. At the top, there's a blue header bar with the Microsoft Azure logo and a search bar that says "Search resources, services, and docs (G+/)". Below the header, the URL "Home > CreateVm canonical/0001 com-ubuntu-server-jammy-2-20250403204938 | Overview >" is visible. The main content area displays a virtual machine named "CGNetVM-NVA3". A red box highlights the VM name. The VM is listed as a "Virtual machine". Below the VM name, there's a "Search" input field and a "Help me copy this VM in any region" button. To the right of these are various management actions: "Connect", "Start", "Restart", "Stop", "Hibernate", "Capture", "Delete", "Refresh", "Open in mobile", "Feedback", and a "Copy" icon. On the left, a sidebar menu lists "Overview" (which is selected and highlighted in grey), "Activity log", "Access control (IAM)", "Tags", "Diagnose and solve problems", "Resource visualizer", "Connect" (with "Connect" and "Action" sub-options), and "Action". The "Overview" section contains an "Essentials" table with the following data:

Essentials	
Resource group ( <a href="#">move</a> )	: <a href="#">CGnetVM</a>
Status	: Running
Location	: East US 2
Subscription ( <a href="#">move</a> )	: <a href="#">Azure for Students</a>
Subscription ID	: eb7c73d0-b299-4137-81d8-b00a83c4e9d7

To the right of the essentials table, there are four empty red-outlined boxes, each with a label: "Operating system", "Size", "Public IP address", and "Virtual network/s". Below these, there are two more empty red-outlined boxes with labels: "DNS name" and "Health state".

# Creating a Route Table

**Create Route table** ...

Basics Tags Review + create

**Project details**

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription \* ⓘ

Resource group \* ⓘ  [Create new](#)

**Instance details**

Region \* ⓘ

Name \* ⓘ  

Propagate gateway routes \* ⓘ  Yes  No



# Adding a route

## Add route

route-table-public

A user defined route (UDR) is a static route that overrides Azure's default system routes, or adds a route to a subnet's route table. [Learn more](#)

Route name \*

to-private-subnet



Destination type \* ⓘ

IP Addresses



Destination IP addresses/CIDR ranges \* ⓘ

10.0.2.0/24



Next hop type \* ⓘ

Virtual appliance



Next hop address \* ⓘ

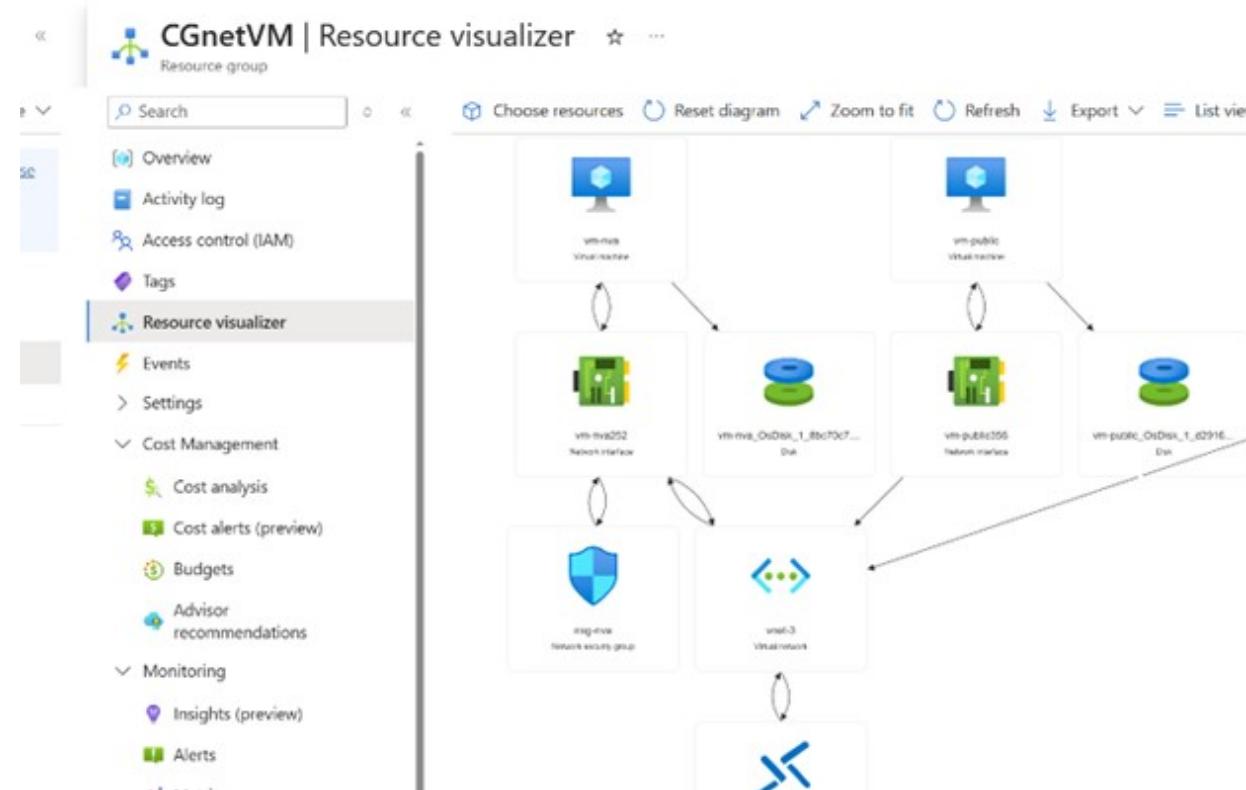
10.0.3.4



# Configure IP Forwarding

The screenshot shows the Microsoft Azure portal interface for managing network configurations. The top navigation bar includes the Microsoft Azure logo, a search bar, and a user sign-in link. Below the navigation is a breadcrumb trail: Home > Compute infrastructure | Virtual machines > vm-nva | Network settings > vm-nva167. The main content area displays a network interface named "CGNetVM-NVA3 | IP configurations". A red box highlights the "IP Settings" section, which contains the "Enable IP forwarding" checkbox (which is checked), the "Virtual network" (set to "vnet3"), and the "Subnet" dropdown (set to "subnet-dmz (10.0.3.0/24) 250 free IP addresses"). The left sidebar lists other configuration options: Overview, Activity log, Access control (IAM), Tags, Resource visualizer, Settings (with IP configurations selected), DNS servers, Network security group, and Properties. At the bottom of the page are standard Azure navigation links: Add, Make primary, and Delete.

# Protocol Mapping



# Protocol Mapping

The screenshot shows a cloud provider's Resource visualizer interface. On the left, a sidebar menu includes options like Overview, Activity log, Access control (IAM), Tags, Resource visualizer (which is selected and highlighted in blue), Events, Settings, Cost Management, Monitoring, Insights (preview), and Alerts. The main area displays a network diagram with nodes: vm-net (Virtual machine), vm-public (Virtual machine), vm-mva252 (Network interface), vm-mva\_OsDisk\_1\_Bsc70cf... (Disk), vm-public356 (Network interface), vm-public\_OsDisk\_1\_d2916... (Disk), nsg-1 (Network security group), and usql-3 (Virtual network). Arrows indicate connections between these components. A red arrow points from the network diagram up towards a terminal window at the top right. The terminal window shows a root shell on a VM named 'vm-nva'. It displays the output of the command 'iptables -L -v -n', showing the INPUT and FORWARD chains with ACCEPT rules. Below this, a message from the system indicates a new release '24.04.2 LTS' is available, with instructions to run 'do-release-upgrade' to upgrade it. The terminal also shows the last login information and a prompt for sudo commands.

```
root@vm-nva:~# iptables -L -v -n
Chain INPUT (policy ACCEPT 126 packets, 24232 bytes)
pkts bytes target  prot opt in     out    source               destination
      0     0 ACCEPT   1  -- *      *      0.0.0.0/0            0.0.0.0/0
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target  prot opt in     out    source               destination

root@vm-nva:~# New release '24.04.2 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Fri Apr  4 04:59:07 2025 from 10.0.1.4
To run a command as administrator (user "root"), use "sudo <command>"
```



# Connecting Virtual Networks and Peering

Beth Israel Lahey Health

# Connecting Virtual Networks

- Connecting Virtual Networks via Peering
- Testing the Peering connection



# Connecting Virtual Networks and Peering

The image shows two side-by-side screenshots of the Azure portal interface for managing virtual network peerings.

**Left Screenshot (CGVNet-1 | Peerings):**

- Header:** CGVNet-1 | Peerings, Virtual network
- Search Bar:** Search resources, services, and docs (G+/)
- Toolbar:** Add, Refresh, Export to CSV, Delete, Sync
- Table Headers:** Name, Peering
- Data Row:** vnet-1-to-vnet-3, Full

**Right Screenshot (CGVNet-3 | Peerings):**

- Header:** CGVNet-3 | Peerings, Virtual network
- Search Bar:** Search resources, services, and docs (G+/)
- Toolbar:** Add, Refresh, Export to CSV, Delete, Sync
- Table Headers:** Name, Peering sync status
- Data Row:** vnet-3-to-vnet-1, Fully Synchronized

In both screenshots, the "Peerings" section is highlighted with a red box, and the table rows are also highlighted with red boxes.

# Testing the Peering connection

```
Chain ufw-user-input (1 references)
target    prot opt source          destination
Chain ufw-user-limit (0 references)
target    prot opt source          destination
LOG      all  --  anywhere        anywhere
FW LIMIT BLOCK]
REJECT   all  --  anywhere        anywhere
          reject-with icmp-port-unreachable

Chain ufw-user-limit-accept (0 references)
target    prot opt source          destination
ACCEPT   all  --  anywhere        anywhere

Chain ufw-user-logging-forward (0 references)
target    prot opt source          destination

Chain ufw-user-logging-input (0 references)
target    prot opt source          destination

Chain ufw-user-logging-output (0 references)
target    prot opt source          destination

Chain ufw-user-output (1 references)
target    prot opt source          destination
dthach2@vm-5:~$ sudo ufw status
Status: active
dthach2@vm-5:~$
```

```
Expanded Security Maintenance for Applications is not enabled.
0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

dthach2@vm-5:~$ ping -c 4 10.1.0.4
PING 10.1.0.4 (10.1.0.4) 56(84) bytes of data.
--- 10.1.0.4 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3057ms
dthach2@vm-5:~$ ping -c 10.0.0.4
ping: invalid argument: '10.0.0.4'
dthach2@vm-5:~$ ping -c 4 10.0.0.4
PING 10.0.0.4 (10.0.0.4) 56(84) bytes of data.
64 bytes from 10.0.0.4: icmp_seq=1 ttl=64 time=1.70 ms
64 bytes from 10.0.0.4: icmp_seq=2 ttl=64 time=0.913 ms
64 bytes from 10.0.0.4: icmp_seq=3 ttl=64 time=1.09 ms
64 bytes from 10.0.0.4: icmp_seq=4 ttl=64 time=0.723 ms
--- 10.0.0.4 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3051ms
rtt min/avg/max/mdev = 0.723/1.107/1.702/0.367 ms
dthach2@vm-5:~$
```



# Takeaways and Considerations

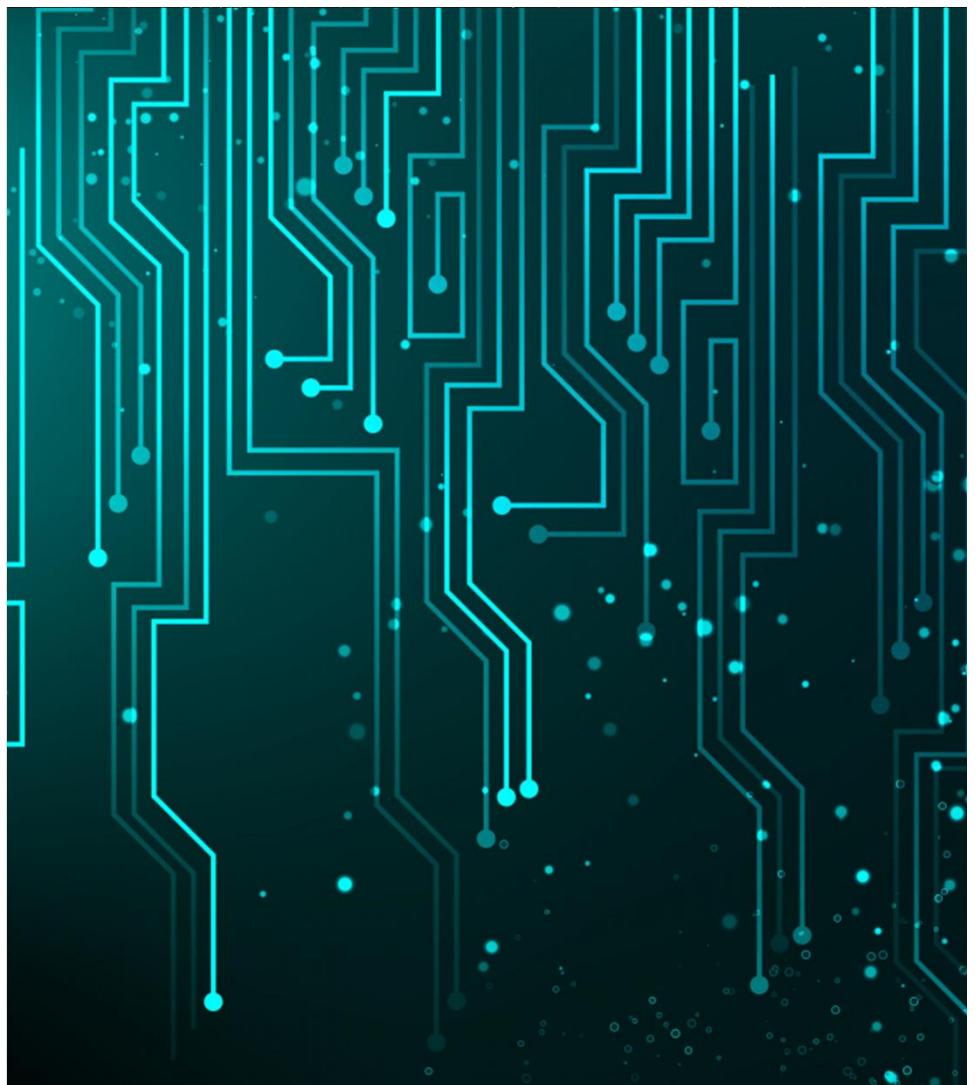
# Summary

- Designed to support BILH's mission of secure, scalable, and collaborative healthcare.
  - Built a virtual network with public and private VMs for flexibility and security.
  - Implemented NSGs and ASGs to manage traffic and protect resources.
  - Used route tables and NVAs to control traffic flow securely.
  - Tested connectivity and routing to validate configurations.
-

## Considerations

- Balance between accessibility and security in VM deployment.
  - Complex configuration of NSGs, ASGs, and routing requires accuracy.
  - Compliance with healthcare regulations requires ongoing updates.
  - Early planning is essential for future scalability and integration.
-

# QUESTIONS?



# REFERENCES

- asudbring. (2023, May 4). *Network security group – How it works*. Microsoft. <https://learn.microsoft.com/en-us/azure/virtual-network/network-security-group-how-it-works>
- asudbring. (2024, August 20). *Tutorial: Filter network traffic with a network security group (NSG)*. Microsoft. <https://learn.microsoft.com/en-us/azure/virtual-network/tutorial-filter-network-traffic?tabs=portal>
- GeeksforGeeks. (2022, July 22). *Fundamentals of virtual networking*. <https://www.geeksforgeeks.org/fundamentals-of-virtual-networking/>
- Khan, A. (2023, March 6). *How network security groups filter network traffic*. LinkedIn. <https://www.linkedin.com/pulse/how-network-security-groups-filter-traffic-ali-khan-/>
- KumudD. (n.d.). *Route network traffic – Tutorial – Azure Portal*. Microsoft. <https://docs.microsoft.com/en-us/azure/virtual-network/tutorial-create-route-table-portal>
- Massachusetts Health Policy Commission. (2018). *Final CMIR report – Beth Israel Lahey Health – Executive summary*. <https://www.mass.gov>
- McFarlan, F. W., & Austin, R. D. (2005). CareGroup (Case No. 9-303-097). Harvard Business School.
- Microsoft. (2024a). *What is Azure Virtual Network?* <https://learn.microsoft.com/en-us/azure/virtual-network/virtual-networks-overview>
- Microsoft. (2025a). *What is a virtual machine and how does it work | Microsoft Azure*. <https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-a-virtual-machine/?msclkid=1b50d6747d616ea30770c3467cf36f18>
- Samanro. (n.d.). *Microsoft cloud architecture models – Enterprise resource planning*. Microsoft. <https://docs.microsoft.com/en-us/microsoft-365/solutions/cloud-architecture-models?view=o365-worldwide>
- Susnjara, S., & Smalley, I. (2024, March 3). *What is a virtual machine (VM)?* IBM. <https://www.ibm.com/think/topics/virtual-machines>