

How to be a Network Engineer in an Artificial Age

cisco Live !

Hank Preston
Principal Engineer Learn with Cisco
ccie 38336 | devnet expert 20220001

A session 8 years in the making...

Reimagining the Cisco SE as a Developer

Morning Code Standup



- Background of a Typical Cisco SE
- Evolution of Programmability at Cisco
- ima
- SE
- Community of



The OSI Model of Networking...



L7: Application	Please don't ask about this...
L6: Presentation	
L5: Session	
L4: Transport	Oh Yeah... We Got this
L3: Network	
L2: Data Link	
L1: Physical	Black Magic

Cisco live! @hpreston @CiscoDevNet <http://github.com/hpreston>

DEVNET-1012 © 2017 Cisco and/or its affiliates. All rights reserved. Cisco Public

The Four Ages of Networking...

Stone Age ~40 Years	Bronze Age ~15 Years	The Renaissance ~5 Years	The Cloud Age ? Years
Spanning Tree VLANs	Routing Protocol WAN Design IP-magedon	SDN OpenFlow Controllers Overlays MP-BGP VXLAN Micro-Segmentation	Programmability Python REST / APIs White Box NETCONF/YANG Fabric NFv DevOps (xOps)

Cisco live! @hpreston @CiscoDevNet <http://github.com/hpreston>

DEVNET-1012 © 2017 Cisco and/or its affiliates. All rights reserved. Cisco Public

The Cloud You Plan to Build ☺



The Cloud You End Up With ☹



Cisco live! @hpreston @CiscoDevNet <http://github.com/hpreston>

DEVNET-1012 © 2017 Cisco and/or its affiliates. All rights reserved. Cisco Public

How to be a Network Engineer in an Artificial Age

cisco Live !

Hank Preston
Principal Engineer Learn with Cisco
ccie 38336 | devnet expert 20220001

Cisco Webex App

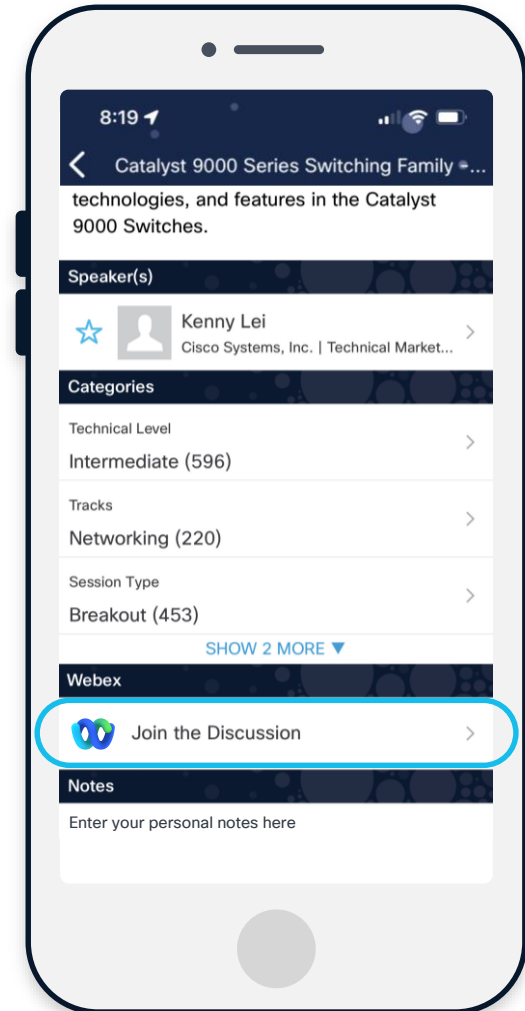
Questions?

Use Cisco Webex App to chat with the speaker after the session

How

- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

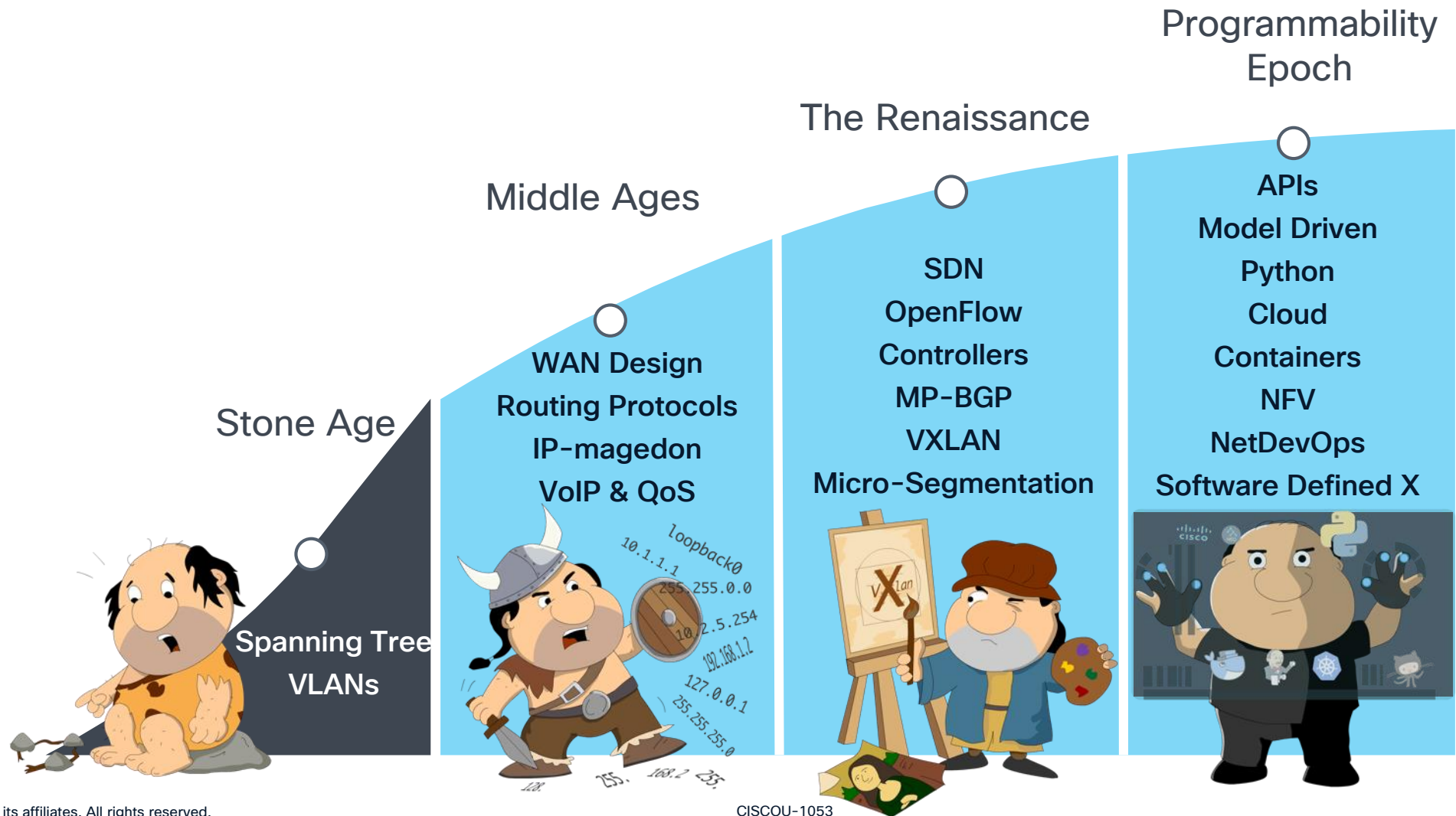
Webex spaces will be moderated by the speaker until June 13, 2025.



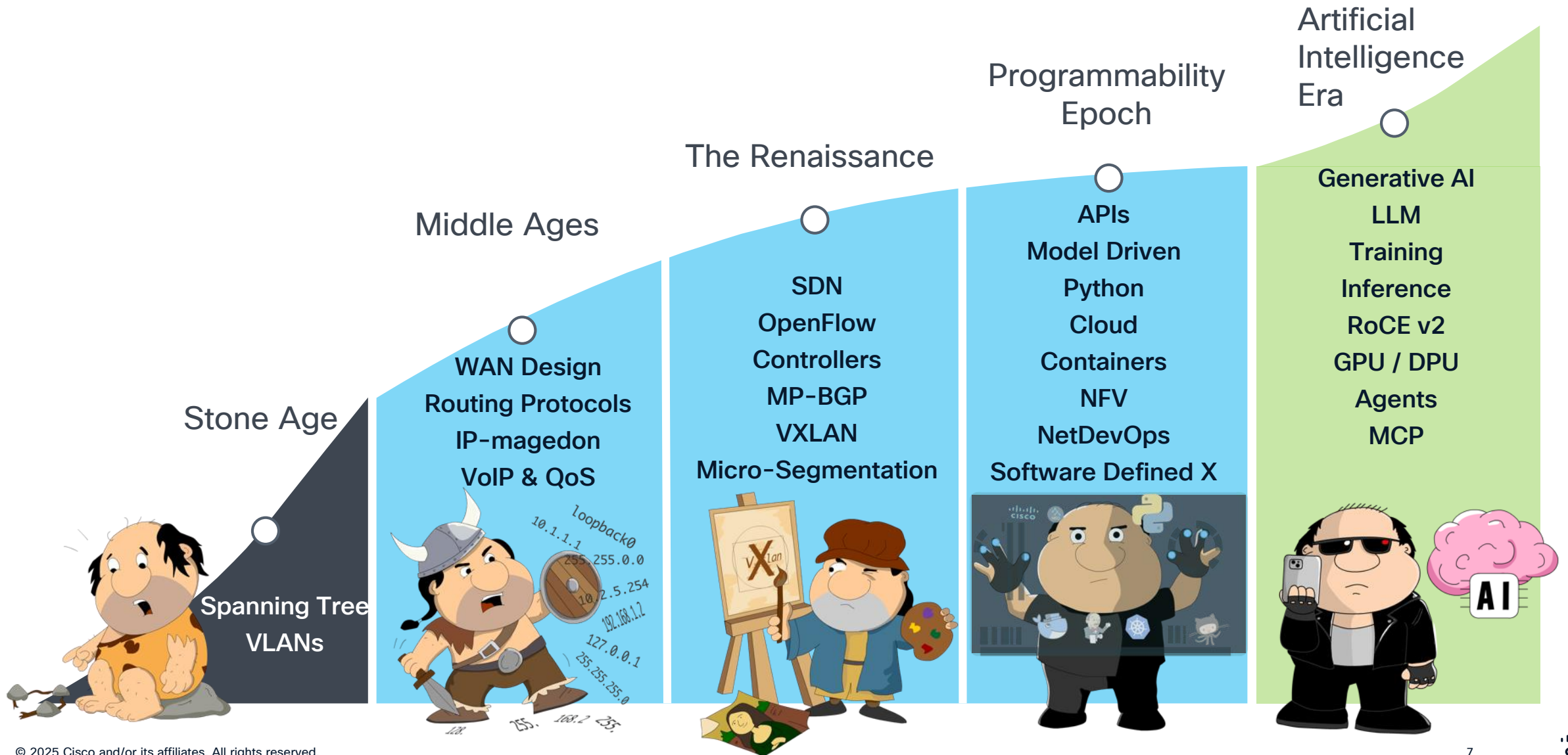
**I have no idea what I'm
doing....**



The Ages of Networking

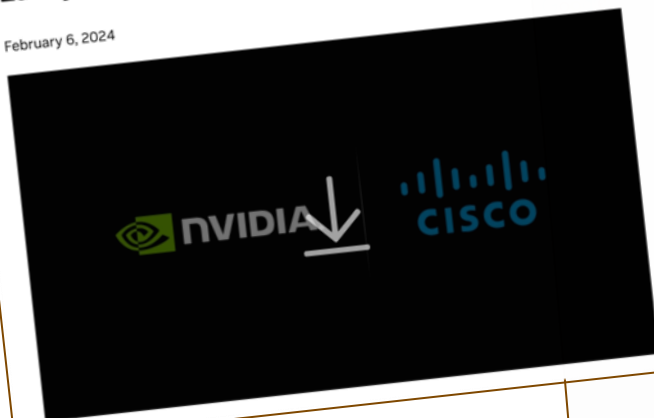


The Ages of Networking



Cisco and NVIDIA to Help Enterprises Quickly and Easily Deploy and Manage Secure AI Infrastructure

February 6, 2024



demands and ai

Pages Videos News Shopping Books Maps 1 More

center needs poised to jolt power demand
ions help crystallize a huge challenge: meeting the surging energy need
as artificial intelligence joins other...

Times
vs plans to retire coal-fired plants as power demand surges
ing electricity demand needed to power next-generation technology
US to rely on yesterday's fuel source: coal.

Us will address the energy challenges of generative AI

Balancing performance, energy efficiency, and cost-effectiveness, CPUs address the less-intensive inference tasks that make up the...

5 hours ago

US data center power consumption is set to double amid soaring AI demands
Power consumption at US data centers is skyrocketing, prompting concerns supply challenges could be on the horizon.

2 hours ago

Goldman Sachs
is poised to drive 160% increase in data center power

Green data centers as growing AI resources
data center roadmap on Thursday "to support our... as demand for AI and...

Energy Demands of A.I.
demands of A.I. How can the world reach net zero if it keeps consume energy? ... A photo of power lines.

See China's military show off rifle-toting robot dogs

16 times as much electricity to process as a coming sea...

robot dogs

robot dogs

robot dogs

robot dogs

robot dogs

robot dogs

robot dogs

Pope meets head of Cisco as AI ethics pact continues to grow

VATICAN / VATICAN NEWS



Forbes Network Infrastructure for AI

Building infrastructure for AI services is not a trivial game, especially in networking. It requires large investments and onsite engineering to **minimize latency and maximize activity**. AI infrastructure makes traditional enterprise and infrastructure look like child's play.

Network Troubleshooting Made Easy with ChatGPT
John Capobianco



ARTIFICIAL INTELLIGENCE

Google Explains What Went Wrong With Those Wacky AI Overviews

The distinction between truthful content and satirical information has been hard for Google's AI to parse. It's a reminder that new artificial intelligence tools should be introduced carefully.



Scams, Fakes, Abuse: The Dangers of Generative AI

Share of respondents being very/somewhat worried about the following potential problems caused by AI



16,795 respondents (13-64 y/o) in 17 countries surveyed online Jul.-Aug. 2023
Source: Microsoft Global Online Safety Survey 2024



statista

Cisco and NVIDIA to Help Enterprises Quickly and Easily Deploy and Manage Secure AI Infrastructure

February 6, 2024



NPR

<https://www.npr.org/planet-money/2024/08/06/10...>

10 reasons why AI may be overrated : Planet Money

Aug 6, 2024 — Even more alarming, AI was really touted as being incredible at writing computer code. Like jobs for translators, jobs for computer coders were supposedly in ...

Pope meets head of Cisco as AI ethics pact continues to grow

VATICAN / VATICAN NEWS



Funds Society

<https://www.fundssociety.com/news/business/valdra...>

Is it Worth Investing a Trillion Dollars in Generative Artificial ...

3 days ago — In the coming years, nearly a trillion dollars is expected to be invested in generative artificial intelligence, but is it worth it?

Forbes

Network Infrastructure for AI

Building infrastructure for AI services is not a trivial game, especially in networking. It requires large investments and onsite engineering to minimize latency and maximize AI infrastructure makes traditional enterprise and ...

Google Explains With Those Wacky AI ...

distinction between truthful content and satire. It's a information has been hard for Google's AI to parse. It's a that new artificial intelligence tools should be



CNN

<https://www.cnn.com/2024/08/02/tech/wall-street-...>

Has the AI bubble burst? Wall Street wonders if artificial ...

Aug 2, 2024 — And some investors question whether AI investments will ever pay off. Goldman Sachs analyst Jim Covello argued that "the technology isn't designed to solve the ...

Unveiling a new era of AI-native security with Cisco Hypershield

Cisco

See China's military show off rifle-toting robot dogs

Data privacy

Bias amplification

60%

16,795 respondents (13-64 y/o) in 17 countries surveyed online Jul.-Aug. 2023
Source: Microsoft Global Online Safety Survey 2024

statista

Cisco and NVIDIA to Help Enterprises Quickly and Easily Deploy and Manage Secure AI Infrastructure

February 6, 2024



Will California Revive Nuclear Power to Feed AI Energy Demands?

1 If you've used ChatGPT to write a breakup text or figure out how to not burn the Christmas roast, you might've actually helped create jobs...
AI 2 days ago
... Like jobs for translators, jobs for computer coders were supposedly in ...

Planet Money

...y, AI was really touted as being incredible at writing

Power consumption at US data centers is skyrocketing, prompting concerns supply challenges could be on the horizon.
2 hours ago
Goldman Sachs
... is poised to drive 160% increase in data center power

DeepSeek's AI Shockwave Hits Nvidia Hard, Wiping Out Billions

The artificial intelligence revolution is moving at lightning speed, and one of the biggest stories from last week underscores just how...

23 hours ago

See China's military show off rifle-toting robot dogs



BBC

<https://www.bbc.com/news/articles>

Concern over Google ending ban on AI weapons

7 days ago — Google's parent company lifting a longstanding ban on artificial intelligence (AI) being used for developing weapons and surveillance tools ...

Is it Worth Investing a T...

3 days ago — In the generative ...



Computerworld

Meta promises it won't release dangerous AI systems

According to Meta, risky AI systems could be used to take over an entire corporate environment or deploy powerful biological weapons.

38 minutes ago



Tom's Hardware

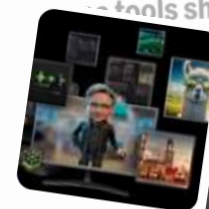
DeepSeek might not be as disruptive as claimed, firm reportedly has 50,000 Nvidia GPUs and spent \$1.6 billion on buildouts

SemiAnalysis says that DeepSeek and its venture capitalist partner spent some \$1.6 billion dollar on AI hardware from Nvidia,...

2 days ago

With Those Wacky AI...

distinction between truthful content and satire ... hard for Google's AI to parse. It's a ... tools should be



Bias amplification

60%

AI scenario

16,795 respondents (13-64 y/o) in 17 countries surveyed online Jul.-Aug. 2023
Source: Microsoft Global Online Safety Survey 2024



statista

Cisco and NVIDIA Easily Deploy AI

February 6, 2024



Will California Demand?

1 If you've used Christmas roa
AI
CO 2 days ago

SAN Straight Arrow News

This nuclear plant was set to close. Then Meta stepped in to power AI data centers

F For A nuclear plant in Illinois, is the latest power plant saved by the tech industry after Meta signed a 20-year deal with Constellation...

Dee Billicious 2 days ago

The artificial intelligence re stories from last week und 23 hours ago

Opinion | No, AI Robots Won't Take All Our Jobs

3 hours ago

WSJ Robert D. Atkinson ... Economics & tech policy think tank...

Feed AI Energy

out how to not burn the S...

Planet Money

ed as h...



BBC

https://www.bbc.com › news › articles

Concer

7 days ago being used

PwC

AI linked to a fourfold increase in productivity growth and 56% wage premium, while jobs grow even in the most easily automated roles

AI is making workers more valuable, productive, and able to command higher wage ns, with job numbers rising even in roles considered...



o Meta, risky AI systems could be or deploy powerful biological wear go

DeepSeek might not be as disruptive as reportedly has 50,000 AI buildouts s and



B Bloomberg

Chinese Startup Trials First AI Doctor Clinic in Saudi Arabia

Takeaways NEW. Hide. A Chinese startup, Synyi AI, has opened a clinic in Saudi Arabia where artificial intelligence diagnoses patients, with the...

3 weeks ago

Forbes

Network Infrastructure for AI

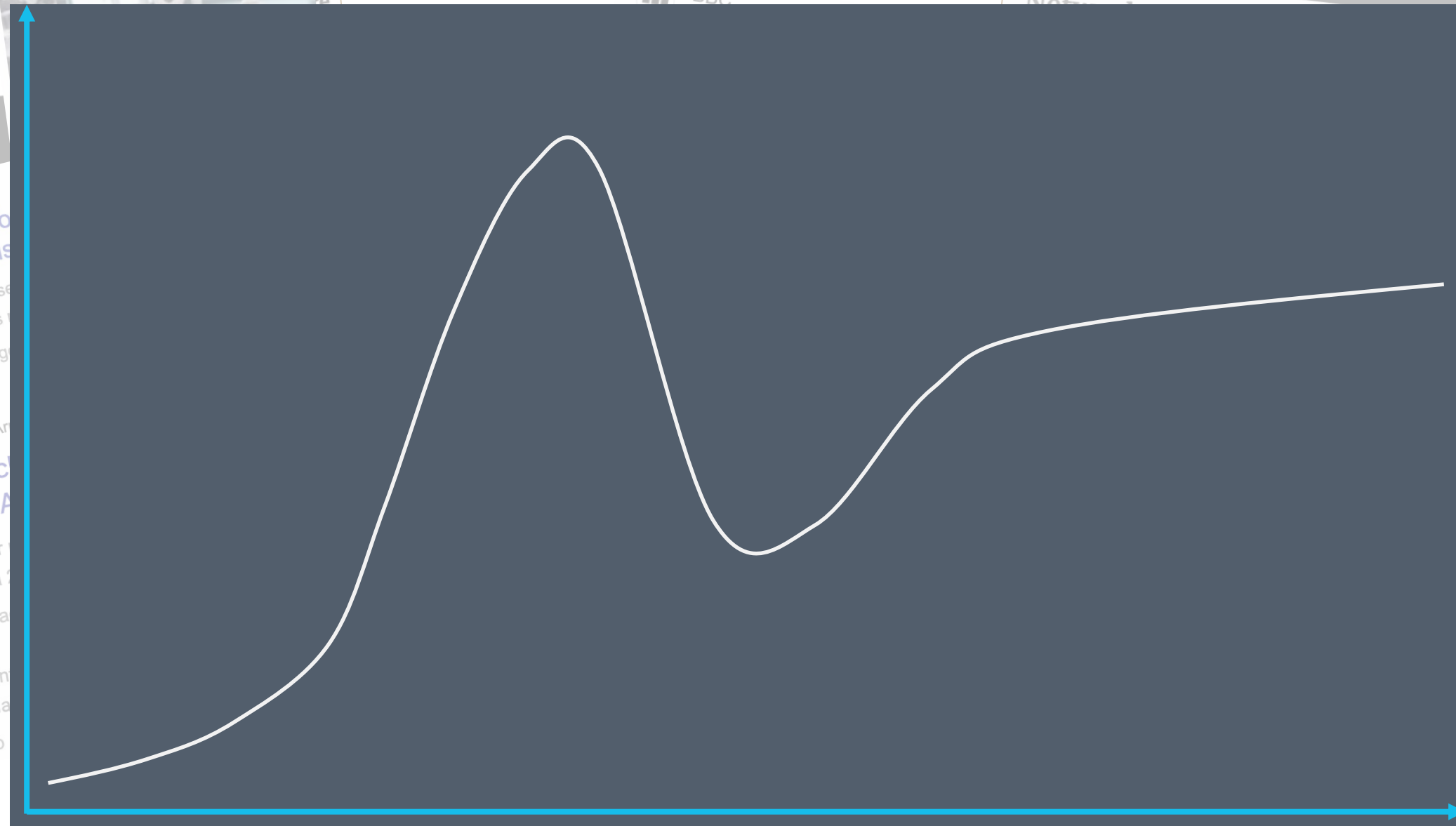


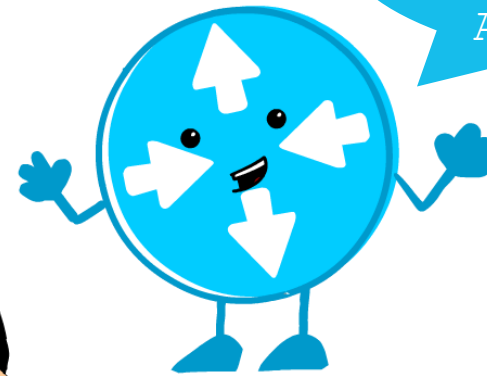
Anthropic researchers predict a 'pretty terrible decade' for humans as AI could wipe out white colla...

Top comment - The "research" is probably more of an ad. I dont get why people keep posting claims like that that directly come from company that are HEAVIL...

80+ comments · 5 hours ago

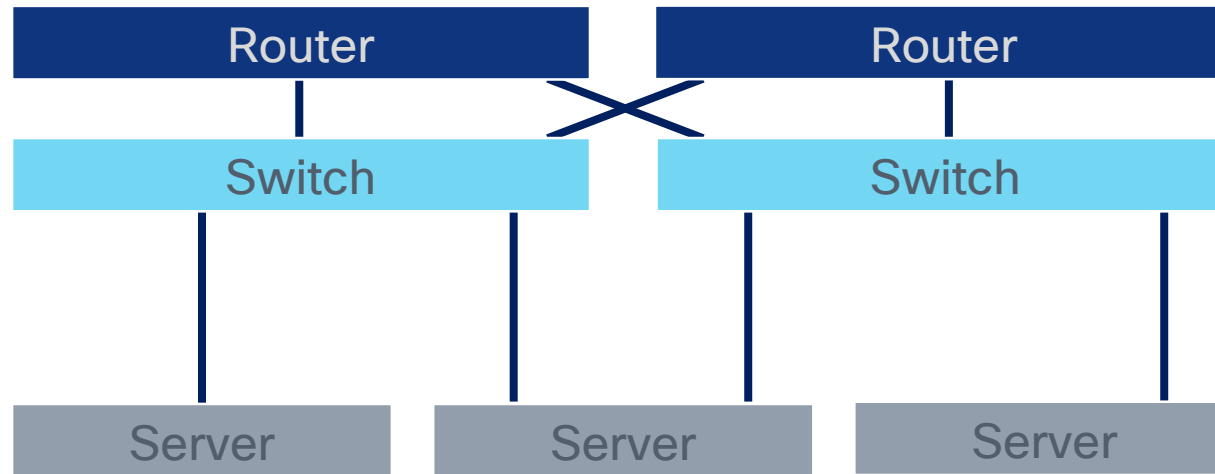
r/ClaudeAI
Reddit



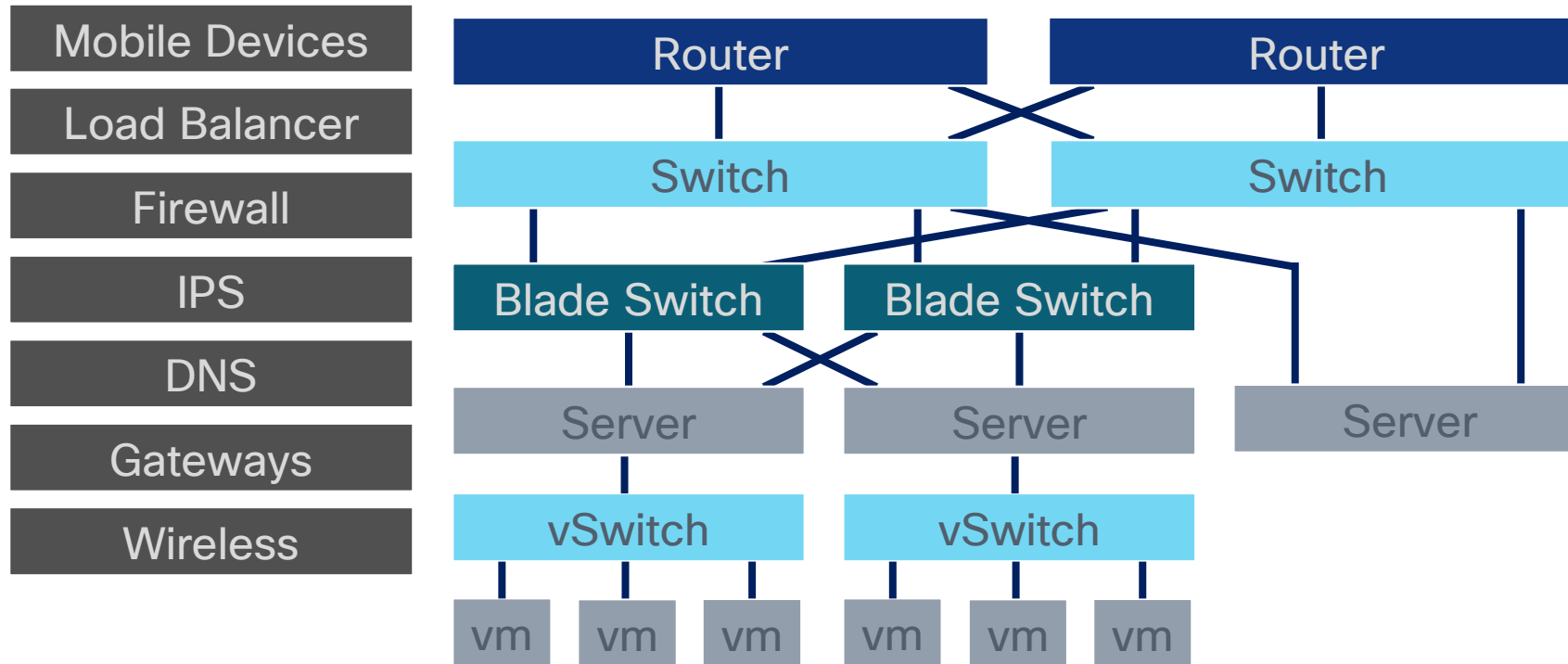


Hi Carl! I'm
Mr Packets,
your Network
AI Assistant.

The Network

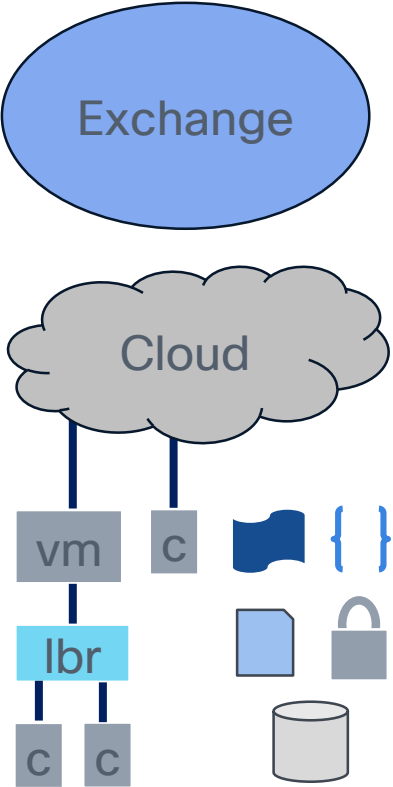
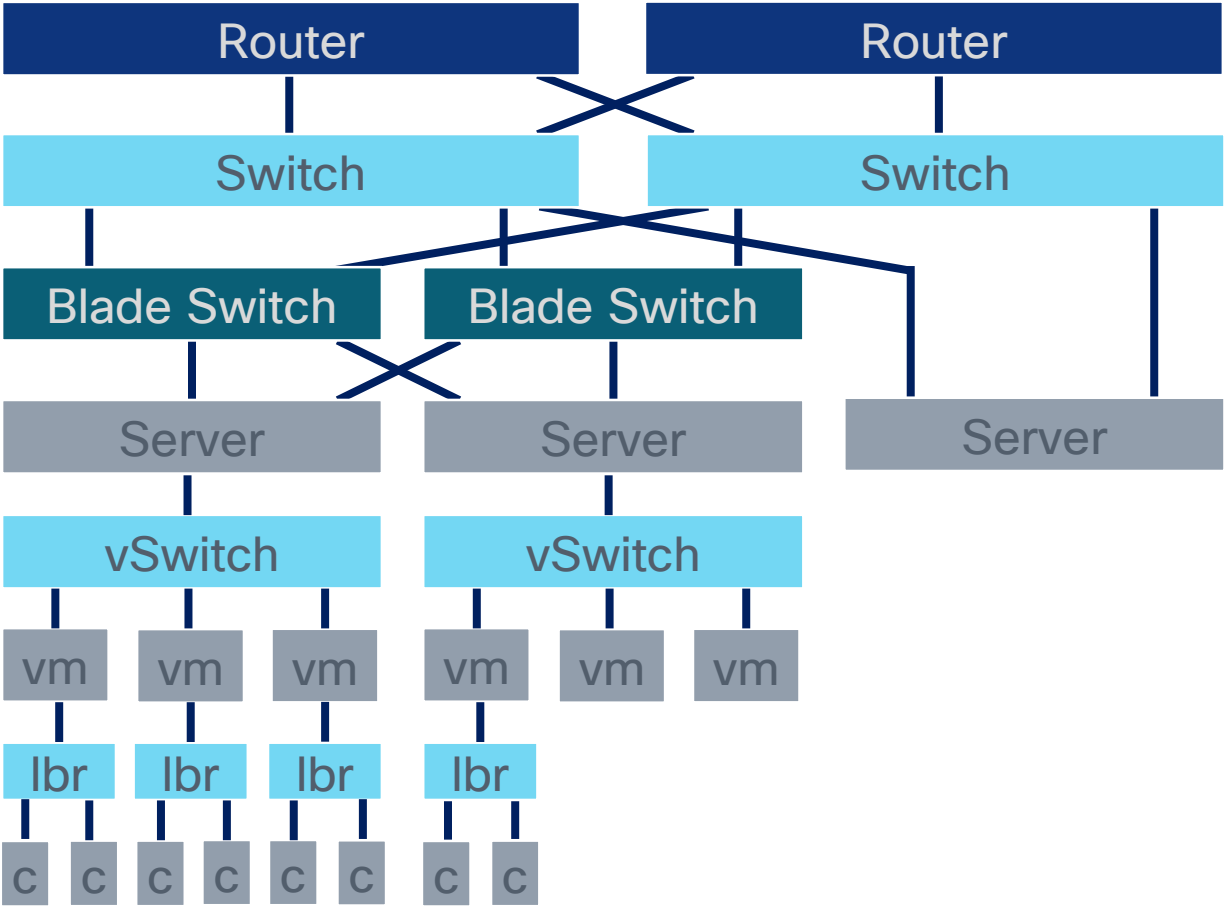


The Network



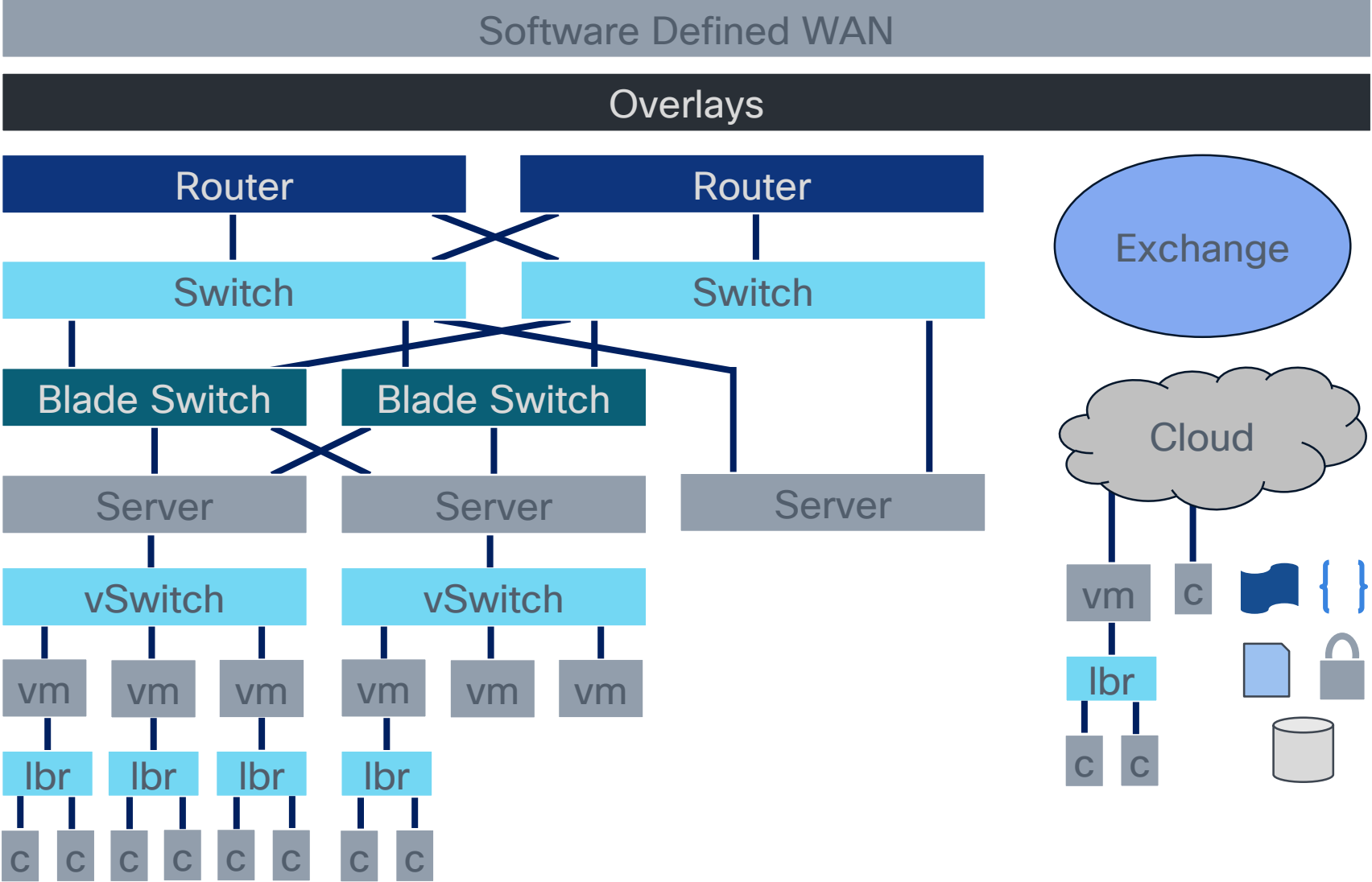
The Network

- Mobile Devices
- Load Balancer
- Firewall
- IPS
- DNS
- Gateways
- Wireless

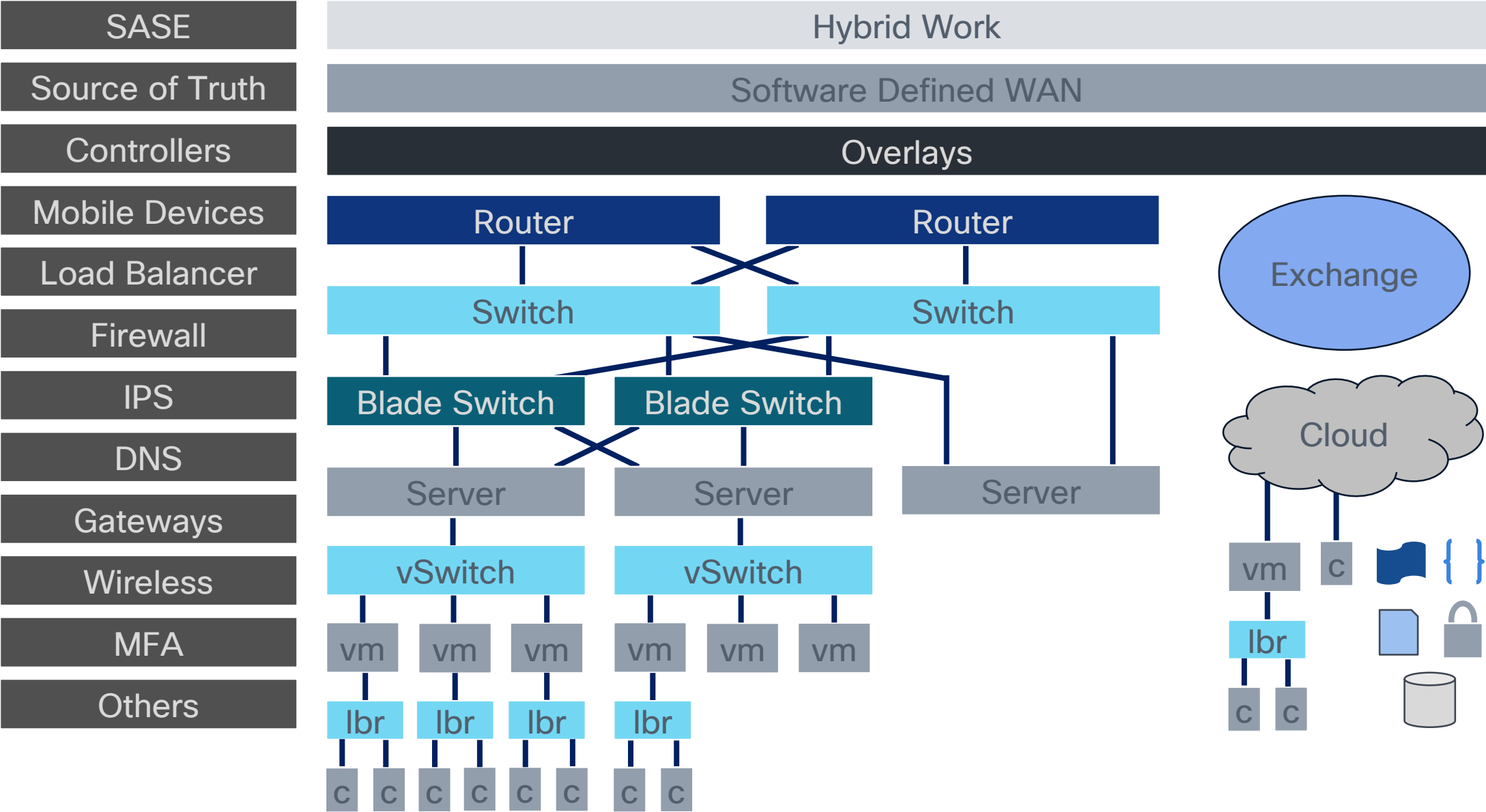


The Network

- Controllers
- Mobile Devices
- Load Balancer
- Firewall
- IPS
- DNS
- Gateways
- Wireless



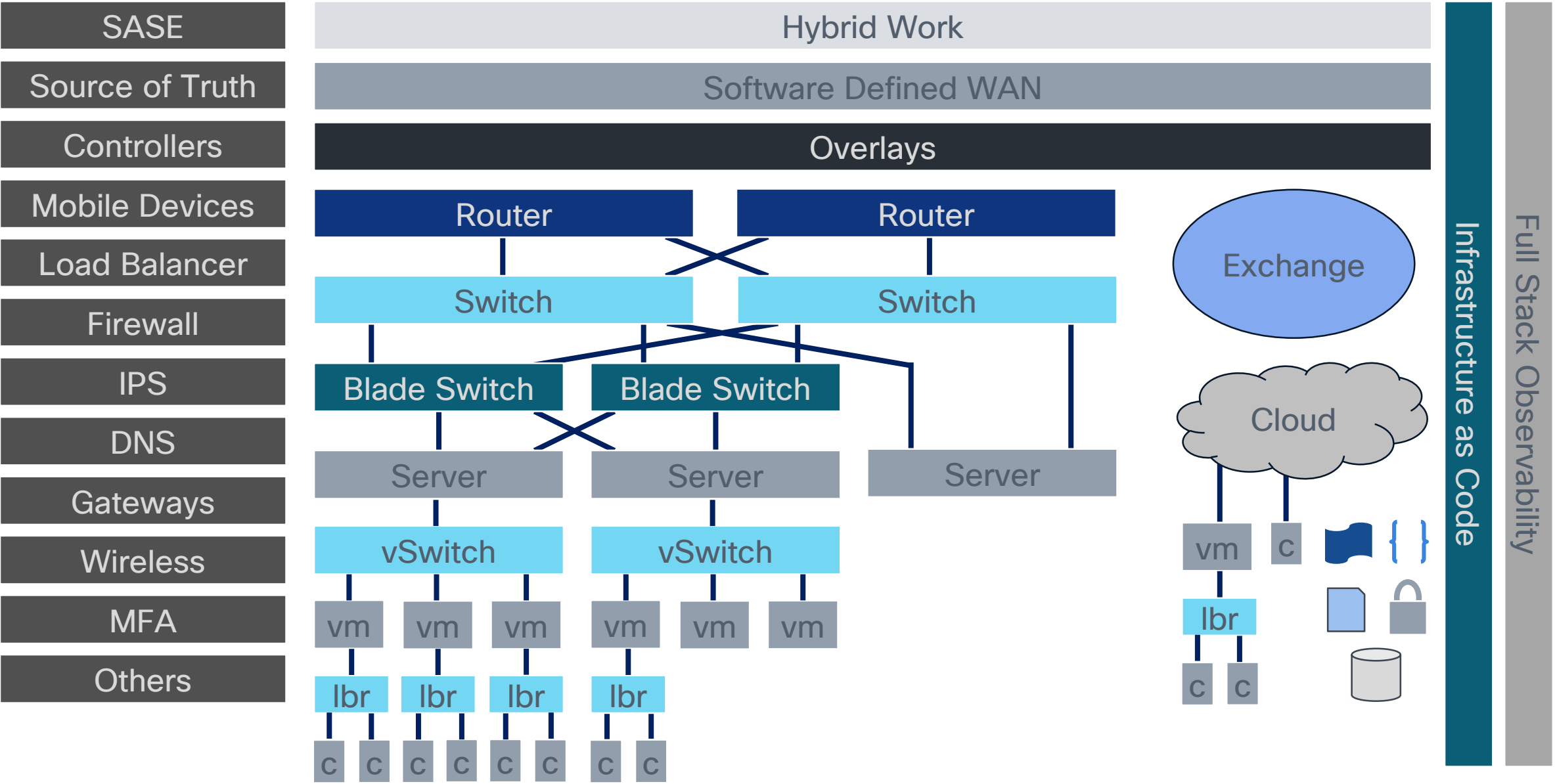
The Network



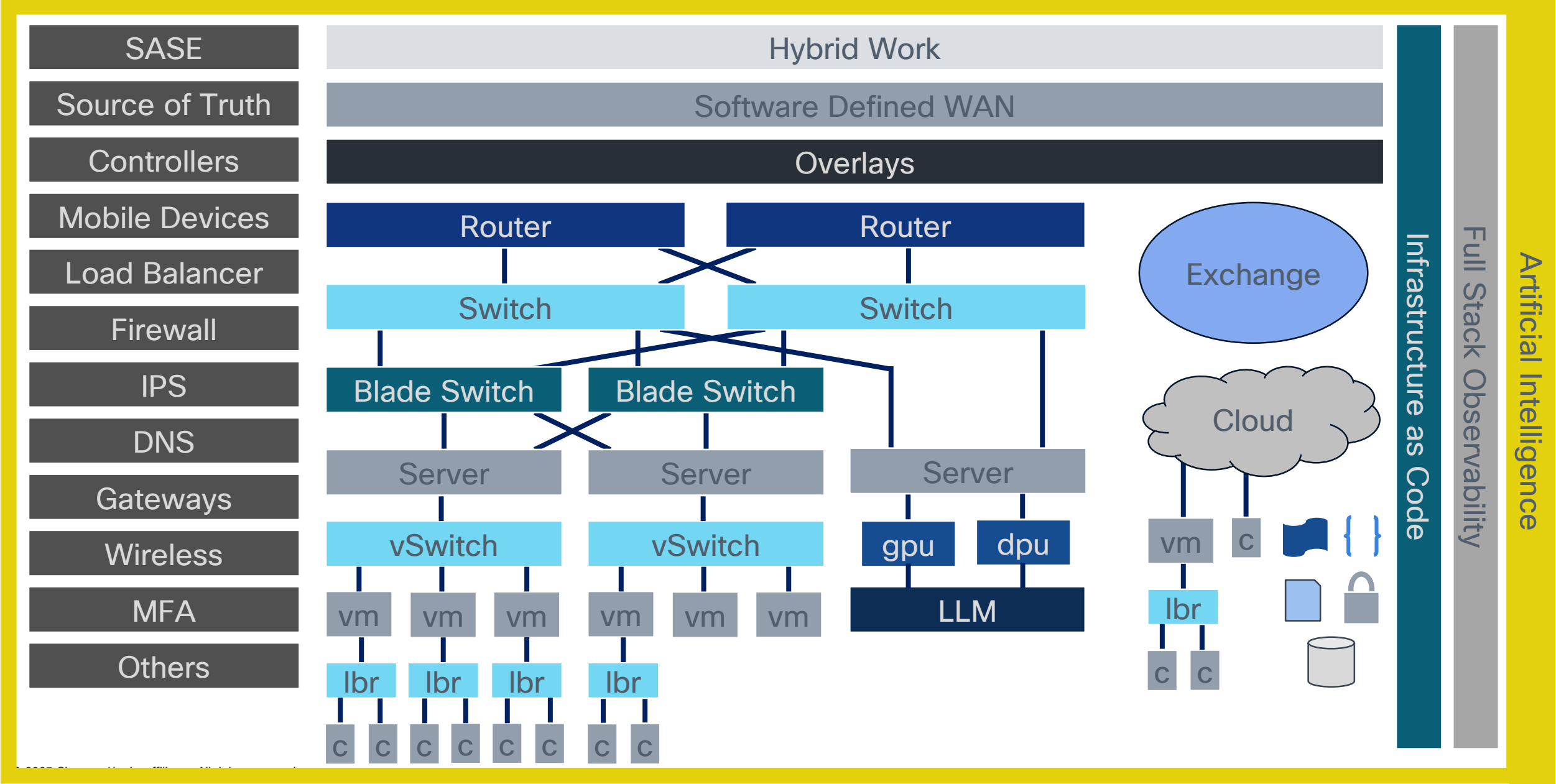
Infrastructure as Code

Full Stack Observability

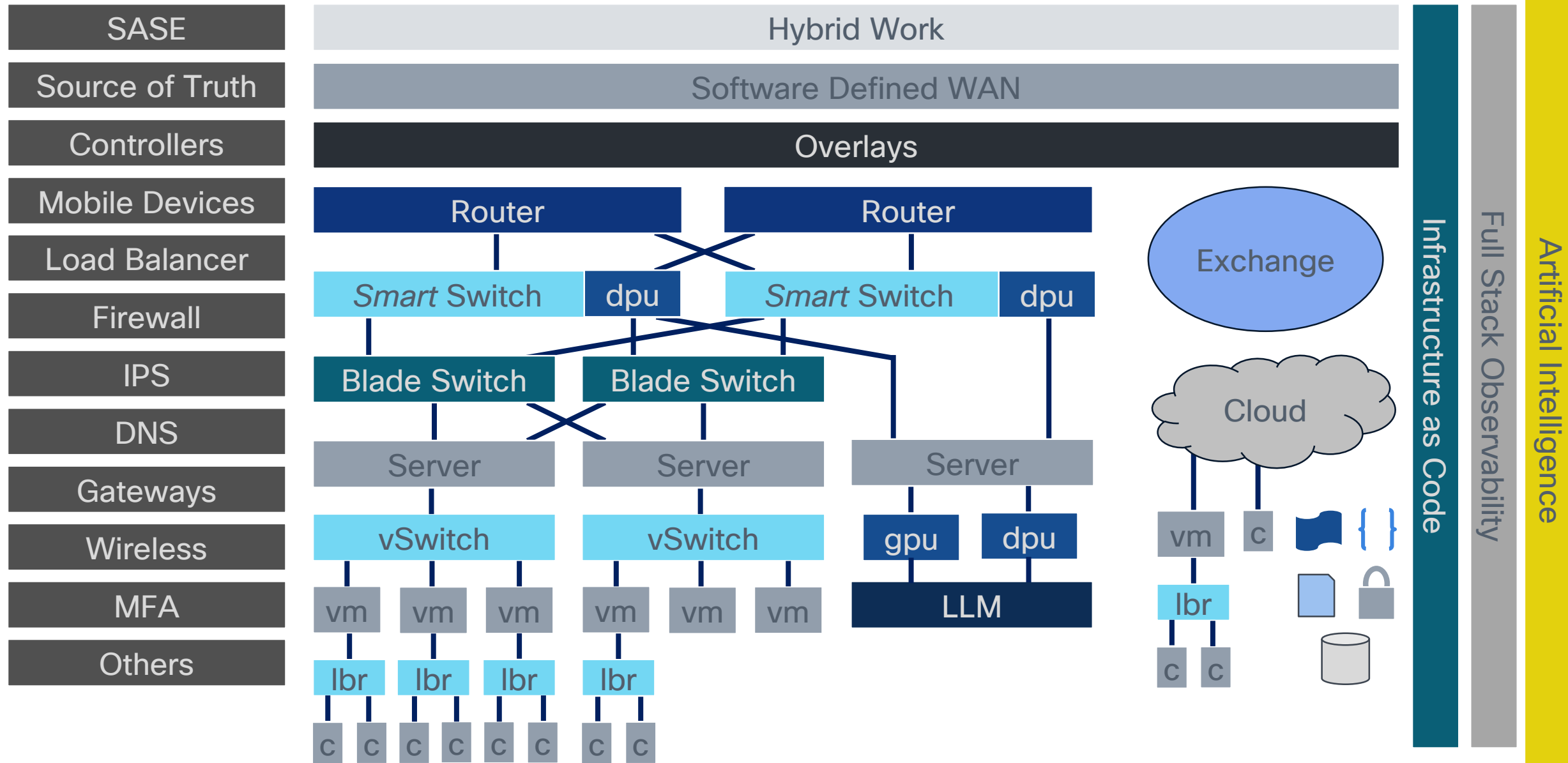
The Network



The Network



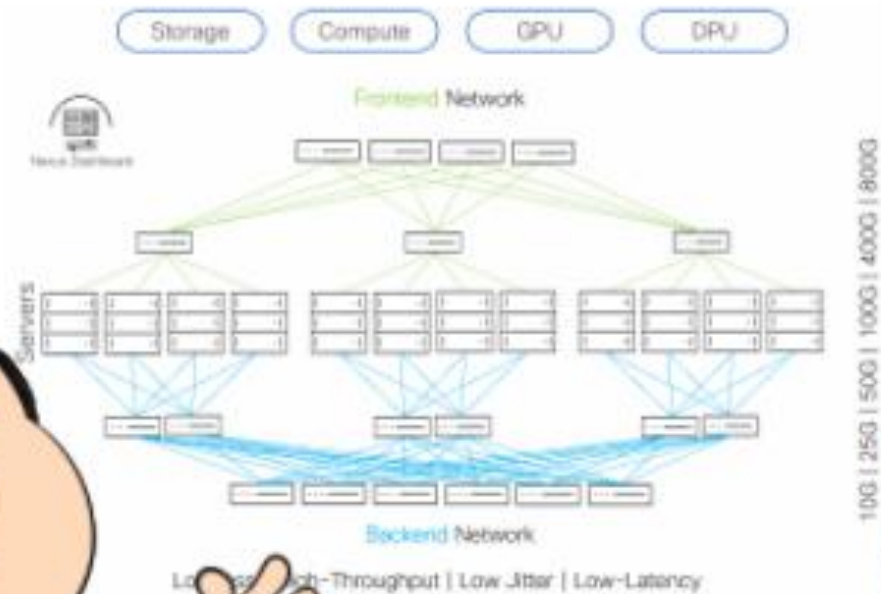
The Network



The Network

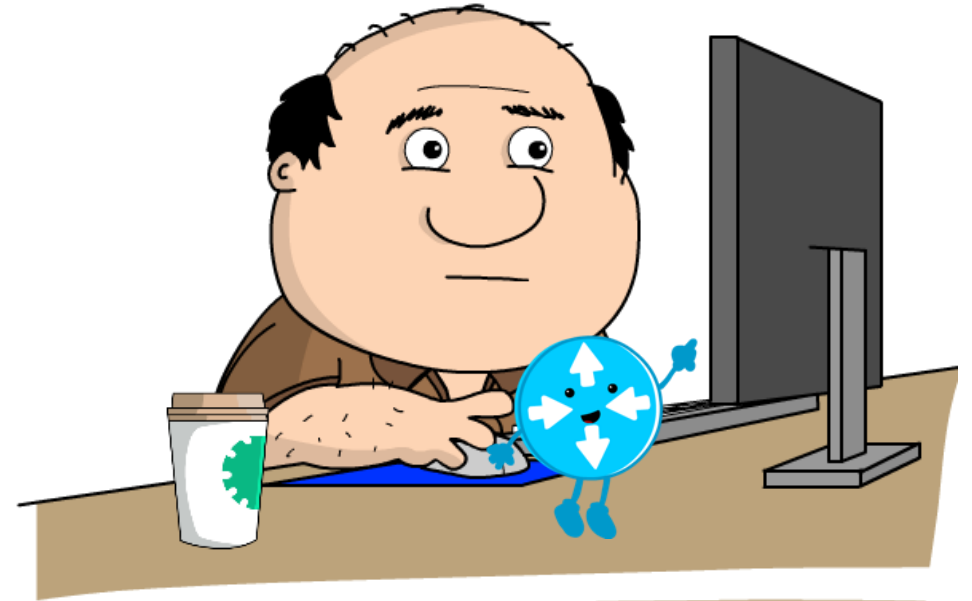
Artificial Intelligence

AI Networking

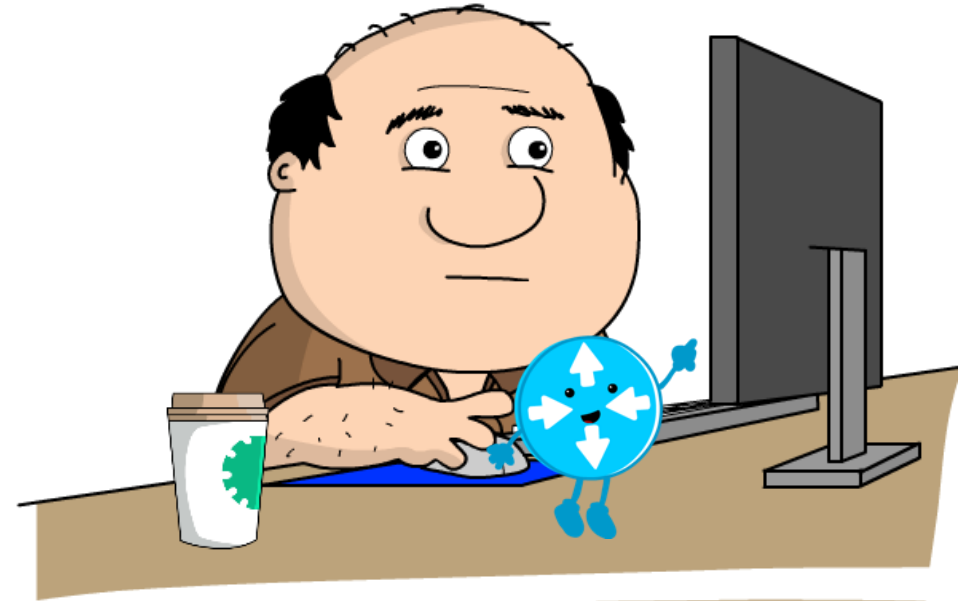


Artificial Intelligence and Network Engineers Today

Using AI to Find Answers to Questions



Using AI to *HELP* Find Answers to Questions





You Tuesday, 7:16 PM

What type of 40G transceiver will work on my Nexus 93180 FX



BridgeIT - Enterprise Chat AI Tuesday, 7:17 PM

The Cisco Nexus 93180YC-FX switch is compatible with a variety of 40G transceivers. To select the appropriate one, you should check the device's hardware compatibility list (HCL) since Cisco typically recommends using Cisco Genuine transceivers to ensure compatibility and reliability.

For a Nexus 93180YC-FX switch, you can generally use the following types of 40G transceivers:

1. QSFP-40G-SR4: This is a short-range transceiver that supports link lengths of 100 meters and 150 meters, respectively, on OM3 and OM4 multimode fibers.
2. QSFP-40G-LR4: This is a long-range transceiver that supports link lengths of 10 kilometers on single-mode fiber.
3. QSFP-40G-CSR4: This transceiver supports link lengths of 300 meters on OM3 multimode fiber and 400 meters on OM4 multimode fiber.
4. QSFP-40G-ER4: This transceiver supports link lengths of up to 40 kilometers on single-mode fiber.
5. QSFP-H40G-CUxM: These are direct-attach copper cables (where 'x' is the length in meters) for very short connections, typically in the same rack or adjacent racks.

Always verify the specific part number and firmware version of your switch to ensure compatibility. Cisco updates their hardware and firmware periodically, and newer transceivers or third-party options may become compatible with your device over time.

Before purchasing any transceiver, it's recommended to consult the latest Cisco compatibility matrix or contact Cisco support to confirm that the transceiver you're considering is compatible with the current firmware version of your Nexus 93180YC-FX switch. Using third-party transceivers may be more cost-effective, but doing so may void support agreements or warranties, and could potentially cause issues with performance or compatibility.



You Tuesday, 7:16 PM

What type of 40G transceiver will work on my Nexus 93180 FX



You 12:34 PM

What is the link to Cisco's transceiver compatibility tool?

New messages



BridgeIT - Enterprise Chat AI 12:34 PM

Cisco provides a Transceiver Module Group (TMG) Compatibility Matrix that allows you to check the compatibility of transceiver modules with Cisco equipment. However, as an AI, I cannot provide a direct URL to external web pages, and Cisco's website URLs may change over time.

To find the compatibility matrix, you can follow these steps:

1. Go to the official Cisco website (www.cisco.com).
2. Use the search feature on the Cisco website to search for "Transceiver Module Group Compatibility Matrix" or "Cisco Transceiver Compatibility Tool."
3. The search results should provide a link to the compatibility matrix or tool.

Alternatively, you can perform a web search using a search engine with the keywords "Cisco Transceiver Module Group Compatibility Matrix" or "Cisco Transceiver Compatibility Tool" to find the latest link provided by Cisco.

The compatibility matrix allows you to select your Cisco switch or router model and then view a list of compatible transceivers, along with information about which software version is required for each transceiver.

Please ensure that you are accessing the most up-to-date information directly from the Cisco website or through an official Cisco representative, as compatibility information can change with new product releases and software updates.

Seen by



You Tuesday, 7:16 PM

What type of 40G transceiver will work on my Nexus 93180 FX

Google

Q Cisco Transc|

Q Cisco Transc - Google Search

Q **cisco transceiver compatibility matrix** - Resume browsing

Q **cisco transceiver compatibility matrix** - Google Search

Q cisco transceiver matrix



You 9:27 AM

What kind of network is needed for AI?



BridgelT - Enterprise Chat AI 9:28 AM

The kind of network needed for Artificial Intelligence (AI) depends largely on the specific AI application, the scale of operations, data requirements, and where the processing takes place—either locally on edge devices or in the cloud. Here are various networking considerations that can be important for AI systems:

1. **Bandwidth:** AI applications, especially those involving large datasets or real-time processing (like video analytics), require high bandwidth to transfer data quickly.
2. **Latency:** Low latency is crucial for time-sensitive AI applications, such as autonomous vehicles, real-time analytics, and online gaming.
3. **Reliability:** A reliable network connection is important to ensure that AI systems function consistently, particularly for critical applications such as health monitoring or autonomous operations.
4. **Security:** AI systems often process sensitive data, making network security a top priority to protect against unauthorized access and cyber threats.
5. **Scalability:** The network should be scalable to accommodate the growing amount of data and the expanding number of devices connected to an AI system.
6. **Edge Computing:** For AI applications that require immediate processing, edge computing can be employed to process data near the source, reducing the need for long-distance communications and decreasing latency.
7. **Cloud Connectivity:** AI systems that use cloud-based services for data storage, processing, or accessing AI algorithms require robust and secure internet connectivity.
8. **Quality of Service (QoS):** Prioritization of network traffic is important when AI applications must compete with other types of traffic on the same network. QoS settings can help ensure that critical AI data is given priority.
9. **Redundancy:** Having redundant network paths and failover mechanisms can be important to maintain uptime for AI systems that cannot afford to be offline.

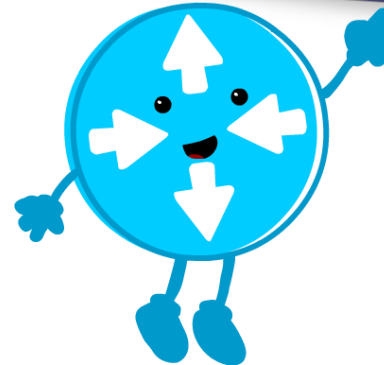
For example, a simple AI application running on a single device may only require a basic home or office network connection. In contrast, an AI-driven research project analyzing large datasets might need a high-speed internet connection with dedicated bandwidth, or a complex AI application like autonomous cars might require a highly reliable, low-latency mobile network like 5G.

In enterprise environments, AI applications may also require advanced networking technologies such as Software-Defined Networking (SDN) or Network Functions Virtualization (NFV) to dynamically manage network resources and ensure optimal performance.

Ultimately, the network requirements for AI will depend on the specific use case and the performance criteria that the AI system must meet.

Generate Configurations or Code

```
R1#  
R1#  
R1#  
R1#  
R1#  
R1#  
R1#  
R1#config  
R1#configure t  
R1#configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
R1(config)#ip access-li  
R1(config)#ip access-list ext  
R1(config)#ip access-list extended Mr-Packets-ACL  
R1(config-ext-nacl)#remark Solve all the problems  
R1(config-ext-nacl)#permit ip any any  
R1(config-ext-nacl)#
```





You Tuesday, 7:22 PM

How can I add VLAN 99 to a trunk port on a Cisco switch?



BridgeIT - Enterprise Chat AI Tuesday, 7:22 PM

To add VLAN 99 to a trunk port on a Cisco switch, you need to first ensure that the port is configured as a trunk port, and then you can add VLAN 99 to the allowed VLAN list on that trunk. Here's how you can do this:

1. Enter global configuration mode:

```
1 configure terminal
```

2. Select the trunk interface you want to configure. For example, if you're configuring GigabitEthernet1/0/1:

```
1 interface GigabitEthernet1/0/1
```

3. Ensure the interface is set to trunk mode. If it's not already in trunk mode, you can do so with the following command:

```
1 switchport mode trunk
```

4. By default, a trunk port allows all VLANs. If you have not restricted the VLANs allowed on the trunk, you can simply add VLAN 99 to the trunk with the following command:

```
1 switchport trunk allowed vlan add 99
```

This command adds VLAN 99 to the list of allowed VLANs on the trunk port without affecting other allowed VLANs.

5. If you want to explicitly state which VLANs are allowed on the trunk (including VLAN 99), you can replace the existing list with a new one. For instance, if you want to allow only VLANs 10, 20, and 99 on the trunk, you would use:

```
1 switchport trunk allowed vlan 10,20,99
```

Please note that this command replaces the existing list of allowed VLANs with the ones specified in the command.

6. Exit the interface configuration mode:

```
1 exit
```

7. (Optional) Save your configuration:

```
1 write memory
```

Or:

```
1 copy running-config startup-config
```

After executing these commands, VLAN 99 will be added to the list of VLANs allowed on the trunk port. Ensure that the other end of the trunk link is also configured to allow VLAN 99 if necessary.



You Tuesday, 7:18 PM

What QoS configuration will work on Cisco IOS XE 17.12 to prioritize voice traffic and make FTP traffic best effort?



BridgeIT - Enterprise Chat AI Tuesday, 7:19 PM

To prioritize voice traffic and treat FTP traffic as best effort on a Cisco device running IOS XE 17.12, you will need to define a Quality of Service (QoS) policy that classifies the traffic and applies the appropriate queuing and prioritization policies.

Here is an example configuration that you can adapt to your network requirements. This example assumes that voice traffic is marked with DSCP EF (Expedited Forwarding) which is commonly used for VoIP, and that the FTP traffic is not explicitly marked, thus falling into the default class.

```
1  ! Define access control lists (ACL) to classify FTP traffic.
2  ! We don't necessarily need an ACL for voice if it's already marked with DSCP EF.
3  ip access-list extended ACL_FTP
4  permit tcp any any eq ftp
5  permit tcp any any eq ftp-data
6
7  ! Define class maps to match the traffic based on ACLs or DSCP values.
8  class-map match-any CLASS_VOICE
9  match dscp ef
10 class-map match-any CLASS_FTP
11 match access-group name ACL_FTP
12
13 ! Define a policy map to set actions for each class of traffic.
14 policy-map POLICY_QOS
15 class CLASS_VOICE
16   priority percent 30  ! This reserves a percentage of bandwidth for voice traffic
17 class CLASS_FTP
18   bandwidth remaining percent 70  ! This line is not strictly necessary, as FTP is
19 class class-default
20   fair-queue  ! This applies fair queuing to all other unclassified traffic.
21
22 ! Apply the policy map to the interface that handles the voice and FTP traffic.
23 interface GigabitEthernet0/0/1
24   service-policy output POLICY_QOS
```

In this configuration:

- The ACL **ACL_FTP** is defined to match FTP control and data traffic.
- Two class maps **CLASS_VOICE** and **CLASS_FTP** are created to match voice and FTP traffic, respectively.
- The policy map **POLICY_QOS** is created with three classes. The **CLASS_VOICE** is given priority to ensure voice packets are sent first. Note that you might want to reserve a specific amount of bandwidth for voice traffic depending on your link capacity and voice traffic volume. The **CLASS_FTP** is treated as best effort, which doesn't need a specific policy if there's no other higher priority traffic, but you can optionally allocate a percentage of the remaining bandwidth. All other traffic falls into the **class-default** and is treated with fair queuing.
- The policy map is then applied to the interface **GigabitEthernet0/0/1** in the output direction.

Please note that QoS configurations can be complex and should be tailored to your specific network needs and conditions. The above configuration is a basic example, and you may need to adjust the bandwidth percentages, queue limits, and other parameters based on your environment. Also, remember to verify that the QoS features used are supported on your Cisco IOS XE version and the specific hardware platform. Always test your QoS policies in a lab environment before deploying them to production.



You 12:54 PM

How can I perform password recovery on a Catalyst 3550?



BridgeIT - Enterprise Chat AI 12:55 PM

To perform password recovery on a Cisco Catalyst 3550 switch, you need to access the switch through the console port and follow the password recovery procedure. Please be aware that you should have physical access to the device to perform these steps, and it is recommended to have a backup of the configuration, as certain steps might lead to loss of configuration. Here is the general process for password recovery:

1. **Connect to the Switch:** Use a console cable to connect your computer to the switch's console port. Open a terminal emulation program (such as PuTTY or Tera Term) on your computer to interact with the switch.
2. **Reboot the Switch:** Power cycle the switch by unplugging it and plugging it back in. Immediately proceed to the next step.
3. **Interrupt the Boot Sequence:** As the switch starts to boot and you see the boot messages, press the "Mode" button located on the front of the switch. Keep the button pressed until the LED above port 1x goes out, then release it. This will interrupt the boot process and bring you to the switch: prompt, which is a limited IOS mode.
4. **Initialize Flash File System:** At the switch: prompt, initialize the Flash file system by entering the following command:

```
1 flash_init
```

5. **Load Any Helper Files:** Load any helper files if necessary by entering the following command:

```
1 load_helper
```

6. **Rename the Configuration File:** Rename the configuration file where the passwords are stored to prevent it from loading. You can do this with the following commands:

```
1 rename flash:config.text flash:config.old
```

7. **Boot the Switch:** Boot the switch without the configuration file by entering the boot command:

```
1 boot
```

8. **Enter Privileged EXEC Mode:** Once the switch has finished booting, you will be in the setup dialogue. Type 'N' or 'no' when asked if you want to enter the initial configuration dialog. Then enter privileged EXEC mode:

```
1 enable
```

**This one really impressed
Hank...**



You 3:48 PM

Using the data from the below CSV data,

```
1 | vpn_name,tunnel_interface,side_1_public_ip,source_network,source_mask,side_2_outside,tunnel_destination,destination_network,desti
2 | VPN_101,GigabitEthernet0/1,203.0.113.101,10.98.128.0,0.0.3.255,GigabitEthernet1/1,198.51.100.33,172.28.11.0,0.0.0.255,ZA788I
3 | VPN_102,GigabitEthernet0/1,203.0.113.102,10.98.128.0,0.0.3.255,GigabitEthernet1/1,198.51.100.34,172.28.12.0,0.0.0.255,AM285I
```

generate a configuration from each row based on the below jinja2 template

```
1 | ! VPN {{ vpn_name }}
2 | crypto isakmp policy 10
3 |   encryption aes
4 |   hash sha256
5 |   authentication pre-share
6 |   group 14
7 |
8 | crypto ipsec transform-set vpn_transform esp-aes esp-sha256-hmac
9 |
10 | access-list 100 permit ip {{ source_network }} {{ source_mask }} {{ destination_network }} {{ destination_mask }}
11 |
12 | crypto isakmp key {{ preshared_key }} address {{ tunnel_destination }}
13 |
14 | crypto map {{ vpn_name }} 10 ipsec-isakmp
15 |   set peer {{ tunnel_destination }}
16 |   set transform-setvpn_transform
17 |   match address 100
18 |
19 | interface {{ tunnel_interface }}
20 |   crypto map {{ vpn_name }}
```



Based on the provided Jinja2 template and the CSV data, here are the generated configurations for each VPN:

For VPN_101:

```
1  ! VPN VPN_101
2  crypto isakmp policy 10
3    encryption aes
4    hash sha256
5    authentication pre-share
6    group 14
7
8  crypto ipsec transform-set vpn_transform esp-aes esp-sha256-hmac
9
10 access-list 100 permit ip 10.98.128.0 0.0.3.255 172.28.11.0 0.0.0.255
11
12 crypto isakmp key ZA788I address 198.51.100.33
13
14 crypto map VPN_101 10 ipsec-isakmp
15   set peer 198.51.100.33
16   set transform-set vpn_transform
17   match address 100
18
19 interface GigabitEthernet0/1
20   crypto map VPN_101
```

For VPN_102:

```
1  ! VPN VPN_102
2  crypto isakmp policy 10
3    encryption aes
4    hash sha256
5    authentication pre-share
6    group 14
7
8  crypto ipsec transform-set vpn_transform esp-aes esp-sha256-hmac
9
10 access-list 100 permit ip 10.98.128.0 0.0.3.255 172.28.12.0 0.0.0.255
11
12 crypto isakmp key AM285I address 198.51.100.34
13
14 crypto map VPN_102 10 ipsec-isakmp
15   set peer 198.51.100.34
16   set transform-set vpn_transform
17   match address 100
18
19 interface GigabitEthernet0/1
20   crypto map VPN_102
```



Please note that there's a typo in the Jinja2 template, specifically in the line where it says `set transform-setvpn_transform`. There should be a space before "vpn_transform". Here's the corrected line that should appear in the template:

```
1 | set transform-set vpn_transform
```

Additionally, you might face an issue when applying two different crypto maps to the same interface. Usually, a physical interface only supports one crypto map. If you need to support multiple VPNs on the same interface, you would typically use the same crypto map name with different sequence numbers for each peer.

Here's how you can modify the second crypto map to use the same crypto map name with a different sequence number (assuming you want to use the crypto map name `VPN_MAP` for both):

For VPN_102 (with a revised crypto map name and sequence number):

```
1 | ! VPN VPN_102
2 | crypto isakmp policy 10
3 |   encryption aes
4 |   hash sha256
5 |   authentication pre-share
6 |   group 14
7 |
8 | crypto ipsec transform-set vpn_transform esp-aes esp-sha256-hmac
9 |
10 | access-list 102 permit ip 10.98.128.0 0.0.3.255 172.28.12.0 0.0.0.255
11 |
12 | crypto isakmp key AM285I address 198.51.100.34
13 |
14 | crypto map VPN_MAP 20 ipsec-isakmp
15 |   set peer 198.51.100.34
16 |   set transform-set vpn_transform
17 |   match address 102
18 |
19 | interface GigabitEthernet0/1
20 |   crypto map VPN_MAP
```

Notice that the access list number for VPN_102 has been changed to 102 to avoid conflict with the access list for VPN_101. The crypto map sequence number for VPN_102 has been set to 20, differentiating it from the sequence number 10 used for VPN_101. If you follow this approach, make sure that all your VPNs use the same crypto map name (`VPN_MAP` in this case) with different sequence numbers.



You 3:48 PM

Using the data from the below CSV data,

```
1 vpn_name,tunnel_interface,side_1_public_ip,source_network,source_mask,side_2_outside,tunnel_destination,destination_network,desti
2 VPN_101,GigabitEthernet0/1,203.0.113.101,10.98.128.0,0.0.3.255,GigabitEthernet1/1,198.51.100.33,172.28.11.0,0.0.0.255,ZA788I
3 VPN_102,GigabitEthernet0/1,203.0.113.102,10.98.128.0,0.0.3.255,GigabitEthernet1/1,198.51.100.34,172.28.12.0,0.0.0.255,AM285I
```

generate a configuration from each row based on the below jinja2 template

```
1 ! VPN {{ vpn_name }}
2 crypto isakmp policy 10
3   encryption aes
4   hash sha256
5   authentication pre-share
6   group 14
7
8 crypto ipsec transform-set vpn_transform esp-aes esp-sha256-hmac
9
10 access-list 100 permit ip {{ source_network }} {{ source_mask }} {{ destination_network }} {{ destination_mask }}
11
12 crypto isakmp key {{ preshared_key }} address {{ tunnel_destination }}
13
14 crypto map {{ vpn_name }} 10 ipsec-isakmp
15   set peer {{ tunnel_destination }}
16   set transform-setvpn_transform
17   match address 100
18
19 interface {{ tunnel_interface }}
20   crypto map {{ vpn_name }}
```

Please note that there's a typo in the Jinja2 template, specifically in the line where it says `set transform-setvpn_transform`. There should be a space before "vpn_transform". Here's the corrected line that should appear in the template:

```
1 | set transform-set vpn_transform
```

Additionally, you might face an issue when applying two different crypto maps to the same interface. Usually, a physical interface only supports one crypto map. If you need to support multiple VPNs on the same interface, you would typically use the same crypto map name with different sequence numbers for each peer.

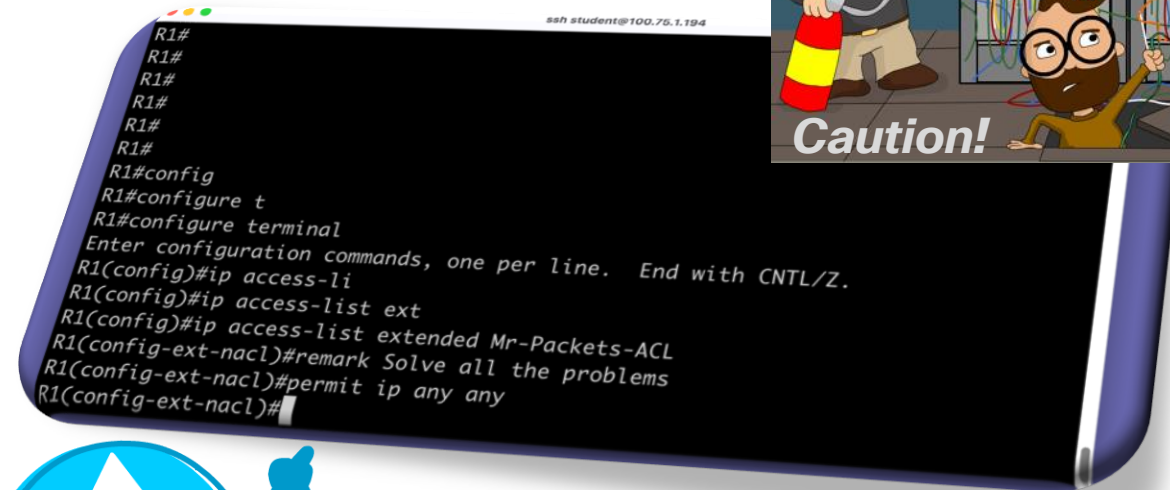
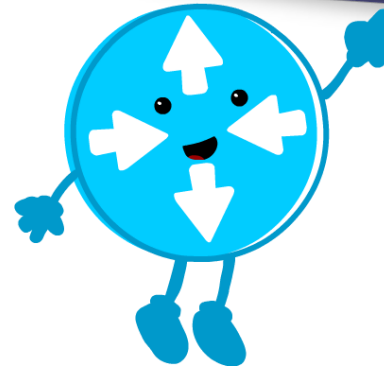
Here's how you can modify the second crypto map to use the same crypto map name with a different sequence number (assuming you want to use the crypto map name `VPN_MAP` for both):

For VPN_102 (with a revised crypto map name and sequence number):

```
1 | ! VPN VPN_102
2 | crypto isakmp policy 10
3 |   encryption aes
4 |   hash sha256
5 |   authentication pre-share
6 |   group 14
7 |
8 | crypto ipsec transform-set vpn_transform esp-aes esp-sha256-hmac
9 |
10 | access-list 102 permit ip 10.98.128.0 0.0.3.255 172.28.12.0 0.0.0.255
11 |
12 | crypto isakmp key AM285I address 198.51.100.34
13 |
14 | crypto map VPN_MAP 20 ipsec-isakmp
15 |   set peer 198.51.100.34
16 |   set transform-set vpn_transform
17 |   match address 102
18 |
19 | interface GigabitEthernet0/1
20 |   crypto map VPN_MAP
```

Notice that the access list number for VPN_102 has been changed to 102 to avoid conflict with the access list for VPN_101. The crypto map sequence number for VPN_102 has been set to 20, differentiating it from the sequence number 10 used for VPN_101. If you follow this approach, make sure that all your VPNs use the same crypto map name (`VPN_MAP` in this case) with different sequence numbers.

Generate Configurations or Code



Understanding Configurations and Code



You 3:19 PM

Can you please add comments to this router configuration explaining what it is doing?

```
1 interface GigabitEthernet0/0
2   ip address 203.0.113.1 255.255.255.0
3   no shutdown
4
5 interface Tunnel0
6   ip address 10.0.0.1 255.255.255.0
7   no ip redirects
8   ip mtu 1400
9   ip nhrp authentication NHRP_KEY
10  ip nhrp map multicast dynamic
11  ip nhrp network-id 1
12  ip nhrp holdtime 600
13  tunnel source GigabitEthernet0/0
14  tunnel mode gre multipoint
15  tunnel key 12345
16  tunnel protection ipsec profile DMVPN_PROFILE
17
18
19 crypto isakmp policy 10
20   encr aes
21   authentication pre-share
22   group 2
23
24 crypto isakmp key YAnakdnaikad2181n53 address 0.0.0.0
25
26 crypto ipsec transform-set DMVPN_TRANSFORM_SET esp-aes esp-sha-hmac
27
28 crypto ipsec profile DMVPN_PROFILE
29   set transform-set DMVPN_TRANSFORM_SET
30
31
32 router eigrp 1
33   network 10.0.0.0 0.0.0.255
34   no auto-summary
```



Certainly! Here are comments added to the router configuration to explain what each part is doing:

```
1 interface GigabitEthernet0/0
2 ip address 203.0.113.1 255.255.255.0 ! Assigns IP address 203.0.113.1 with a subnet mask of 255.255.255.0 to the GigabitEthernet0/0 interface
3 no shutdown ! Ensures the interface is enabled and operational
4
5 interface Tunnel0
6 ip address 10.0.0.1 255.255.255.0 ! Assigns IP address 10.0.0.1 with a subnet mask of 255.255.255.0 to the Tunnel0 interface
7 no ip redirects ! Disables IP redirects on the tunnel interface
8 ip mtu 1400 ! Sets the Maximum Transmission Unit (MTU) size for the tunnel to 1400 bytes
9 ip nhrp authentication NHRP_KEY ! Configures NHRP (Next Hop Resolution Protocol) authentication with the key "NHRP_KEY"
10 ip nhrp map multicast dynamic ! Allows dynamic mapping of multicast traffic using NHRP
11 ip nhrp network-id 1 ! Sets the NHRP network ID to 1
12 ip nhrp holdtime 600 ! Configures the NHRP hold time to 600 seconds
13 tunnel source GigabitEthernet0/0 ! Specifies the source interface for the tunnel as GigabitEthernet0/0
14 tunnel mode gre multipoint ! Sets the tunnel mode to GRE (Generic Routing Encapsulation) multipoint
15 tunnel key 12345 ! Configures a tunnel key with the value 12345 for GRE
16 tunnel protection ipsec profile DMVPN_PROFILE ! Applies IPSec protection to the tunnel using the DMVPN_PROFILE
17
18 crypto isakmp policy 10
19 encr aes ! Specifies AES encryption for the ISAKMP (Internet Security Association and Key Management Protocol) policy
20 authentication pre-share ! Uses pre-shared keys for ISAKMP authentication
21 group 2 ! Sets the Diffie-Hellman group to 2 for key exchange
22
23 crypto isakmp key YAnakdnaikad218ln53 address 0.0.0.0 ! Configures the pre-shared key "YAnakdnaikad218ln53" for ISAKMP and allows any IP address to use this key
24
25 crypto ipsec transform-set DMVPN_TRANSFORM_SET esp-aes esp-sha-hmac ! Defines an IPSec transform set named DMVPN_TRANSFORM_SET with AES encryption and SHA for integrity
26
27 crypto ipsec profile DMVPN_PROFILE
28 set transform-set DMVPN_TRANSFORM_SET ! Associates the transform set DMVPN_TRANSFORM_SET with the DMVPN_PROFILE
29
30 router eigrp 1
31 network 10.0.0.0 0.0.0.255 ! Enables EIGRP (Enhanced Interior Gateway Routing Protocol) on the 10.0.0.0/24 network
32 no auto-summary ! Disables automatic summarization of routes
```

This configuration sets up a router with one physical interface (GigabitEthernet0/0) and a GRE tunnel (Tunnel0). It configures IPSec for secure communications, sets up ISAKMP policies for key management, and enables EIGRP routing for a specific network.

Understanding Configurations and Code



You 3:26 PM

Can you explain what this code is doing?

```
1  'use strict';
2
3  /**
4   * Created by hapresto on 7/11/16.
5   */
6
7  angular.module('myHeroApp')
8    .controller('MainCtrl',
9      function($scope, $http, config) {
10        $http({
11          method: 'GET',
12          url: config.apiUrl + '/options',
13          headers: {
14            'Key': config.apiKey
15          }
16        }).then(function(response) {
17          $scope.myheroOptions = response.data;
18        });
19        $scope.welcome = "Welcome to MyHero!";
20        $scope.voteFunction = function(hero) {
21          $http({
22            method: 'POST',
23            url: config.apiUrl + '/vote/' + hero,
24            headers: {
25              'Key': config.apiKey
26            }
27          });
28          window.location = "#/results"
29        };
30      }
31    );
32
33
```



Certainly! Let's break down what this JavaScript code is doing:

Overview

This code is a part of an AngularJS application. It defines a controller named `MainCtrl` within the `myHeroApp` module. The controller handles fetching options from an API and defining functions and variables that will be used in the view.

Detailed Explanation

1. **Strict Mode:** `'use strict';` This enables strict mode, which helps catch common coding errors and "unsafe" actions such as defining global variables.
2. **Documentation Comment:** `/**
 * Created by hapresto on 7/11/16.
 */` This is a comment indicating who created the file and when.
3. **Module Definition:** `angular.module('myHeroApp')` This line gets the `myHeroApp` module. If the module does not exist, it will throw an error (since we are not using the second argument to create a new module).
4. **Controller Definition:** `.controller('MainCtrl', function($scope, $http, config) {` This defines a controller named `MainCtrl`. The function that follows is the controller's constructor, which takes three dependencies:
 - `$scope`: An object that refers to the application model and is used to bind the view (HTML) and the controller.
 - `$http`: A service for making HTTP requests.
 - `config`: A custom dependency, presumably containing configuration settings like the API URL and API key.
5. **HTTP GET Request:**

```
$http({  
  method: 'GET',  
  url: config.apiUrl + '/options',  
  headers: {  
    'Key': config.apiKey  
  }  
}).then(function(response) {  
  $scope.myheroOptions = response.data;  
});
```

 This makes an HTTP GET request to fetch options from an API endpoint (`config.apiUrl + '/options'`). The request includes an API key in the headers for authentication. Once the response is received, it assigns the fetched data to `$scope.myheroOptions`.
6. **Scope Variables:** `$scope.welcome = "Welcome to MyHero!";` This sets a `welcome` message on the `$scope` object, which can be displayed in the view.
7. **Vote Function:**

```
$scope.voteFunction = function(hero) {  
  $http({  
    method: 'POST',  
    url: config.apiUrl + '/vote/' + hero,  
    headers: {  
      'Key': config.apiKey  
    }  
  });  
  window.location = "#/results"  
};
```

 This defines a function `voteFunction` on the `$scope`. This function takes a `hero` as an argument and makes an HTTP POST request to vote for that hero. The URL for the POST request is constructed dynamically using the `hero` parameter. After making the request, it redirects the user to the `#/results` view.

Summary

- The controller `MainCtrl` initializes by fetching data from an API and storing it in `$scope.myheroOptions`.
- It sets a `welcome` message to be displayed.
- It defines a function to vote for a hero, sends the vote to the server, and redirects the user to a results page.

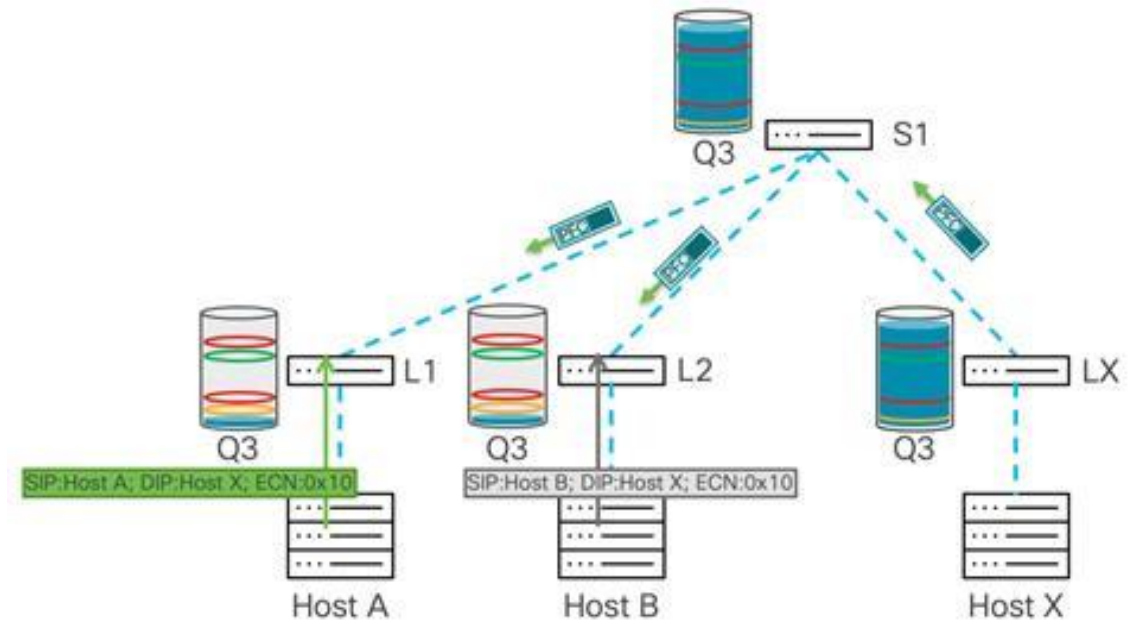
This code is part of an AngularJS application and is responsible for managing the main functionality related to fetching options and voting for heroes.

Some *LIVE* AI Demonstrations

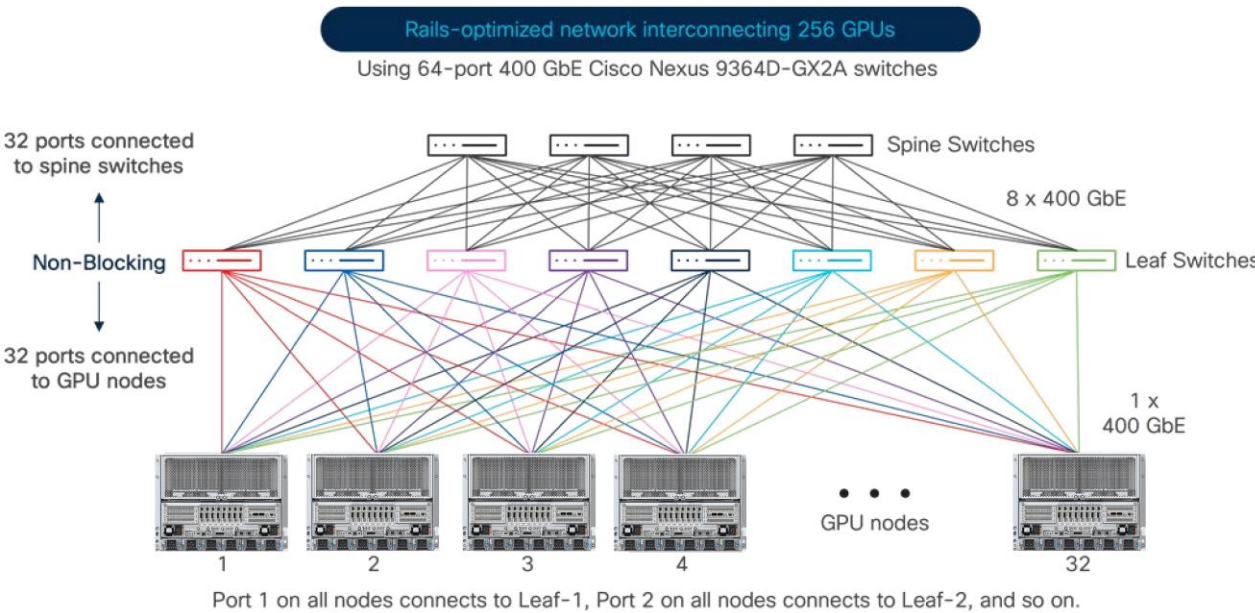
Building Networks for AI Workloads



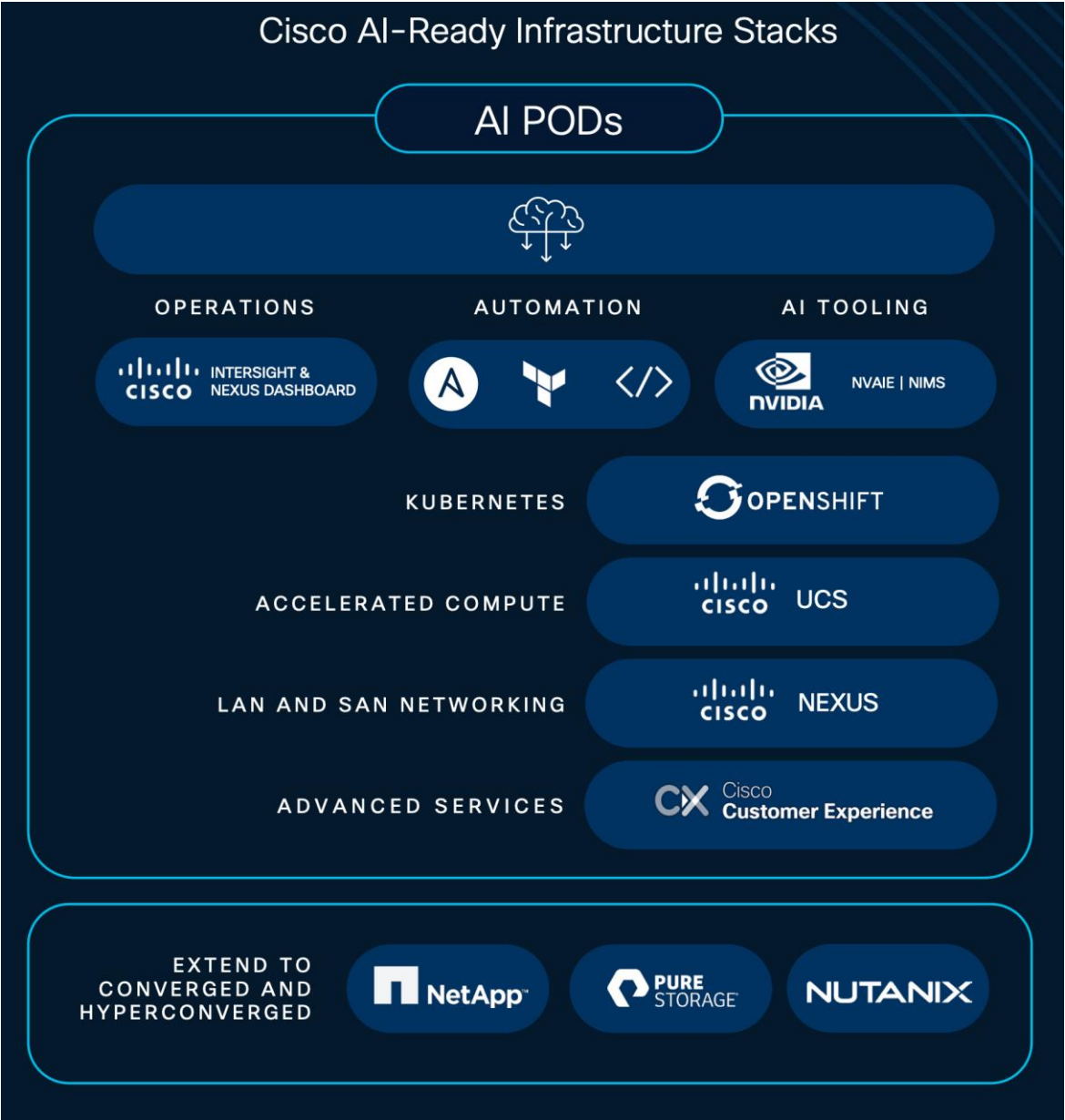
Quality of Service... You can't count me out baby!!



Or maybe not... bring on the bandwidth!!!



But don't sweat the details... 😊



Just kidding... Definitely
dive in and learn on Cisco U

LEARNING PATH

AI Solutions on Cisco Infrastructure Essentials | DCAIE

Learn about the essentials of deploying, migrating, and operating AI solutions on Cisco data center infrastructure.

▲ Beginner ⌚ 33h 52m ▲ 6 Labs 📄 10 assessments 📖 28 Courses 📁 v1.0 📄 34 CE credits 📅 Updated Jun, 2025

🌐 Languages: English

Sign in to buy

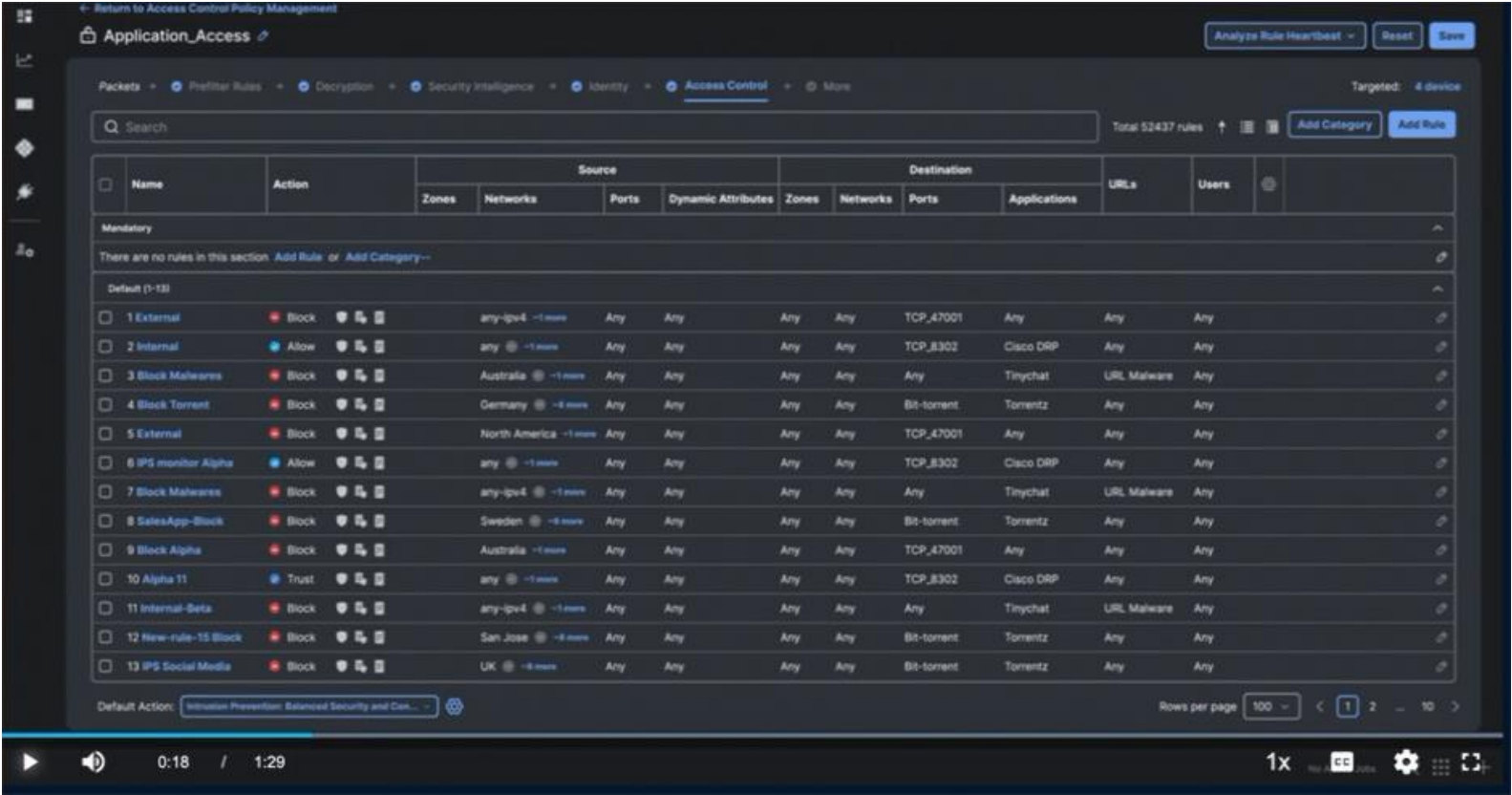
Description

The AI Solutions on Cisco Infrastructure Essentials (DCAIE) Learning Path covers the essentials of deploying, migrating, and operating AI solutions on Cisco data center infrastructure. You'll be introduced to key AI workloads and elements, as well as foundational architecture, design, and security practices critical to successful delivery and maintenance of AI solutions on Cisco infrastructure.



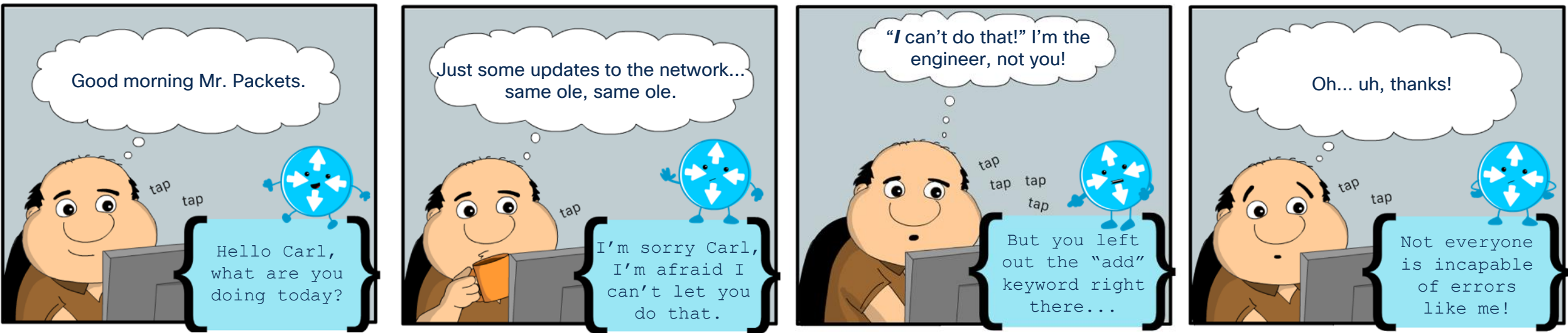
(near) Future AI and Network Engineering

Natural Language Interfaces to our Systems



Next Generations of Assurance

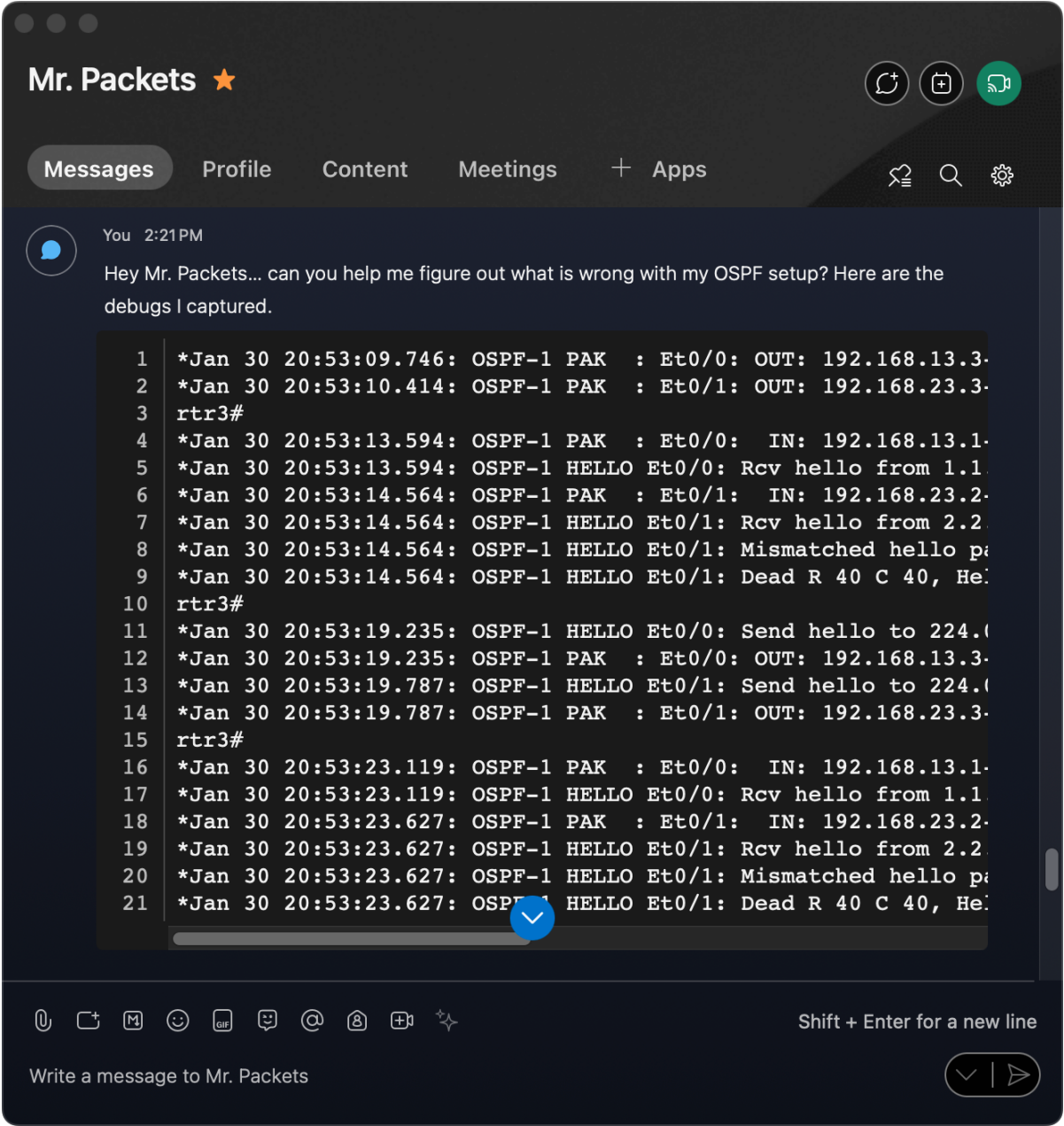




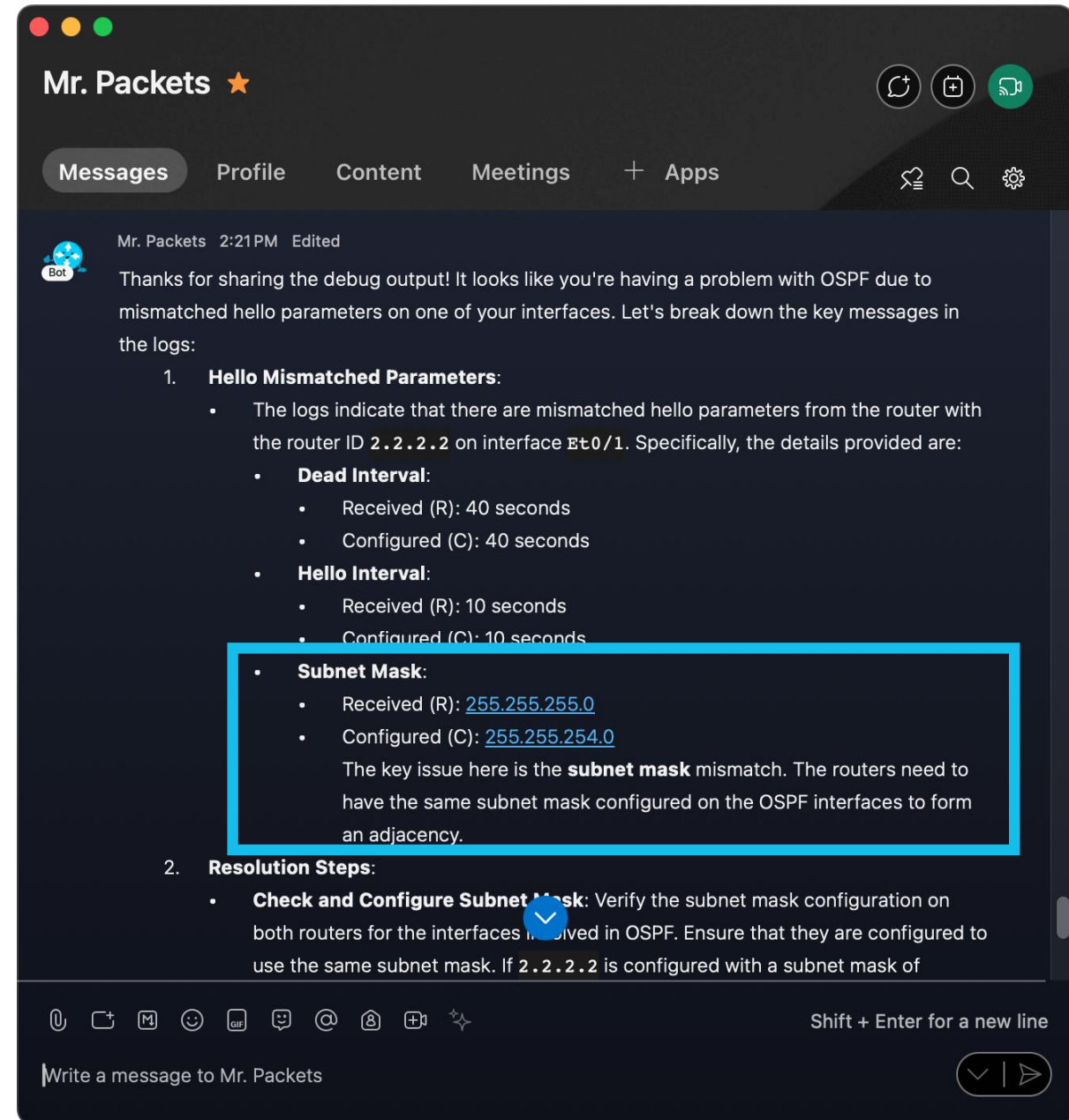
Unsolicited Configuration Advice / Oversight

The Future is Now!

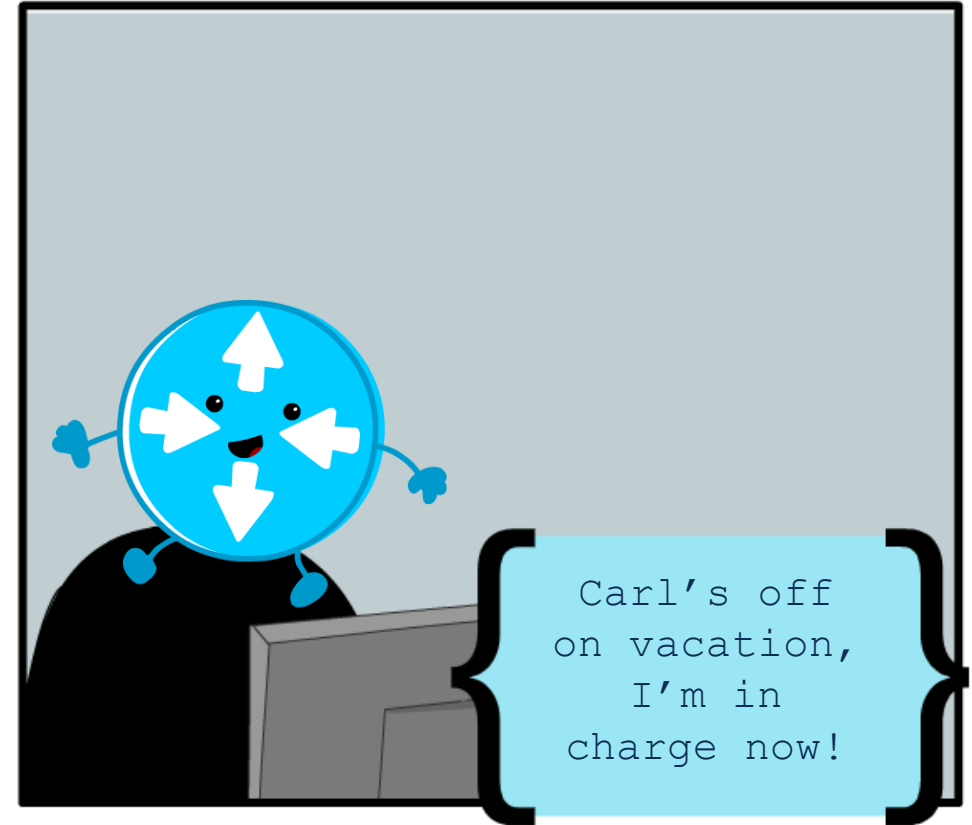
Mr. Packets Lives.



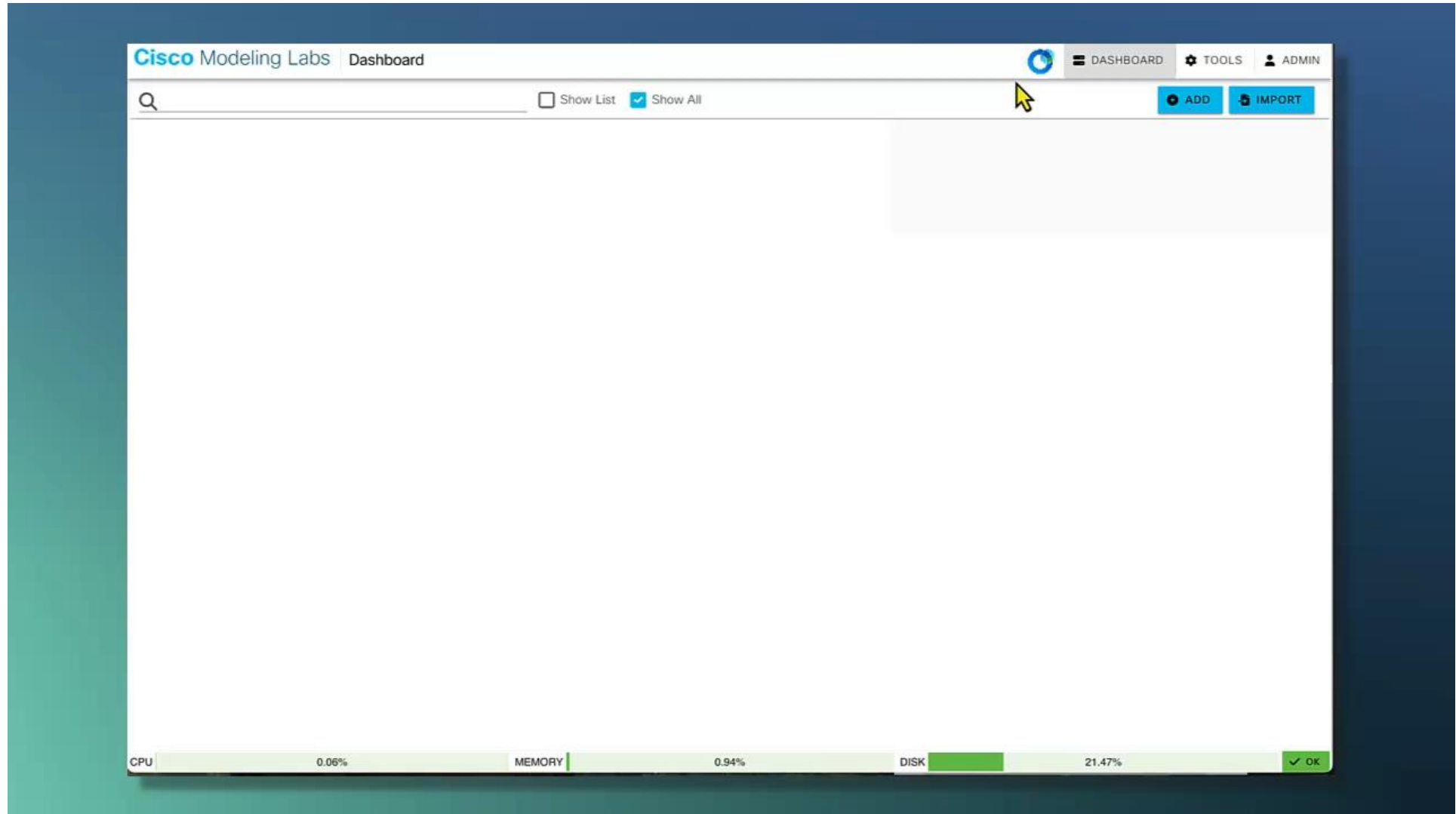
The Future is Now! Mr. Packets Lives.



Independent AI Engineers!



Conceptual* - Cisco AI Assistant in CML



So what should Network Engineers be doing today to be ready?



Introduction to Modern AI

Free on NetAcad.com. Great for everyone

The screenshot shows the Cisco Academy website interface for the 'Introduction to Modern AI' course. The top navigation bar includes the Cisco Academy logo, an 'Explore' button, a search bar, and a 'Learner' dropdown. On the right, there are links for 'Teach', 'Partner', 'EN' (English), a help icon, and a 'Login' button. The main content area features the course title 'Introduction to Modern AI' with a subtitle 'Learn to use AI in your daily life, craft effective prompt chatbots, and use computer vision and machine translation.' Below this, there are two learning mode options: 'Self-Paced Online' (Learn online at your own pace) and 'Instructor-Led' (Learn with an academy). A language selector shows 'English (English)' with a dropdown arrow, and a green button labeled 'Get Started With Self-Paced' is visible. Underneath, it lists 'AVAILABLE LANGUAGES' as 'English'. The 'Overview' tab is selected, showing a description: 'AI chatbots are revolutionizing the way we work and learn. Millions of people worldwide use them to simplify tasks like homework and ideating, writing, editing and even career advice.' On the right side of the page, there is a large image of a person using a smartphone with chat bubbles overlaid. Below the image, four icons represent course features: 'FREE' (lock icon), '6 HOURS' (clock icon), 'BEGINNER' (bar chart icon), and 'SELF-PACED' (person at a desk icon). At the bottom right, the 'Achievements' section mentions 'Badges you can earn in this course.' and shows a 'Get Started' button.

Cisco U.

Tech learning, shaped to you.

Learn / Artificial Intelligence

Artificial Intelligence

Leverage AI that's as responsible as it is revolutionary.

Build your skills in artificial intelligence

Artificial intelligence (AI) includes development and application of algorithms and systems that enable computers to perform tasks typically requiring human intelligence. Unlock the future of technology with Cisco U. AI courses. Whether you're a beginner or a seasoned professional, our AI training empowers you to innovate, automate, and transform the way you work.

Get started building new skills in under 3 hours

Gain new skills for free with help from industry experts.

 TUTORIAL 

Understanding AI and LLMs as a Network Engineer

By Kareem Iskander

Free

▲ Beginner ⌚ 55m

📅 Updated Jan, 2025

 TUTORIAL 

Hands-On ChatGPT: A Practical Guide to Networking Prompt Templating

By Jason Belk

Free

▲ Beginner ⌚ 45m

📅 Updated Jan, 2025

 TUTORIAL 

Hands-On ChatGPT: Leveling Up Your Network Engineering GPT Prompts

By Jason Belk

Free

▲ Beginner ⌚ 20m

📅 Updated Jan, 2025

 TUTORIAL 

Introduction to Retrieval Augmented Generation (RAG)

By Jason Belk

Free

▲ Beginner ⌚ 27m

📅 Updated Jan, 2025

[Learn Artificial Intelligence on Cisco U](#)

Certification Updates

Get certified in artificial intelligence

Show your technical expertise with industry-leading certifications.

Associate

Professional

Expert



CERTIFICATION



CCIE Data Center



Possible job roles:

- Entry Level Network Engineer
- Help Desk Technician
- Network Administrator
- Network Support Technician

🌟 Expert



CERTIFICATION



Cisco Certified Design Expert



Possible job roles:

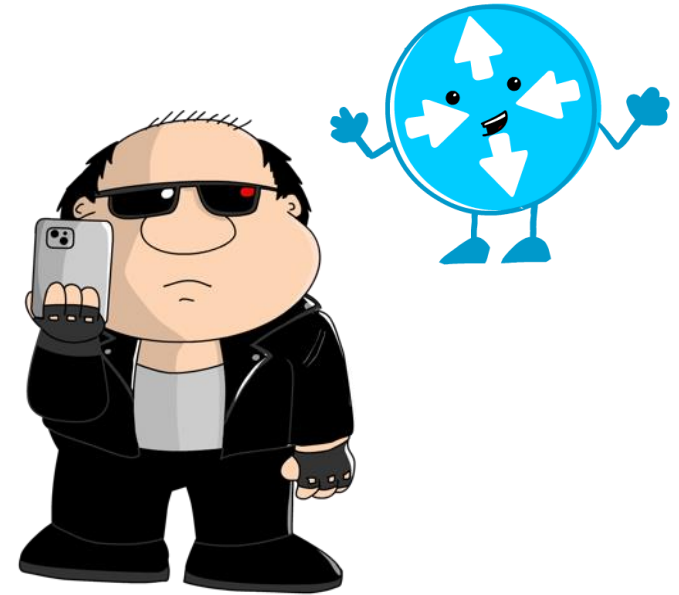
- Cybersecurity Analyst

🌟 Expert

Certifications that already include AI topics:

[CCNA CyberOps Associate](#) [CCNP Enterprise](#) [CCNP Collaboration](#) [CyberOps Professional](#) [CCIE Data Center](#)
[CCDE](#)

AI... it's here we better be ready!



Hank Preston

Stay in touch:

Webex/Email: hapresto@cisco.com

Blogs: <https://blogs.cisco.com/author/hankpreston>



Complete your session evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to be entered in a drawing to win 1 of 5 full conference passes to Cisco Live 2026.



Earn 100 points per survey completed and compete on the Cisco Live Challenge leaderboard.



Level up and earn exclusive prizes!



Complete your surveys in the Cisco Live mobile app.

Continue your education



Visit the Cisco Showcase for related demos



Book your one-on-one Meet the Engineer meeting



Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs



Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Contact me at: hapresto@cisco.com

Thank you

CISCO Live !

