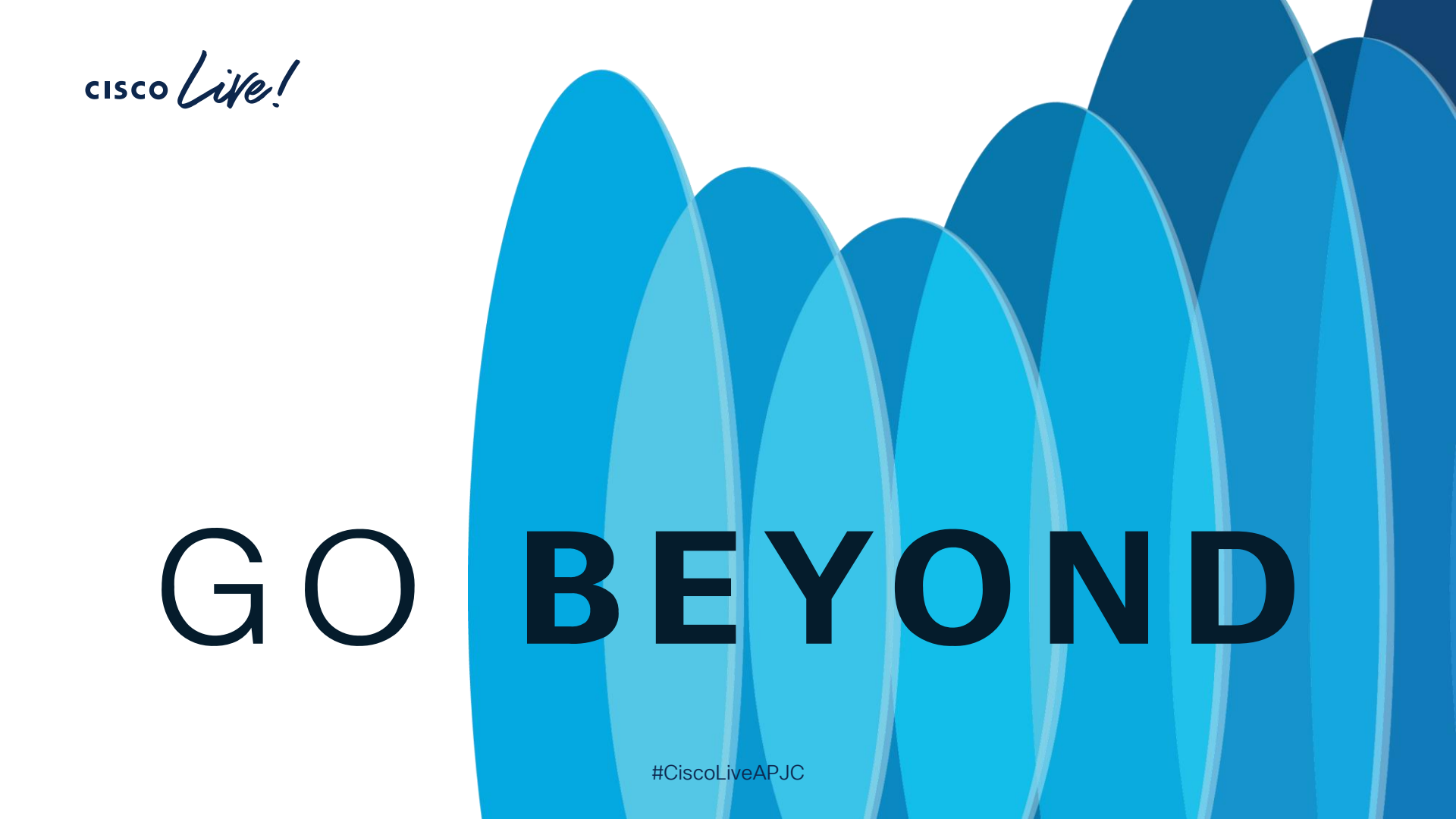

cisco Live!
GO BEYOND
#CiscoLiveAPJC

Starlink Security Advanced

Andrew Benhase, Federal Architect
@CyberSecOps

BRKSEC-2150

Cisco Webex App

https://ciscolive.ciscoevents.com/ciscolivebot/# BRKSEC-2150

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 November 15, 2024.

cisco Live!

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Agenda

- Catch up on current events
- What is Starlink
- Starlink Security
- Deployment Models
- Thousand Eyes and Network Performance
- Theater Based Concerns
- Quantum Updates
- Direct to Cell
- SDWAN

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

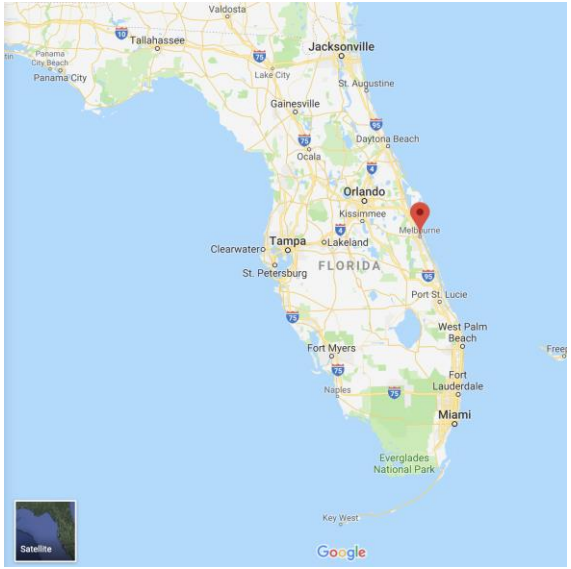
What I do here @cisco

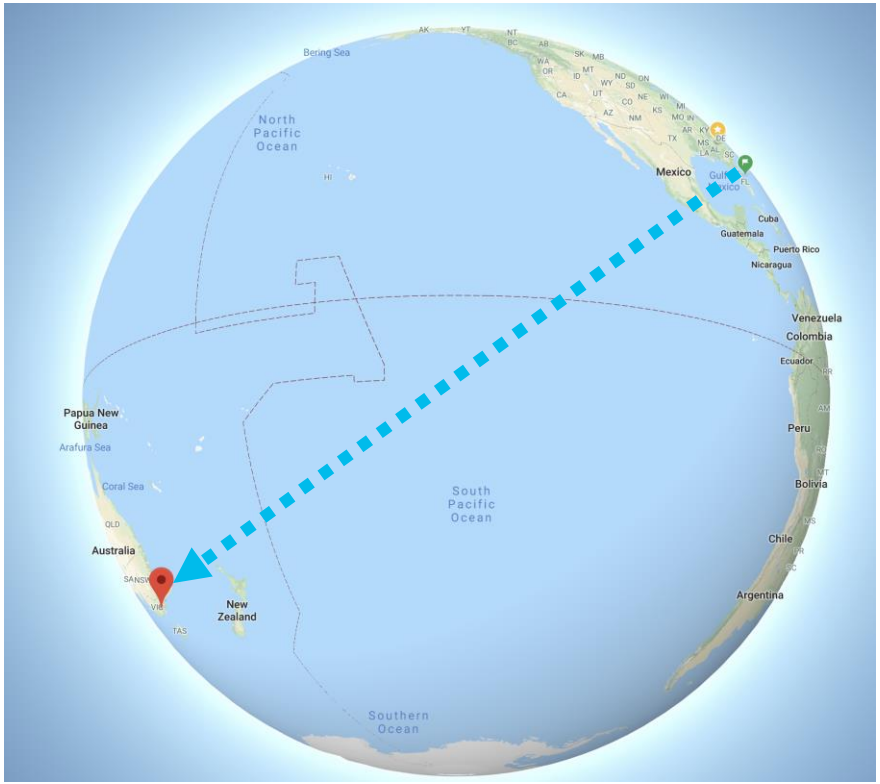
- Federal Security Architect
- At Cisco 25 years, supporting US Federal Government
- 32 years primarily supporting US Defense, Civilian and Intelligence Communities
- Deep focus on defensive cyber operations, advanced encryption, making security work!
- My first Networkers was in 1995…
- https://www.linkedin.com/in/andrewbenhase/

@CyberSecOps
@ThreatCowboy
abenhase@cisco.com

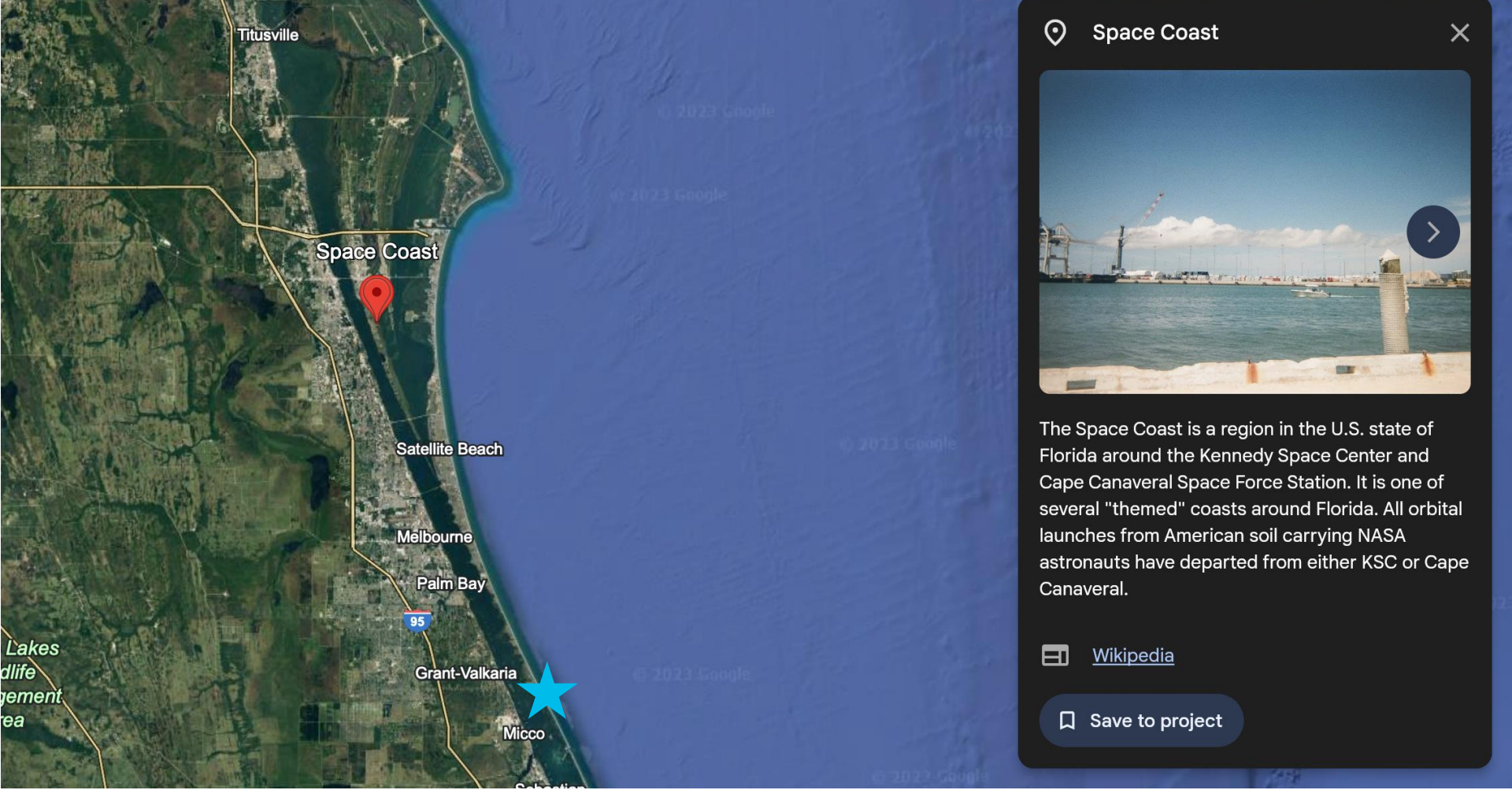
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

From MLB to MEL



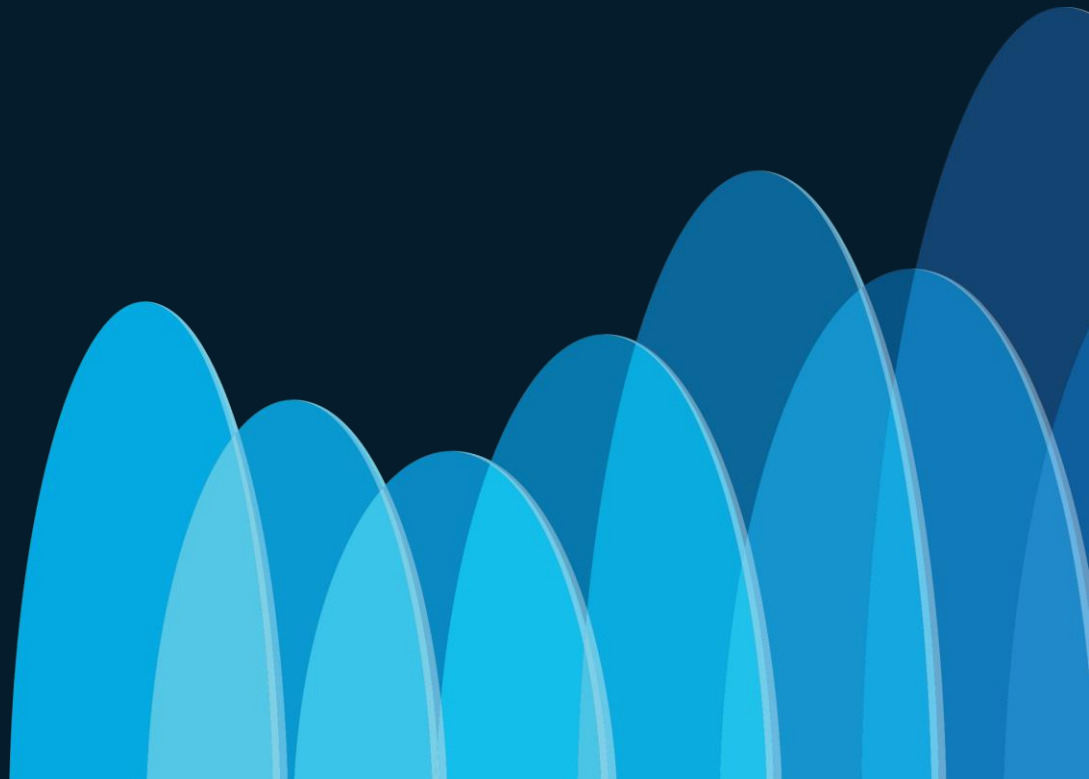


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public



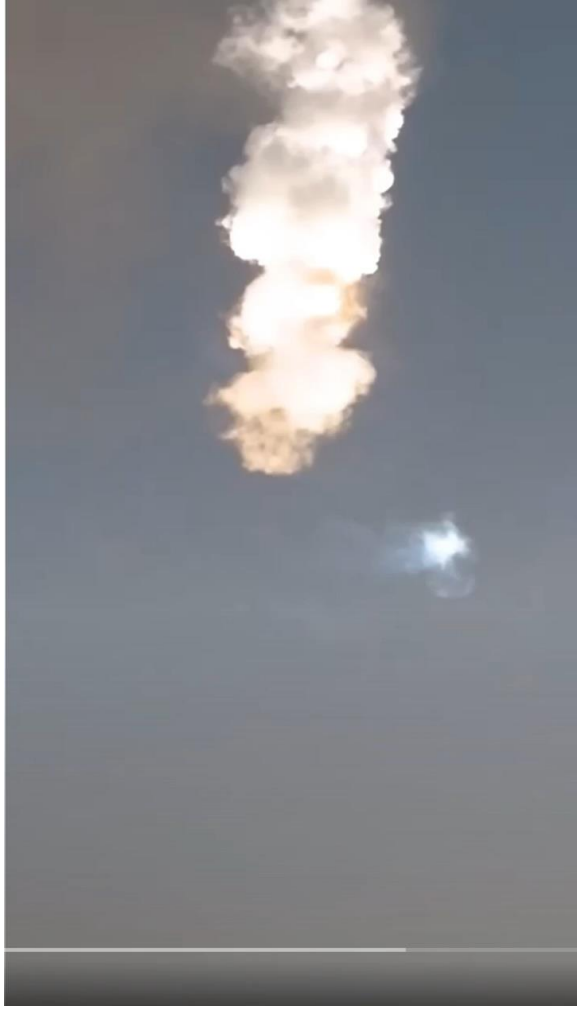
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Latest News Updates (since last year)



cisco Live!

Starship Booster Capture

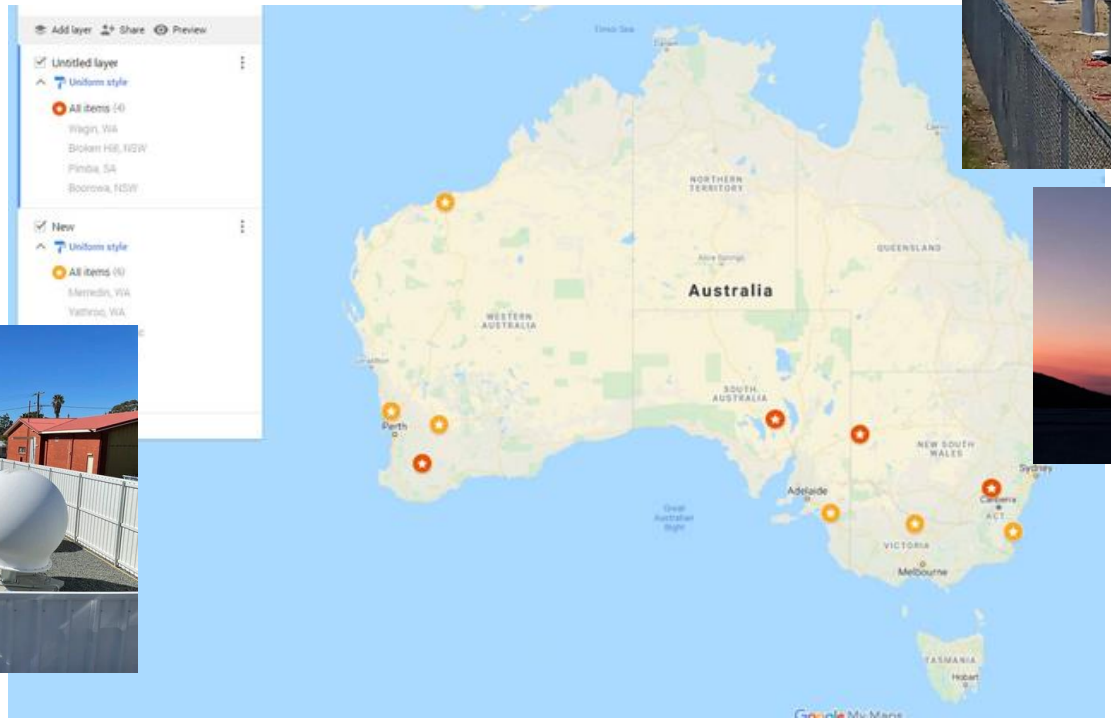


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Canberra Deep Space Communication Complex

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Where we are today



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

13:07 5GE

We call them “V2 Mini”. They represent a step forward in Starlink capability

12:37 · 2/26/23 · **843K** Views

6,931 Likes **815** Retweets **91** Quotes

SpaceX @SpaceX · 29m

V2 minis include key technologies—such as more powerful phased array antennas and the use of E-band for backhaul—which will allow Starlink to provide ~4x more capacity per satellite than earlier iterations

24 115 1,681 166K

SpaceX @SpaceX · 29m

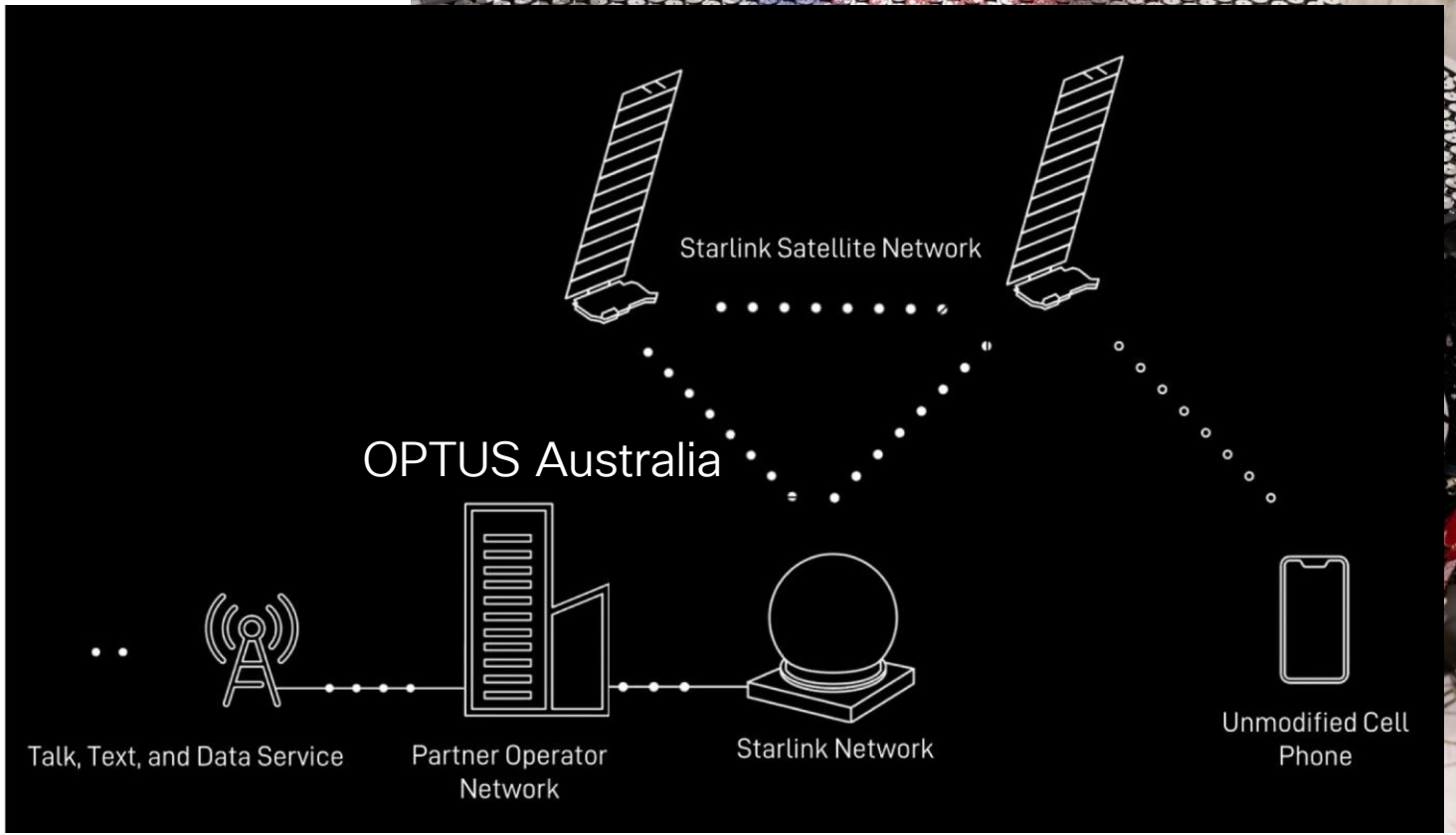
This means Starlink can provide more bandwidth with increased reliability and connect millions of more people around the

Tweet your reply

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

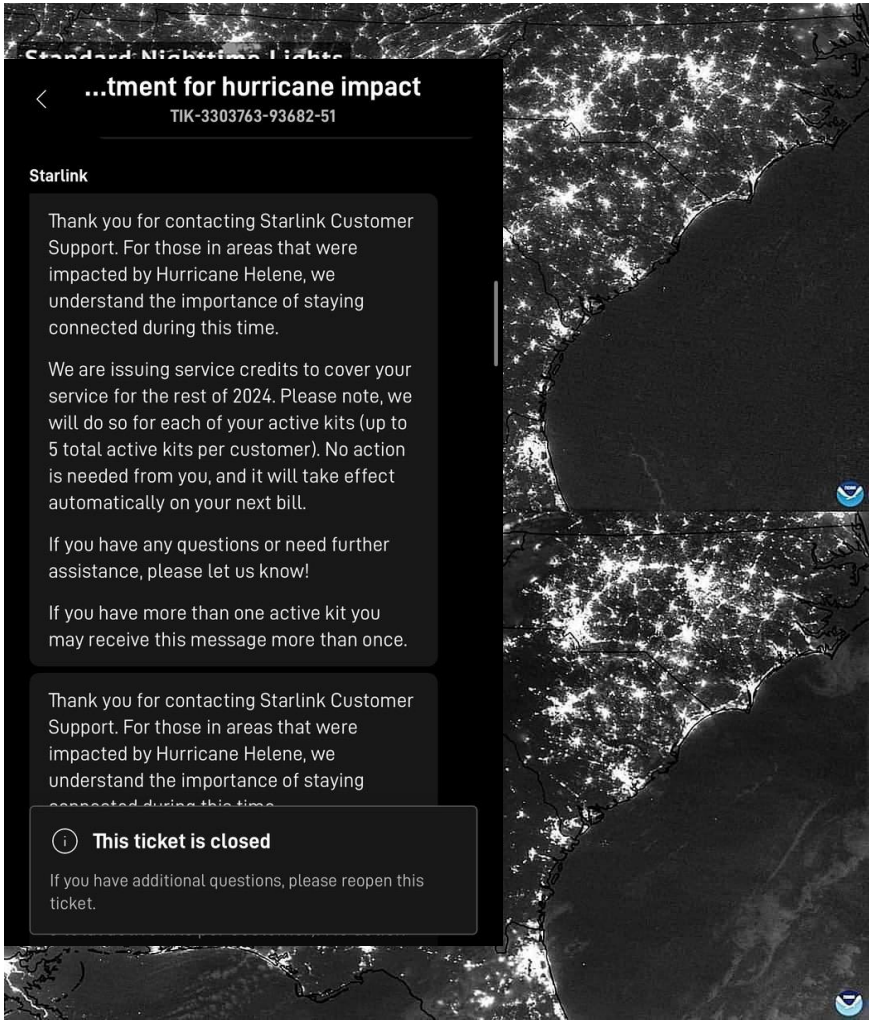
Direct to Cell

As of 9 NOV – 285 DTC enabled Satellites in orbit



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

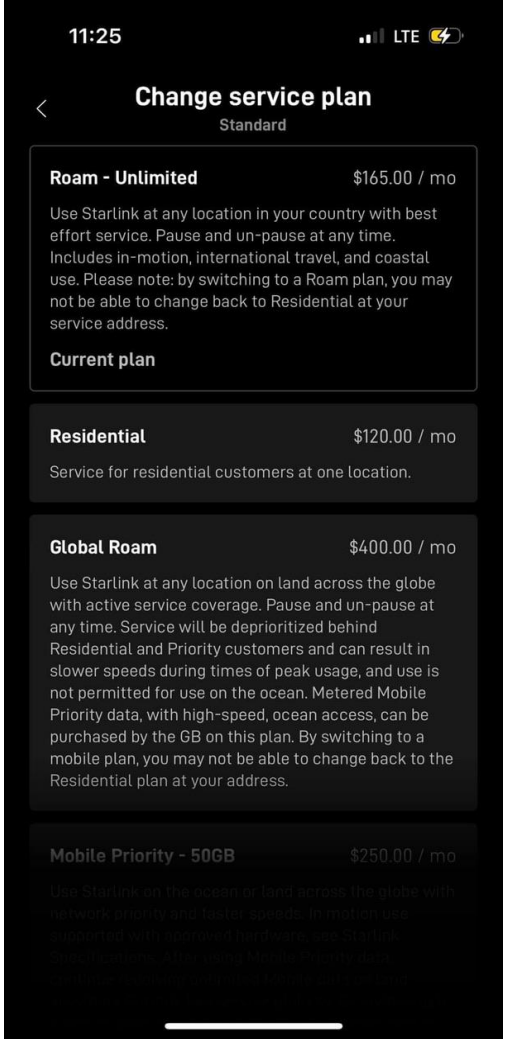
Before and After Hurricane



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

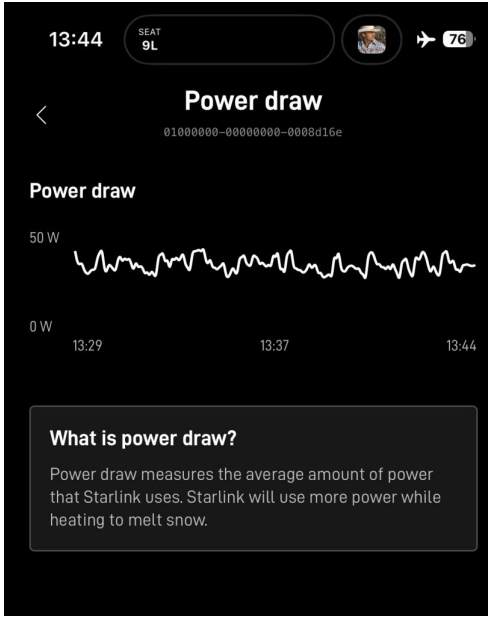
Services Changes:

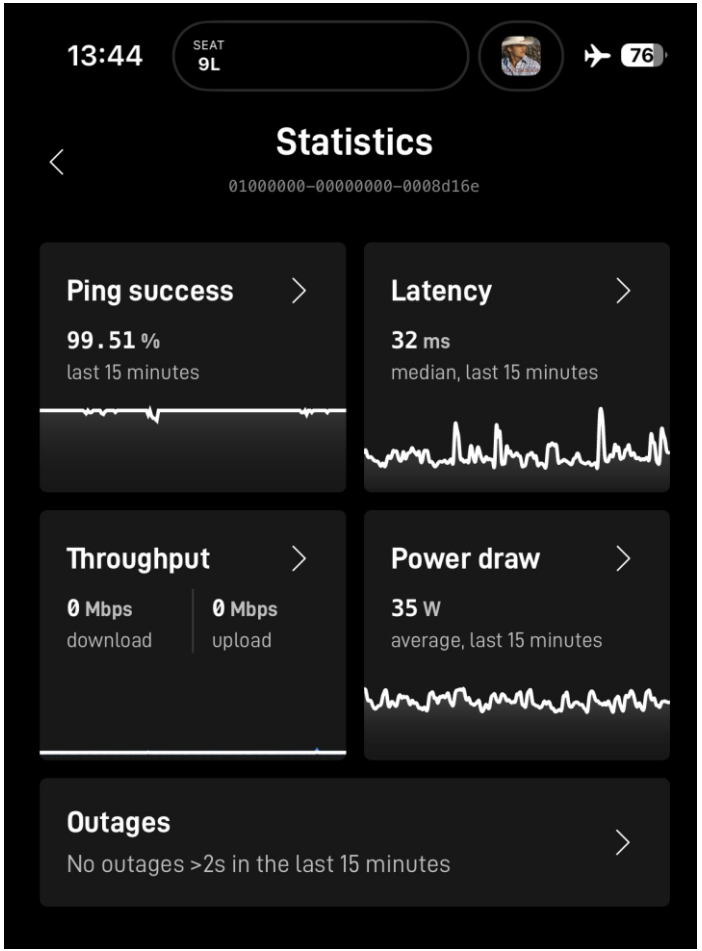
Public IP
Global Roam
Unlimited Roaming



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Starlink App Updates





© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

STARLINK

You're Invited!

Enjoy an opportunity to experience the next generation Starlink!

The next generation Starlink is slimmer and more portable, with a more elegant design than its predecessor. This Starlink Kit also includes our Gen 3 router with improved range and speeds.

The cost of the Starlink Standard kit is **$599** + Tax and Shipping.

EARLY ACCESS SPECIAL OFFER:
Enjoy your first month of service on us!*

ORDER NOW

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

How things have changed in one year!

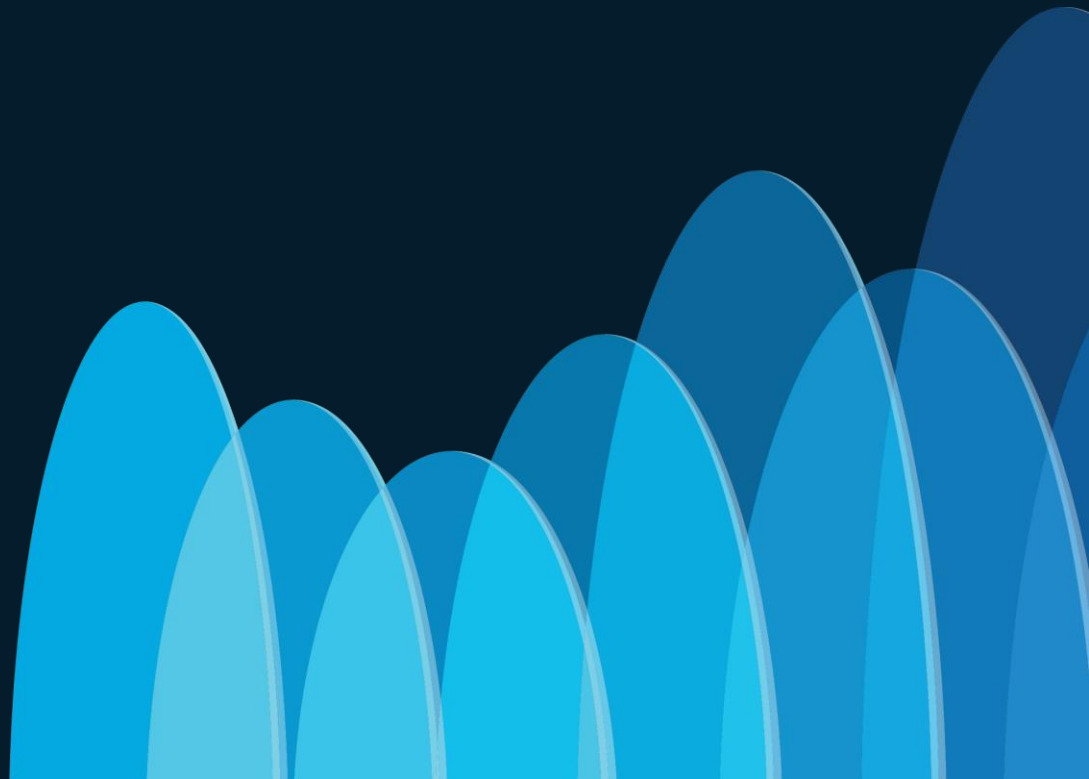
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cats love Starlink

New Flat Array!

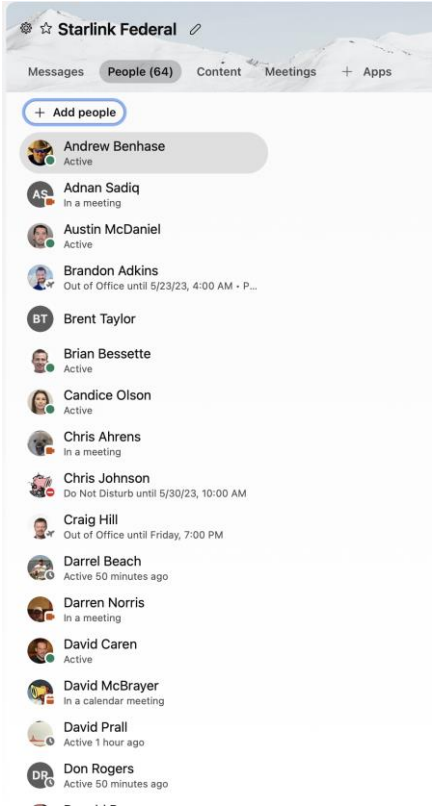
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

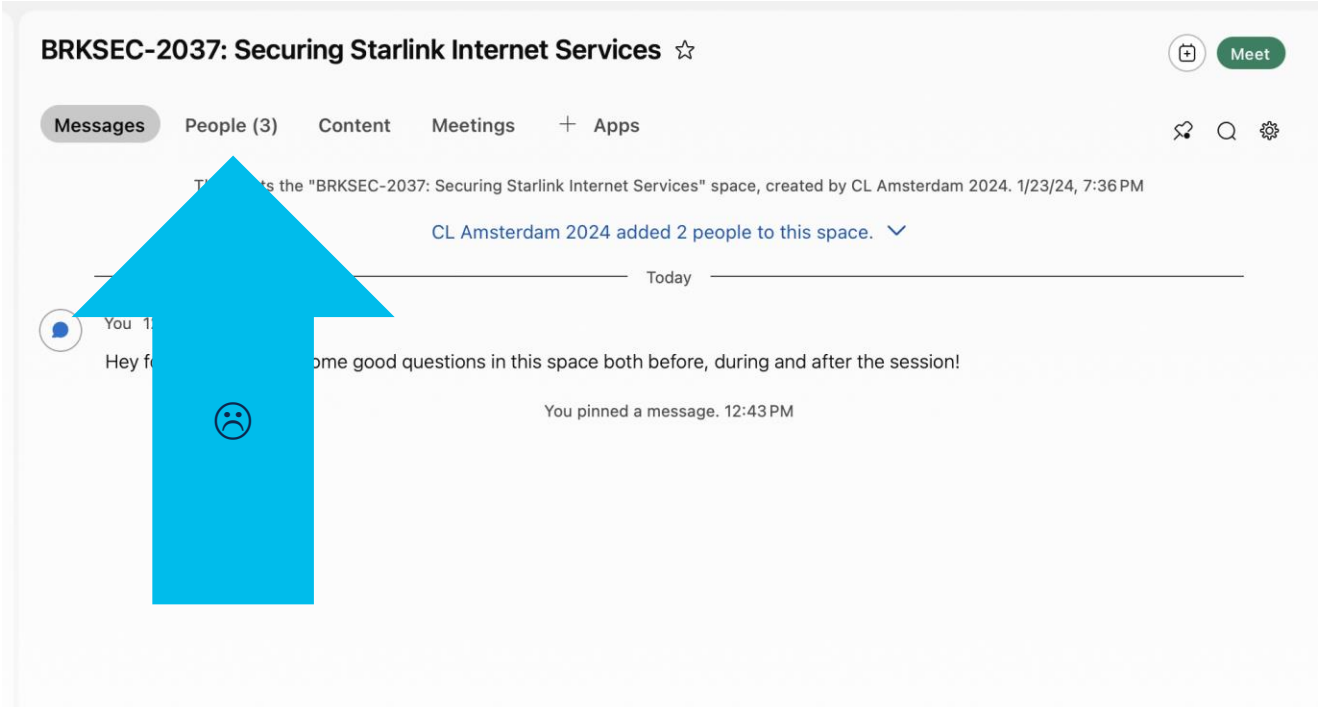
How do you keep up?



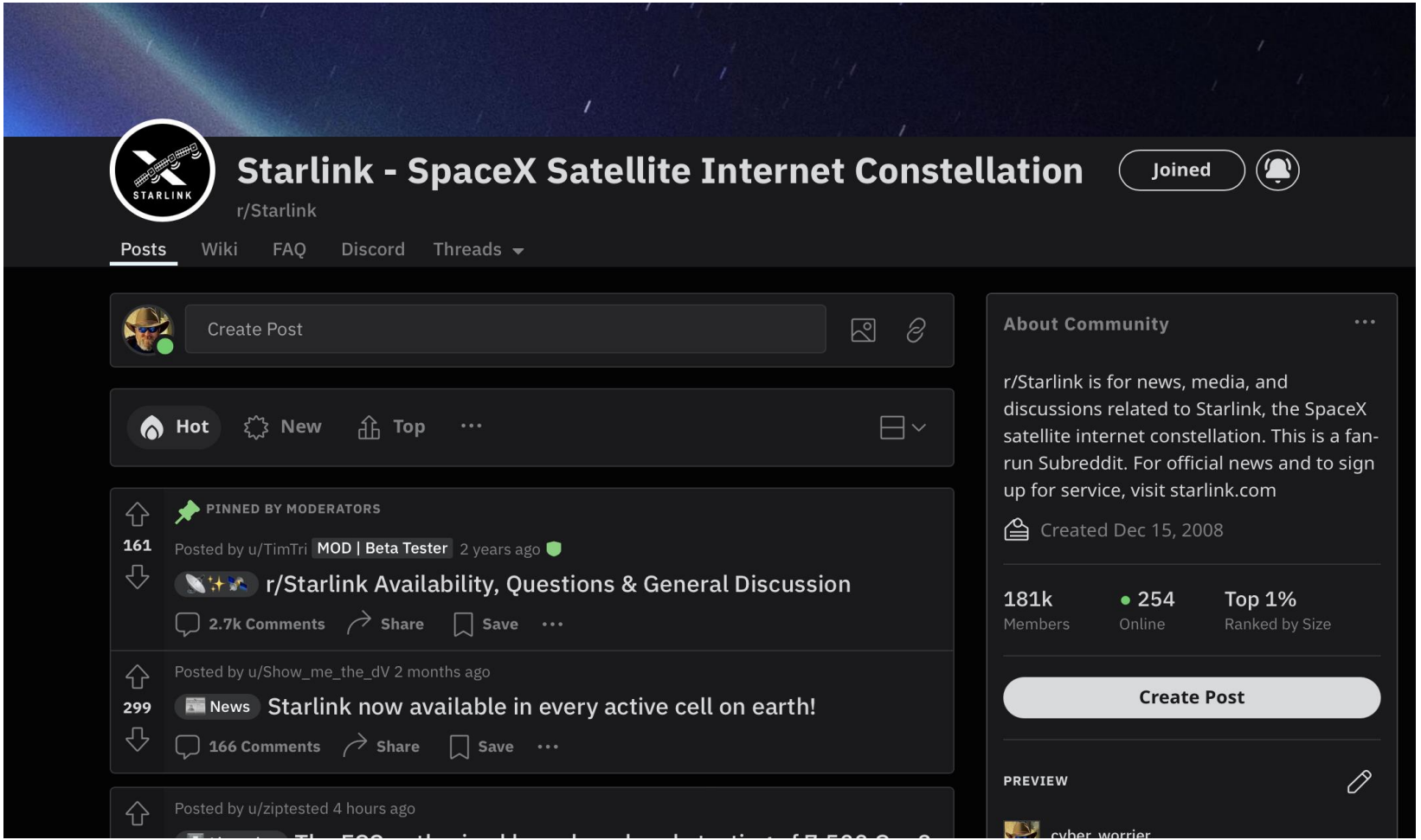
cisco Live!

Starlink Internal Rooms (SL-OSINT)



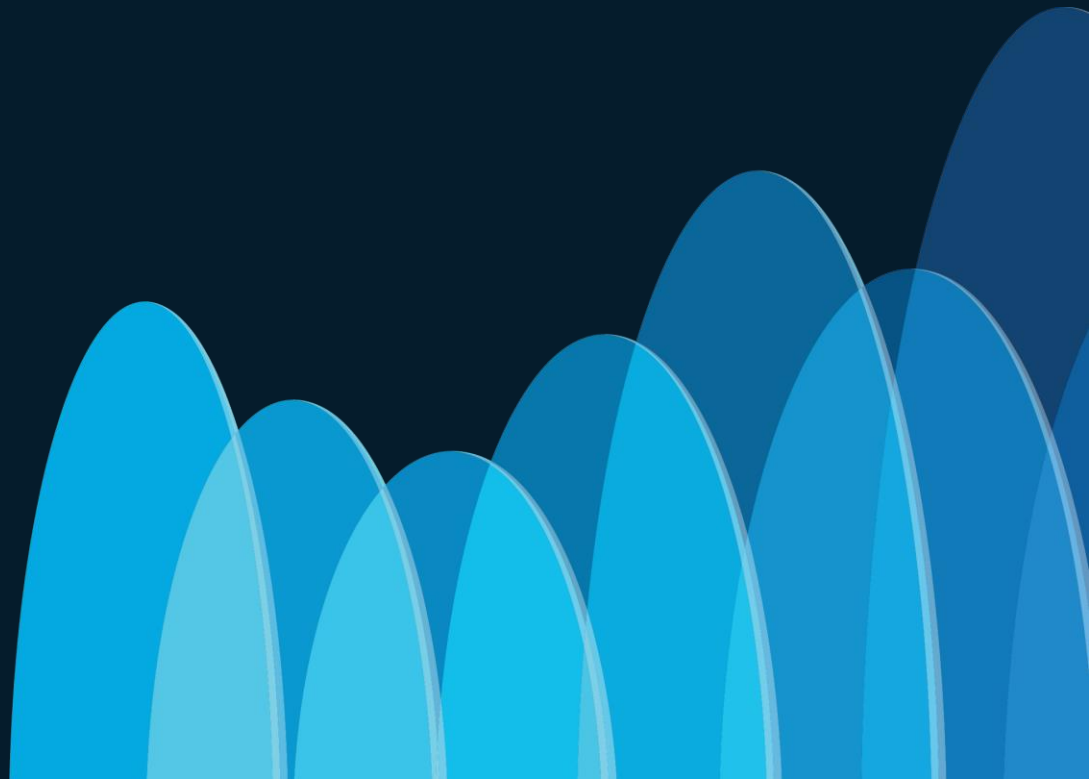


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

What's happening with Kuiper?



cisco Live!

First Kuiper Launch

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

KUIPER Updated Launch Schedule

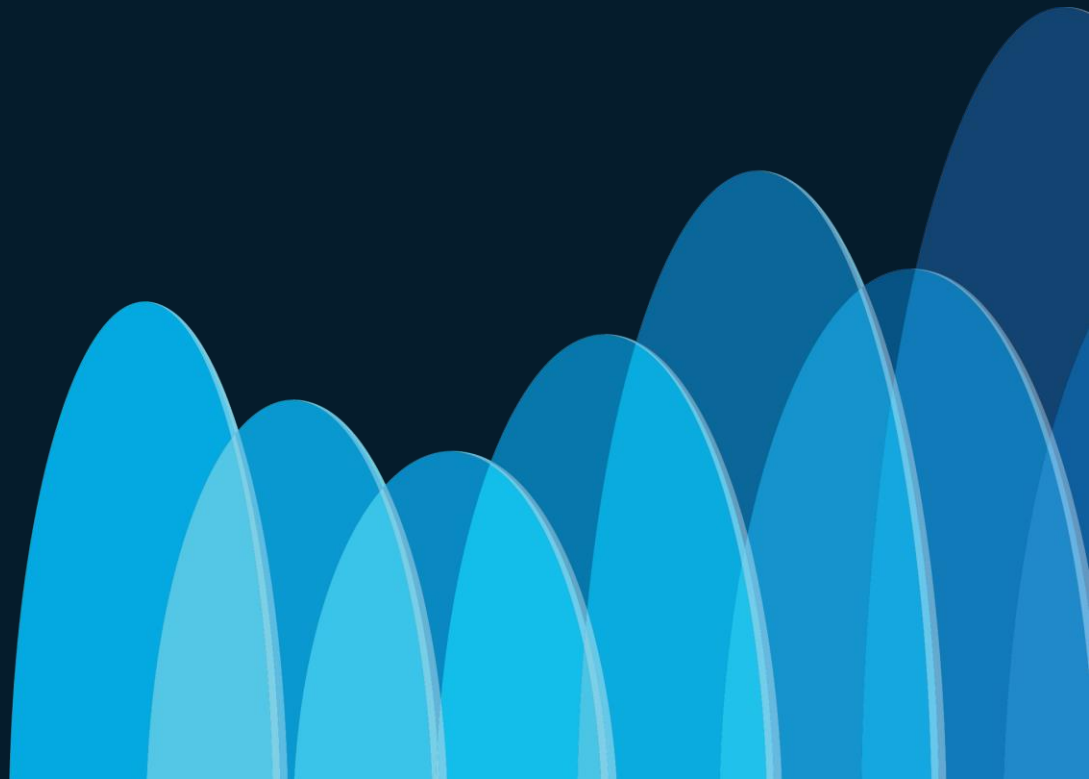
"We will continue to increase our rates of satellite production and deployment heading into 2025, and we remain on track to begin offering service to customers next year," Amazon said in a June 27 blog post.

Amazon faces an FCC deadline to have half of the 3,232-satellite constellation launched by July 2026.

Think lots of 2025 launches!

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Whats happening with OneWeb?



cisco Live!

OneWeb- catering towards Enterprise

- Polar Orbits
- Higher Orbit
- >600 satellites in orbit
- Broad Coverage over Australia
- Focused towards Enterprise Networking

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Compare Oneweb Canada & US Satellite Internet Plans

PLAN	MONTHLY ALLOWANCE	MIR DOWN / UP	CIR DOWN / UP	OW50SL & KYMETA	OW70L & OW130L
BROADBAND 100	100 GB	100 / 20 MBPS		US$575.00	US$450.00
BROADBAND 250	250 GB	100 / 20 MBPS		US$975.00	US$795.00
BROADBAND 500	500 GB	100 / 20 MBPS		US$1965.00	US$1350.00
BROADB[illegible]D 1000	1000 GB	100 / 20 MBPS		US$2675.00	US$2175.00
[illegible]	UNLIMITED	10 / 2 MBPS	2.5 / 0.5 MBPS	US$1875.00	US$1495.00
ENTER[illegible]SE 1	UNLIMITED	50 / 10 MBPS	5 / 1 MBPS	US$3750.00	US$2995.00
ENTERPRISE 2	UNLIMITED	50 / 10 MBPS	10 / 2 MBPS	US$7500.00	US$5990.00
ENTERPRISE 3	UNLIMITED	100 / 20 MBPS	15 / 3 MBPS	US$11250.00	US$8985.00

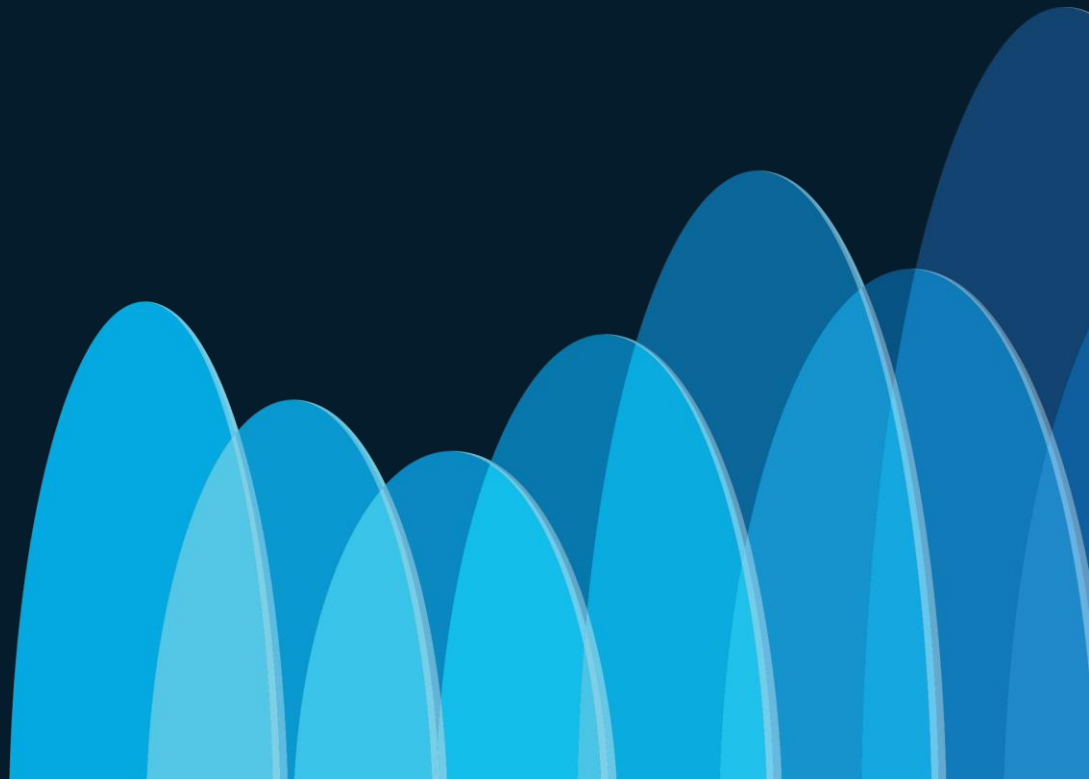
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Agenda

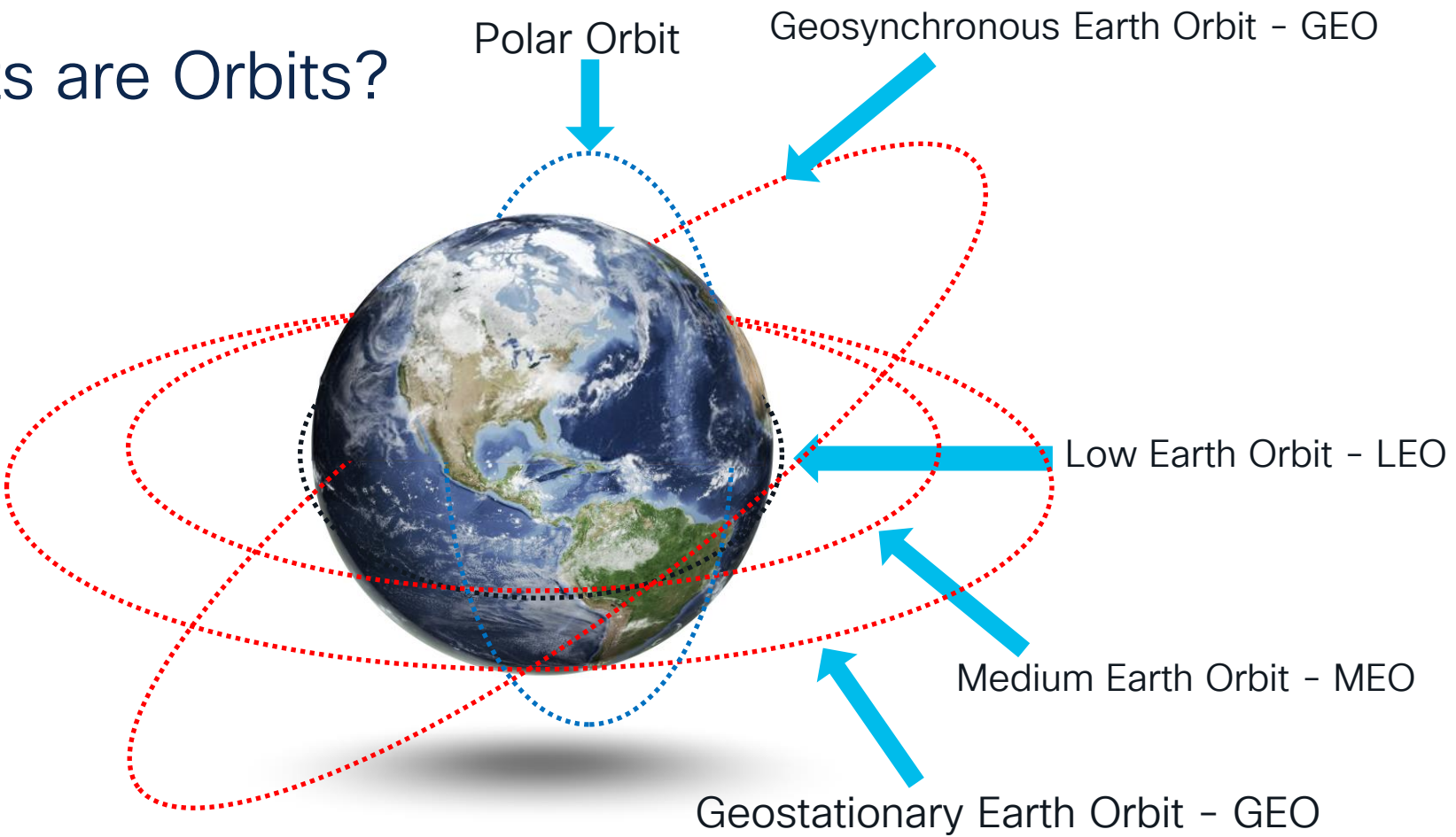
- Orbital Mechanics 101
- What is Starlink today?
- How does Cisco work with Starlink?
- Securing Starlink
- Things you need to know

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Orbits are orbits right?

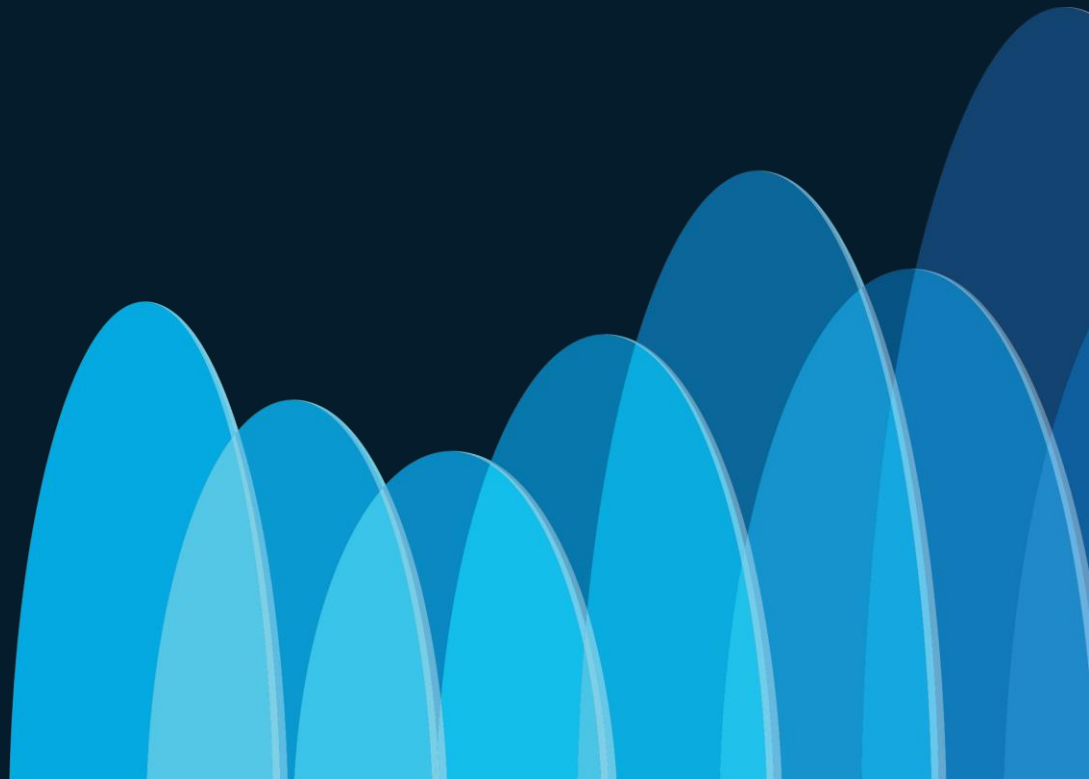


Orbits are Orbits?

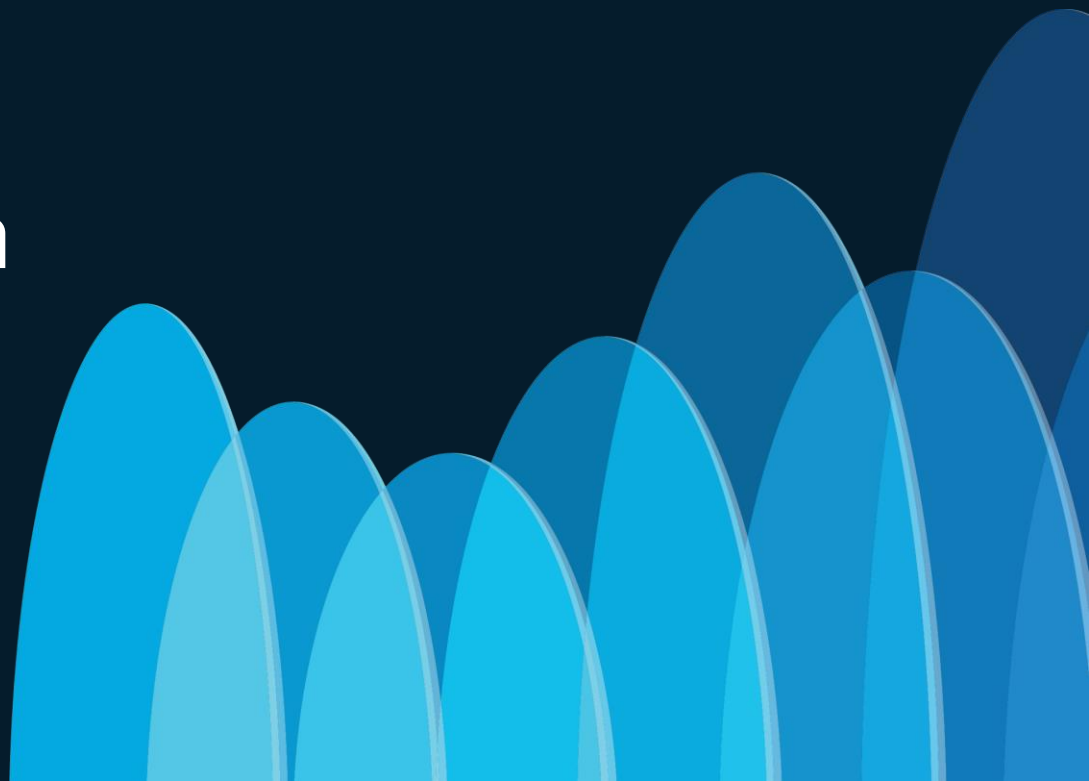


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

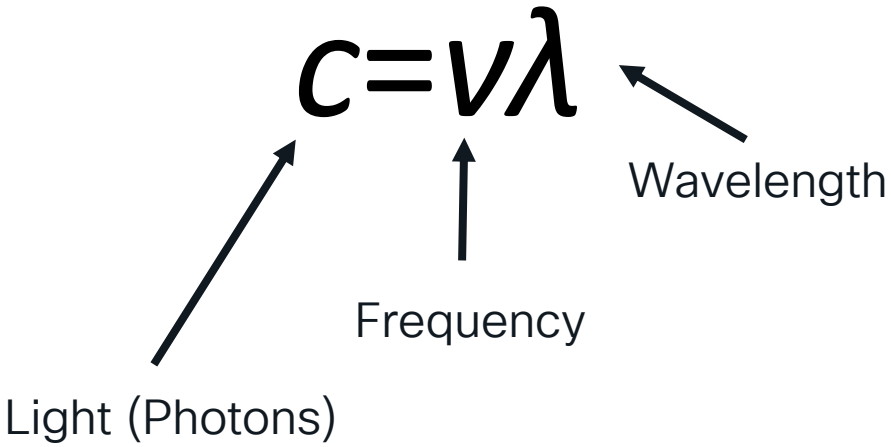
Hey Andrew, this is Cisco Live.... Why do I need to know about physics, orbits, altitudes and latency?



Answer:
Because this is an Engineering discussion, not a sales and marketing pitch ☺

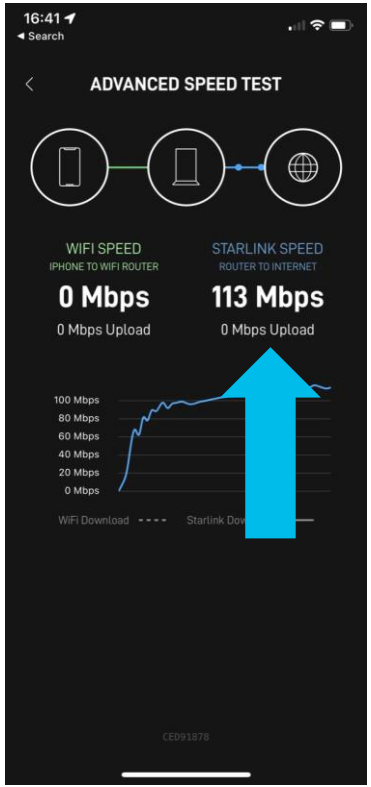


Speed of Light in a Vacuum



300,000 km/s

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public



Speed of Light in a Vacuum

Speed of Light in an Atmosphere

Loss Calculation

40ms Great

700ms Not-Great

Terrestrial Ground Delay

10-200ms

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Orbits and Networking

- LEO – 1000 kilometers and below
  - Starlink 540km (345 miles)
  - One way latency – ~12-25ms
  - RTT - ~25-50ms

Happy Network Zone

- MEO – 8000 kilometers (5,000 miles)
  - ~RTT 350ms

Sad Network Zone

- GEO – 36,000 kilometers (22,000 miles)
  - ~RTT 725ms

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Physics Matters

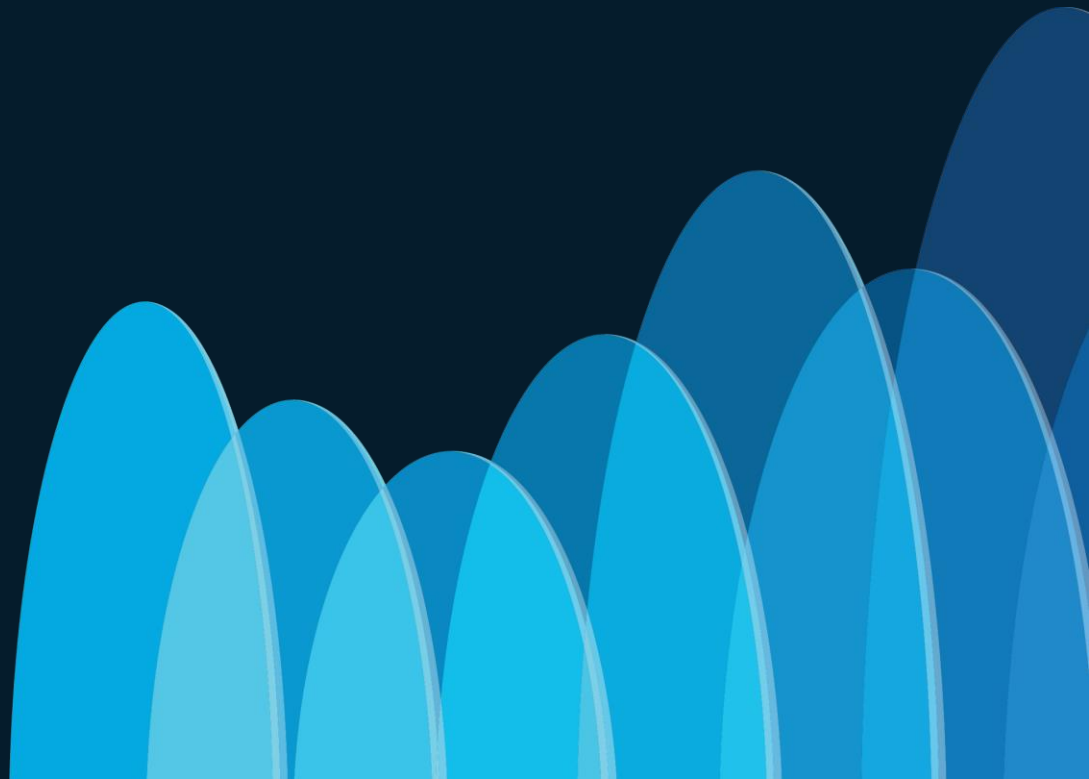
700ms

350ms

40ms

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

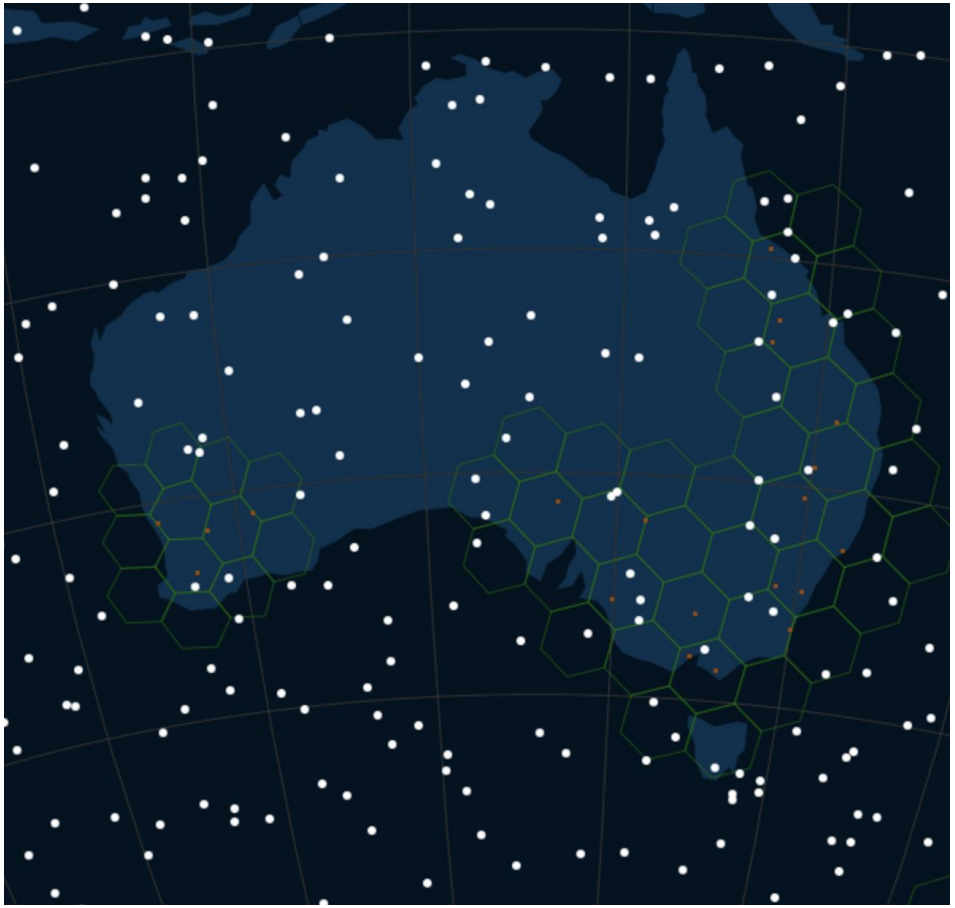
What really is Starlink?



cisco Live!

Starlink Australia

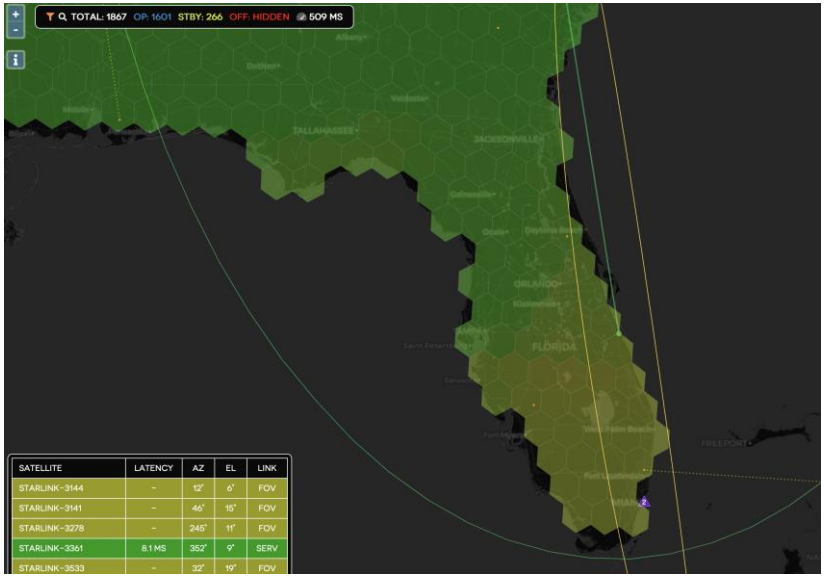
- Estimation of pathing using currently published ephemeris
- Broad coverage of urban areas
- Rural areas would be serviced by polar orbits
- Coverage in remote area may be inconsistent

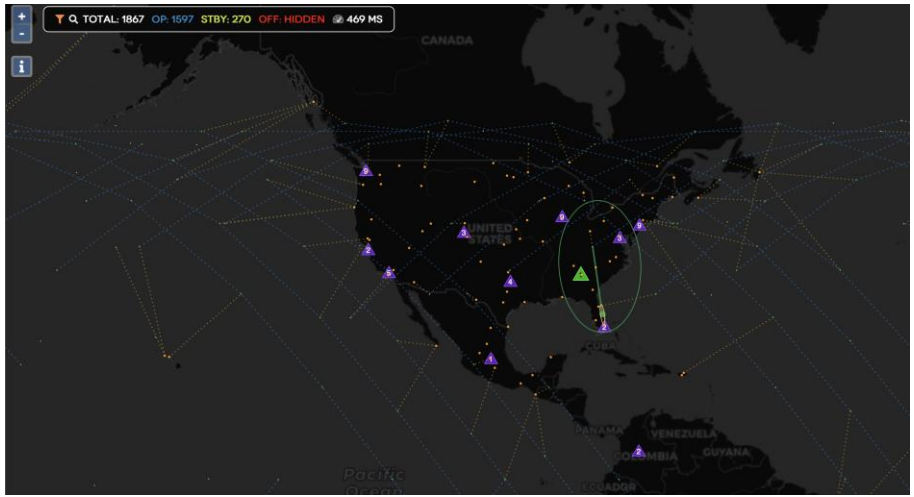


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

What is Starlink?

- A global satellite network in Low Earth Orbit currently consisting of ~3000 satellites*





*groups of 53 being launched on a regular basis

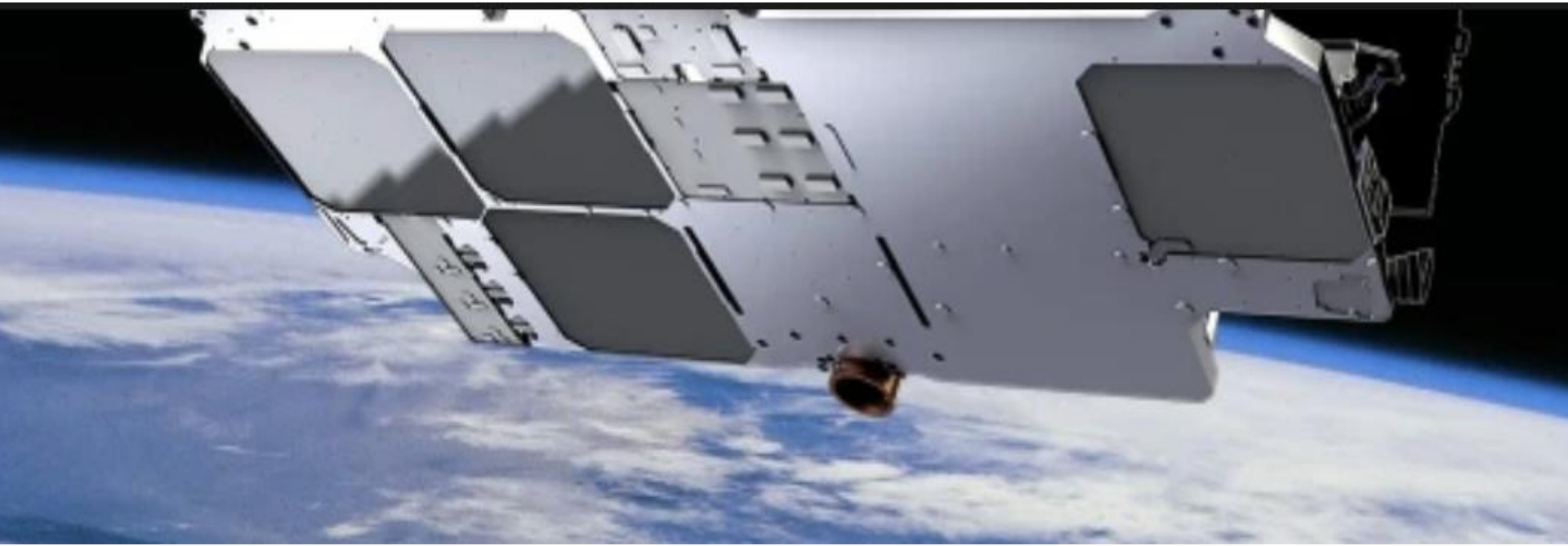
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Satellite v1.5

- Each satellite features four antennas in Ku band, one for uplink, three for downlink
- Each antenna is capable of projecting eight beams in two polarizations (RHCP/LHCP), for a total 48 downlink beams and 16 uplink beams.
- The maximum bandwidth available to Starlink in Ku band is 8x 250 MHz channels in downlink (total 2 GHz), and 8x 62.5 MHz channels in uplink (total 500 MHz)
- Each Satellite nominally operates at 10Gbps capacity with future expansion to 20Gbps

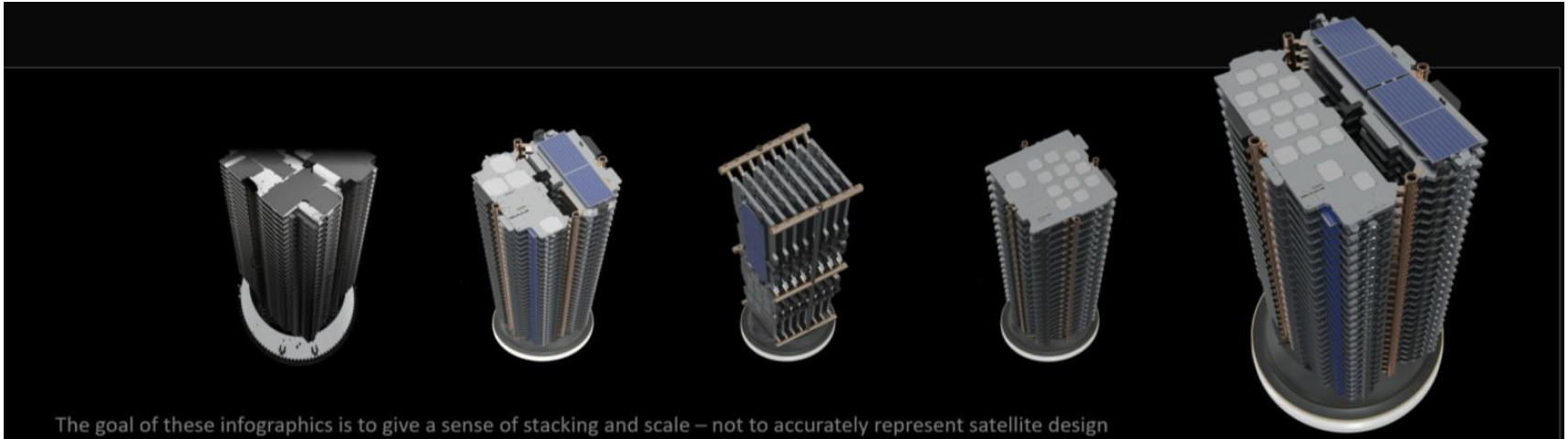
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Faced towards Ground



Credit: Starlink

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public



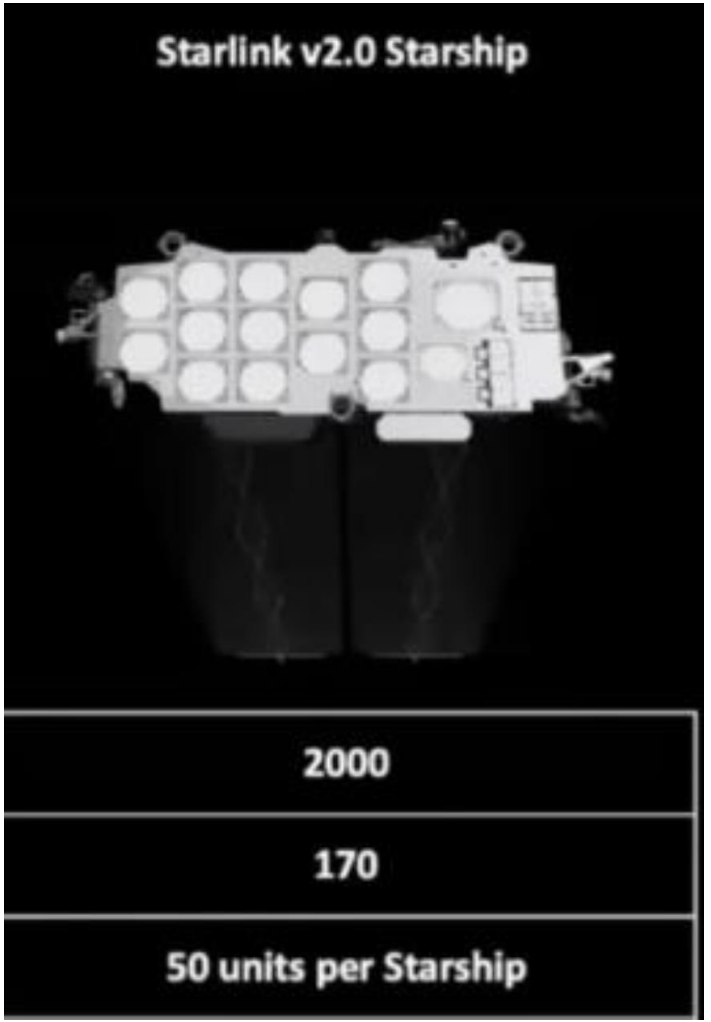
The goal of these infographics is to give a sense of stacking and scale – not to accurately represent satellite design

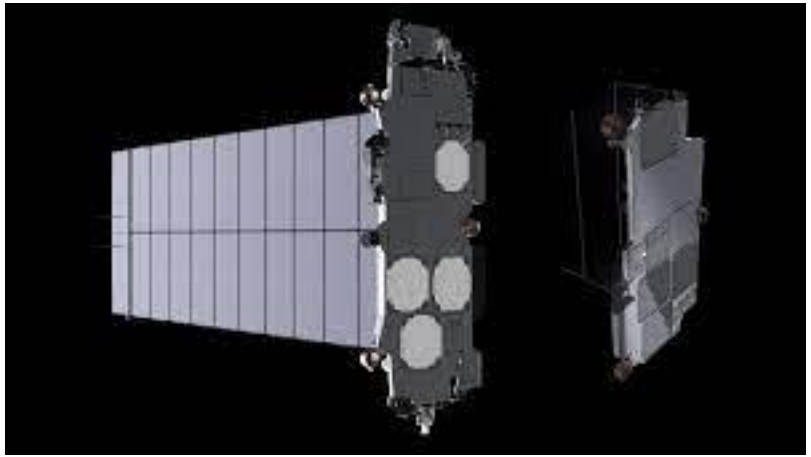
Assumptions

Designation	Starlink V1.5	Starlink V2 F9-1	Starlink V2 F9-2	Starlink V2 mini	Starlink V2 Starship
Status	Launched	FCC filing – may not realize	FCC filing – may not realize	Launched	FCC filing
Mass kg	306	303	800	800	2000
Gbps / sat	15	18	70	60	170
Launch	60 units per Falcon 9	60 units per Falcon 9	16 units per Falcon 9	21 units per Falcon 9	50 units per Starship
Tbps / launch	0.9	1.1	1.1	1.3	8.5
m$ / launch	Sats 18 + launch 30 = 48m$	Sats 18 + launch 30 = 48m$	Sats 11 + launch 30 = 41m$	Sats 15 + launch 30 = 45m$	Sats 60 + launch 15 = 75m$
$ / Mbps	53	45	37	35	9

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

V2.0 Satellite





V1.5 Satellite

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Gen 1.5 in Low Earth Orbit

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Observations of the Starlink Network

- CGNAT Employed
- Array to Satellite to Ground Station are all Flat
- Appears that Ground to NAP is a series of Exit MPLS Networks
- Exit Routing is based on your specific Terminal
- *Network Configuration changes are frequent and unannounced

- Exit Path is currently static based on your Service Class
- Portabililty, Marine, RV, Aviation means that you can be placed in different exit VPNs, we assume dynamically

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Infrared “Space Lasers”

- 3 Beam Optical Head using Infrared Laser
- Same Orbital Plane Operation
- Theoretically could offload to parallel polar plane satellite

Credit: SpaceX/Starlink

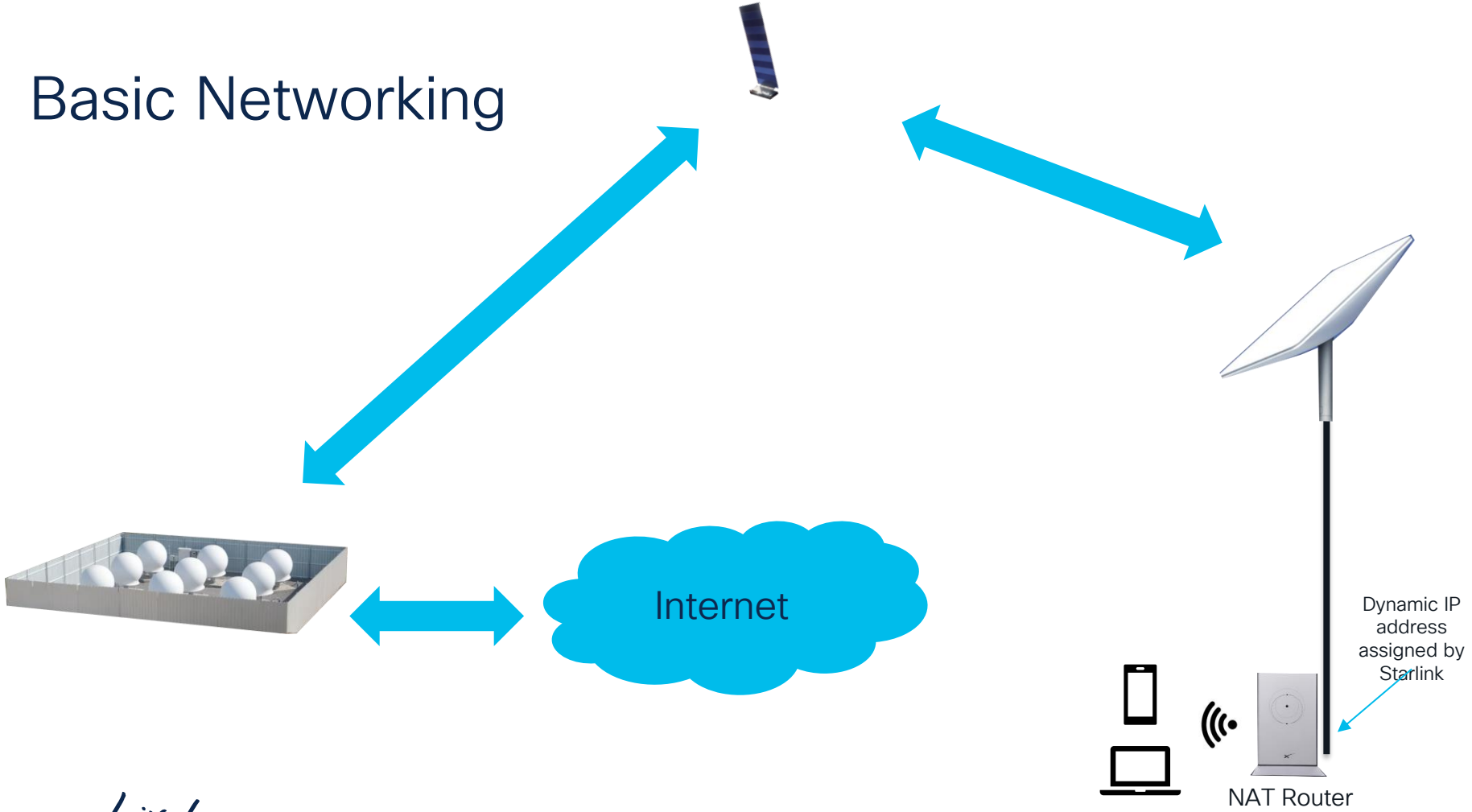
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Ground Station

- Each gateway antenna has available a maximum of 4x 500 MHz channels (total 2 GHz) in uplink, and 5x 250 MHz channels (total 1.25 GHz) in downlink
- In this configuration – where 8 antennas are active – would be 10Ghz total active Down and 6Ghz Up per site
- Ground stations are positioned on top of existing Fiber Paths
- Each Parabolic Antenna can support 10Gbps x 2)
- So that's up to 1.6Tbps theoretical bandwidth for a site with 8 active

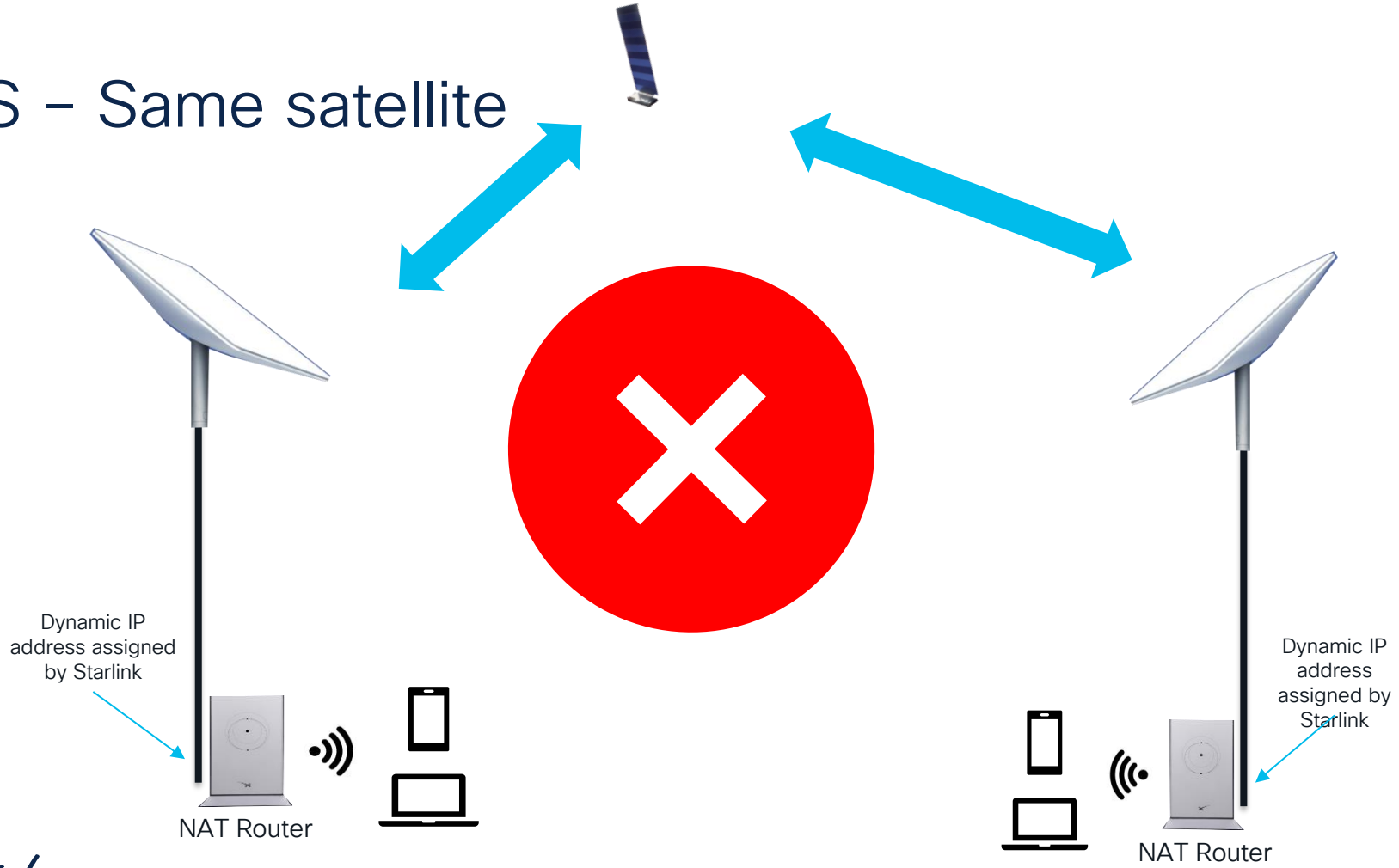
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Basic Networking



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

BLOS – Same satellite



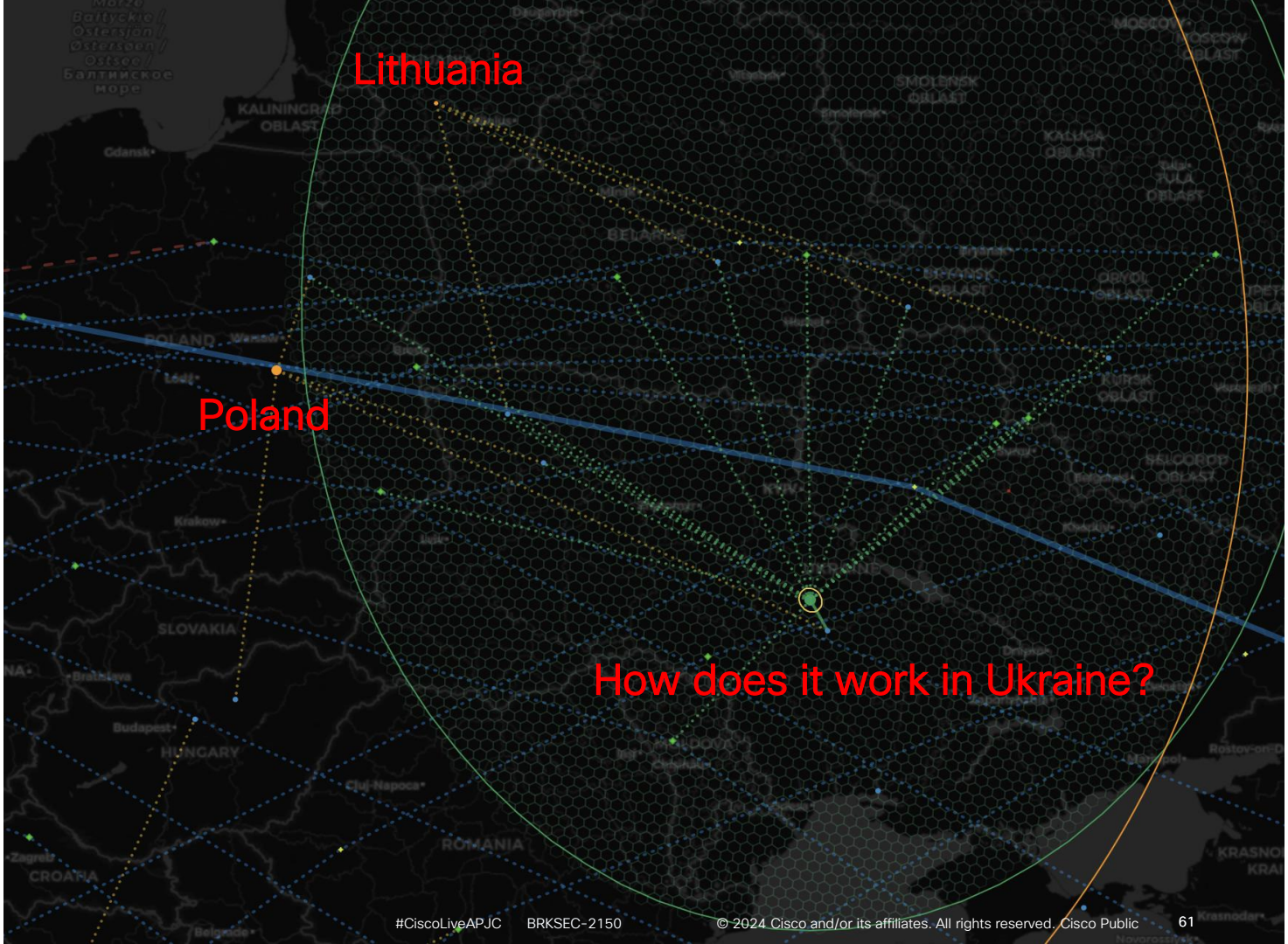
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Radio Gateways

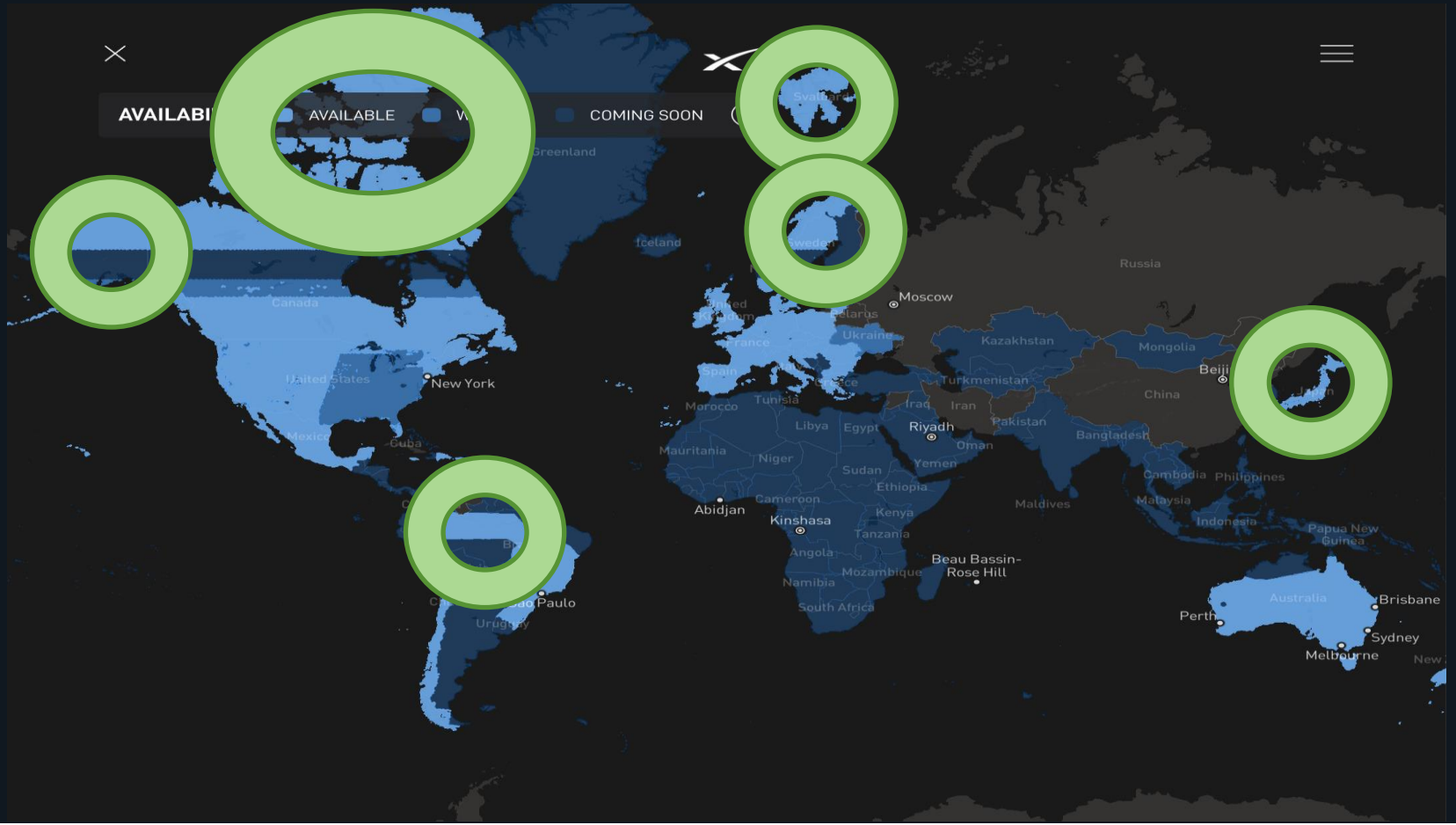
Lithuania
Poland

Internet Gateways

Frankfurt
London



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

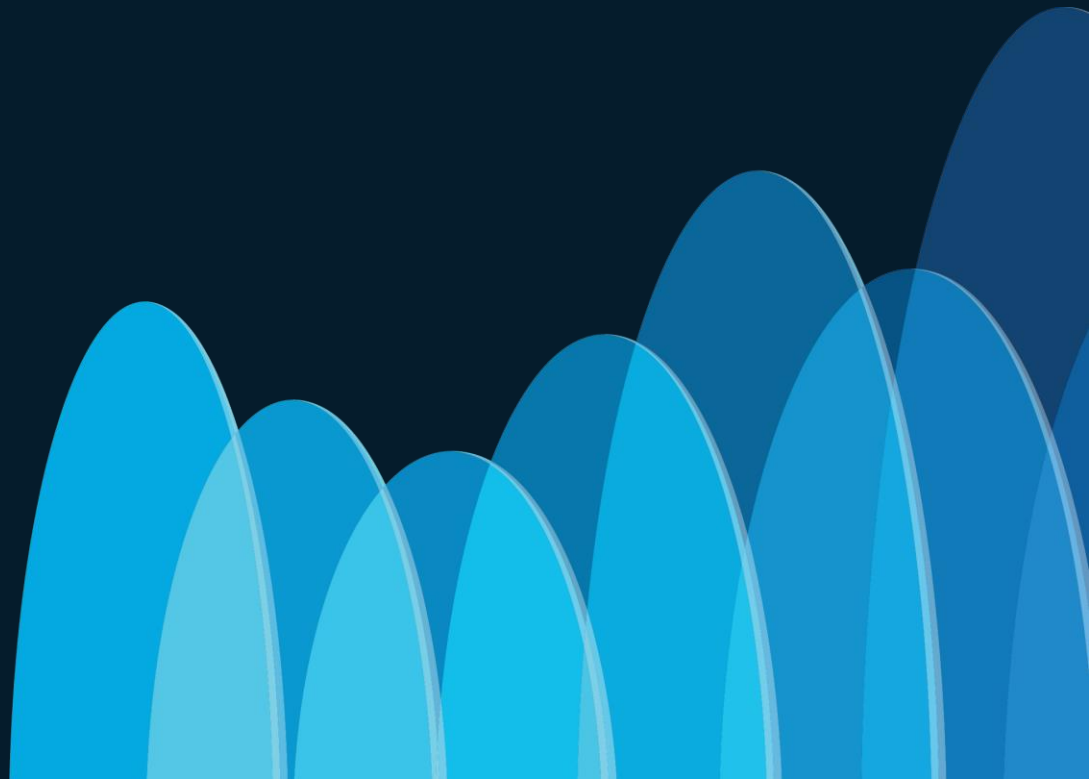
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Things we know

- Dense Orbital shells are extremely robust
- Frequency shifts can be simple software operations
- Receive only satellite arrays are critically important
- Low observability packages are important
- Low cost Software Defined Radios (SDRs) are being used for offensive hunt operations

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

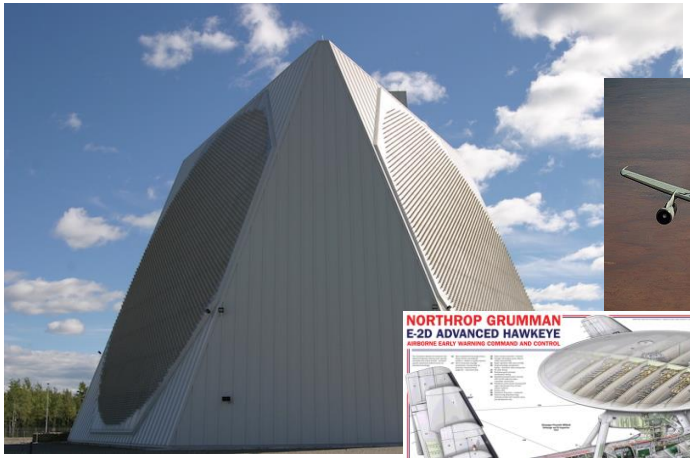
Phased Array Antenna



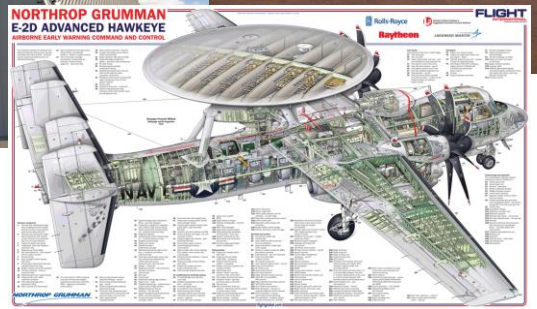
cisco Live!

Examples of Phased Arrays

- Space Observation Radar



E-3 Sentry
AWACS



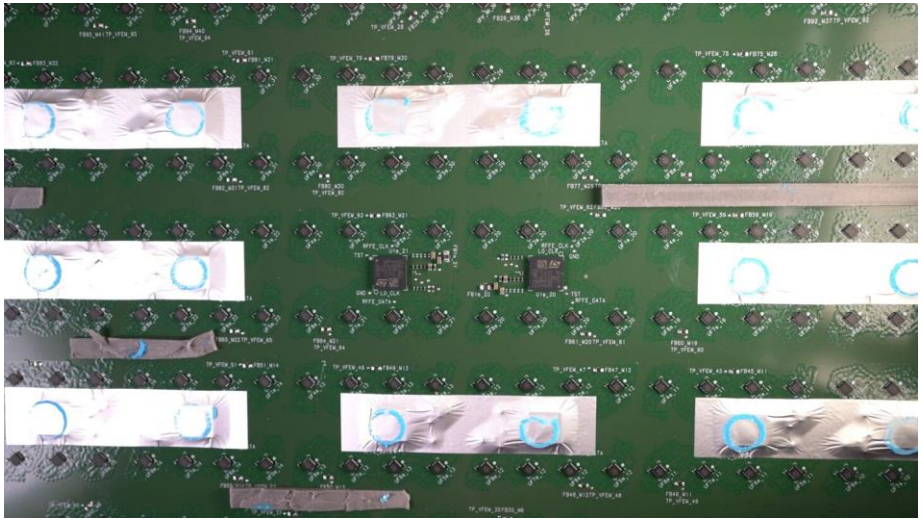
E-2D
Early Warning

- AN-SPY-1 Phased Array
- AEGIS Deployed and Ashore

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

How does Starlink work?

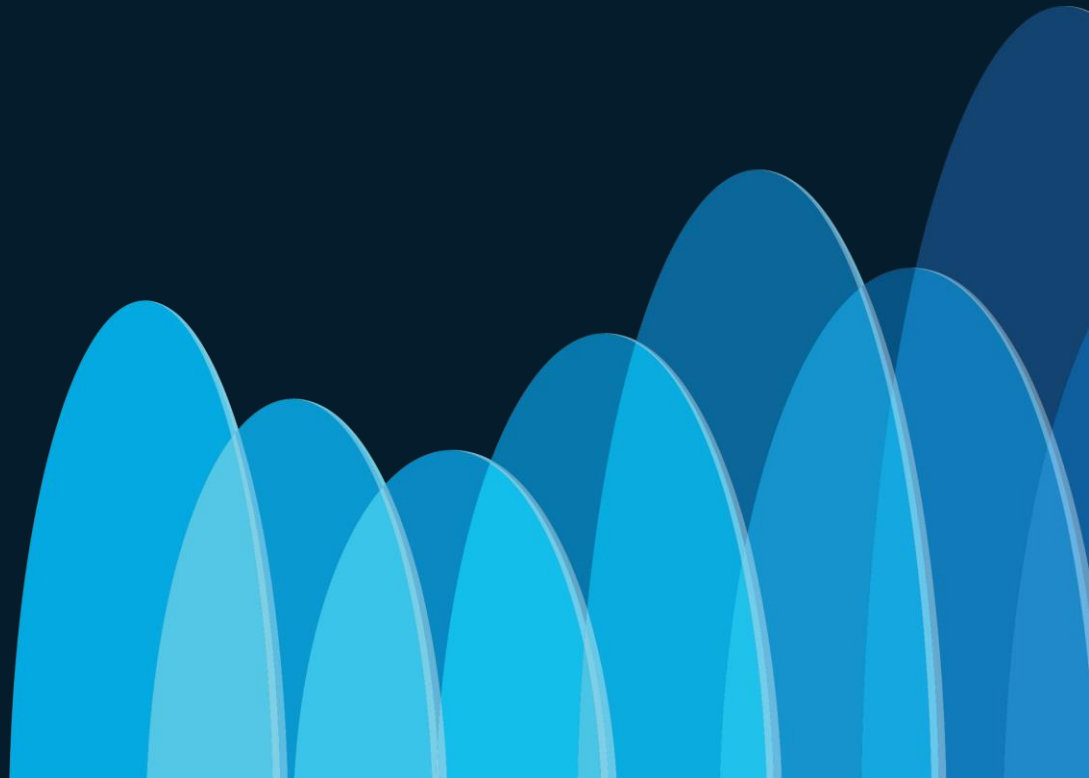
- Up / Down configuration
- Ground Terminal is a phased array antenna in one of two current configurations – Round (Gen1) or Rectangle (Gen2)
- Each array has hundreds of transceivers



- 12-18 and 26.5-49 GHz bands

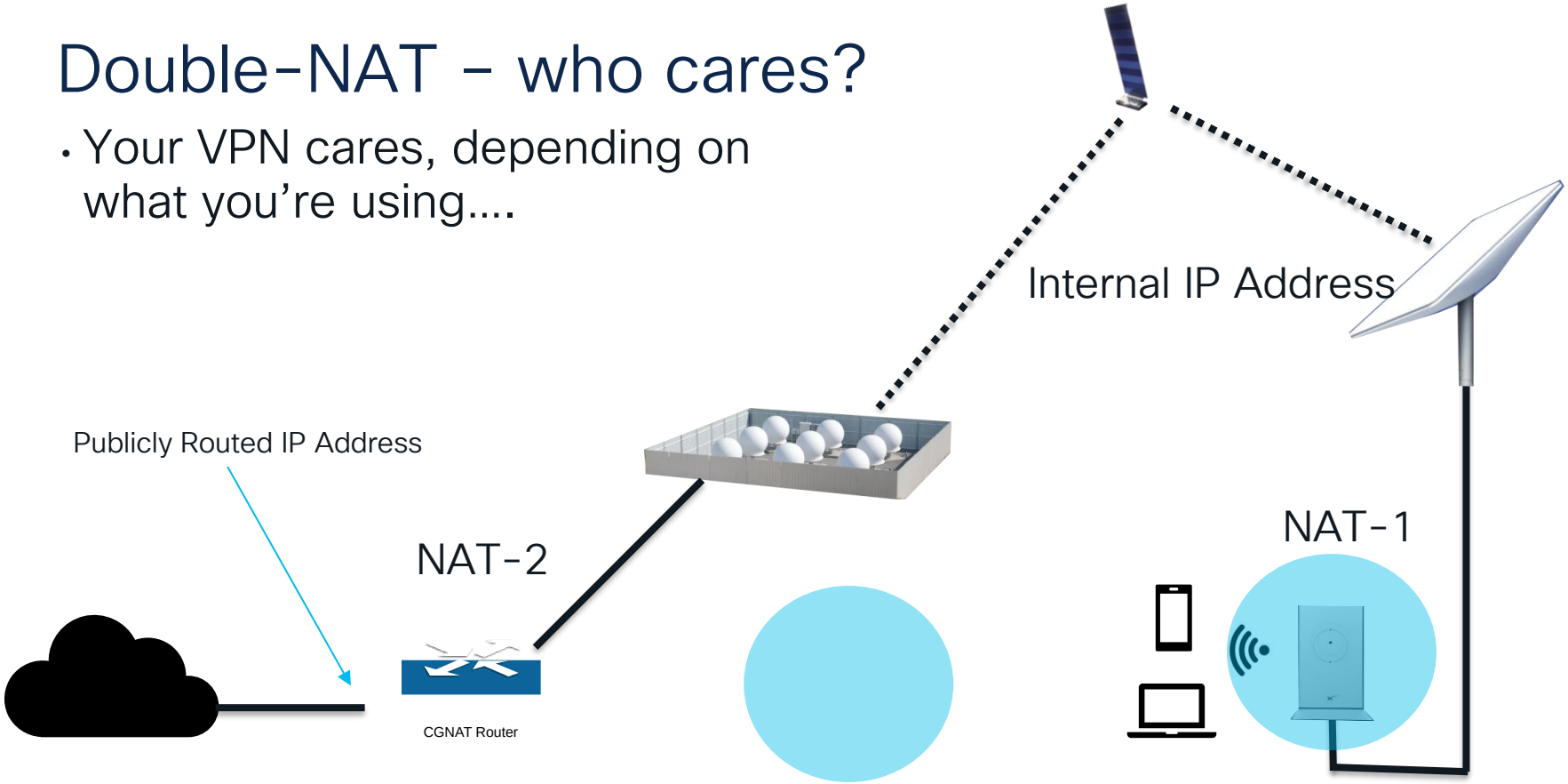
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Double/Triple NAT



Double-NAT – who cares?

- Your VPN cares, depending on what you're using....



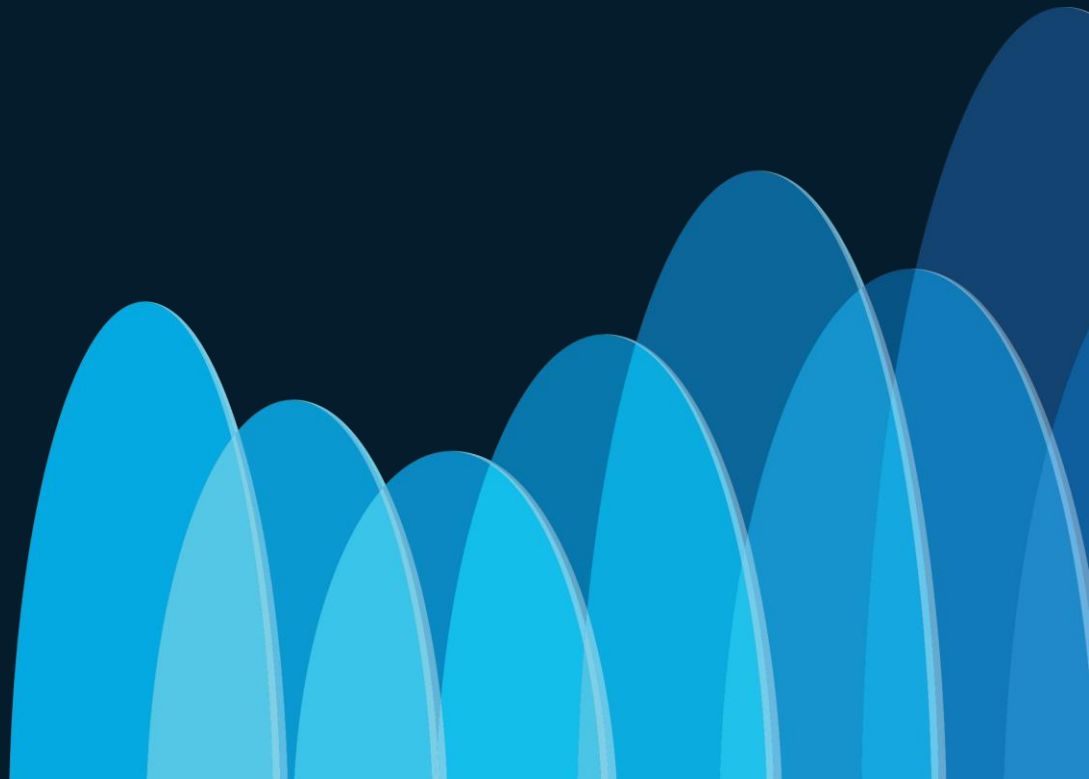
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Things that Fix NAT Problems

- Static NAT configuration – impossible with Starlink and CG-NAT carriers
- GRE/IPSec+NAT-T Tunnels
- Straight NAT-T Tunnels
- IPv6**** (maybe)
- TCP VPN Tunnels

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Polar Orbits and “Space Lasers”



cisco Live!

Satellite Truths and Myths

- All Starlink Satellites have “Lasers” – FALSE
- All Starlink Satellites can cross communicate to each other – FALSE
- Some Starlink Satellites have laser based optics that can point ahead of them to the next satellite – TRUE
- On-orbit Satellites can calculate multi-planar ephemeris to dynamically communicate to satellites in different orbits – FALSE

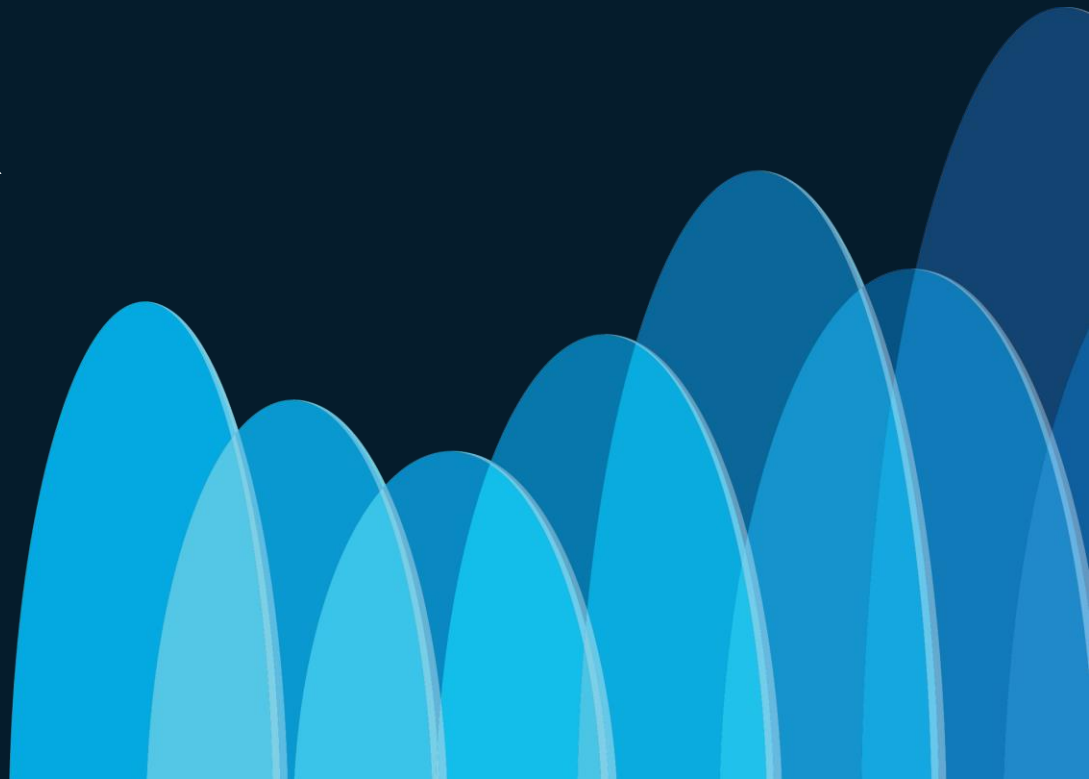
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Polar Orbit Satellites and Free Space Optics

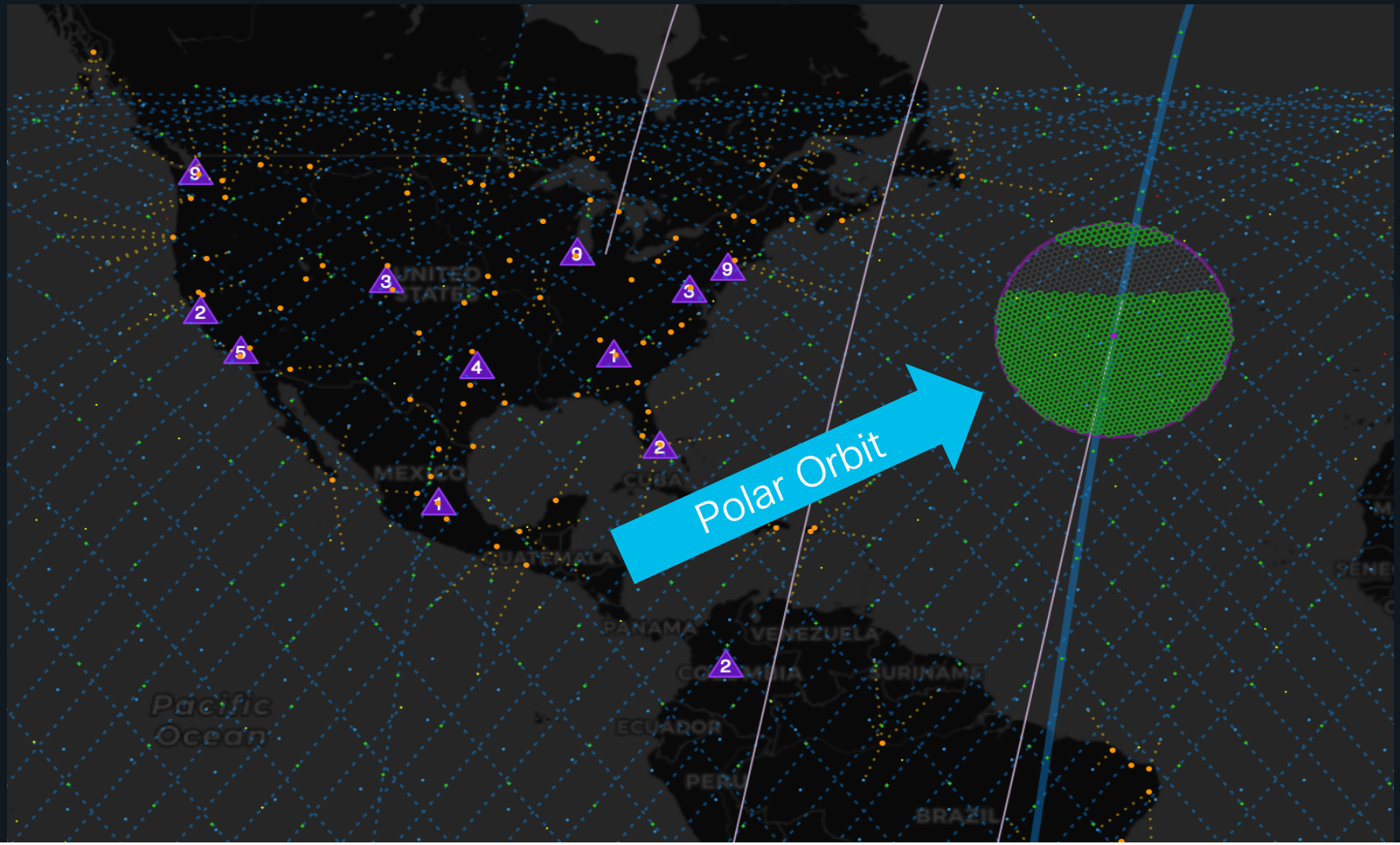
- Generation 1 Satellites are Radio Only
- Generation 1.5 and 2.0 Satellites are capable of Inter-Satellite Links (ISL)
- ISL Links work currently in a follow-me configuration
- A polar string of satellites provide hop to hop communications in single file
- Closest Radio Gateway provides the downlink for the chain of satellites
- Only use for satellites in polar orbits and where there is a Gateway connection
- You may not pop-out onto the Internet in a country that you expect
- You may not come out in a country you want

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

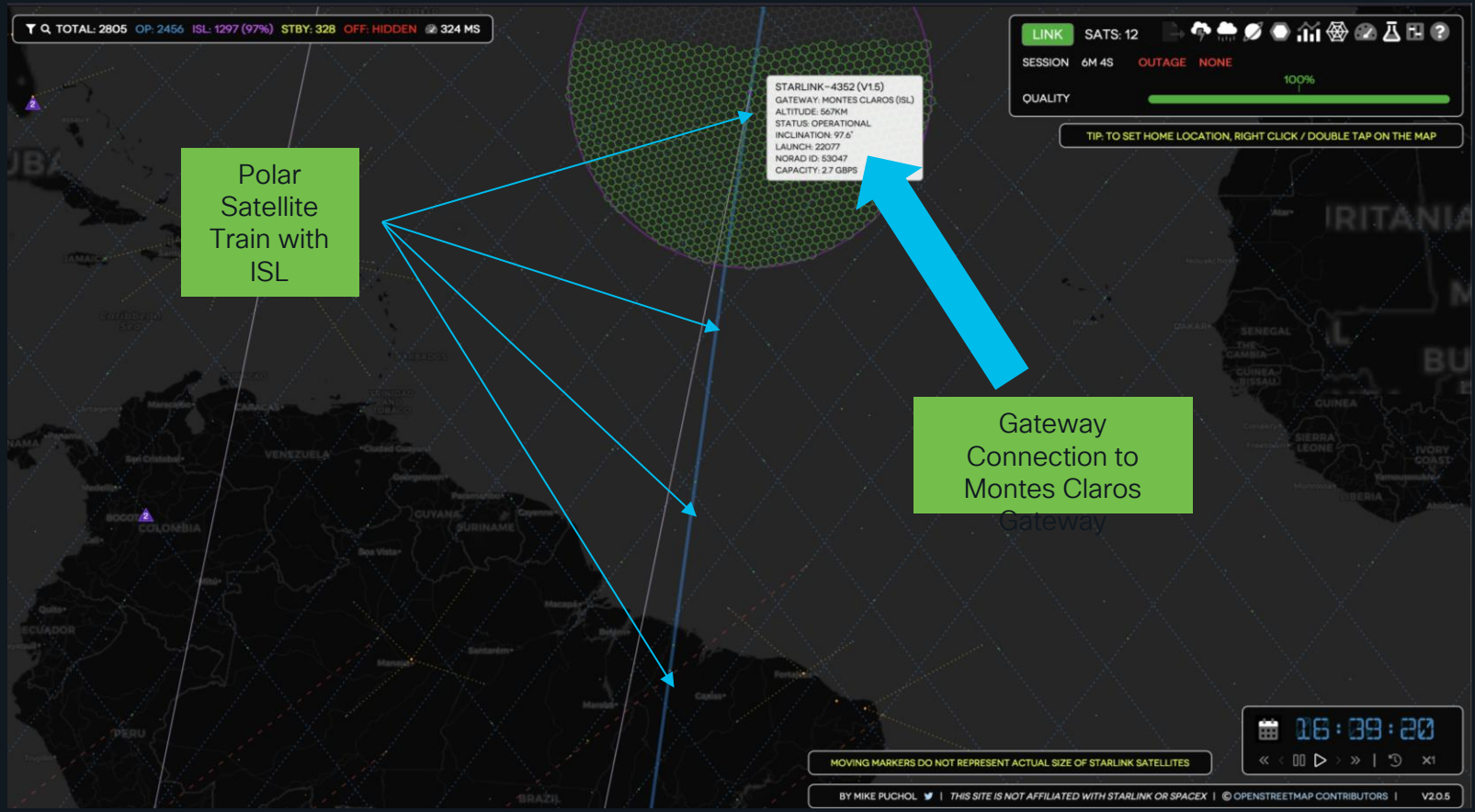
Space Lasers fix my networking issues



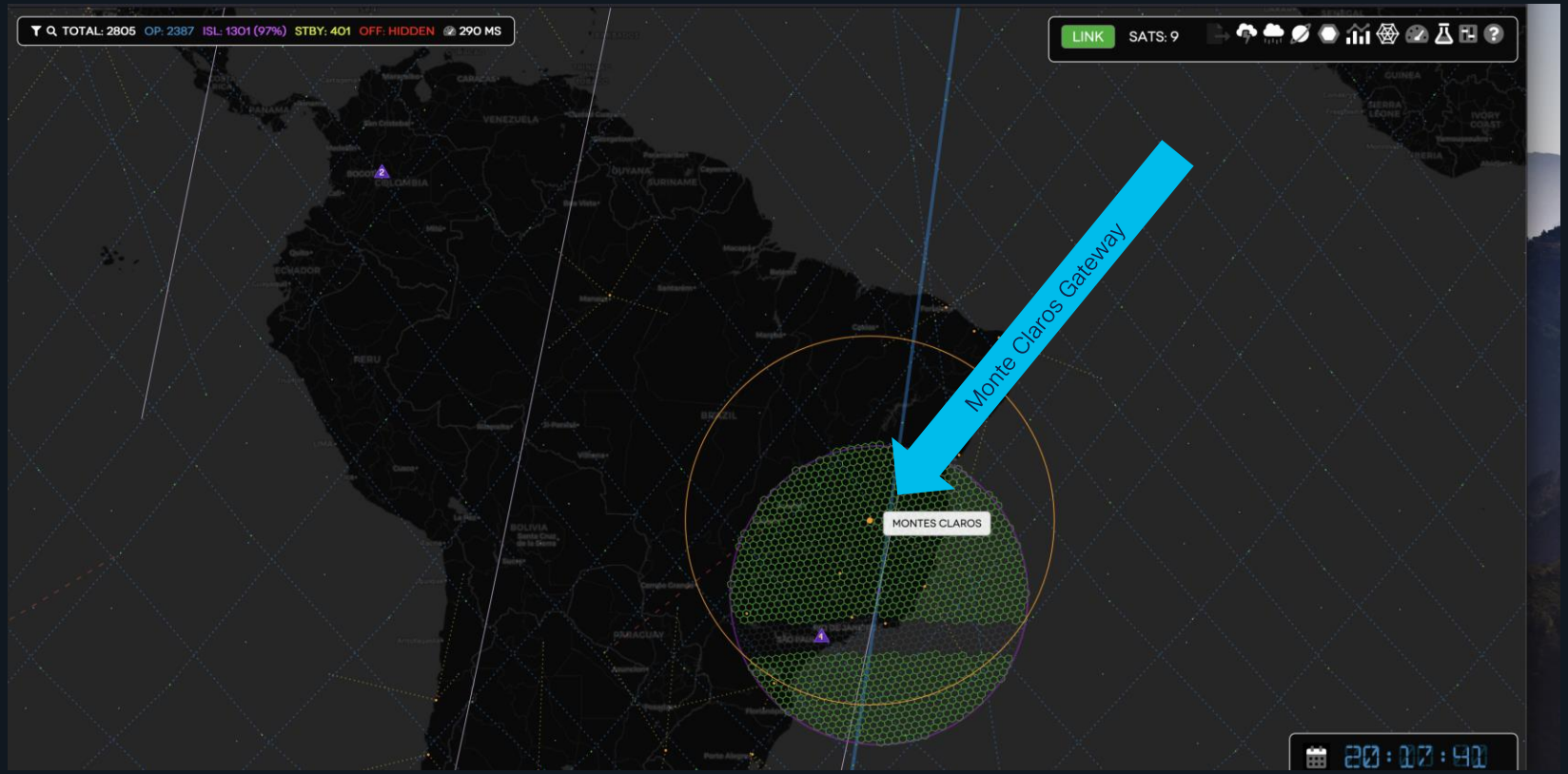
cisco Live!



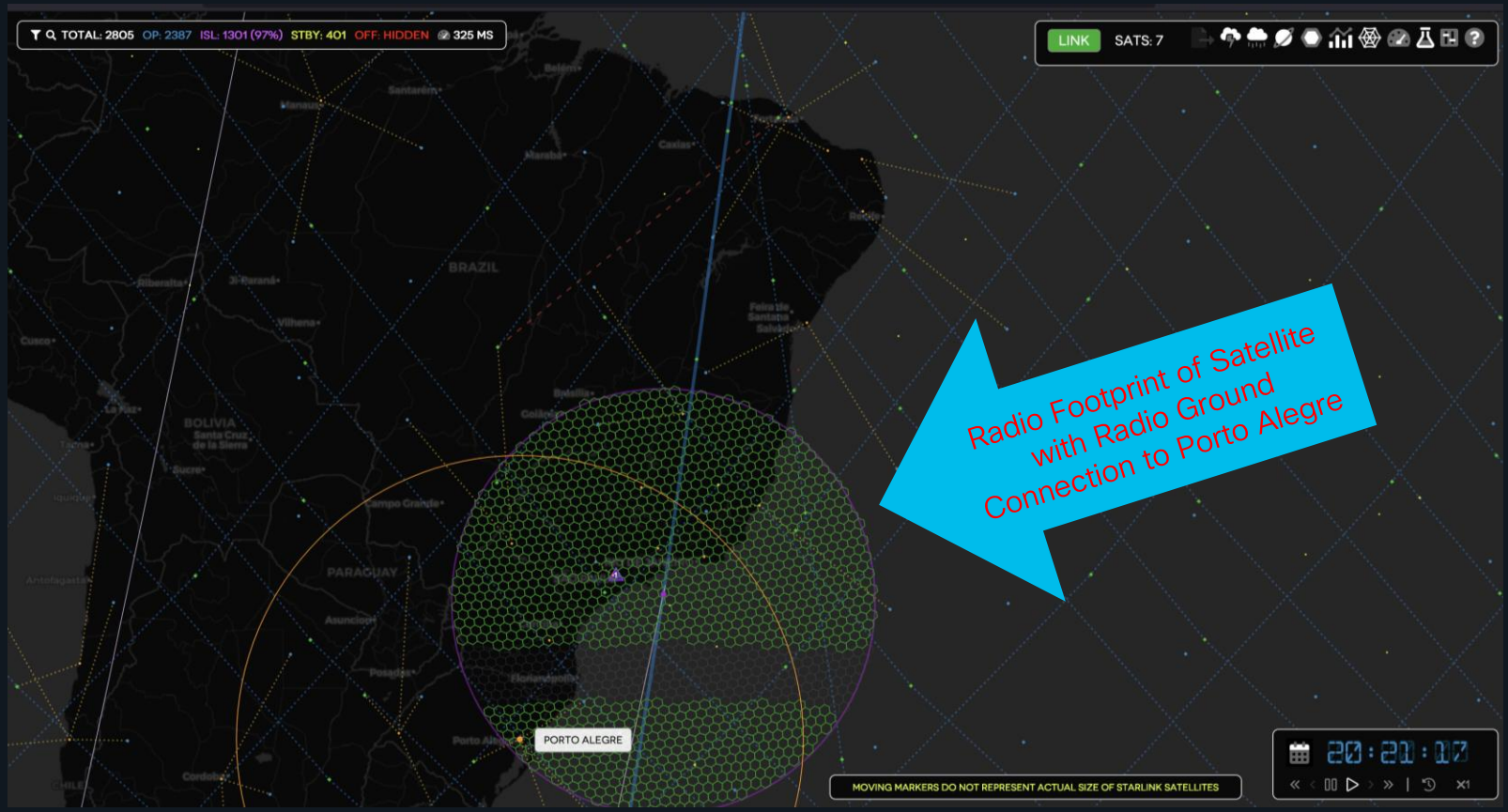
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public



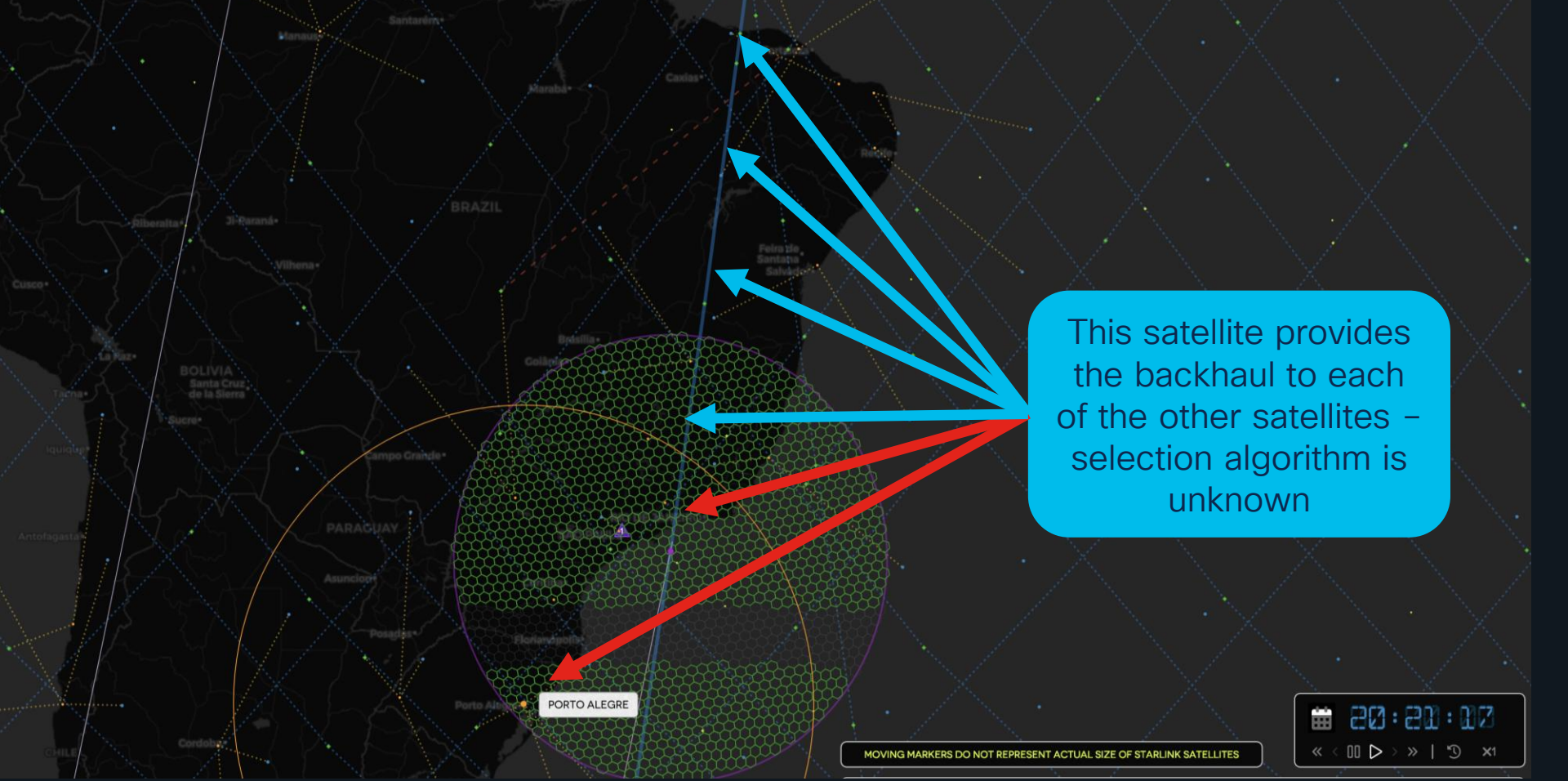
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

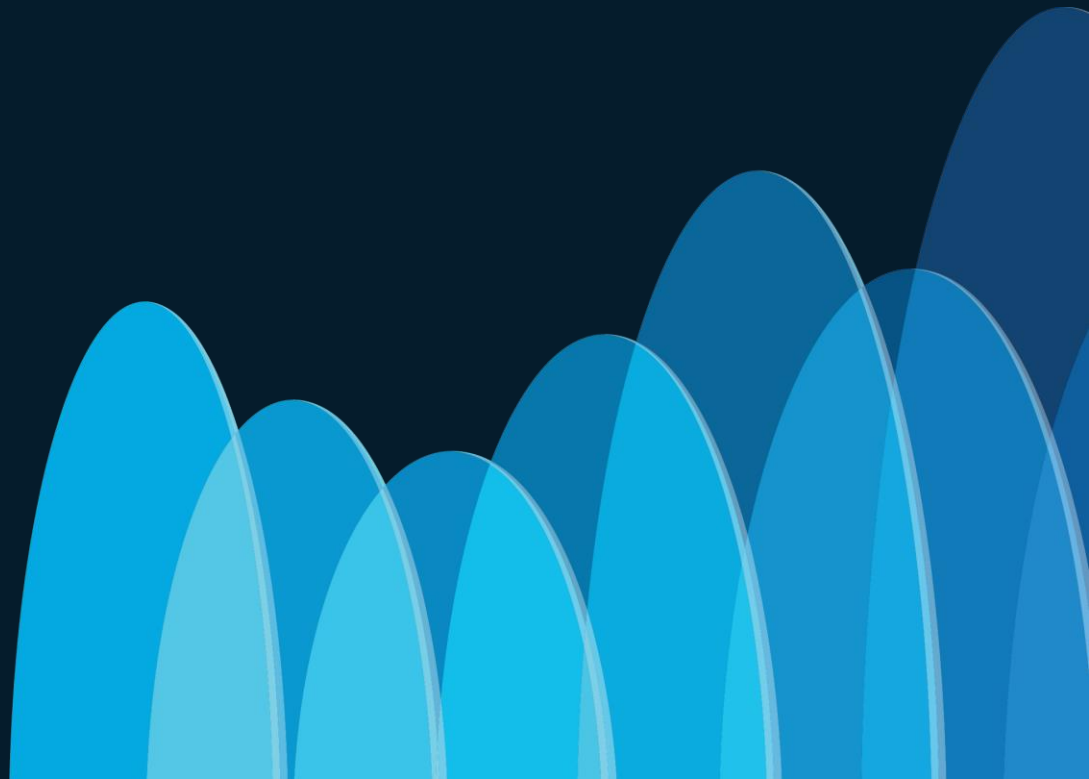


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Enterprise Customer Service Assumptions



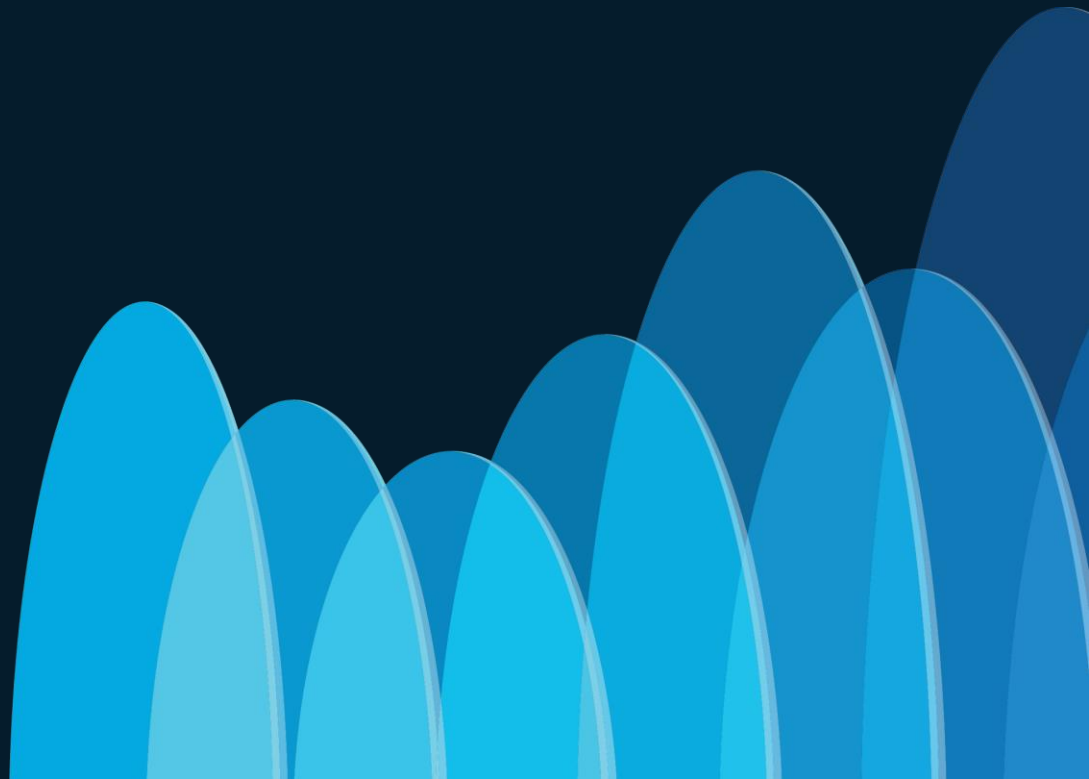
cisco Live!

Setting Expectations

- You like Customer Service
- You want a phone number to call
- You like an email address for your SE
- You have normal Enterprise customer networking and security requirements
- You want security transparency over WAN operations
- You want to be able to control your path to the Internet

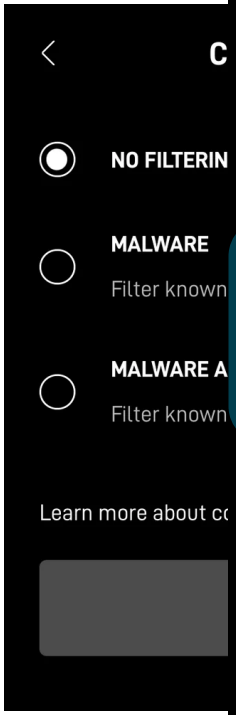
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Starlink Security



cisco Live!

Sum Total of available



Content Filtering

Content Filtering allows you to block access to certain types of websites on your Starlink network. This feature is accessed through the Settings screen in the Router tab of the Starlink App. It offers three filtering options:

- **No Filtering:** All websites are accessible.
- **Malware:** Blocks websites that may contain malware.
- **Malware and Adult Content:** Blocks both malware and adult content websites.

How does it work?

Headless Cloudflare

- Under the hood, the Content Filtering feature works by setting a custom DNS server provided by Cloudflare (Cloudflare for Families). When Content Filtering is enabled, your router uses one of Cloudflare's DNS servers to help prevent access to specific categories of websites.

Important considerations:

- **Best Effort:** This feature is a best effort solution to block certain types of websites. No filtering solution is perfect, and some sites may bypass these DNS filters.
- **Over-blocking:** In some cases, legitimate sites may be unintentionally blocked.
- **Limited Control:** Starlink uses Cloudflare's DNS filtering, and as a result, we cannot control the specific websites that are blocked.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

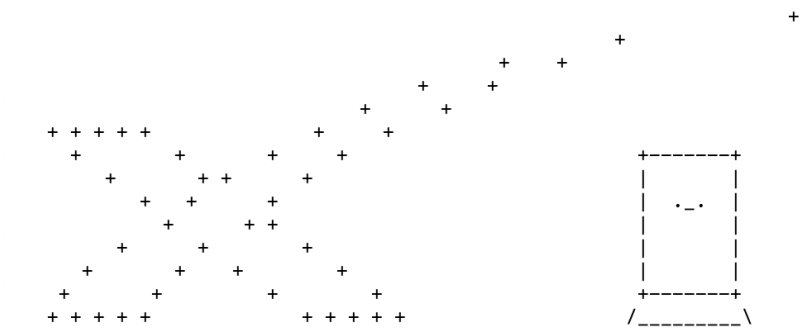
Starlink Security

BYOS – Bring Your Own Security

There is “very limited" security other than what you bring yourself

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Starlink Router



```
When I was a kid, I wanted to be a WiFi router more than anything in the world.
I stretched my arms out wide, and I hid in the corner. I tried to glue antennas
to my head, I had ethernet cables, I had an LED indicator. Everybody knew me
and was afraid of me. And one day, my dad said, "Bobby, you're 17. It's time to
throw childish things aside," and I said, "OK, Pop." But he didn't really say
that. He said, "Stop being a WiFi router and become a Dishy."

  2022.19.0.mr13442                      Router-01000000000000001F2F12
```

```
abenhase@192.168.1.1: Permission denied (publickey,keyboard-interactive).
abenhase@ABENHASE-M-526H .ssh %
```

- Nmap scan report for 192.168.1.1
- Host is up (0.0040s latency).
- Not shown: 994 filtered tcp ports (no-response)
- PORT STATE SERVICE
- 22/tcp open ssh
- 53/tcp open domain
- 80/tcp open http
- 9000/tcp open cslistener
- 9001/tcp open tor-orport
- 9002/tcp open dynamid

- Nmap done: 1 IP address (1 host up) scanned in 45.68 seconds

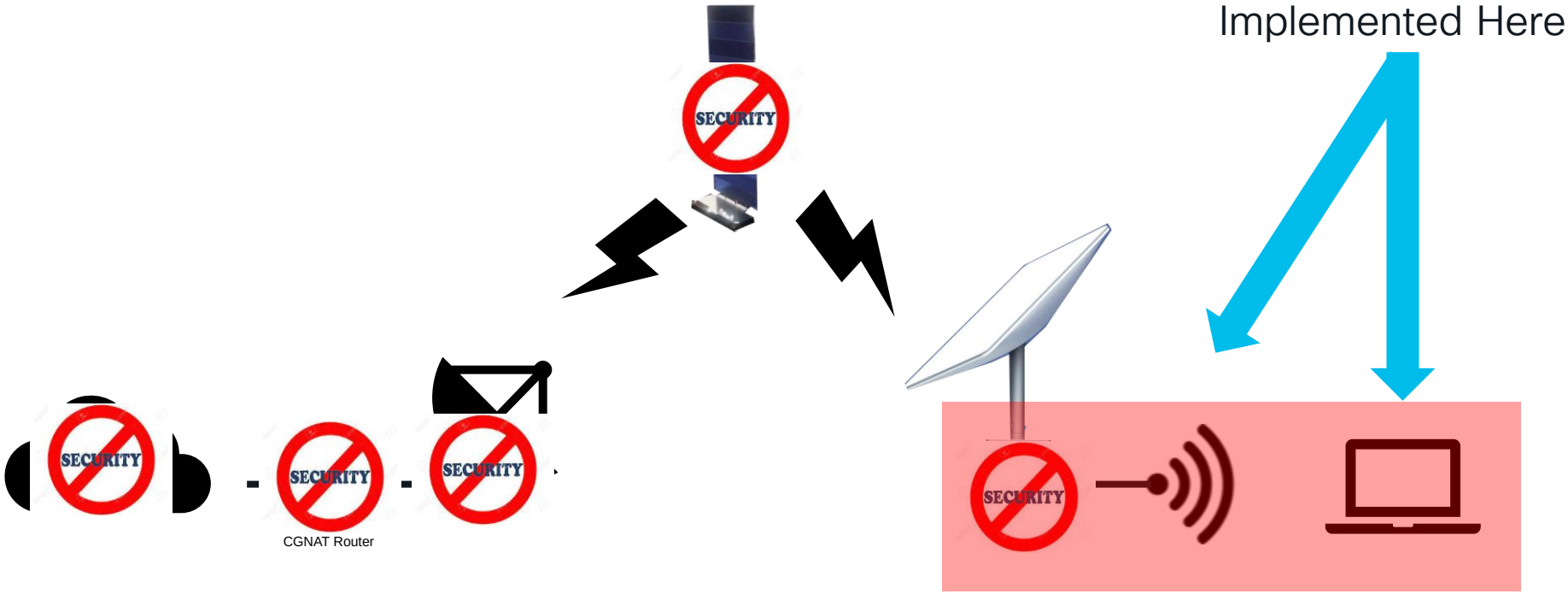
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Things we know about Starlink Network

- Carrier Grade NAT (CGNAT) at the Internet Gateway
- IPv4 DHCP is assigned across the network
- IPv6 Prefix Delegation works on some Gateways
- Layer 2 network from terminal to ground to exit point (MPLS)
- Native IPSec will not work (CGNAT)
- IPSec Encapsulation works – NAT-T (udp4500)
- TLS VPNs work
- There is NO local NAT configuration possible on the SL Router

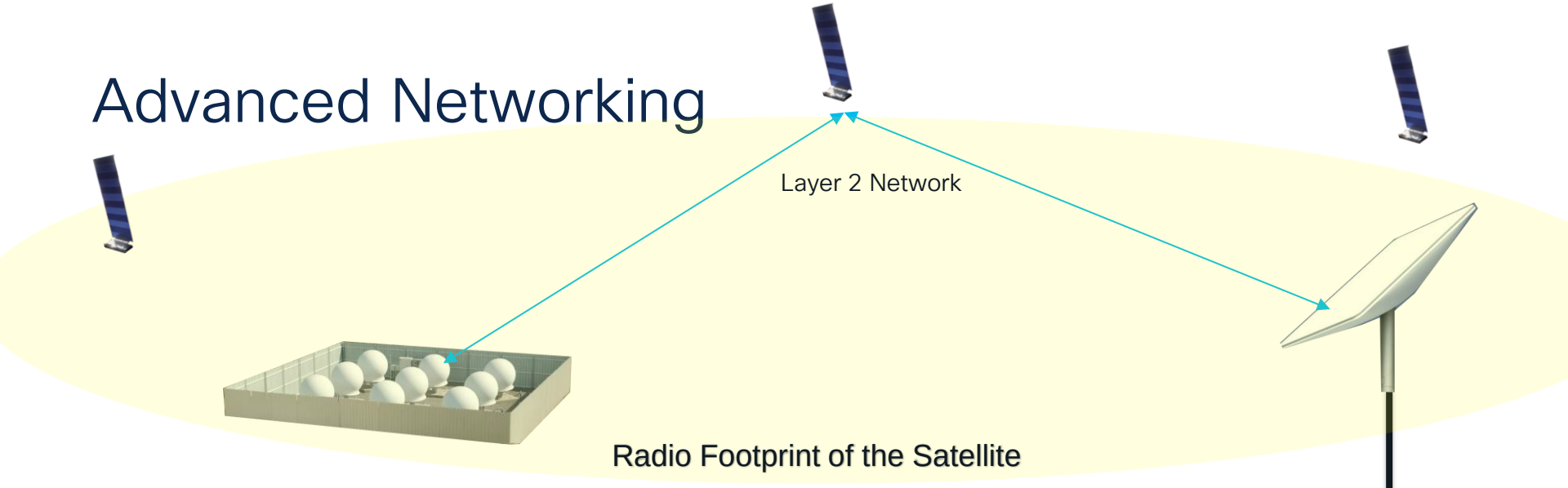
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Starlink Security Today

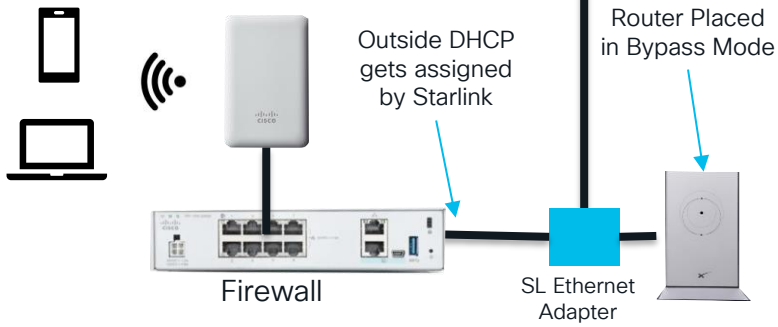


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Advanced Networking

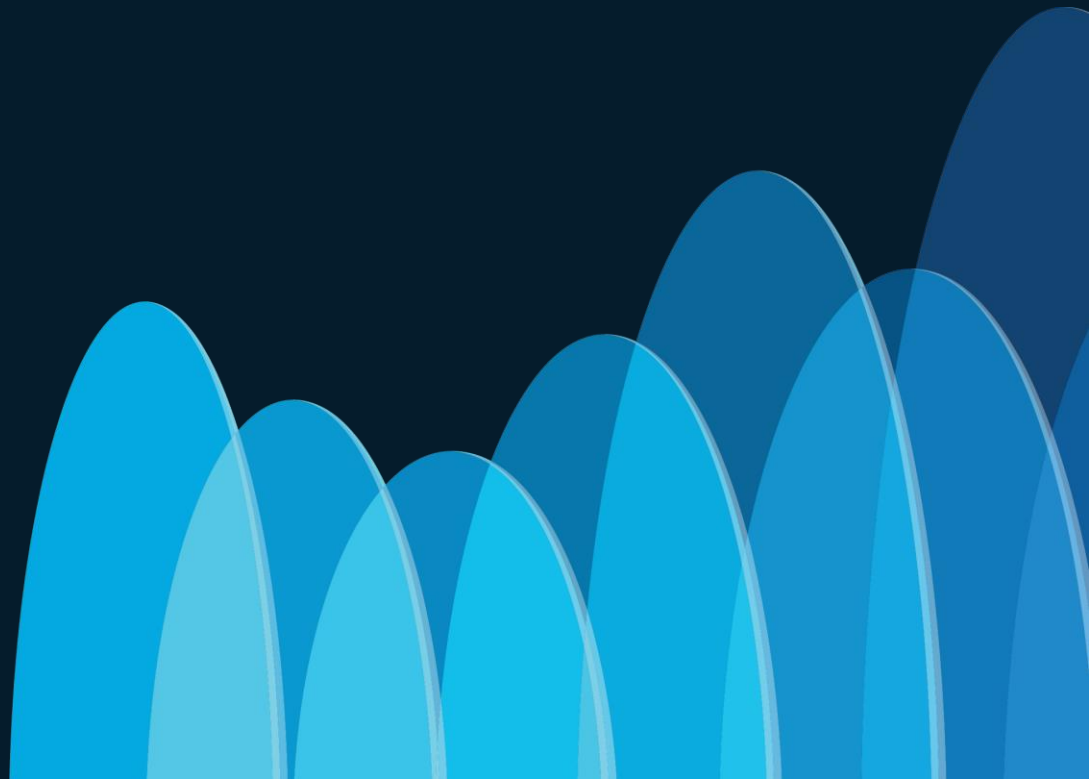


SL Router in Bypass Mode:
WIFI Gets disabled
Router is no longer locally accessible
Statistics are stored in SL Cloud
Array connects to SL Cloud and delivers updates



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

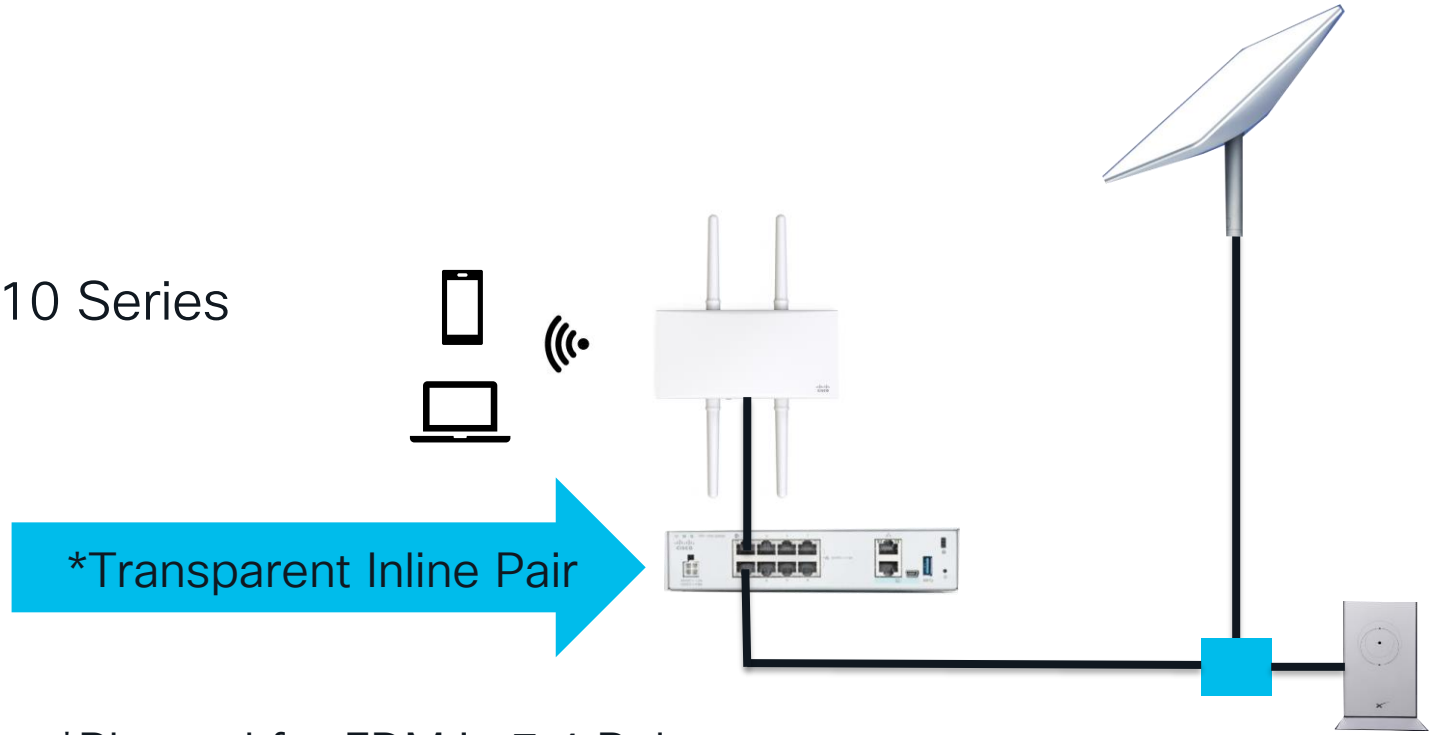
Cisco Security + Starlink



cisco Live!

Meraki+Firepower Deployment

- MX Series
- MR Series
- Z3 Series
- Firepower 1010 Series

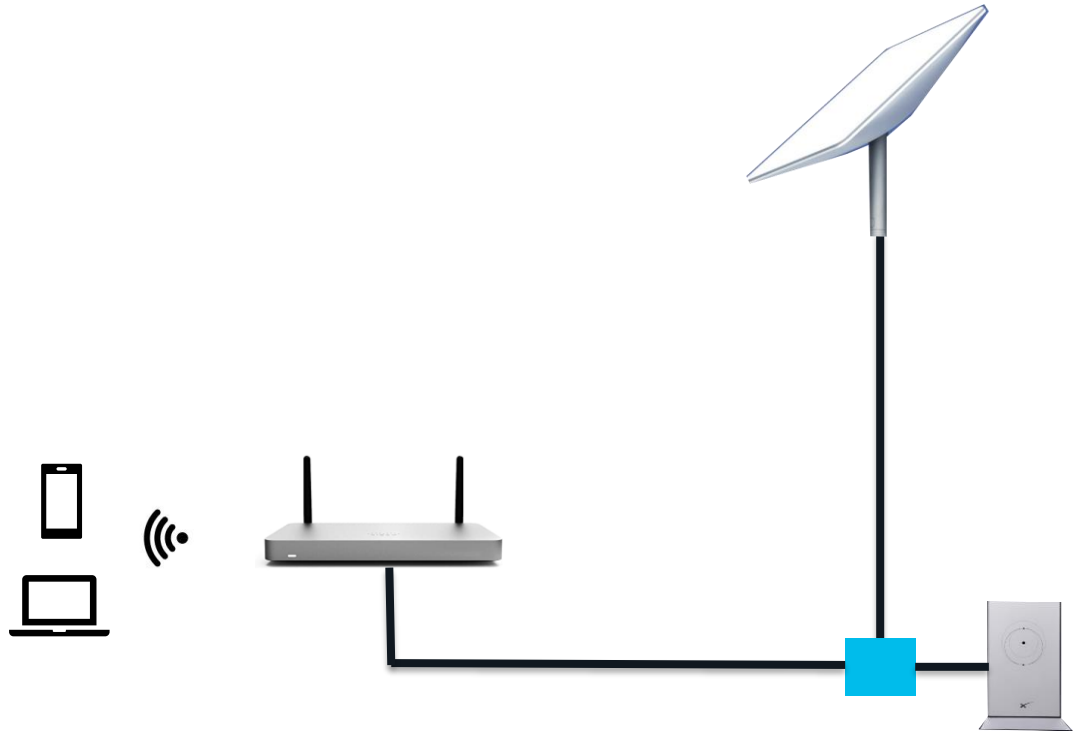


*Planned for FDM in 7.4 Release

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Meraki MX/MR/Z3 Deployment

- MX Series
- MR Series
- Z3 Series



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Native IPv6 Support on MX and MR Platforms

IPv6 Support on MX Security & SD-WAN Platforms [Core Fundamentals]

Last updated: Nov 12, 2022

+ TABLE OF CONTENT

Note: IPv6 is an ongoing cross-product initiative for Meraki as IPv4 addresses are being exhausted and with more hosts such as IoT devices requiring addressing, IPv6 provides a new structure to accommodate a larger number of hosts.

This article describes general information on IPv6 Support on MX Security & SD-WAN Platforms. For more information on compatible devices, please see our IPv6 Device Compatibility documentation.

Overview

- This document describes the IPv6 functionality and configuration available on the MX Security & SD-WAN Platforms. It will include information such as: supported MX and teleworker models, minimum firmware, and how to configure and use IPv6 on a network.

Note:

- MX cannot currently function in a native IPv6-only environment. It is recommended that dual-stack is implemented in order to leverage IPv6 functionality and management.
- High-availability (HA) and template deployments are not supported at this time.

Minimum Firmware

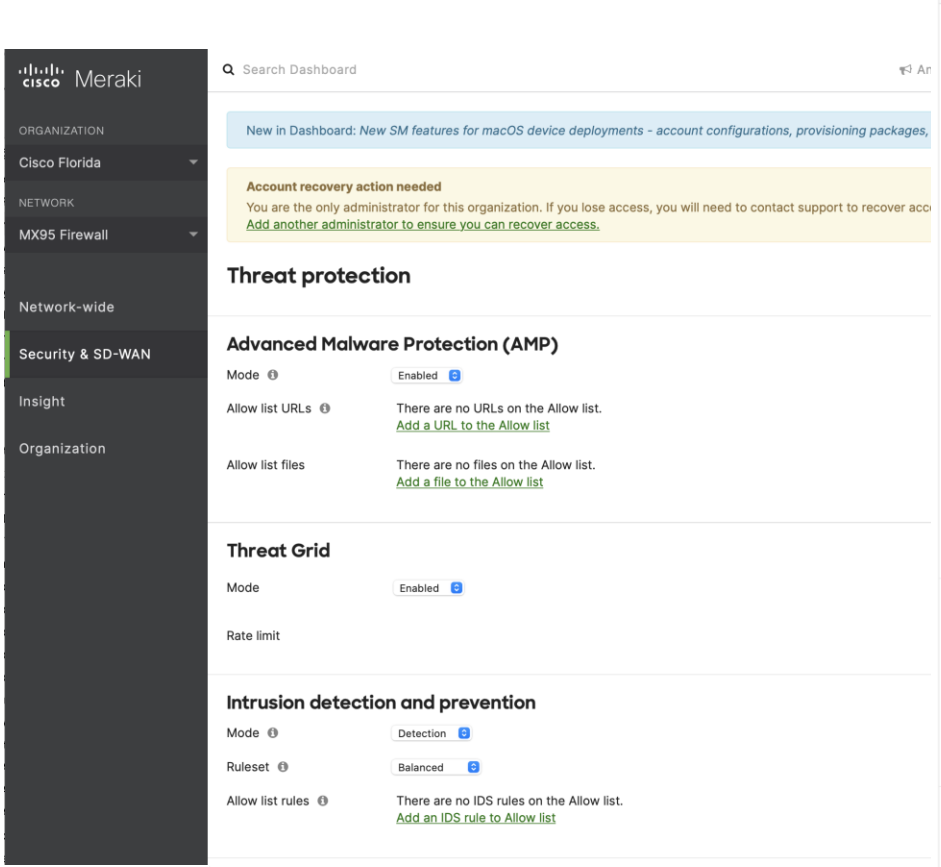
- MX 17.5+ firmware is required for IPv6 functionality on MX Security & SD-WAN Platforms.

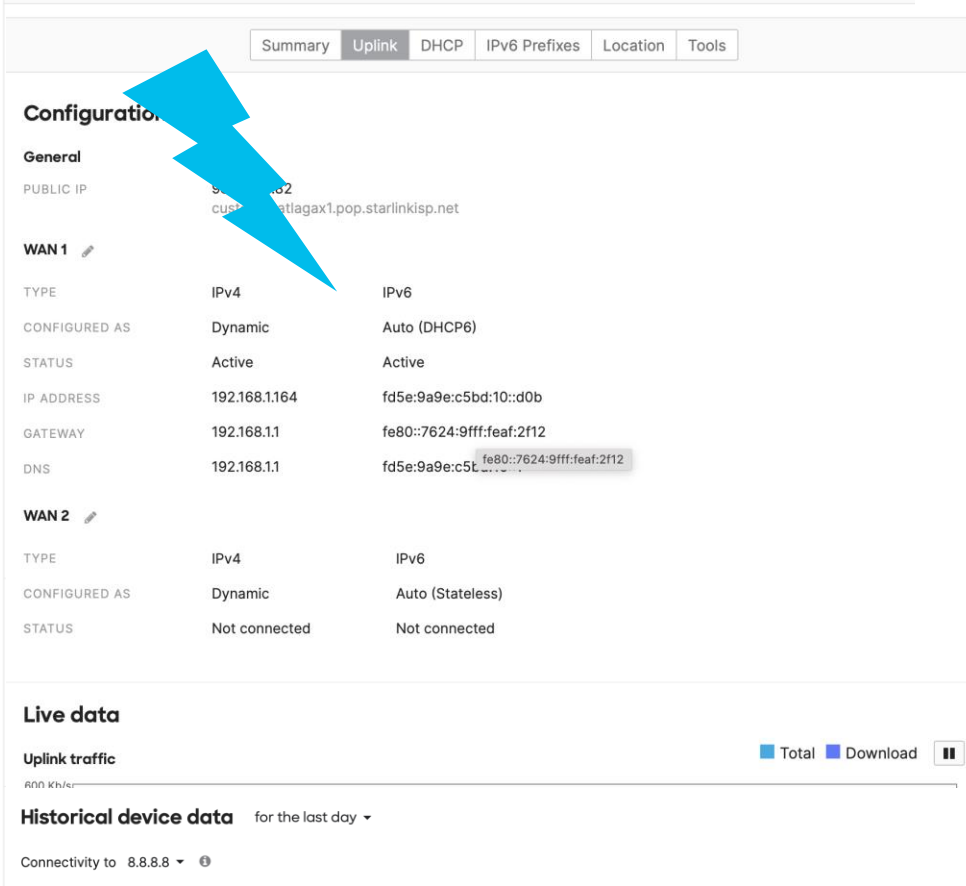
Supported Models

- Z3, Z3C, MX64, MX64W, MX65, MX65W, MX67, MX67W, MX67C, MX68, MX68W, MX68CW, MX75, MX84, MX85, MX95, MX100, MX105, MX250, MX450.
- All current MX/Z models listed on our website here.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Meraki is the simplest security option

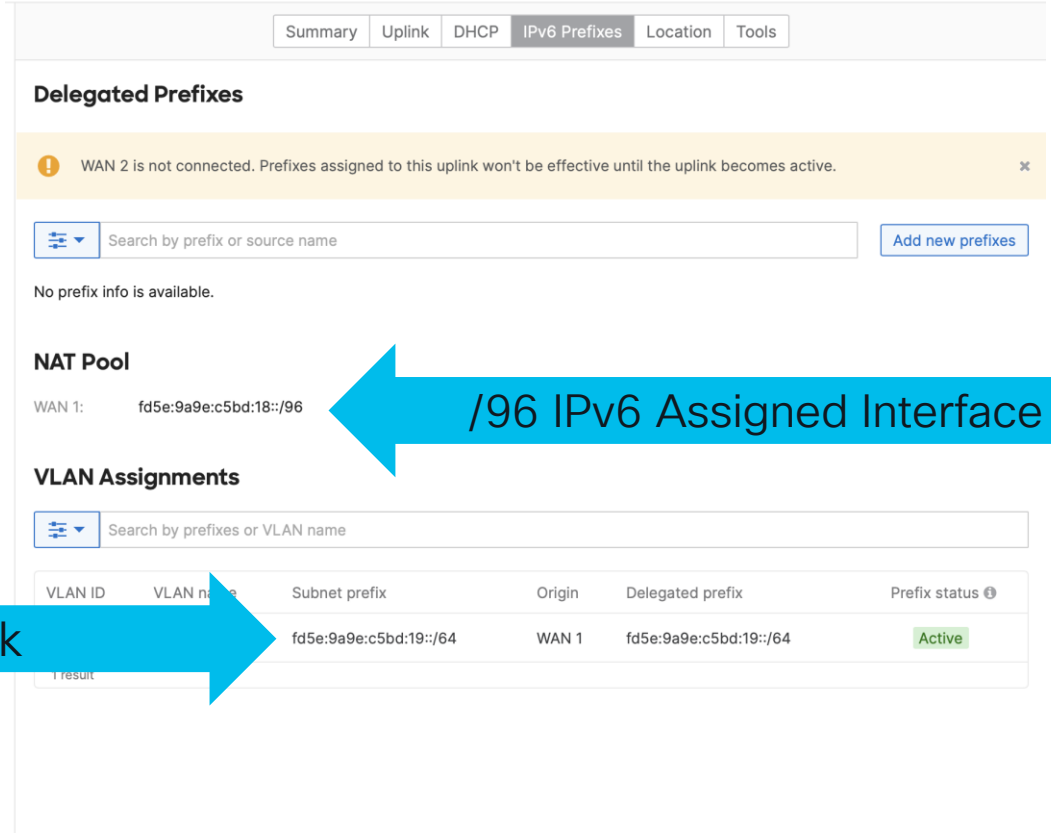




© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

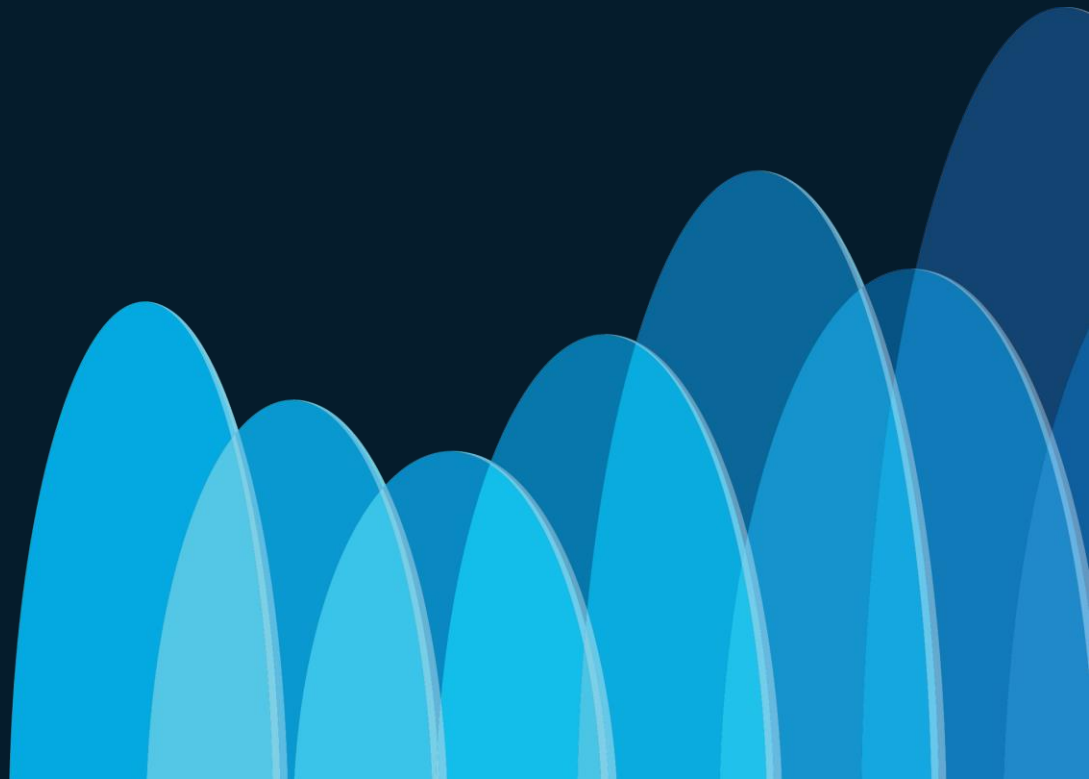
Meraki is the simplest IPv6 Deployment Option

- Takes the downstream Prefix Delegation
- Automatically deploys it to the downstream networks
- Clients will be assigned IPv6 address out of your assigned Prefix



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Actual Working Things



Add another administrator to ensure you can recover access.

Global Overview

Organization
Cisco Florida

Network
MX95 Firewall

Network-wide

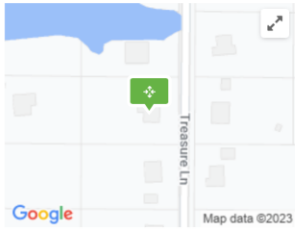
Security & SD-WAN

Insight

Organization

Starlink-MX95

MX95 a8:46:9d:3c:b6:d2



ADDRESS
5840 Treasure Lane, Grant, Florida 32949

WARM SPARE
Configure warm spare

WAN 1
98.97.181.203 Active
2605:59c8:6087:3a10::d0b Active

WAN 2

HOSTNAME
grant-florida-rckhqznmqc.dynamic-m.com

SERIAL NUMBER
Q2XN-CRBC-3HG5

TAGS

NOTES

Configuration

General

PUBLIC IP

WAN 1

TYPE

CONFIGURED AS

PREVIOUS STATUS

IP ADDRESS

GATEWAY

DNS

WAN 2

TYPE

CONFIGURED AS

STATUS

Live data

Uplink traffic

1 b/s
0.75 b/s
0.5 b/s
0.25 b/s
0 b/s

peplink | Dashboard | SFC Protect | Network | Advanced | AP | System | Status | Apply Changes

General

Logout

WAN Connection Status

Independent from Priority

Starlink	Connected via Starlink	192.168.1.21
1 Verizon-Cisco	Connected to Verizon LTE-A	100.103.182.178
2 WAN-WIFI	Connected to GigE-Spectrum	192.168.1.108

Priority 1 (Highest)

1 WIFI-WAN 2.4Ghz	Scanning...	(No IP Address)

Priority 2

2 T-Mobile	No Device Detected	(No IP Address)

Priority 3

Drag desired (Priority 3) connections here

Disabled

VLAN WAN 1	Disabled	(No IP Address)

LAN Interface

Router IP Address: 192.168.50.1

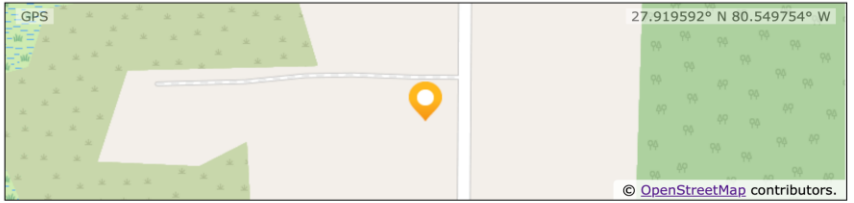
Wi-Fi AP ON Status

2.4 GHz 5 GHz Pepwa (United ... | 2.4 GHz 5 GHz Pepwa (United ... | 2.4 GHz 5 GHz Pepwa (United ... | 2.4 GHz 5 GHz Pepwave-WIFI

SpeedFusion Connect Protect

SFC-ATL	Established
SFC-CHI	Established
SFC-MIA	Established

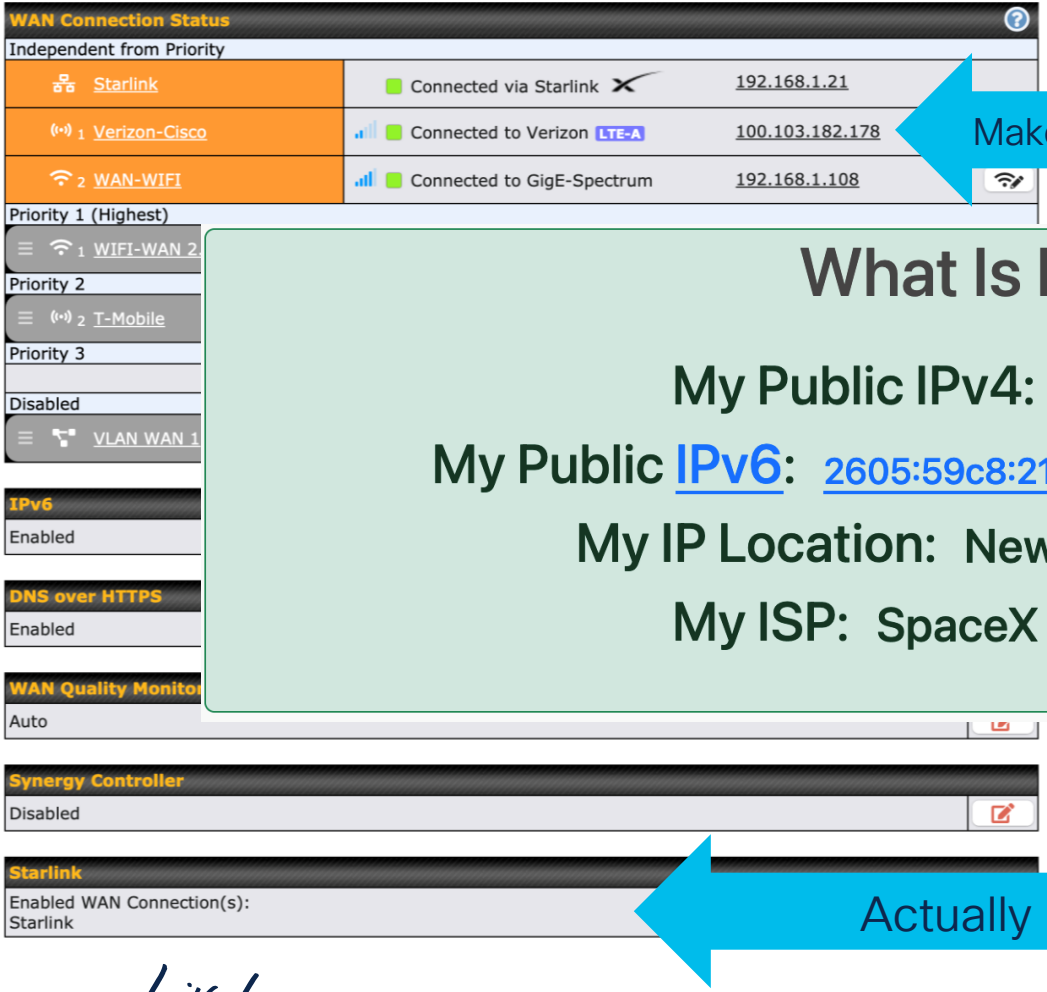
Data usage allowance: 1003.20 GB (Expiry date: Apr 11, 2024)



Device Information

Model: Peplink MAX Transit Duo Pro

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public



Makes forwarding decision based on API feedback

What Is My IP?

My Public IPv4: 98.97.18.37

CG-NAT IP

My Public IPv6: 2605:59c8:2103:7310:654e:1122:4a82:e20a

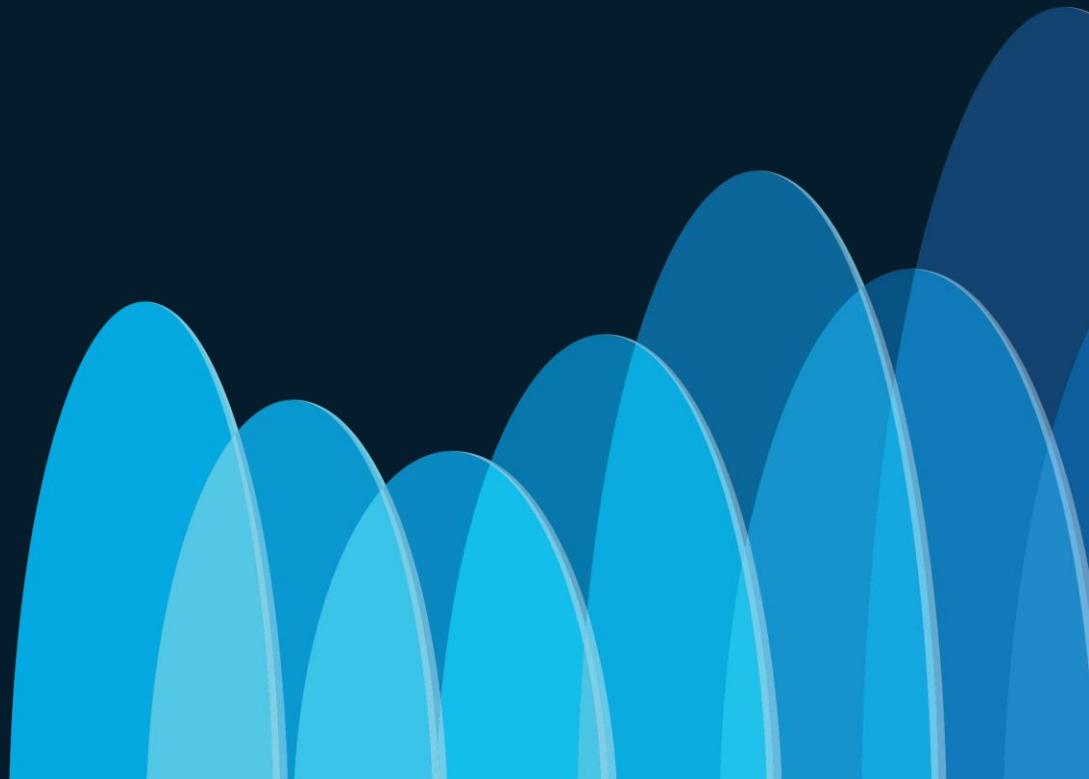
My IP Location: New York City, NY US

My ISP: SpaceX Services Inc.

Actually does API lookups

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

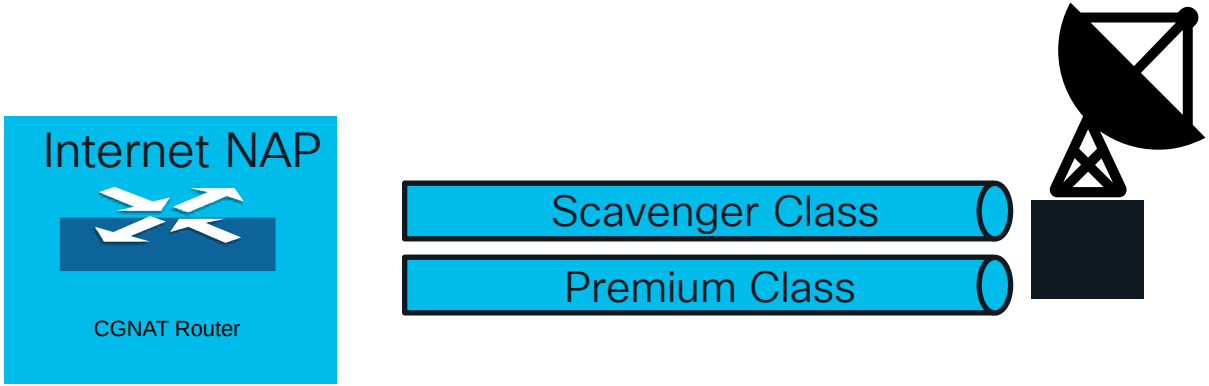
Deployment Considerations



QoS Observations

- Terminals (arrays) are statically linked to what we believe to be MPLS VPNs with static exits to the Internet

Scavenger class QoS



Residential QoS

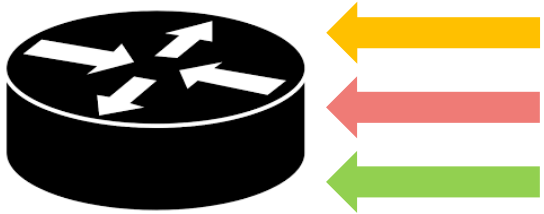
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

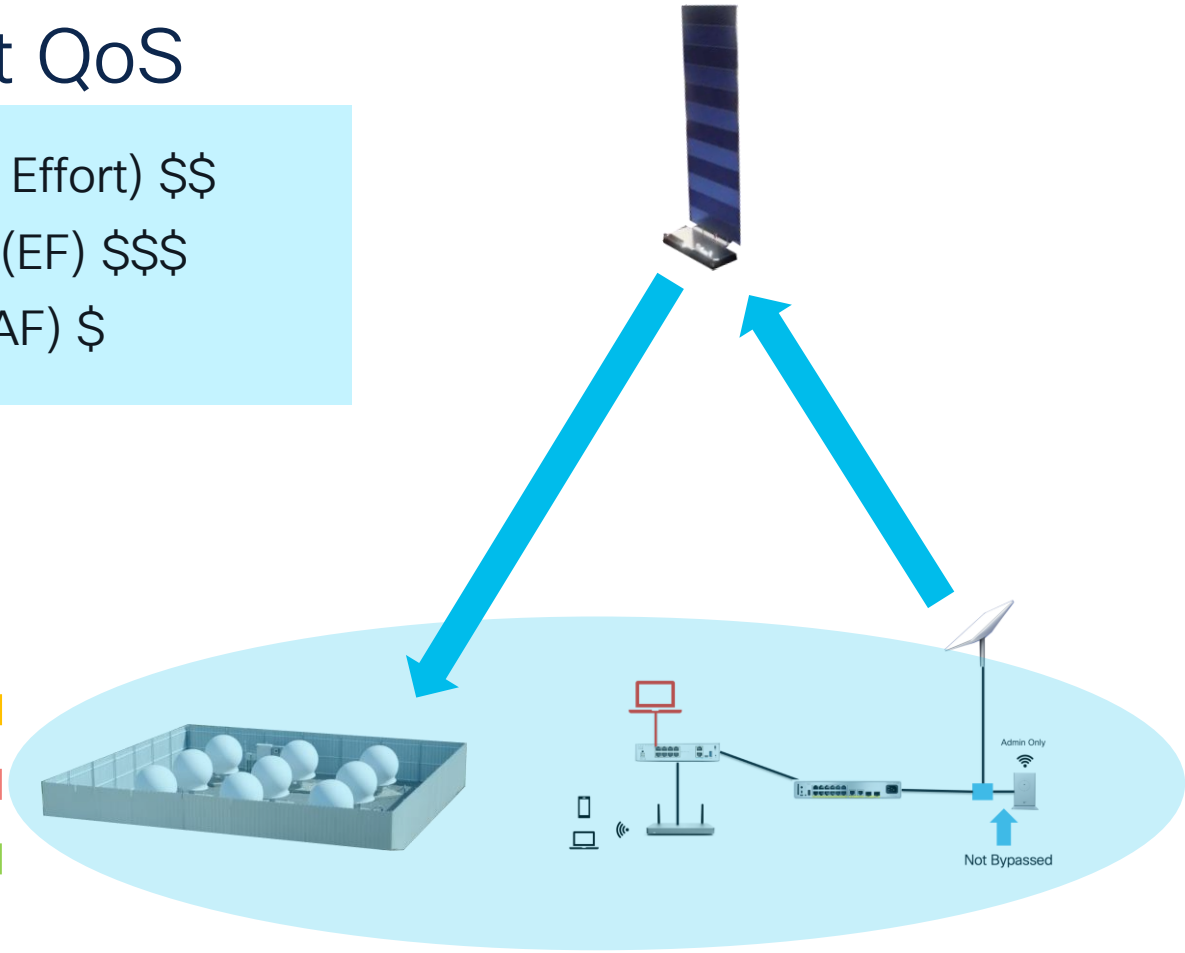
Observed Current QoS

Mobile (Best Effort) $$

Priority Data (EF) $$$

Residential (AF) $

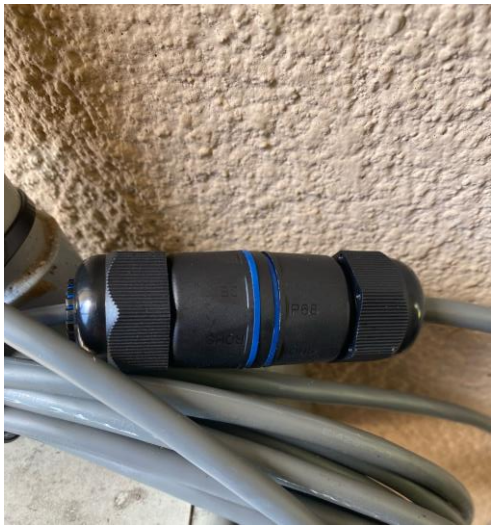




© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

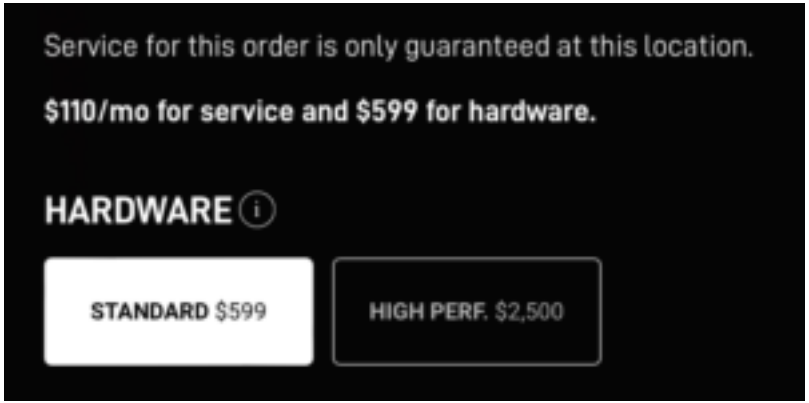
Deployment Considerations

- You will probably want a 150 foot cable
- You can make a 300+ foot cable easily by inserting Ethernet in the middle
  - Use High Quality watertight connectors



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Decisions



- “High Performance” is simply double the array
- They have a single GigE output – but have doubled the transceivers
- They are clearly creating a Service Class for High Performance users and doing traffic engineering to support it

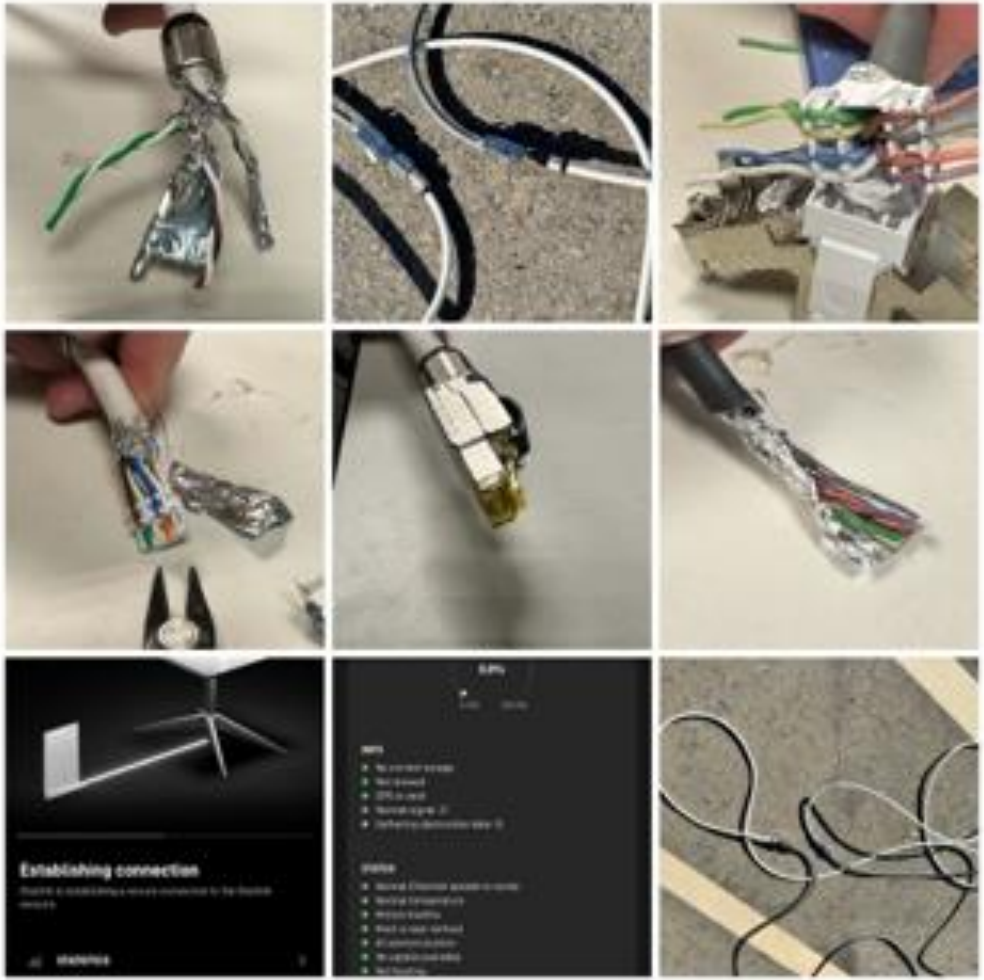
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

High Performance Terminal Considerations

HP Wires are 22AWG!

HP pin / Pot / Dish Wire Color / RJ-45 pin & Color using 568B standard
A1 + Green 1 Orange/White
A2 + Yellow 2 Orange
A3 + Blue 3 Green/White
A4 + White 6 Green
B1 - Orange 7 Brown/White
B2 - Purple 8 Brown
B3 - Brown 5 Blue/White
B4 - Gray 4 Blue
B5 × Shield / Shell

CAT8 22AWG STP RJ45



*Courtesy: Lyle Tanner

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

IR1101 Ruggedized Router

cisco Live!

IR1101 – Starlink Integration

- Ruggedized Router meant for harsh conditions
- Pluggable LTE – including Multi-SIM
- New LTE P-LTEA7-NA= capable of support T-Mobile waveform for Starlink Direct to Cell frequencies

- SDWAN Capable
- 802.1AE MACSEC on LAN
- IPSec on WAN
- Runs full IOS-XE – 17.15

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

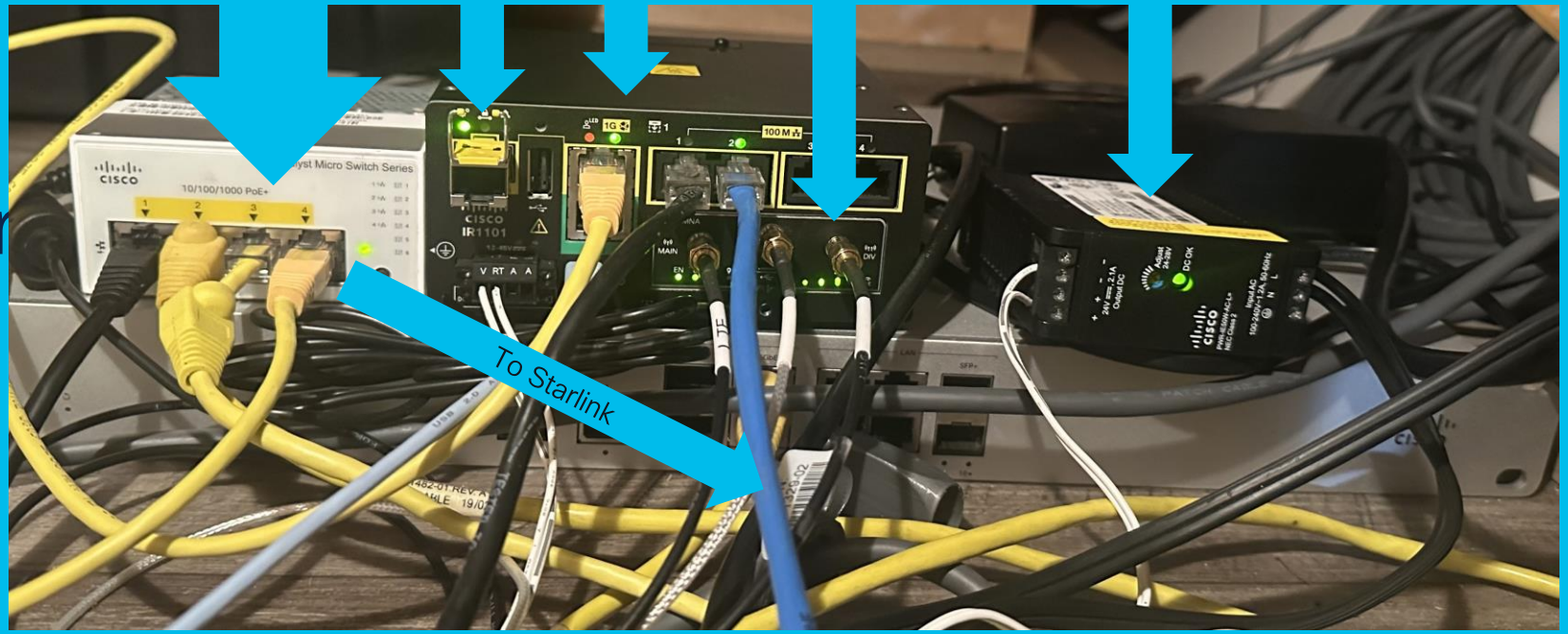
AC to DC Power Brick

GigE to Catalyst

Pluggable LTE Radio

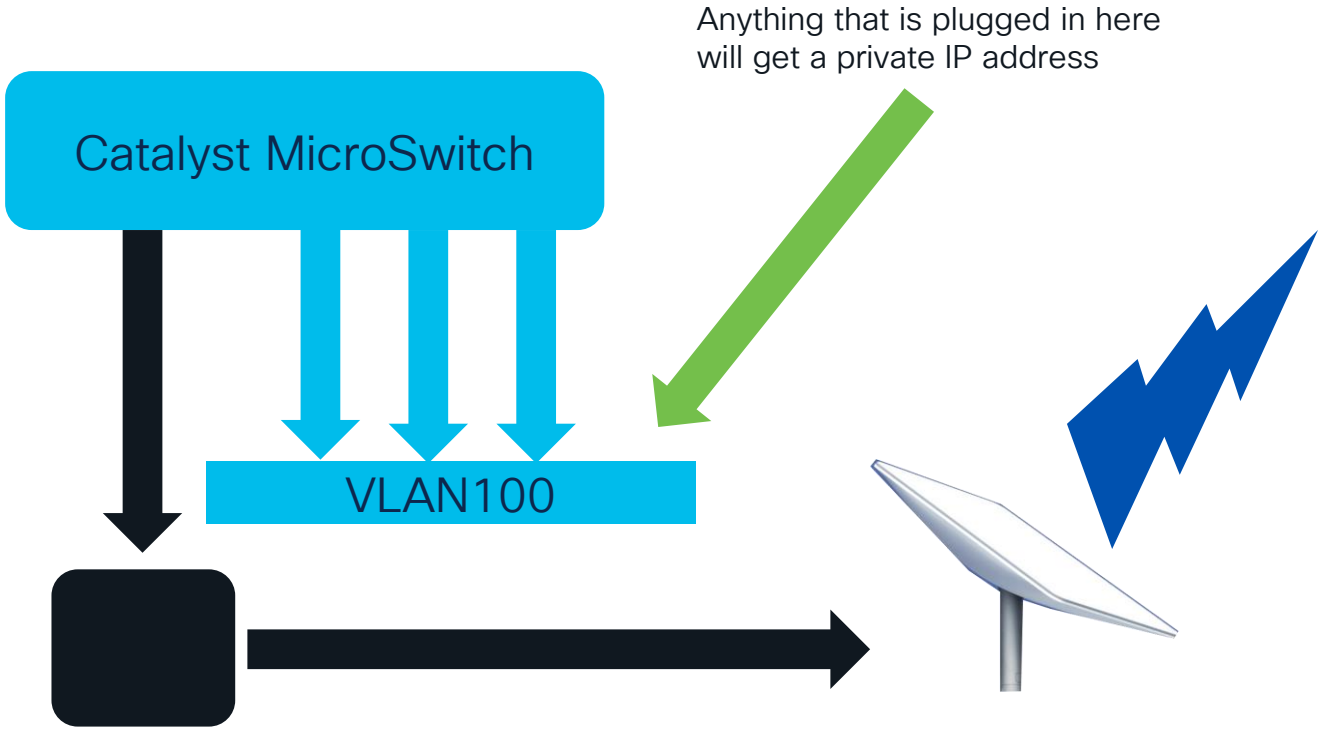
Catalyst Micro Switch
Single VLAN

SFP



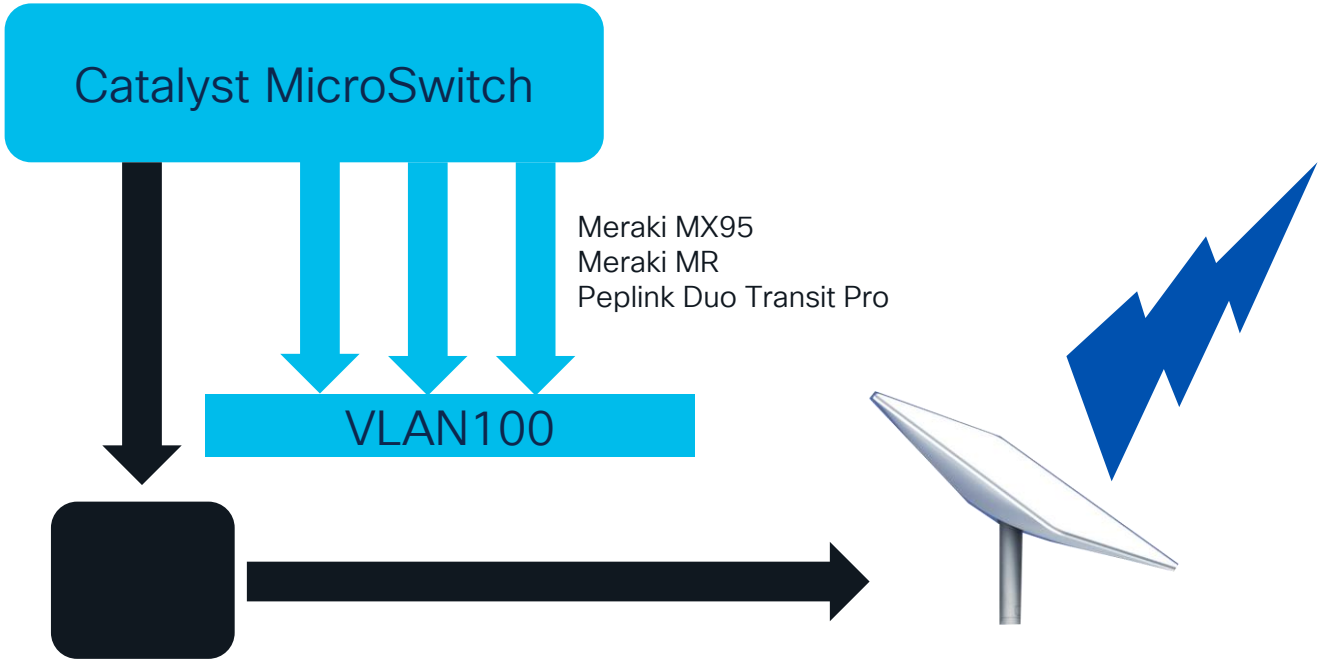
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

How it works



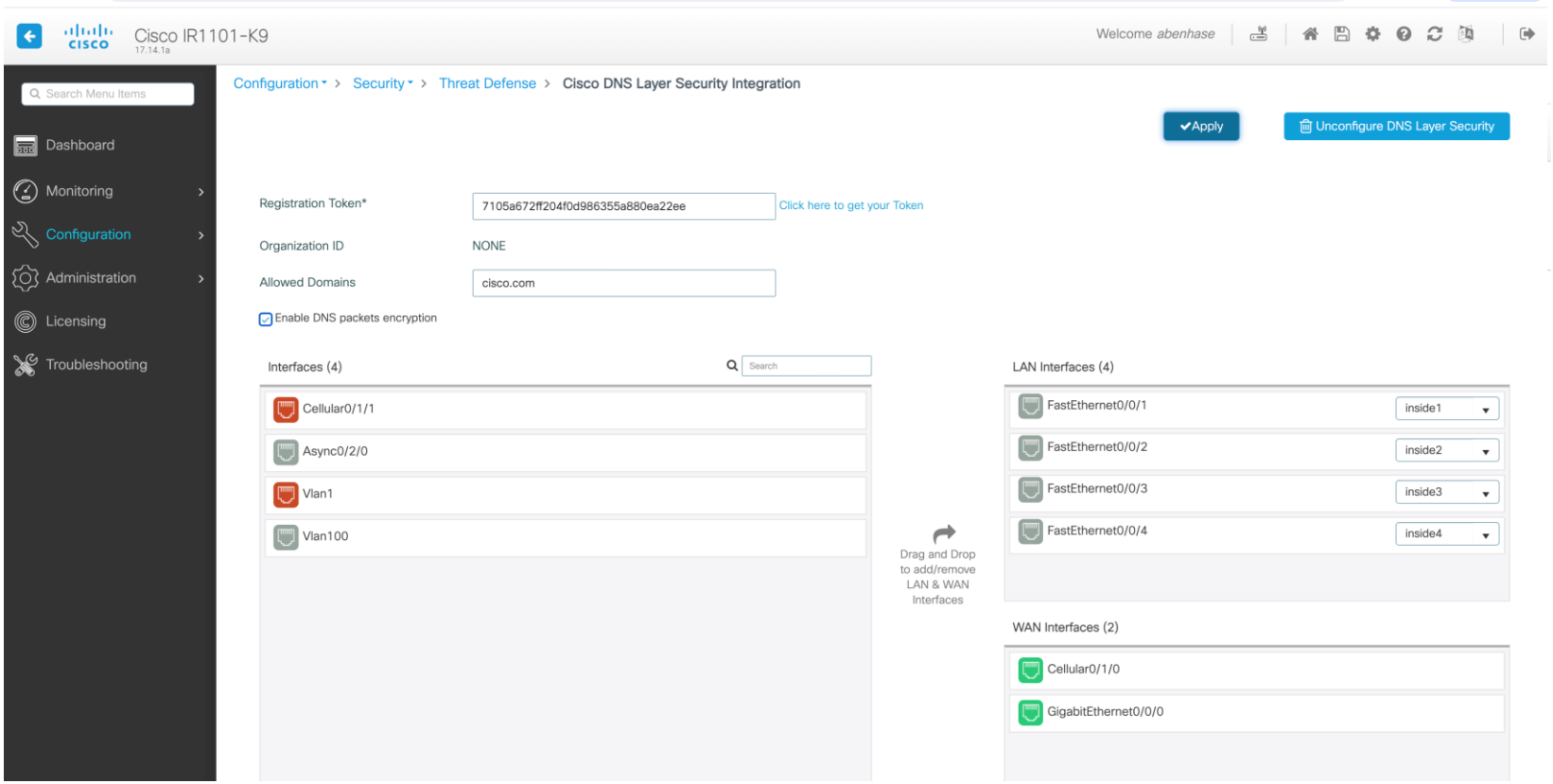
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

How it works



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

What can I do with an IR1101 to secure SL?



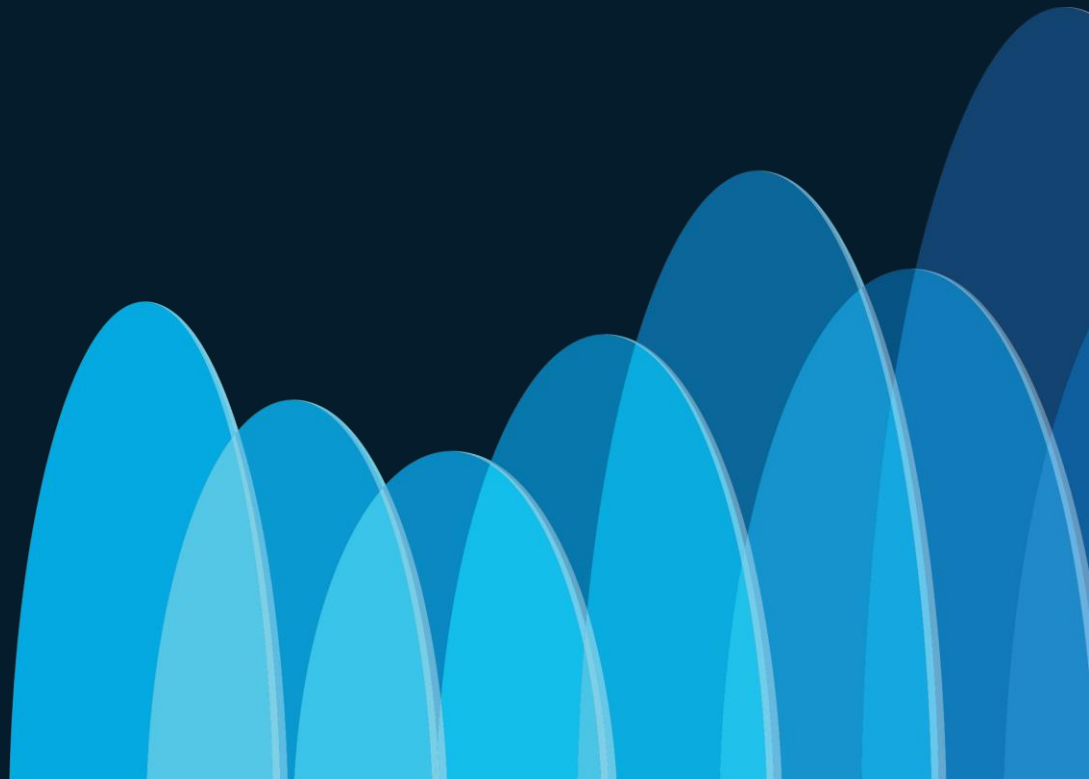
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cellular Gateway/Starlink

- Starlink can be primary link using phased array
- LTE model can be secondary backup in the event that primary waveform fails
- LTE failover to cellular network if primary path fails

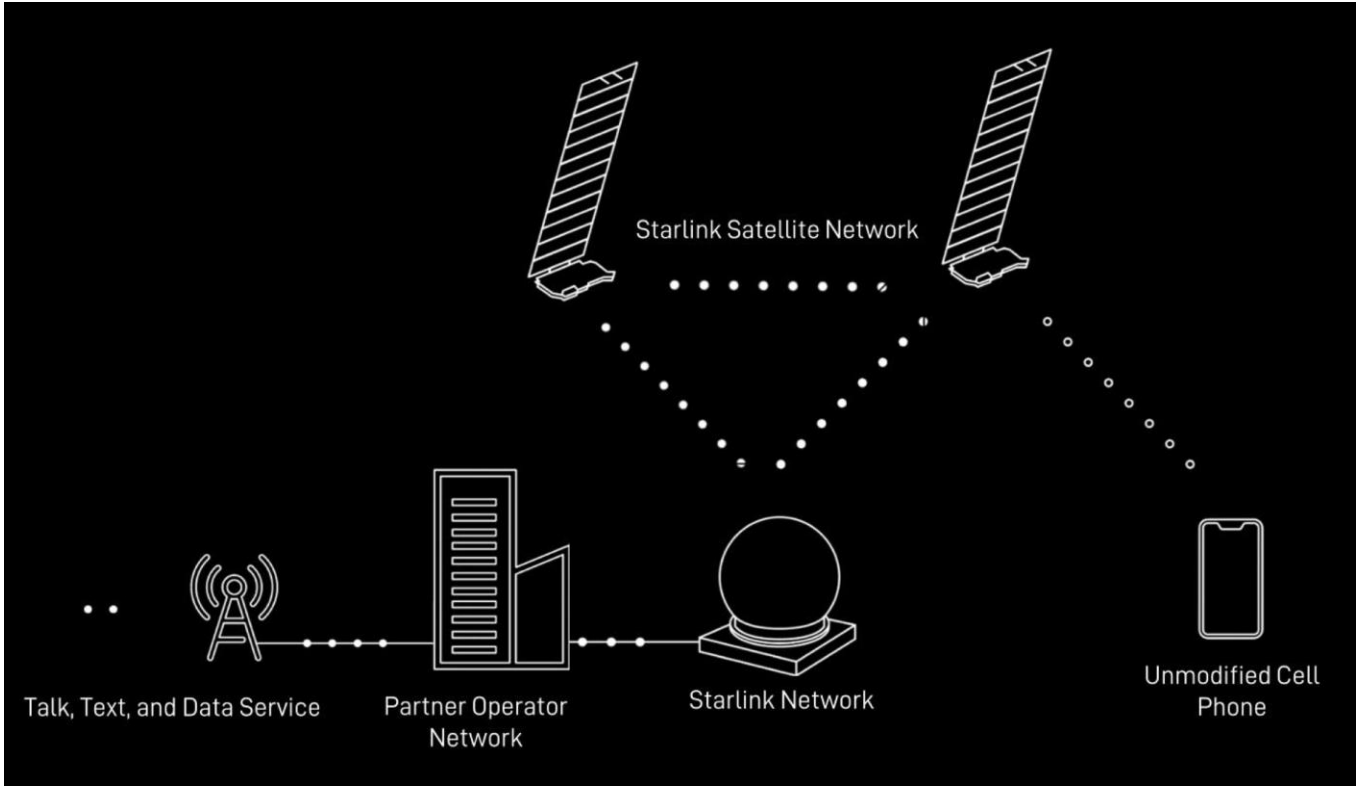
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Starlink Direct to Cell (DTC)



cisco Live!

Direct to Cell

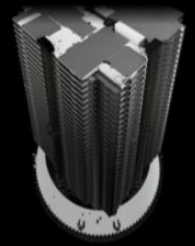
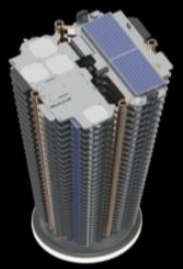


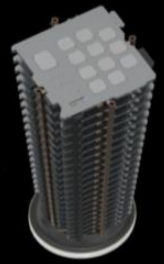
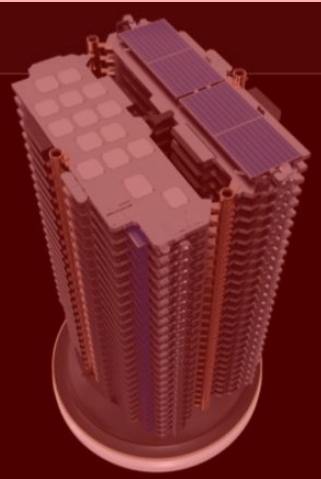
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Starlink – Direct to Cell

- Contract with T-Mobile to provide capability in CY2025
- Operates at 1.6Ghz to 2.7Ghz
- No Phased Array required!!!
- ~300 satellites in orbit currently
- New satellites are being launched each week
- Starlink v2 MINI Only capability
- Starship will be a critical enabler

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

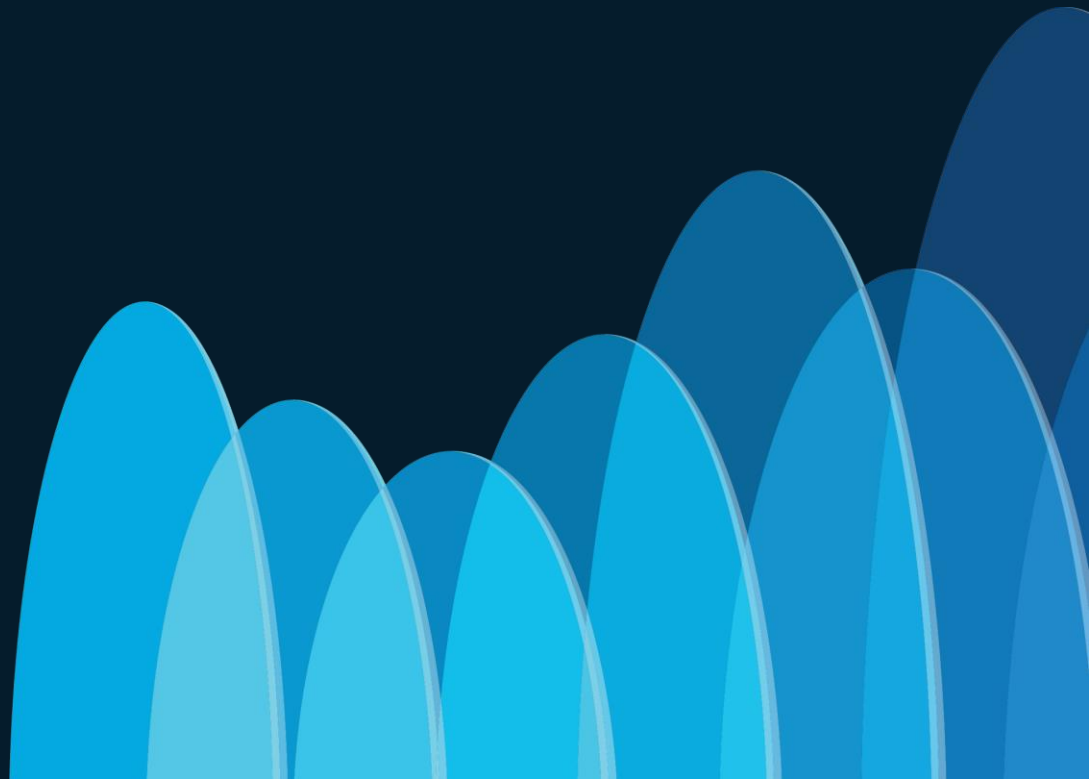
The goal of these infographics is to give a sense of stacking and scale – not to accurately represent satellite design

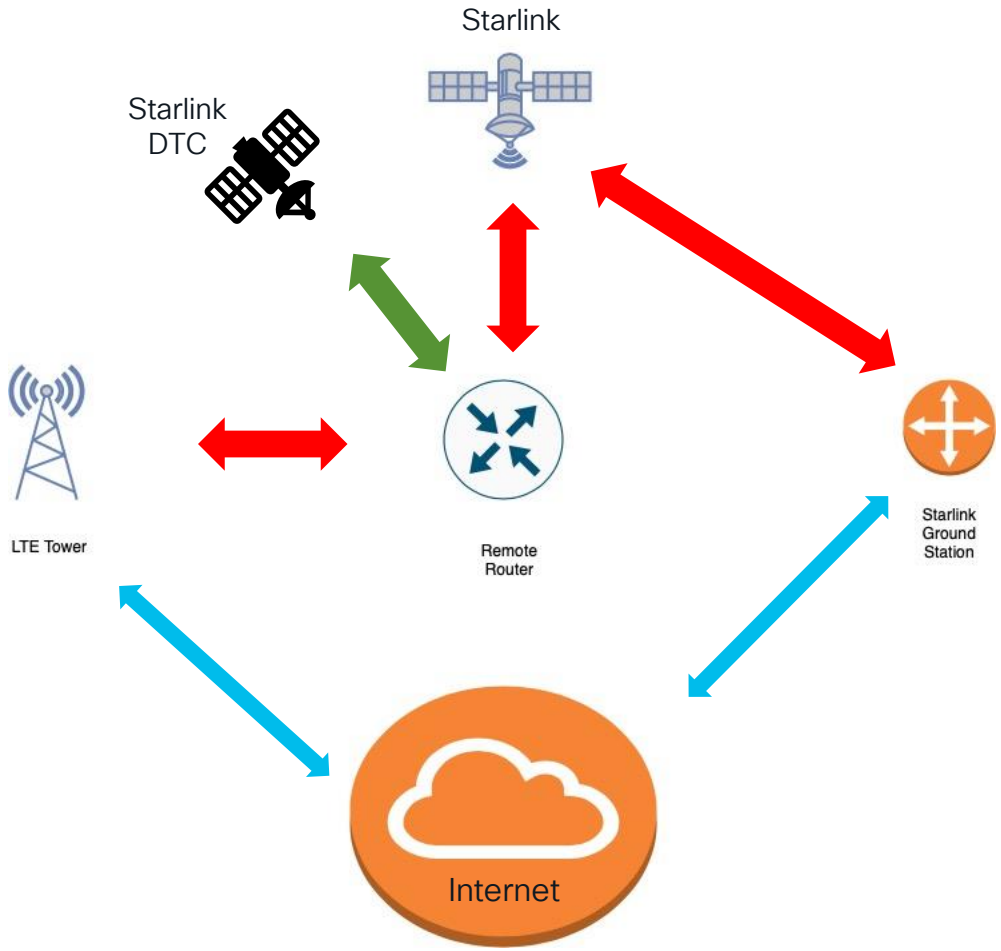
Assumptions

Designation	Starlink V1.5	Starlink V2 F9-1	Starlink V2 F9-2	Starlink V2 mini	Starlink V2 Starship
Status	Launched	FCC filing – may not realize	FCC filing – may not realize	Launched	FCC filing
Mass kg	306	303	800	800	2000
Gbps / sat	15	18	70	60	170
Launch	60 units per Falcon 9	60 units per Falcon 9	16 units per Falcon 9	21 units per Falcon 9	50 units per Starship
Tbps / launch	0.9	1.1	1.1	1.3	8.5
m$ / launch	Sats 18 + launch 30 = 48m$	Sats 18 + launch 30 = 48m$	Sats 11 + launch 30 = 41m$	Sats 15 + launch 30 = 45m$	Sats 60 + launch 15 = 75m$
$ / Mbps	53	45	37	35	9

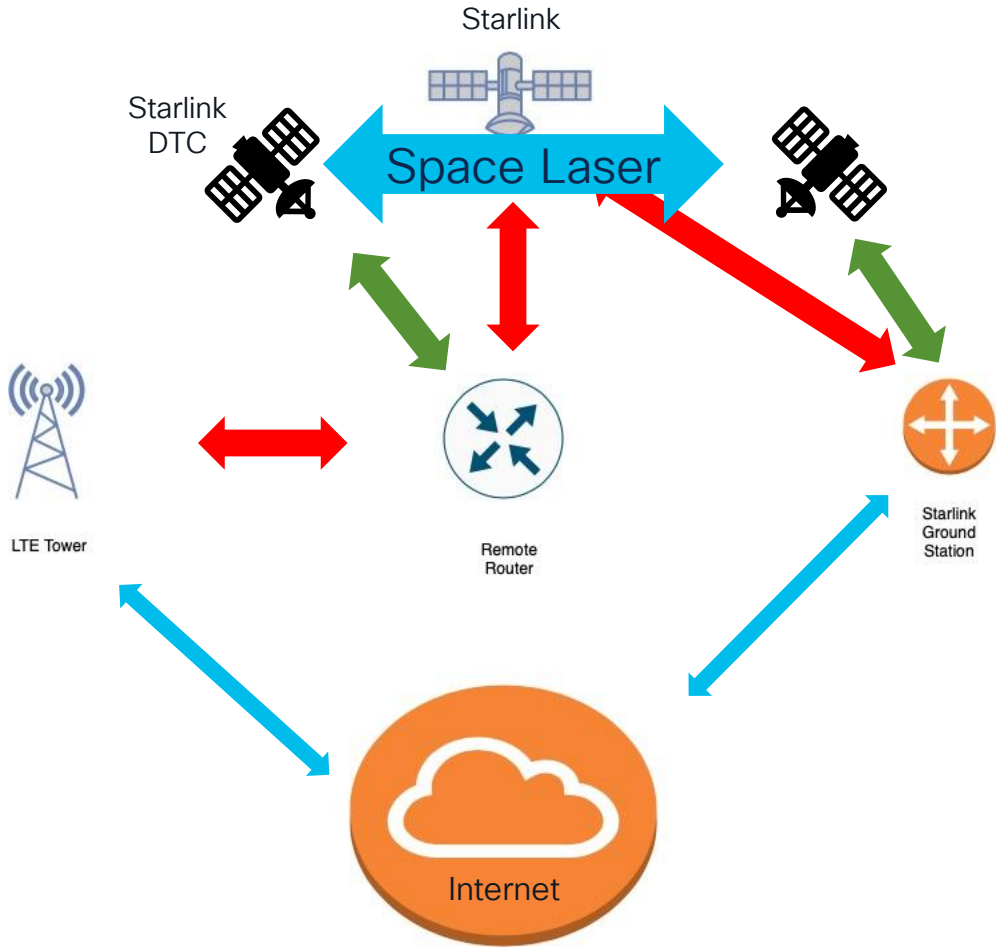
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

How DTC Works





© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Remote Sensor Package Details

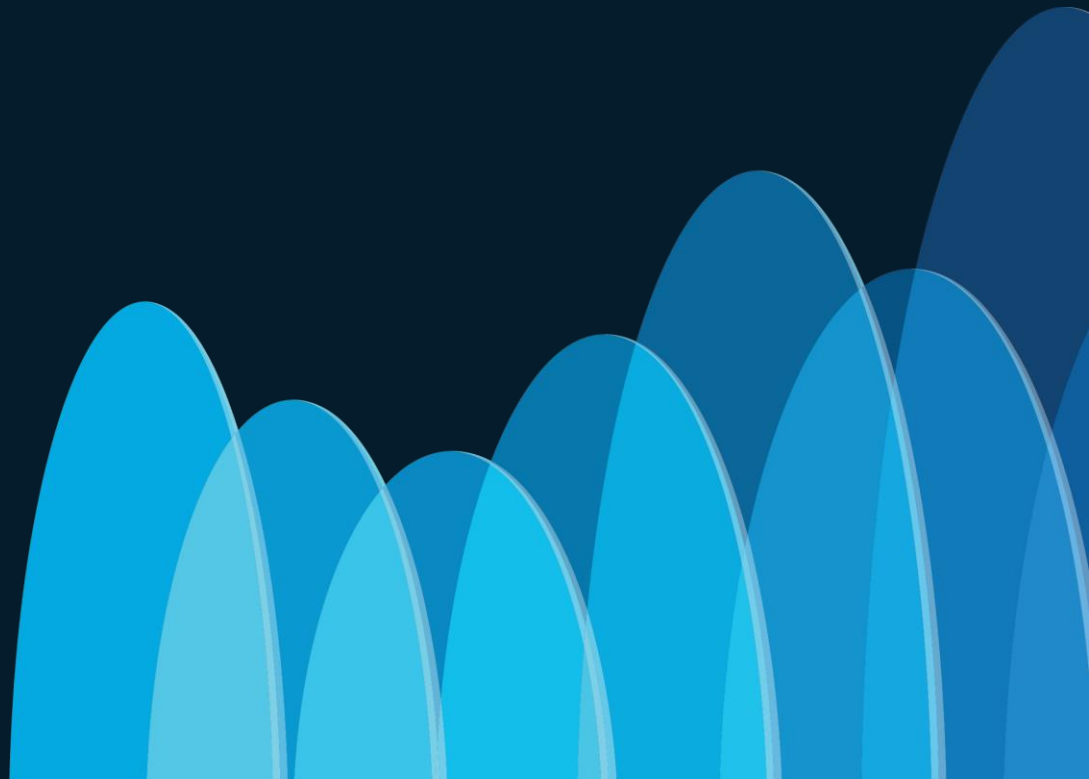
- Low power Router+Radio combination
- Man portable
- **Requires no external phased array!**
- **Low bandwidth use cases – sub 7mbps**
- **Remote Sensor packages are a huge use case**
- **With LiFEPO4 battery, 30w solar array and a scheduled power on, you could collect, upload and run indefinitely**

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

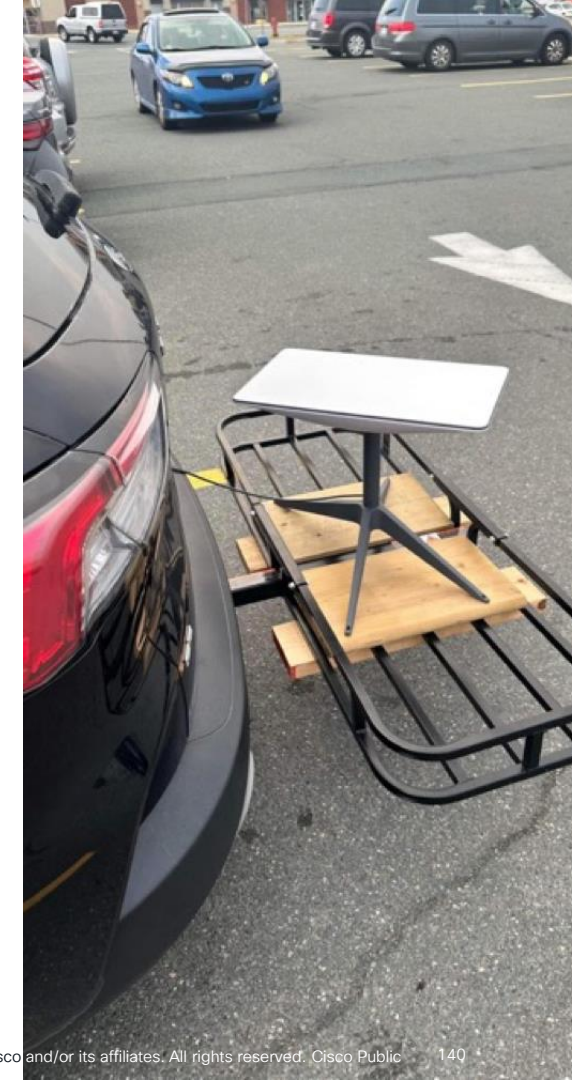
We are rapidly approaching a time when there will be no place on Earth that will be without Internet access

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Austere Deployment Options



cisco Live!

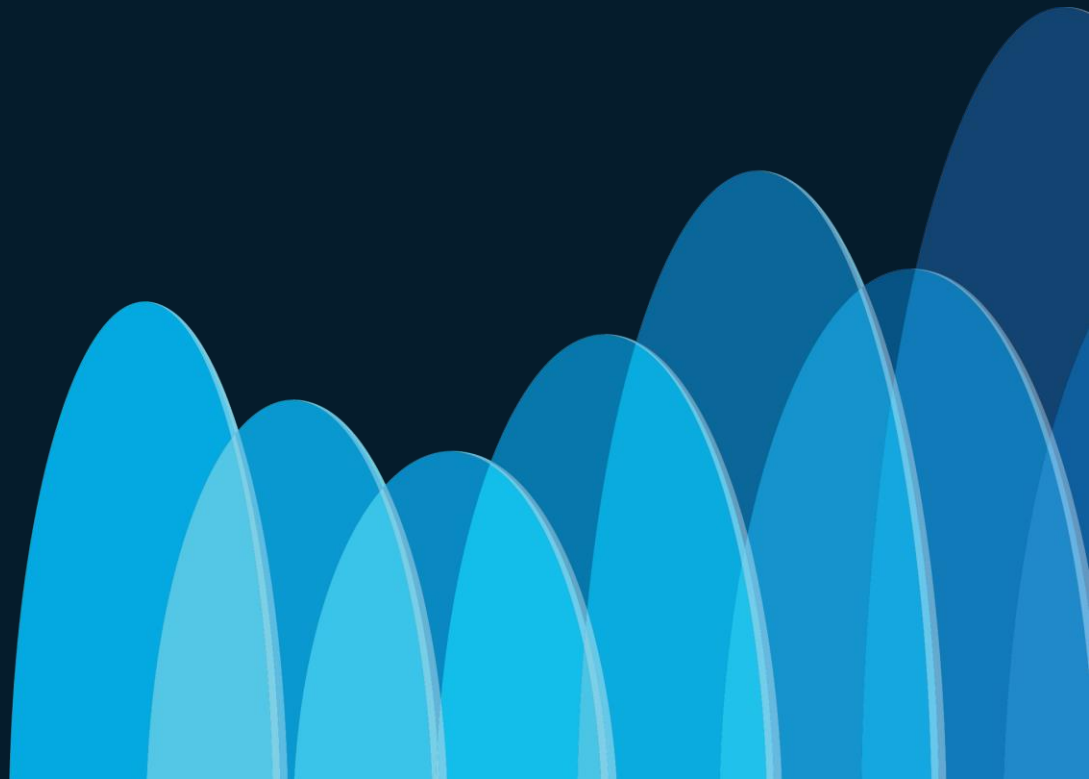


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

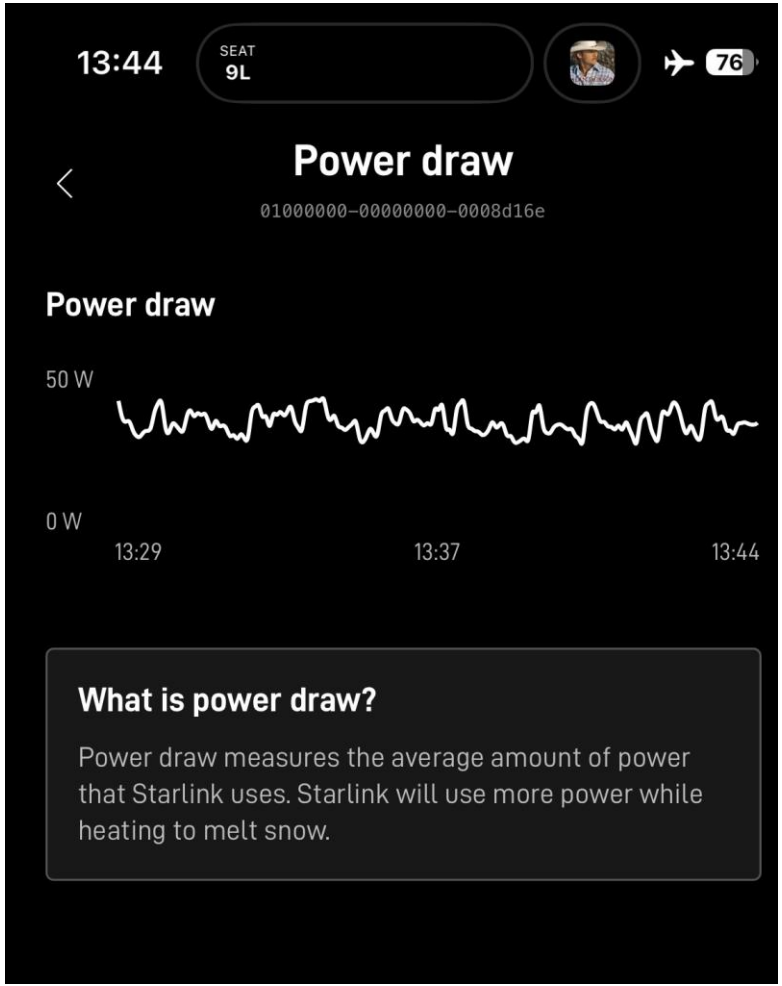
Austere Deployments

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

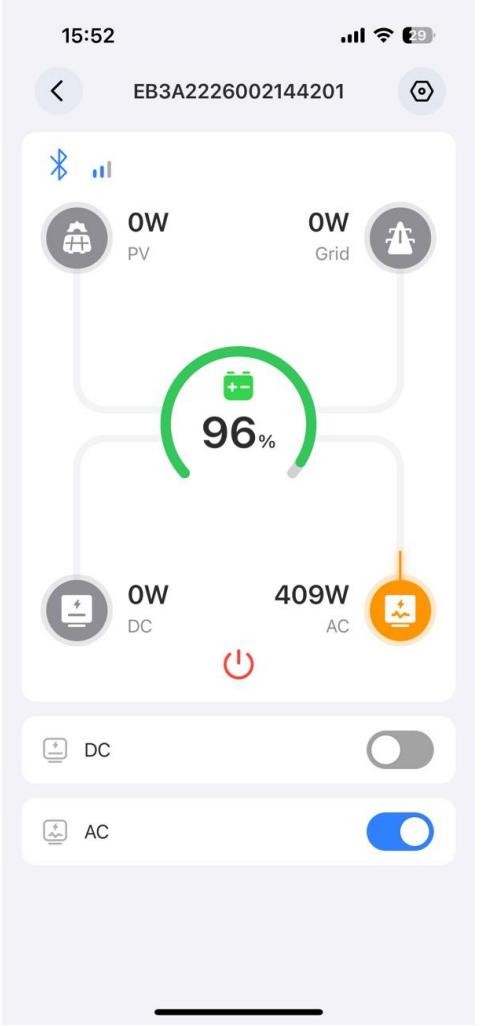
SOLAR POWER (this year)



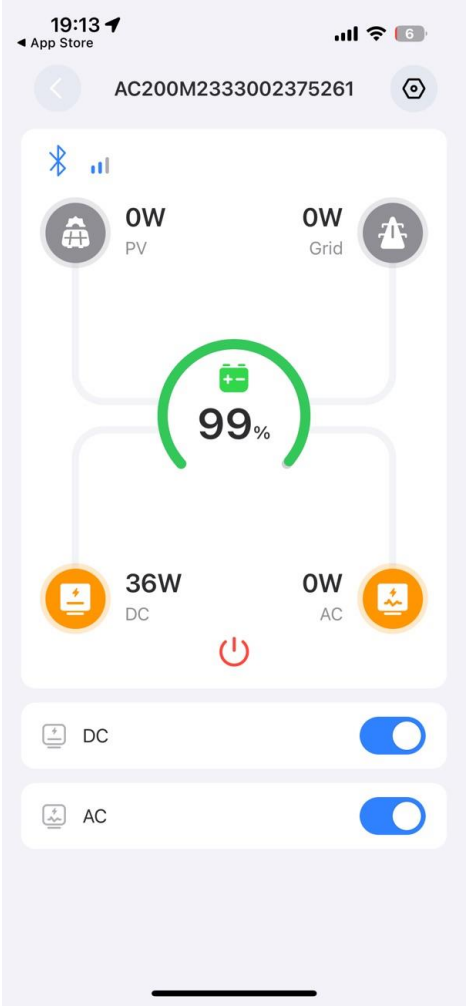
This is super useful!



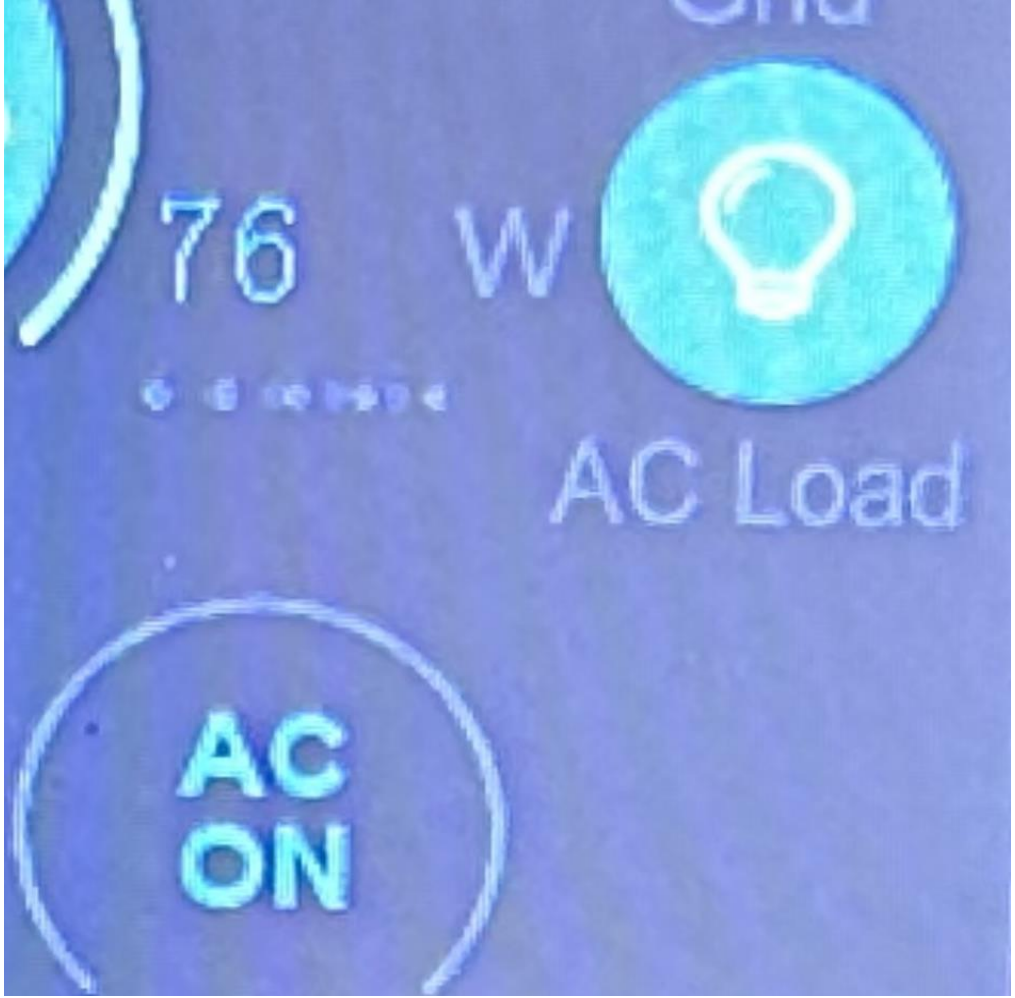
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Power/Solar Conclusions (from last year)

1

You will need more stored power than you think

2

You will need more solar power than you think

3

You will have to trial 24hr operation to be sure it works

4

You will have to account for lack of full solar cycles

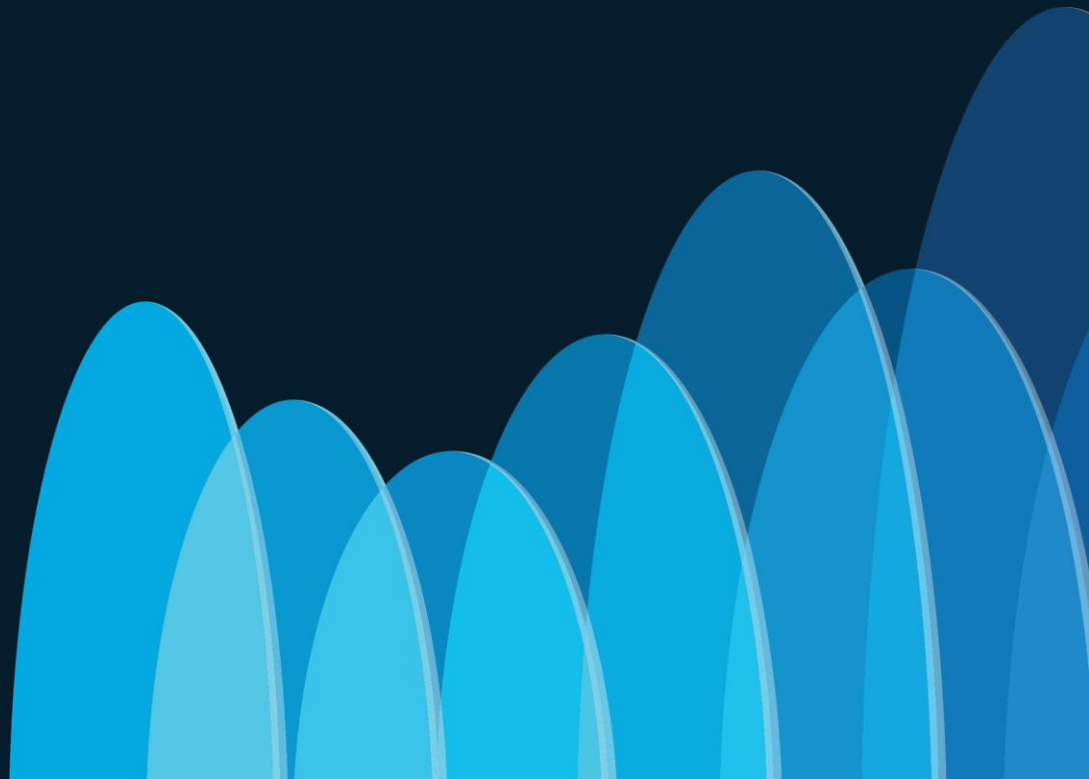
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Updated Solar Guidance

- Minimum 1000Wh between solar cycles
- Gen 2 dish consumes between 43-50watts consistently
- 200watts of solar panel will reliably recharge 800Wh in 4-5 hours of direct sun
- 24 hour remote operation is completely achievable

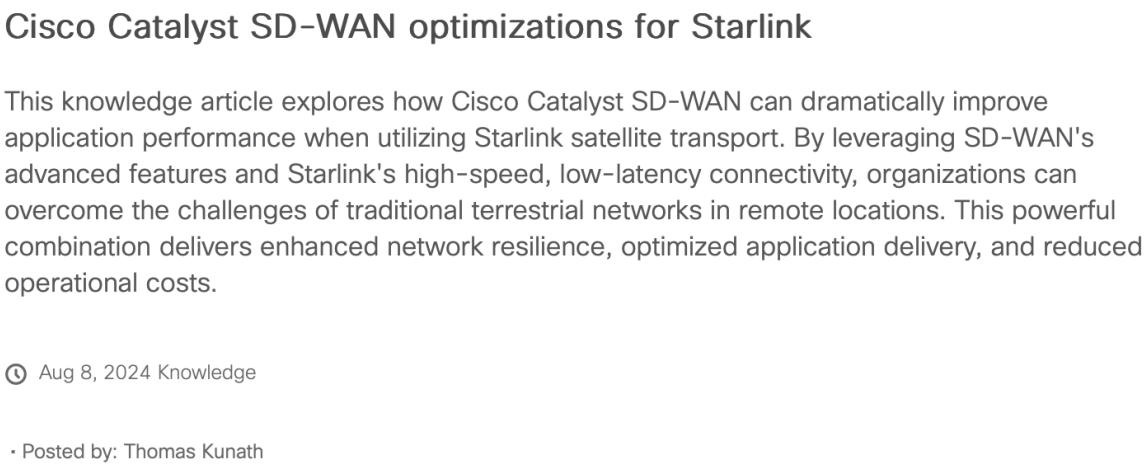
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

SDWAN



cisco Live!

Cisco Starlink SDWAN Paper



Cisco Catalyst SD-WAN optimizations for Starlink

This knowledge article explores how Cisco Catalyst SD-WAN can dramatically improve application performance when utilizing Starlink satellite transport. By leveraging SD-WAN's advanced features and Starlink's high-speed, low-latency connectivity, organizations can overcome the challenges of traditional terrestrial networks in remote locations. This powerful combination delivers enhanced network resilience, optimized application delivery, and reduced operational costs.

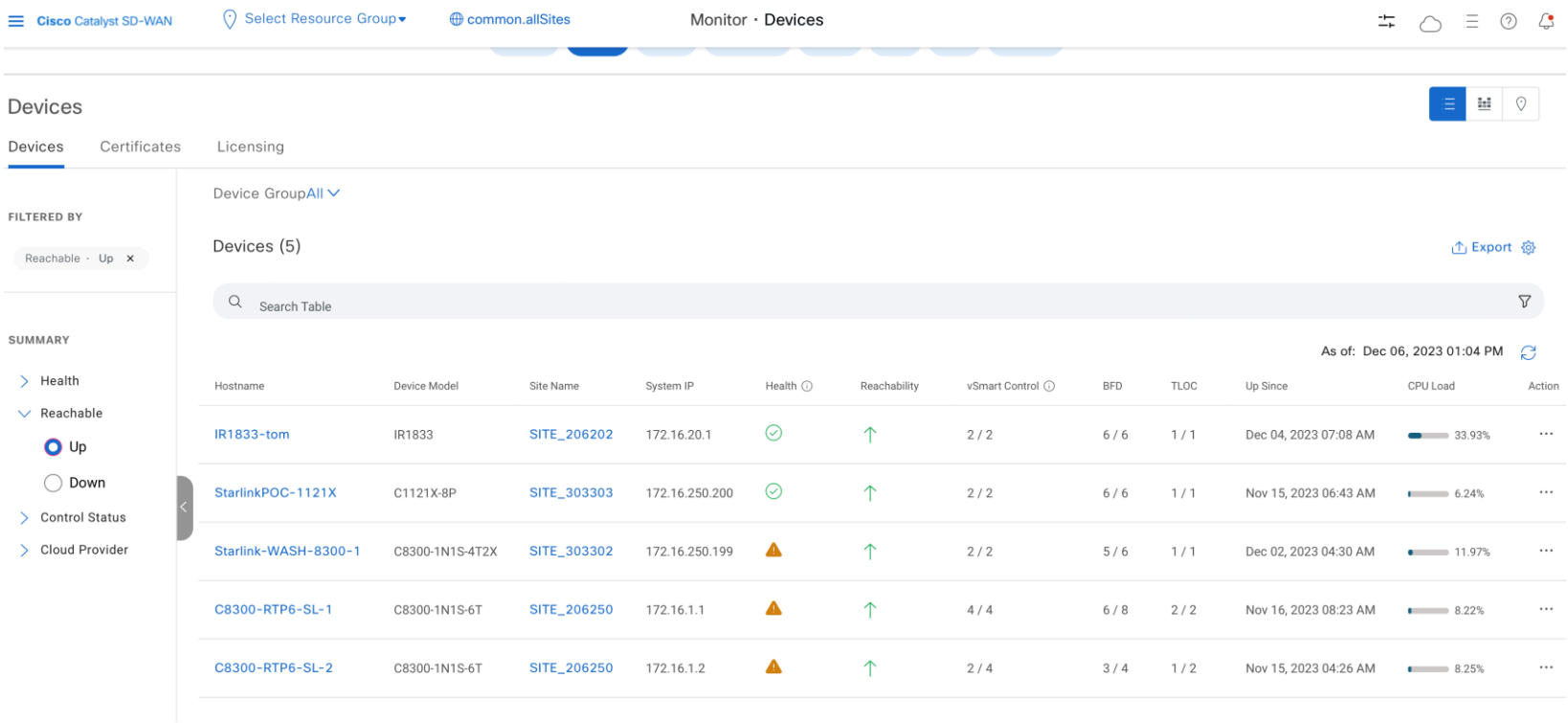
Aug 8, 2024 Knowledge

• Posted by: Thomas Kunath

https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2024/pdf/BRKENT-2660.pdf BRKENT-2660

https://learningnetwork.cisco.com/s/article/cisco-catalyst-sd-wan-optimizations-for-starlink White Paper

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Things we know

- CG-NAT is a reality for all Residential and Mobile Plans
- High Performance Array is allocated a public IP address
- This is NOT a static IP address!
  - DHCP 5 minute renewal
  - IPv6 Prefix Delegation = 5 minutes

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

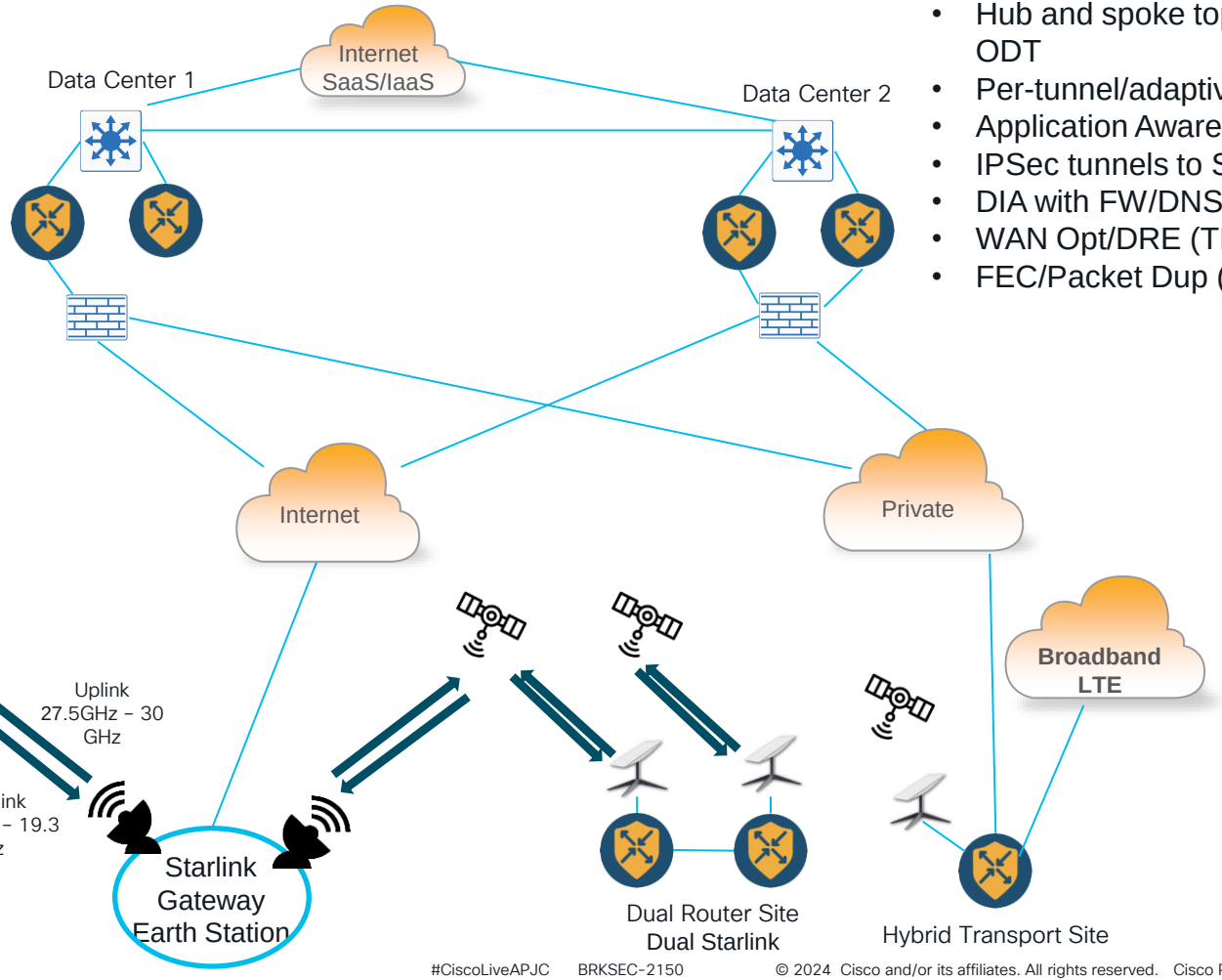
Starlink Reference Architecture

Catalyst SD-WAN Controllers
On Premise in DC or Cloud
Hosted

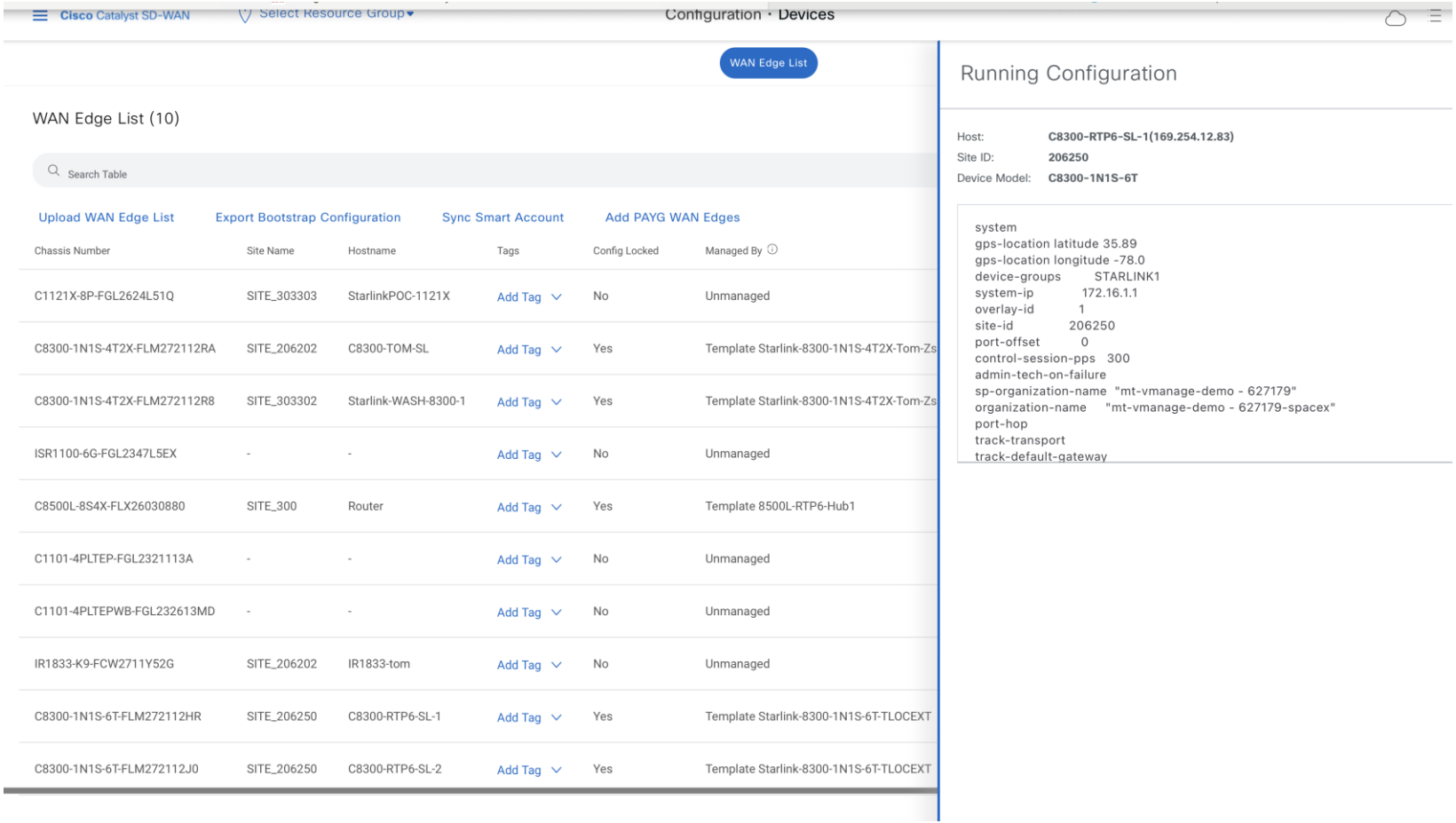
Manager Validator

Controllers

- SD-WAN version 17.x
- Hub and spoke topology with ODT
- Per-tunnel/adaptive QoS
- Application Aware Routing
- IPSec tunnels to SIG
- DIA with FW/DNS-Sec
- WAN Opt/DRE (TBD)
- FEC/Packet Dup (TBD)



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

SD WAN Configuration

```
interface GigabitEthernet0/0/0
 description   Ethernet to Starlink LEO satellite
 no shutdown
 arp timeout 1200
 ip address dhcp client-id GigabitEthernet0/0/0
 no ip redirects
 ip tcp adjust-mss 1360
 ip dhcp client default-router distance 1
 ip mtu    1500
 ip nat outside
 load-interval 30
 mtu          1500
 negotiation auto
```

```
interface Tunnel100201
 no shutdown
 ip unnumbered       GigabitEthernet0/0/0
 no ip clear-dont-fragment
 ip mtu              1400
 tunnel source GigabitEthernet0/0/0
 tunnel destination dynamic
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile if-ipsec201-ipsec-profile
 tunnel vrf multiplexing
 tunnel route-via GigabitEthernet0/0/0 mandatory
exit
interface Tunnel100202
 no shutdown
 ip unnumbered       GigabitEthernet0/0/0
 no ip clear-dont-fragment
 ip mtu              1400
 tunnel source GigabitEthernet0/0/0
 tunnel destination dynamic
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile if-ipsec202-ipsec-profile
 tunnel vrf multiplexing
 tunnel route-via GigabitEthernet0/0/0 mandatory
exit
```


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

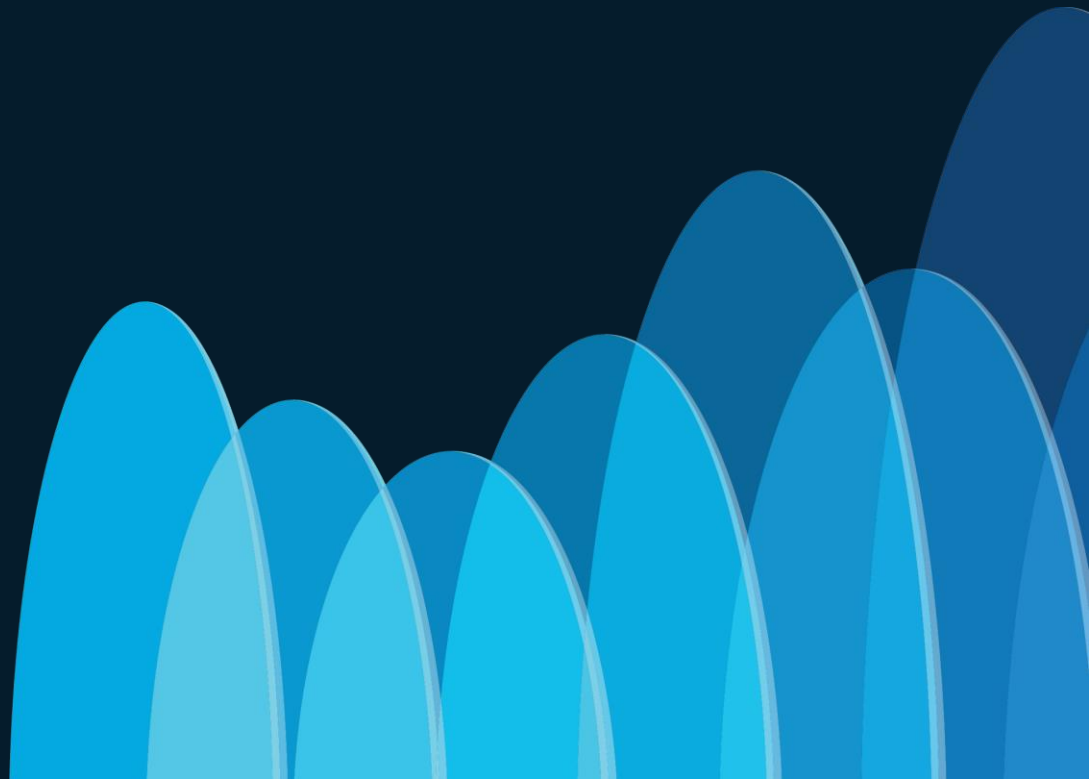
Crypto Configuration

```
crypto ikev2 policy policy1-global
 proposal p1-global
!
crypto ikev2 profile if-ipsec201-ikev2-profile
 no config-exchange request
 dpd 60 10 on-demand
 dynamic
 lifetime 14400
!
crypto ikev2 profile if-ipsec202-ikev2-profile
 no config-exchange request
 dpd 60 10 on-demand
 dynamic
 lifetime 14400
!
crypto ikev2 proposal p1-global
 encryption aes-cbc-128 aes-cbc-256
 group 14 15 16 19 20 21
 integrity sha1 sha256 sha384 sha512
```

```
crypto ipsec transform-set if-ipsec201-ikev2-transform esp-null esp-sha-hmac
 mode tunnel
!
crypto ipsec transform-set if-ipsec202-ikev2-transform esp-null esp-sha-hmac
 mode tunnel
!
crypto ipsec profile if-ipsec201-ipsec-profile
 set ikev2-profile if-ipsec201-ikev2-profile
 set transform-set if-ipsec201-ikev2-transform
 set security-association lifetime kilobytes disable
 set security-association lifetime seconds 3600
 set security-association replay window-size 1024
!
crypto ipsec profile if-ipsec202-ipsec-profile
 set ikev2-profile if-ipsec202-ikev2-profile
 set transform-set if-ipsec202-ikev2-transform
 set security-association lifetime kilobytes disable
 set security-association lifetime seconds 3600
 set security-association replay window-size 1024
```


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Design optimizations for LEO Satellite Transport



cisco Live!

Reducing SD-WAN control plane traffic on Satellite links

Problems

LEO satellite have low transmit speeds (2-20 Mbps up) relative to download speeds of 25-220 Mbps down). SD-WAN control traffic can consume a high proportion of this bandwidth in heavily meshed topologies with default timers. This includes:

- BFD probes over each IPSec tunnel (2.2 Kbps per SD-WAN tunnel)
- OMP hellos and updates to/from Catalyst controllers (up to 80 Kbps)
- Statistics upload to the Catalyst Manager (up to 1.2 Mbps)

Control traffic is automatically mapped to Q0 on the WAN edge, which can contend with user realtime traffic also in Q0 resulting in drops and instability

Solutions

- Dynamic OnDemand tunnel design (reduces # of BFD sessions)
- BFD low bandwidth link
- Last-resort-circuit in cases where Starlink is for backup
- vManage connection preference 1
- Administration Settings for Statistics – disable some, all or vAnalytics only?
- QoS design with Adaptive QoS and 2-level policer / Split LLQ

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Tunnel Optimizations for low bandwidth links

Low bandwidth link: Reduces BFD overhead by 50% per tunnel

Last-Resort-Circuit: No tunnel or traffic unless all other transports down

vManage connection preference 1: Prefer terrestrial (if available) over Satellite for vManage control connections to reduce overhead of statistics publishing.

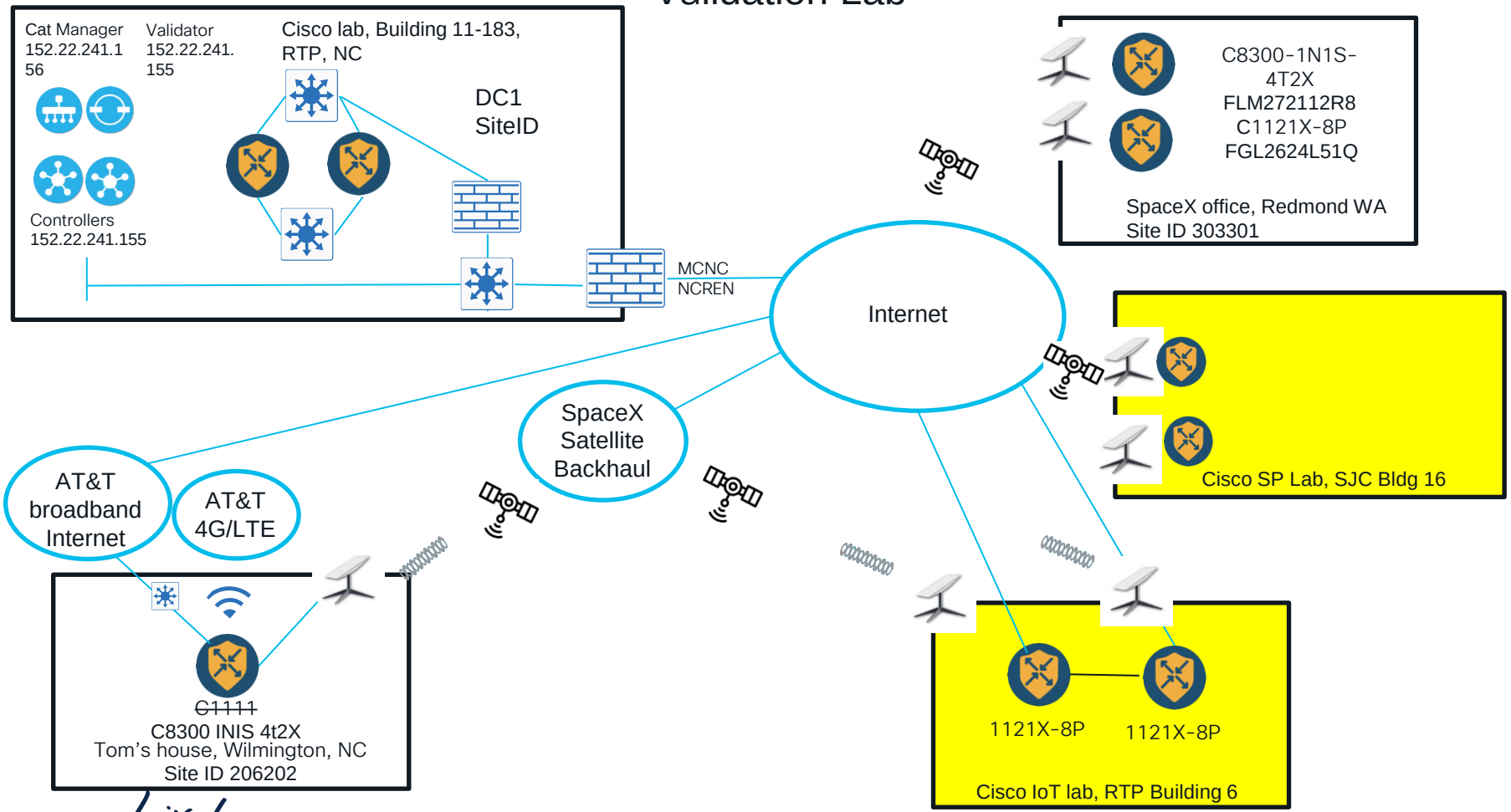
OMP Hello tuning: Reduce Hello-interval to further optimize bandwidth

```
sdwan

 interface GigabitEthernet 0/1/0
Description connected to Starlink
  tunnel-interface
   encapsulation ipsec weight 1
   no border
   color
   no last-resort-circuit
   low-bandwidth-link
   hello-interval              6000
   hello-tolerance              600
   vmanage-connection-preference 1
```


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Validation Lab

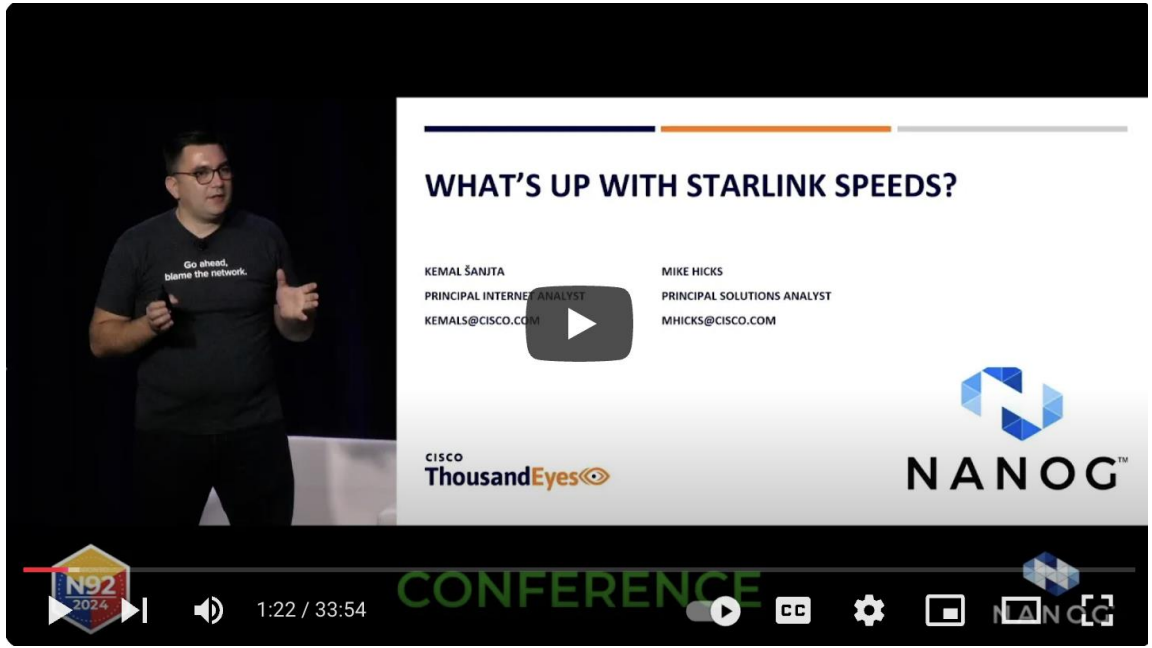


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Starlink Network Performance with Thousand Eyes

cisco Live!

Thousand Eyes Testing of the Starlink Network



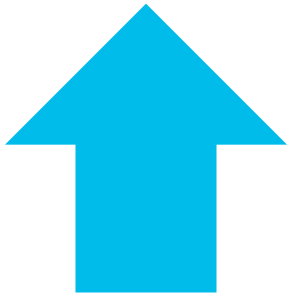
https://www.youtube.com/watch?v=bR99OxQTRuc&t=82s

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

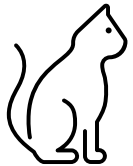
Quantum Resistance and Post Quantum Encryption with Starlink

cisco Live!

Serious talk about Quantum Realities



And I am not talking about Schrodinger's cat



*Or the Multiverse

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Starlink (and LEO) is a generational asymmetric advantage

Leaning forward and coupling it with quantum safe cryptography represents an equivalent generational security event

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Nation State Adversaries have serious concerns about Starlink and about breaking encryption

Chinese scientists hack encryption in quantum computer experiment: paper

Breakthrough poses a ‘real and substantial threat’ to password-protection mechanism employed across critical sectors, team says

Reading Time: **2 minutes**

Why you can trust SCMP

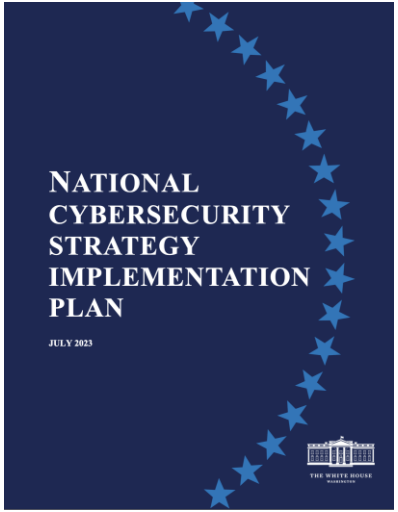
17

Listen

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

- US Government has provided clear direction for requirements on Quantum Resistance for protection of National Security Systems
  - (ref: NCSIP and NSM-10)
- Quantum Key Distribution is an open topic and lacks standards
- Cisco SKIP should be an acceptable interim option
- All aspects of encryption should drive towards Quantum Resistance encryption options
- Site to Site VPN, VPN Client along with TLS stack implementations for control plane operations

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public



Strategic Objective 4.3: Prepare for Our Post-Quantum Future

Initiative Number: 4.3.1

Initiative Title: Implement National Security Memorandum-10

The Predicate

Initiative Description

The Office of Management and Budget and the National Manager for National Security Systems, in coordination with ONCD, will continue to prioritize implementation of National Security Memorandum-10 and transitioning vulnerable public networks and systems to quantum-resistant cryptography-based environments, focusing first on Federal information systems and NSS. OMB will work with NIST to develop complementary mitigation strategies to provide cryptographic agility in the face of unknown future risks.

NCS Reference

The Federal Government will prioritize the transition of vulnerable public networks and systems to quantum-resistant cryptography-based environments and develop complementary mitigation strategies to provide cryptographic agility in the face of unknown future risks.

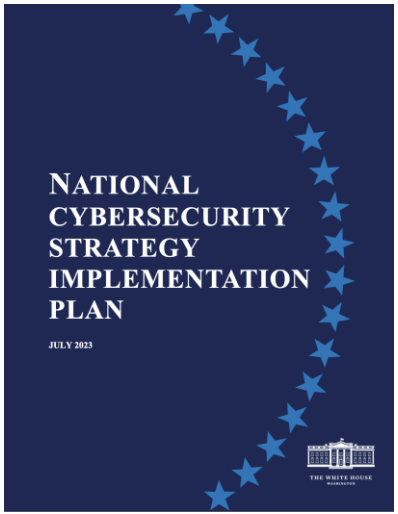
Responsible Agency: OMB

Contributing Entities: NSA, ONCD

Completion Date: 1Q FY25

First Quarter, next year!

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public



★ ★ ★ ★ ★ ★

Initiative Number: 4.3.2
Initiative Title: Implement NSM-10 for National Security Systems (NSS)

Initiative Description

Implement the transition of NSS to quantum-resistant cryptography.

NCS Reference

The Federal Government will prioritize the transition of vulnerable public networks and systems to quantum-resistant cryptography (QRC)-based environments and develop complementary mitigation strategies to provide cryptographic agility in the face of unknown future risks.

Responsible Agency: NSA

Contributing Entities: DOD, ODNI

Completion Date: 3Q FY25

QR Mandatory

3rd Quarter, 2025

Initiative Number: 4.3.3
Initiative Title: Standardize, and support transition to, post-quantum cryptographic algorithms

Initiative Description

The National Institute of Standards and Technology will finalize its process to solicit, evaluate, and standardize one or more quantum-resistant public-key cryptographic algorithms. New public-key cryptography standards will specify one or more additional unclassified, publicly-disclosed digital signature, public-key encryption, and key-establishment algorithms that are available worldwide, and are capable of protecting sensitive government information well into the foreseeable future, including after the advent of quantum computers.

NCS Reference

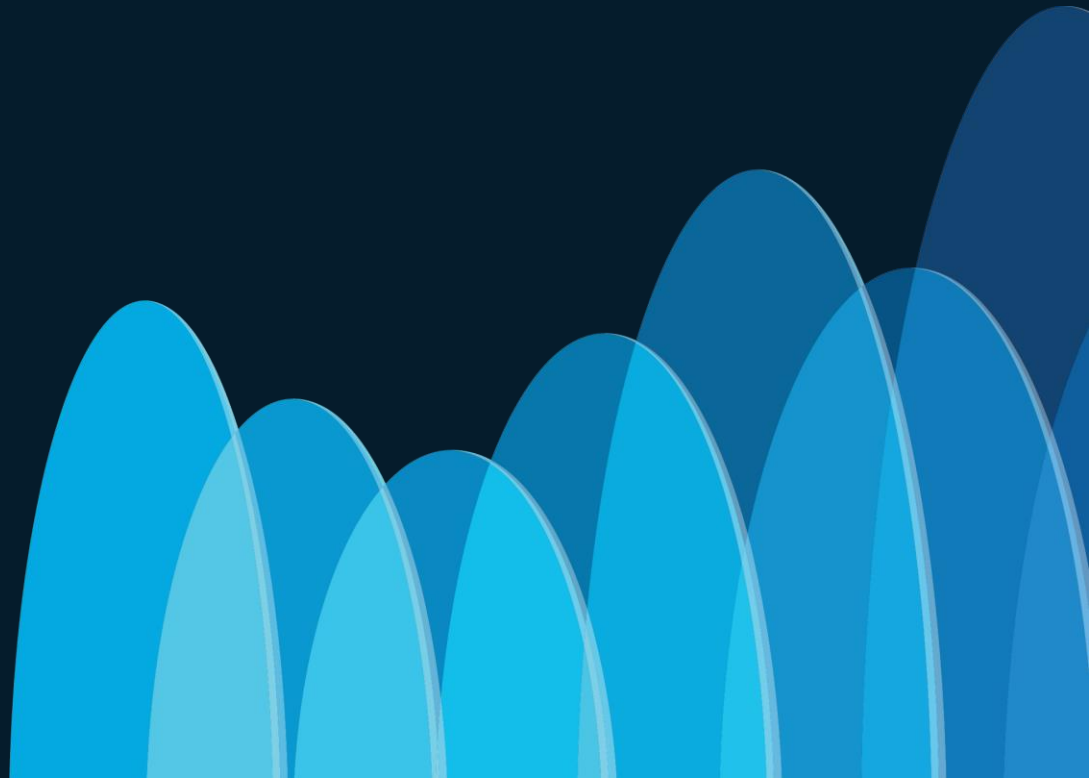
To balance the promotion and advancement of quantum computing against threats posted to digital systems, National Security Memorandum (NSM) 10, "Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems," establishes responsibilities and oversight to enable a timely transition of the country's cryptographic systems to interoperable quantum-resistant cryptography.

Responsible Agency: NIST

Completion Date: 1Q FY25

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Quantum Primer



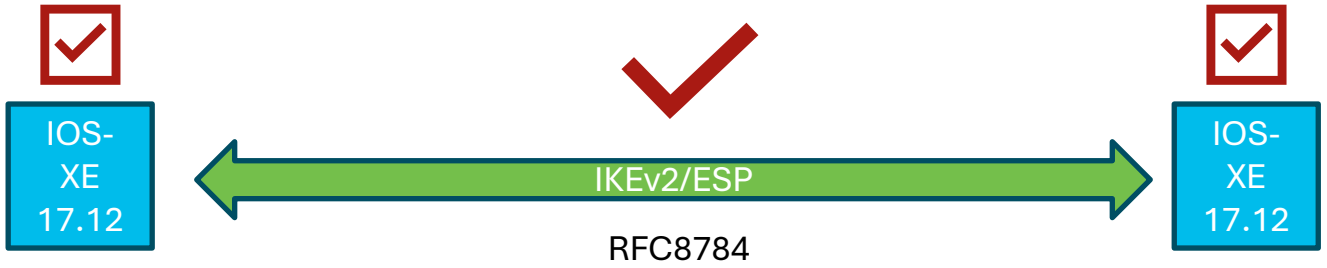
cisco Live!

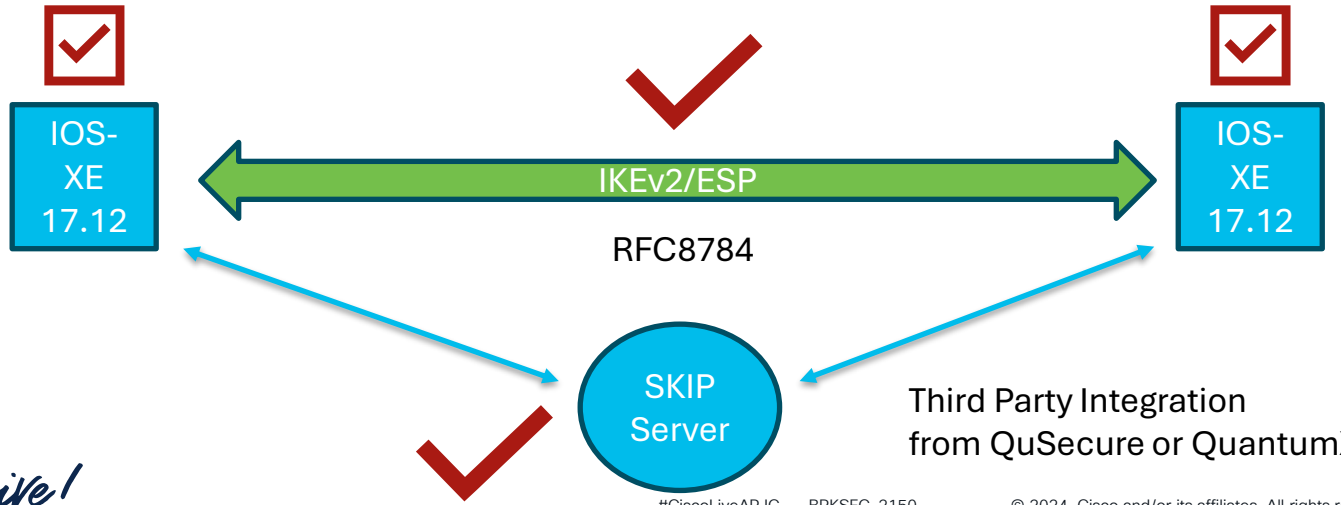
Quantum Primer

- SSH, TLS 1.3 and IKEv2
- RFC 8784
- RFC 9242
- RFC 9370
- Future FIPS 203, 204, 205
- Future TLS1.3+PQ
- Future IKEv2+PQ
- Future SSH+PQ

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco IOS-XE Based Catalyst Routers

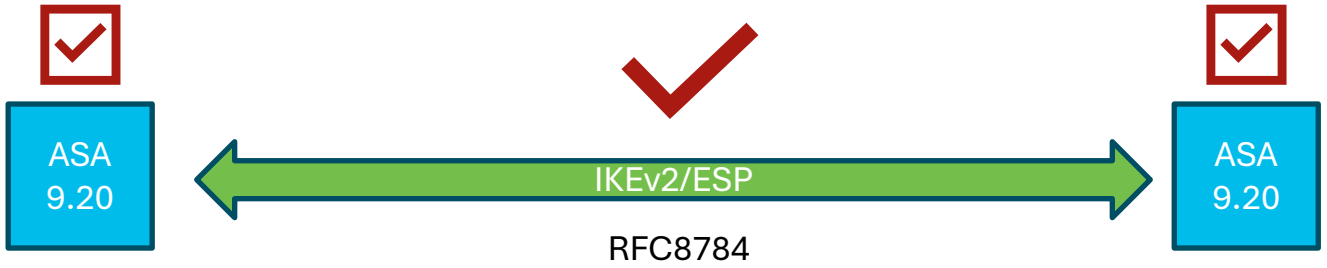


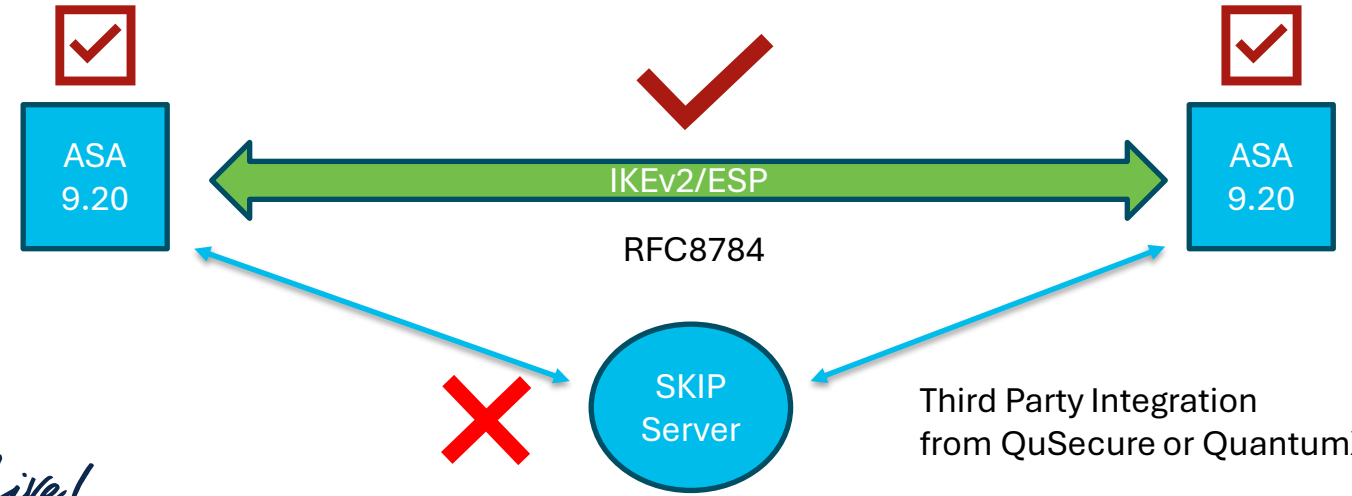


Third Party Integration
from QuSecure or QuantumXchange

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

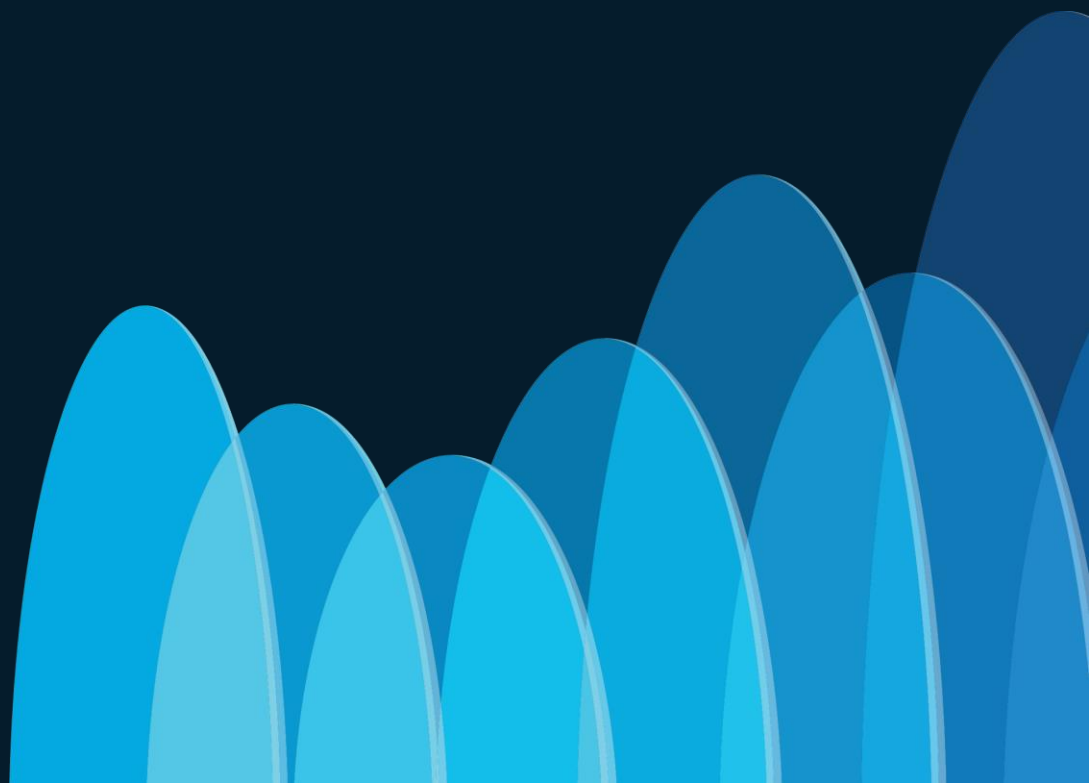
Cisco ASA Firewalls





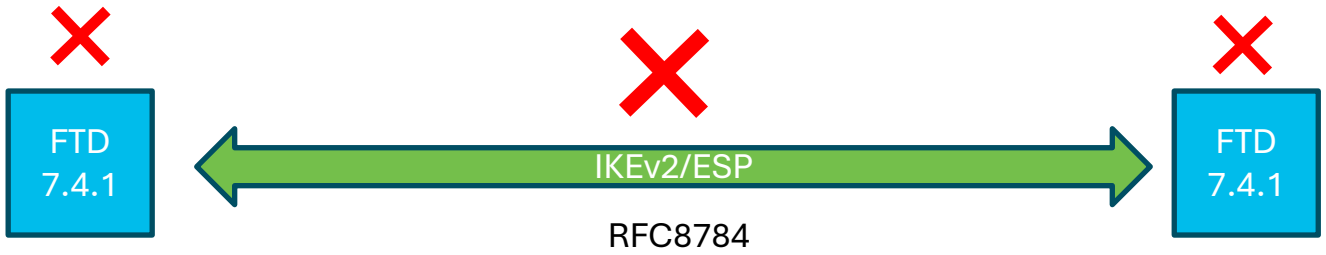
Third Party Integration
from QuSecure or QuantumXchange

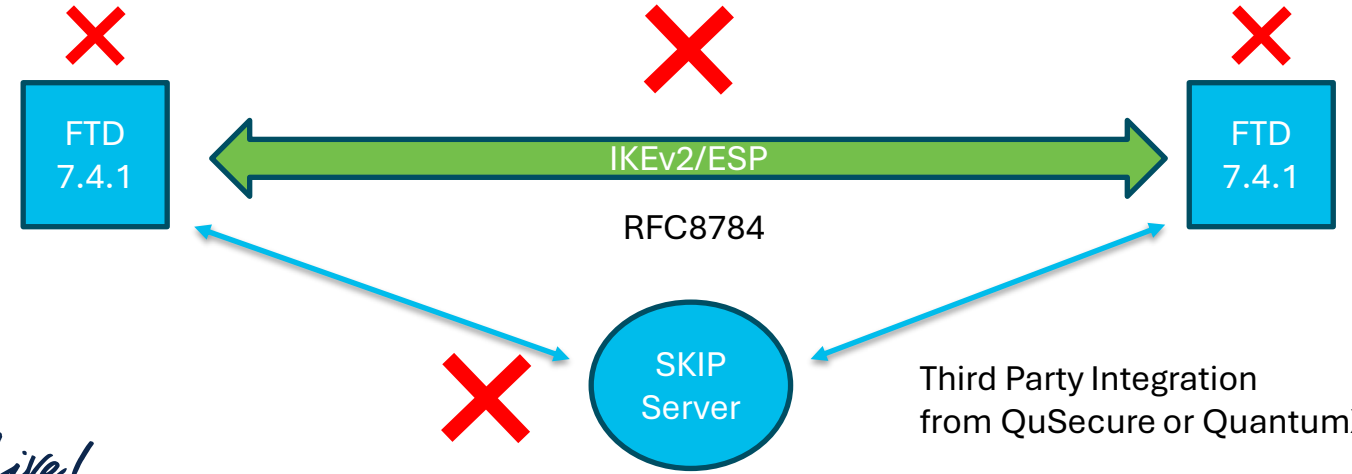
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public



Firepower – FTD

Cisco FTD Based Firewalls





Third Party Integration
from QuSecure or QuantumXchange

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

SKIP IETF

draft-cisco-skip-00

Internet Engineering Task Force
Internet-Draft
Intended status: Informational
Expires: 3 March 2025

R. Singh, Ed.
C. Hill
Cisco Systems, Inc.
S. Kawaguchi
J. Lupo
QuSecure, Inc.
30 August 2024

Secure Key Integration Protocol (SKIP)
draft-cisco-skip-00

Abstract

This document specifies the Secure Key Integration Protocol (SKIP), a two-party protocol that allows a client to securely obtain a key from an independent Key Provider. SKIP enables network and security operators to provide quantum-resistant keys suitable for use with quantum-resistant cryptographic algorithms such as AES-256. It can also be used to provide an additional layer of security to an already quantum-resistant secure channel protocol for a defense-in-depth strategy, and/or enforce key management policies.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

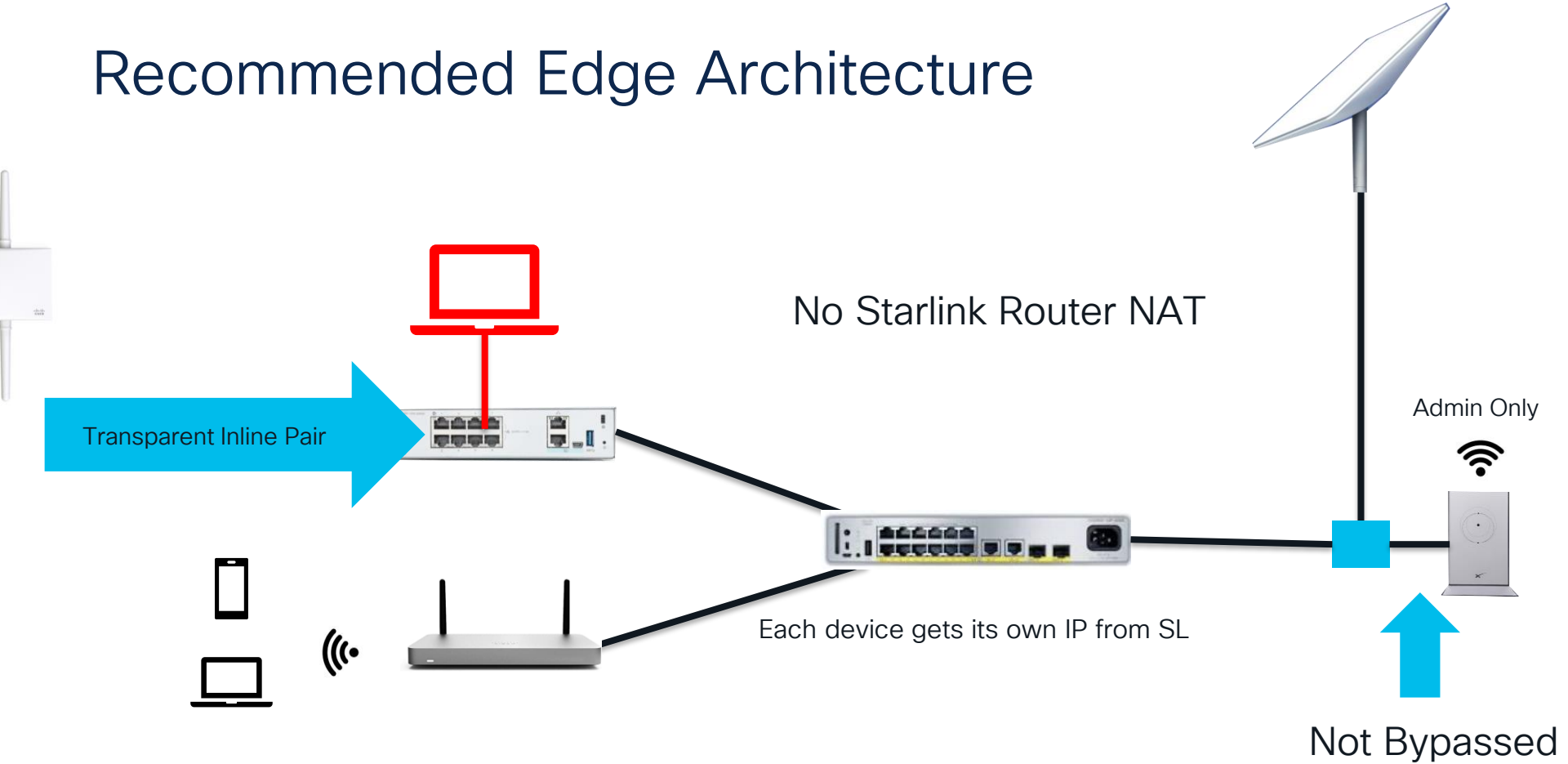
This Internet-Draft will expire on 3 March 2025.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Ground/Space Security Architectures

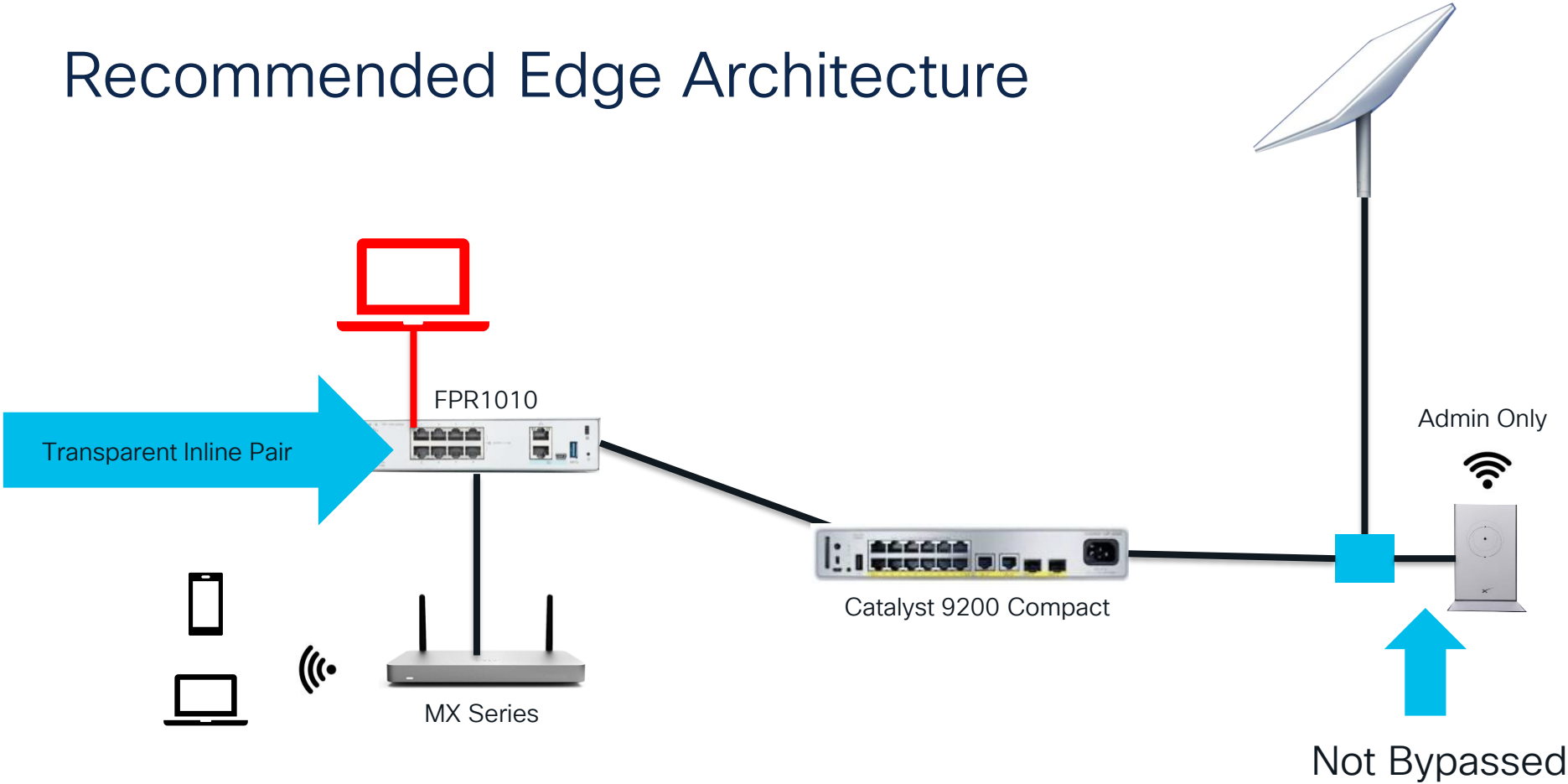
cisco Live!

Recommended Edge Architecture



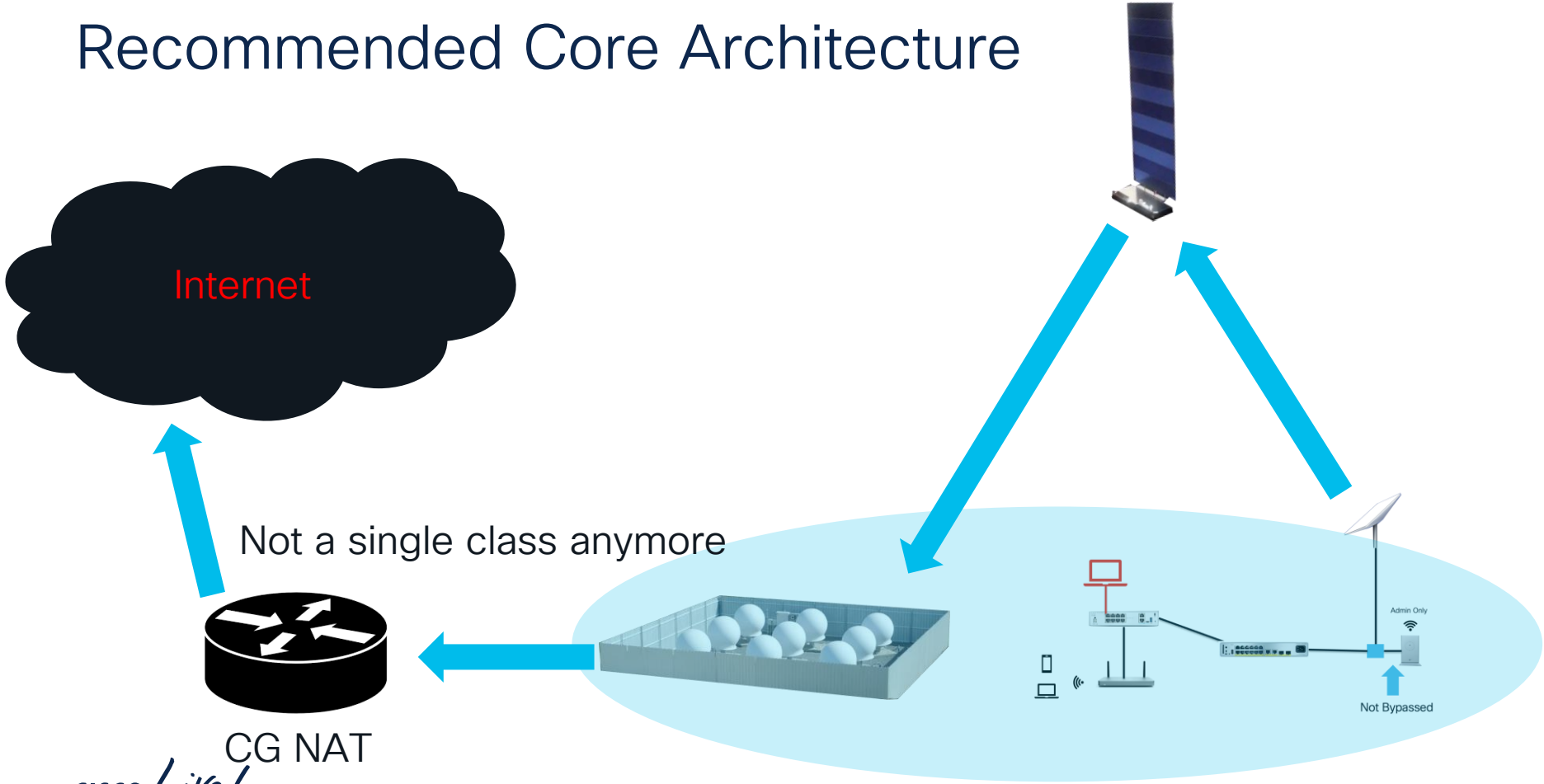
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Recommended Edge Architecture



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Recommended Core Architecture



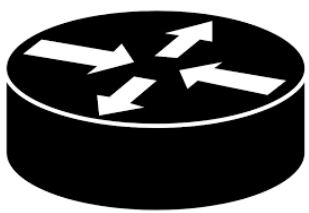
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

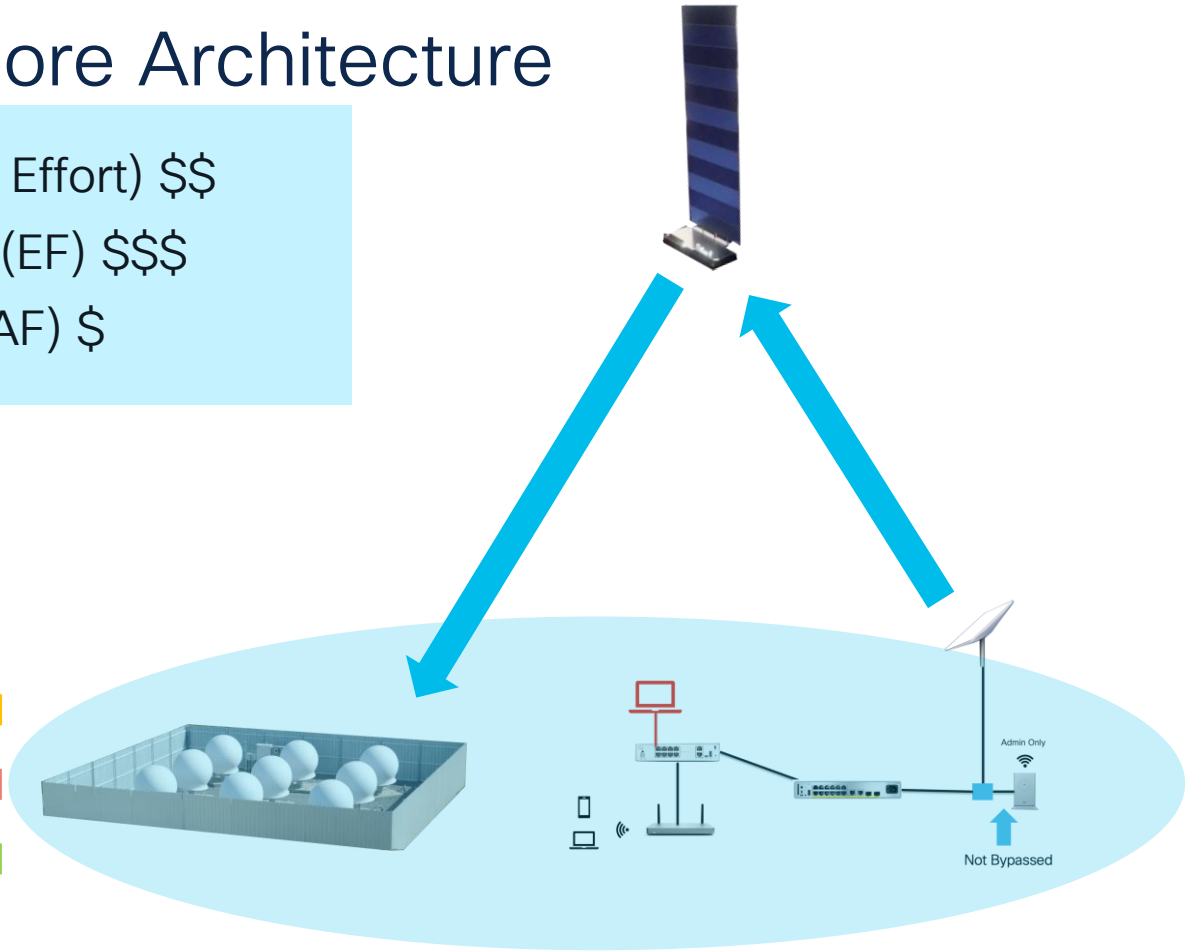
Recommended Core Architecture

Mobile (Best Effort) $$

Priority Data (EF) $$$

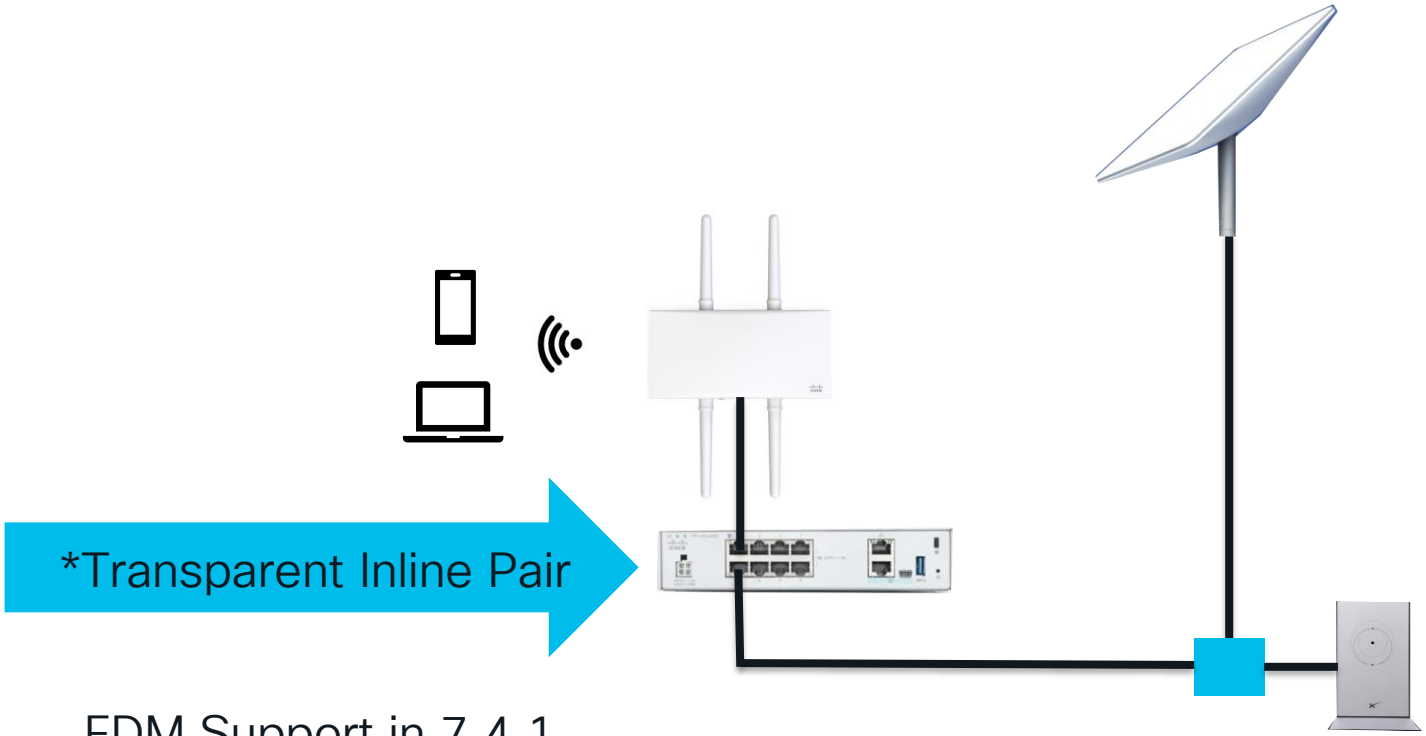
Residential (AF) $





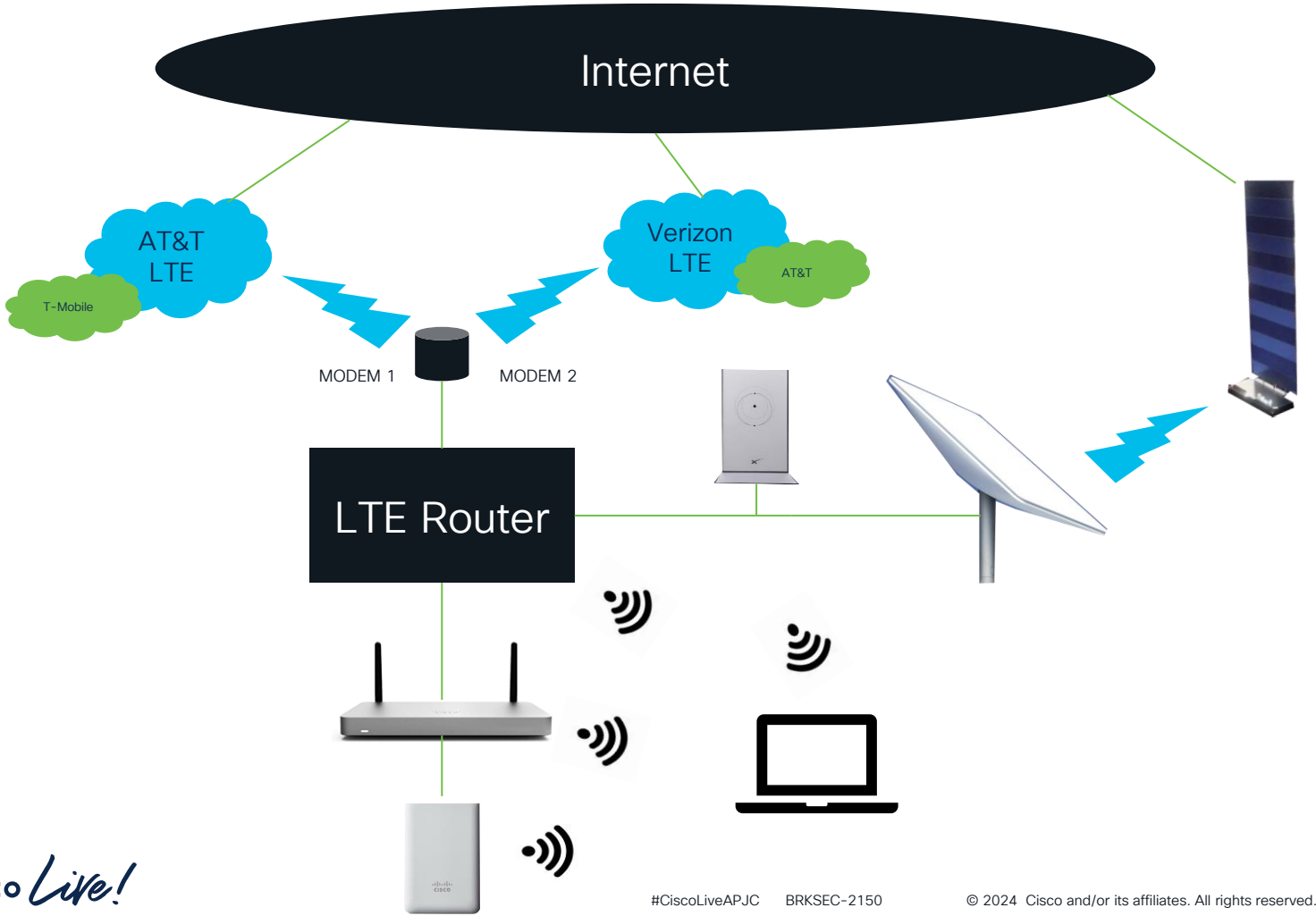
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Recommended Architecture



FDM Support in 7.4.1

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

When Starlink goes down for 20 minutes

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Please Fill Out The Survey!

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

cisco Live!

Keynote Deep Dives

Wednesday
10:30am –11:30am

Experiences Amplified: How AI Can Fuel Better Employee and Customer Experiences

Level 1
Room 106

Smart, Secure, Seamless: Transforming Experiences with Next-Generation Networking

Level 2
Room 204

Harness a Bold New Era: Transform Data Centre and Service Provider Connectivity

Level 2
Room 203

Securing User to Application and Everything in Between

Level 2
Melbourne Room 2

Unlocking Digital Resilience through Unified Observability

The HUB
Centre Stage

#CiscoLiveAPJC

Complete Your Session Evaluations

Complete a minimum of 4 session surveys and the Overall Event Survey to claim a **Cisco Live T-Shirt**.

Complete your surveys in the **Cisco Live mobile app**.

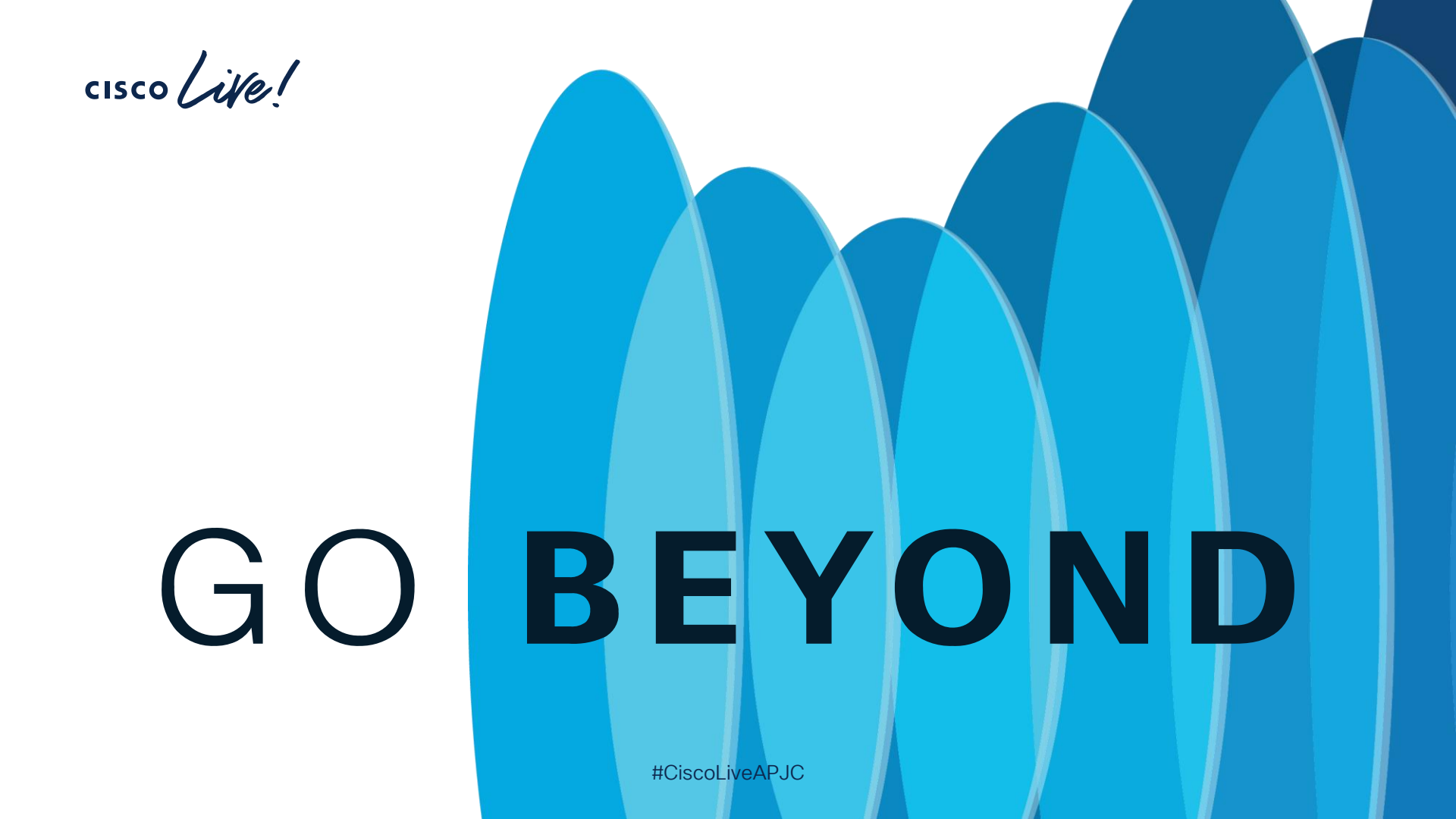
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Continue your education

- Visit the Cisco Stand for related demos
- Book your one-on-one Meet the Expert 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

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

cisco
Thank you
cisco Live!
#CiscoLiveAPJC


cisco Live!
GO BEYOND
#CiscoLiveAPJC