



pervasivet^echnologylabs
AT INDIANA UNIVERSITY

www.pervasivetchnologylabs.iu.edu

IPv6 from an Abilene Perspective

Gregory Travis
Indiana University
greg@iu.edu



pervasivetechlabs
AT INDIANA UNIVERSITY

www.pervasivetechlabs.iu.edu

What's Abilene?

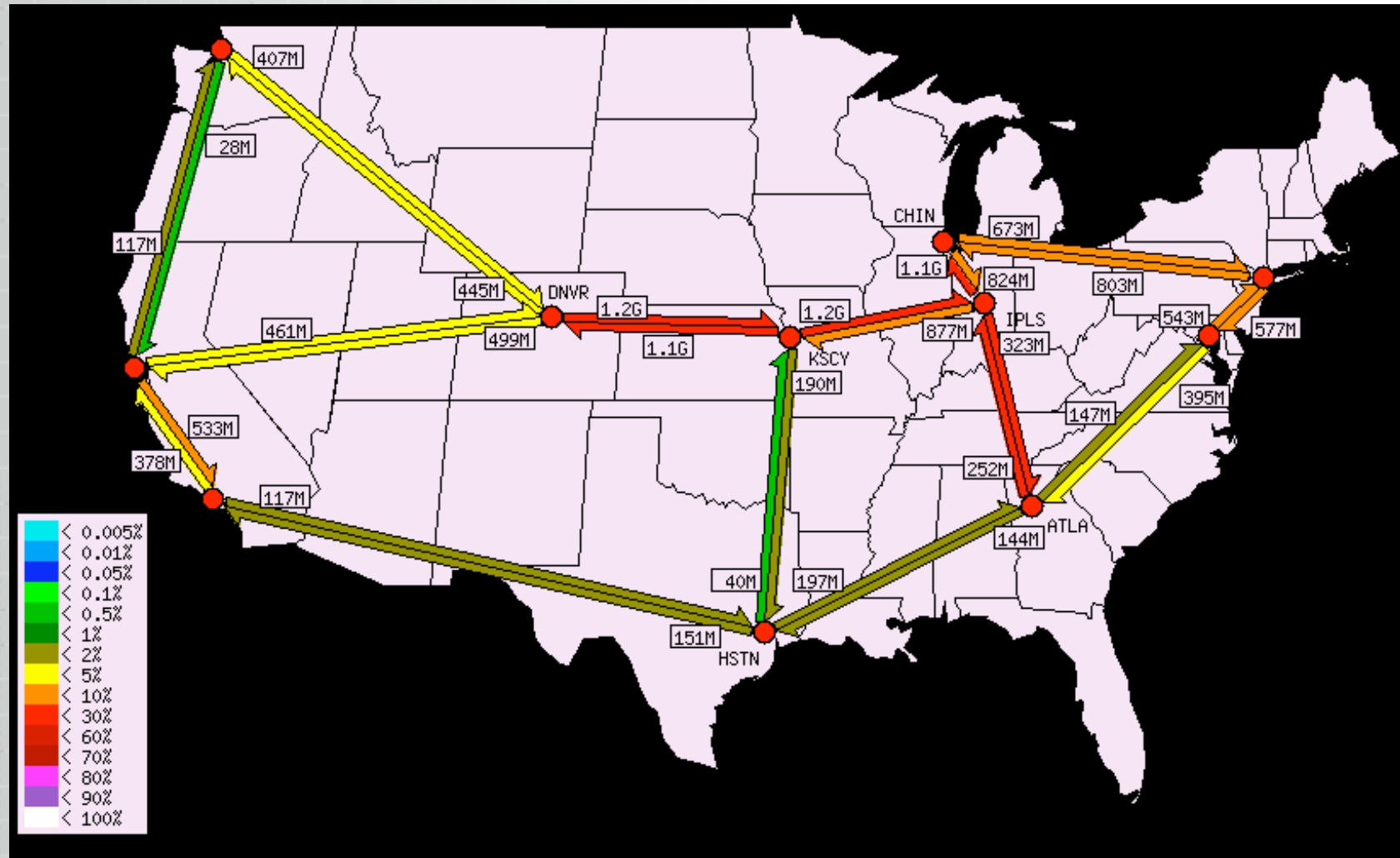
- Physical network, sometimes known as “Internet2”
 - Internet2 is actually the collection of participating institutions, Abilene is the physical network
- Created in acknowledgement that the Internet had “gone commercial” but there was still a need for non-comm research network



pervasivetechlabs
AT INDIANA UNIVERSITY

www.pervasivetechlabs.iu.edu

Abilene Logical





pervasivetechlabs
AT INDIANA UNIVERSITY

www.pervasivetechlabs.iu.edu

Abilene Structure

- Originally built out using Qwest fiber facilities (this is still true) and Cisco “core” routers
- Now consists of Juniper T640 core routers (the red dots)
- All connections between routers are over OC192 (nominally ~10Gb/s)



pervasivetechlabs
AT INDIANA UNIVERSITY

www.pervasivetechlabs.iu.edu

Abilene traffic

- Institutions/Corporations/etc connect via Abilene “gigapops” -- the red dots.



pervasivetechlabs
AT INDIANA UNIVERSITY

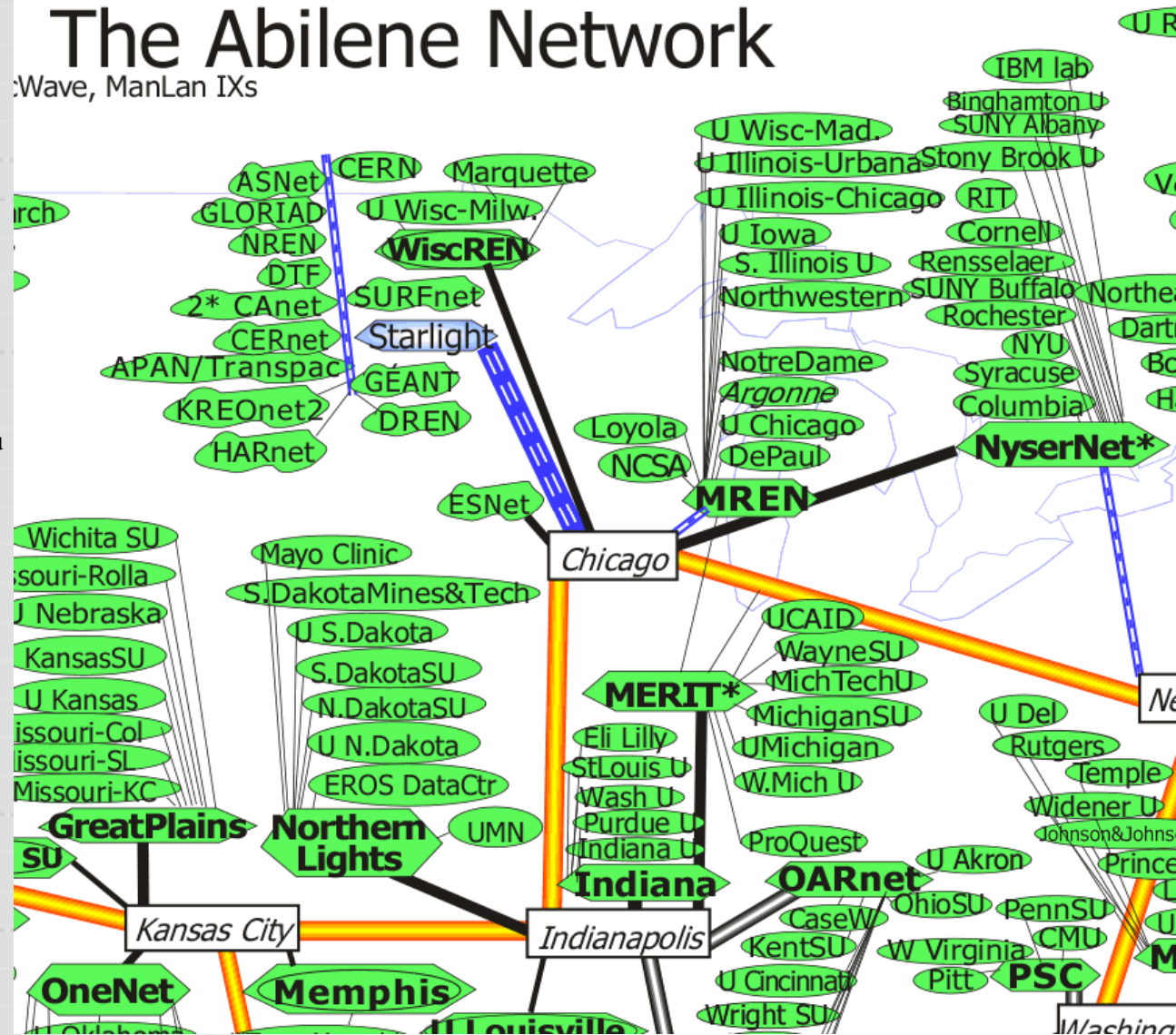
www.pervasivetechlabs.iu.edu

traceroute to rl.af.mil

- 1 156.56.103.253
- 2 ul-iub.indiana.gigapop.net
- 3 abilene-ul.indiana.gigapop.net
- 4 chinng-iplsng.abilene.ucaid.edu
- 5 ge-0-1-0.starlight.dren.net
- 6 t3-0-0-0.rome.dren.net
- 7 cperouter.rome.dren.net

The Abilene Network

Wave, ManLan IXs





pervasivetechlabs
AT INDIANA UNIVERSITY

www.pervasivetechlabs.iu.edu

Who's on Abilene?

- You are!
- Lots of government, research, corporations, etc.
- In almost all cases, if two organizations both have Abilene connections, in addition to other network connections, traffic between them will flow over Abilene
- Abilene also provides significant “transit” services
 - E.g. between Europe and Asia



pervasivetechlabs
AT INDIANA UNIVERSITY

www.pervasivetechlabs.iu.edu

Abilene Services

- Abilene natively supports several “advanced” services:
 - Multicast
 - QoS (Quality of Service)
 - IPv6!



pervasivet^echnologylabs
AT INDIANA UNIVERSITY

www.pervasivetchnologylabs.iu.edu

IPv6



pervasivetechlabs
AT INDIANA UNIVERSITY

www.pervasivetechlabs.iu.edu

"our soldiers need better information in order to make better decisions -- who to help and who to kill. The lack of security and flexibility in the current IPv4 protocol is a drag on our wing. This isn't about do you trust the Internet for your kid's homework, it's do you trust your kid's life. If we fail, people die."

- Defense Department Will Require IPv6 Compliance, Says DoD's John Osterholz. Market Wire, June 26, 2003.

In the long run DoD's transition to IPv6 will

- Maintain the ability to support the end-to-end model of internetworking
- Offer more options for mobile communications
- Provide flexibility in allocation of network addresses
- Accelerate US industry competitiveness in advanced networking

In the near term, a transition to IPv6 will

- Increase the challenge to provide network security
- Increase the overall complexity of the network and its operations
- Increase downtime and instability of the network
- Require re-training of networking staff
- Require re-writing of applications
- Probably change network design strategy to accommodate limitations in current equipment

In the short term, a transition to IPv6 will

- Increase the hype from equipment and software vendors
- Make it more difficult to evaluate specifications to determine their IPv6 support
- Reduce network security
- Reduce the working life of new equipment purchased
- Increase the risk of *spectacular failures*

Key differences in IPv6 itself

- The addresses are longer (128bits vs. 32)
 - + no need to use NATs to increase usable IP space
 - + possible to preserve end-to-end model
 - + more flexible support of IP option headers
 - + use of multicast rather than broadcast in the LAN
 - + no need for IP fragmentation in network devices
 - could lead to explosion in routing table size
 - addresses take more special memory in routing equipment (e.g., TCAMS)
 - more flexible support of IP option headers
 - harder to optimize for low bandwidth connections and resource limited devices (e.g., sensors, PDAs, cell phones)

Key differences in today's IPv6 implementations

- Eight years ago the industry starting putting IPv4 functions in ASICs, generally, this is not yet the case for IPv6. This translates to slower firewalls, encryption hardware, routers, switches, and end-systems.
- There are lots of layer 3 snooping functions in layer 2 equipment (more later)
- IPv6 implementations mean newer, less tested, more complex code.
- Despite purchasing pressure from the DoD and Asia, IPv6 still treated as an extra feature, not a core requirement

IPv6 support needed where it shouldn't be (layer 2 devices)

- IP is a network layer protocol that sits above a data link layer like Ethernet
- In theory IP and Ethernet are separate, such that Ethernet-only devices like switches need not support IP
- Five years ago vendors starting adding *value* to their Ethernet switches that included snooping IP information
- This snooping allowed the switches to better support IP multicast, enforce security policies, enhance management, QoS, etc.

IPv6 support in layer 2 devices

- Somehow this issue has slipped under the radar for vendors and IPv6-savvy customers
- Increasingly important as strategies for network security evolve
- Single mostly likely component to prevent migration away from IPv4
- Very difficult to define what IPv6 compliant means in this space
- Does not easily map to IETF standards
- Often is the most expensive part of the network to replace

IPv6 support in layer 2 devices (cont.)

- Practices evolving to quarantine network devices until they are known to be patched/up to date, preventing IP spoofing, providing edge QoS, correctly forwarding IP multicast, and E911 support for VoIP applications are some of the examples of layer 2 devices snooping layer 3 information to perform critical functions
- Support for IPv6 in this space is not currently a priority for vendors, technically their layer 2 devices are IPv6 ready now (sans the added features)



pervasivetechlabs
AT INDIANA UNIVERSITY

www.pervasivetechlabs.iu.edu

Suggestion

- DoD needs to establish a set of specific criteria for evaluating the IPv6 readiness of layer 2 equipment.
- Standards bodies (e.g., IEEE and the IETF) need to formally acknowledge this overlap of layers
- Selecting layer 2 equipment (Ethernet switches) will be the most complex part of a purchasing program designed to enable IPv6 transition (next hardest will be VoIP equipment)



pervasivetechlabs
AT INDIANA UNIVERSITY

www.pervasivetechlabs.iu.edu

Supports IPv6

- Means different things. Let's examine a real issue of IPv6 support in two different vendor's core routers, Cisco and Juniper
- The test scenario: define and apply a filter to IPv6 TCP packets destined for port 139
- Remember that IPv6 has support for option headers that are at different positions in the packet



pervasivetechlabs
AT INDIANA UNIVERSITY

www.pervasivetechlabs.iu.edu

Supports IPv6 (cont.)

- The access list will cause the Cisco GSR, regardless of line card to send all IPv6 packets to which the filter applies to be processed by the central CPU, rather than being forwarded at high speed.
- The Juniper will forward the filtered packets at line-speed.
- The Juniper is better, right? Perhaps not...



pervasivetechlabs
AT INDIANA UNIVERSITY

www.pervasivetechlabs.iu.edu

Supports IPv6 (cont.)

- The Juniper can filter at line-speed in part because it assumes that the TCP header will be the first header in the IPv6 packet. If it's not, if there is an option header before the TCP header, the Juniper filter will fail to match.
- The Cisco will search through the headers until it finds the TCP header, then make the right forwarding decision.
- Both strategies have their advantage, but they are both very different. Both vendors support IPv6 filtering, but in extremely different ways

IPv6 Doesn't fix everything

- A recent survey of CERTs top 100 vulnerabilities shows only 1 to be specific to IPv6, the rest are accessible via IPv4
- True the exploits might requiring different host discovery strategies, the host vulnerabilities exist for IPv4
- A host vulnerable to the slammer worm, is also vulnerable to an IPv6 packet using the same bug to run arbitrary code on the target machine
- Spyware, stack over flow vulnerabilities, e-mail worms, etc., are NOT fixed with IPv6!

There's nothing about IPv6 that's security related

- There's nothing in the packet that adds to IPv6 security relative to IPv4
- IPsec exists and is functionally the same for both IPv4 and IPv6
- IPv6 has no additional QoS features (although some would argue that the unused flow label is such a feature)
- IPv6 offers no performance improvements over IPv4
- IPv6 is about more addresses and some mobility features

More Addresses is a Big Deal

- If the Internet is to preserve its end-to-end model, then eventually IPv6 will be needed
- However, increasingly security practices are leaning towards breaking the end-to-end model in favor of better security mechanisms
- NATs do provide a layer of security, and they do completely break the end-to-end model
- There will be IPv6 NATs



pervasivetechologylabs
AT INDIANA UNIVERSITY

www.pervasivetechologylabs.iu.edu

Experience

- Today's use of the Internet Protocol is the result of decades of experience and sometimes painful teeth cutting. IPv6 will set us back. Fortunately it will also set the hackers back
- The DoD has a mixed track record for driving the adoption of standards in networking, history would suggest a bit of caution in assuming that DoD procurement incentive will accelerate the broader adoption of a new protocol (remember OSI)



pervasivetechlabs
AT INDIANA UNIVERSITY

www.pervasivetechlabs.iu.edu

IPv6 Best Practices

Q: If I ran an IPv6 network, what are some best practices to consider?

A: We're not sure. There is a very good first stab at this in a document titled "IPv6 and IPv4 Threat Comparison and Best-Practice Evaluation (v1.0)" by Sean Convery and Darrin Miller of Cisco. You can retrieve a copy via

www.cisco.com/security_services/ciag/documents/v6-v4-threats.pdf



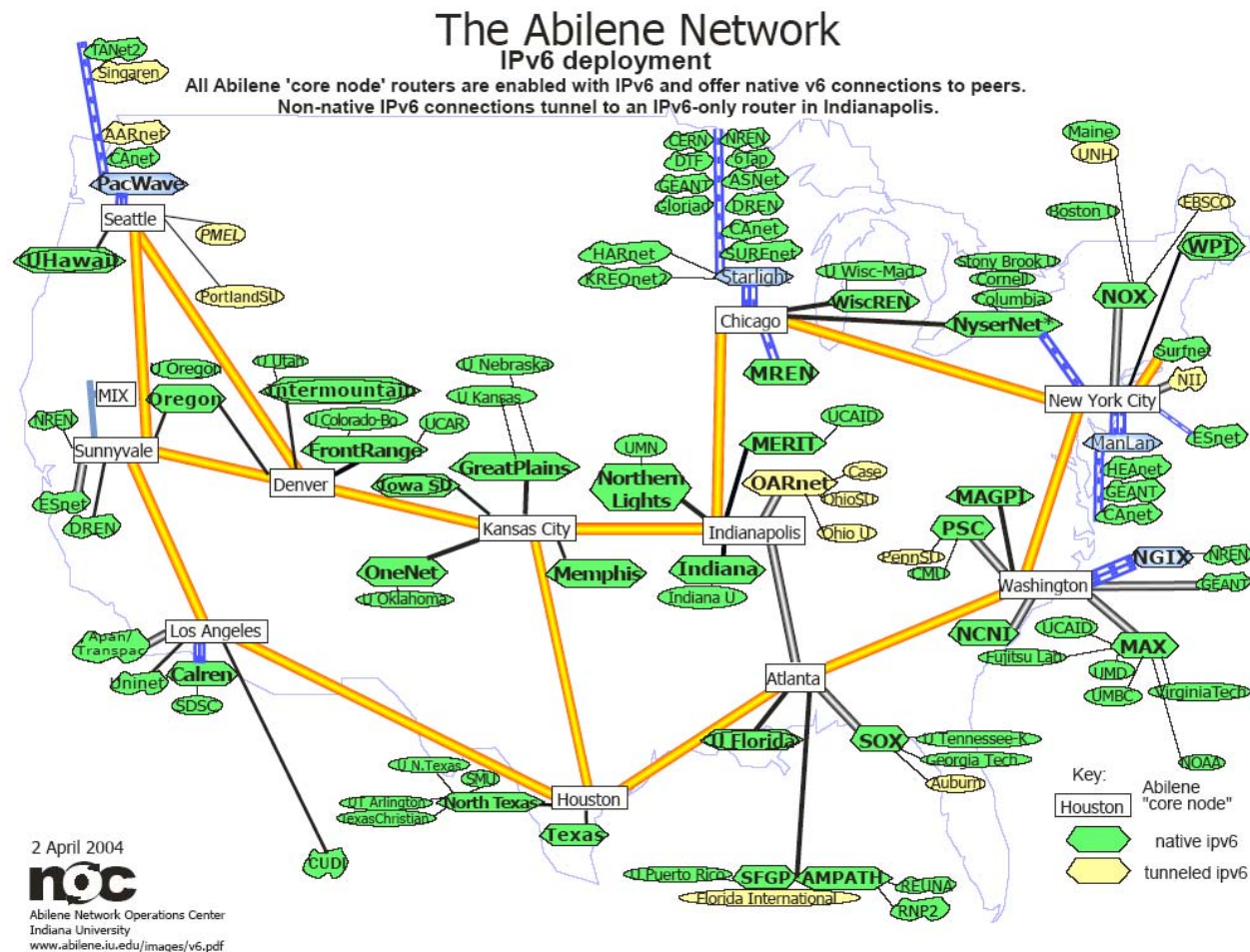
pervasivetechlabs
AT INDIANA UNIVERSITY

www.pervasivetechlabs.iu.edu

Who's running IPv6 now

- A few ISPs in the US offer IPv6 (Qwest is one)
- There are numerous test beds in Japan
- The US R&E network infrastructure (I.e. Abilene), and its counterparts in Europe and the Pacific rim have a large, high-speed, dual stack inter-network of native IPv6

The Internet2/Abilene IPv6 network



Examples of IPv4/IPv6 routes

www.pervasivetechlabs.iu.edu

traceroute to orange.kame.net (203.178.141.194), 30 hops max, 40 byte packets

```
1 156.56.103.253 (156.56.103.253) 2.029 ms 1.979 ms 1.589 ms
2 ul-iub.indiana.gigapop.net (192.12.206.65) 2.306 ms 2.536 ms 2.369 ms
3 abilene-ul.indiana.gigapop.net (192.12.206.249) 2.634 ms 2.647 ms 2.669 ms
4 kscyng-iplsng.abilene.ucaid.edu (198.32.8.81) 12.468 ms 15.231 ms 11.988 ms
5 dnvrng-kscyng.abilene.ucaid.edu (198.32.8.13) 22.915 ms 24.201 ms 23.199 ms
6 snvang-dnvrng.abilene.ucaid.edu (198.32.8.1) 47.415 ms 47.484 ms 46.888 ms
7 losang-snvang.abilene.ucaid.edu (198.32.8.94) 56.659 ms 57.768 ms 58.188 ms
8 tpr2-transpac-la.jp.apan.net (203.181.248.130) 160.638 ms 209.072 ms 161.37 ms
9 tpr3-ae0-4.jp.apan.net (203.181.248.238) 161.413 ms 161 ms 159.891 ms
10 wide-ge-tpr3.jp.apan.net (203.181.249.41) 160.362 ms 160.512 ms 160.548 ms
11 fe-fxp1.pc3.yagami.wide.ad.jp (203.178.138.245) 160.972 ms 161.906 ms 162.072 ms
12 fe-2-0.hitachi1.k2.wide.ad.jp (203.178.138.218) 163.29 ms 164.112 ms 163.885 ms
13 orange.kame.net (203.178.141.194) 162.945 ms 162.398 ms 163.189 ms
```

traceroute6 to orange.kame.net (2001:200::8002:203:47ff:fea5:3085) from 2001:468:402:193:20a:95ff:fea7:ea10, 30 hops max, 12 byte packets

```
1 2001:468:402:193::1 2.692 ms 0.936 ms 10.387 ms
2 iugw-iub.indiana.gigapop.net 9.059 ms 1.603 ms 1.759 ms
3 iplsngngig.abilene.ucaid.edu 1.966 ms 1.613 ms 1.8 ms
4 kscyng-iplsng.abilene.ucaid.edu 11.728 ms 19.131 ms 11.411 ms
5 dnvrng-kscyng.abilene.ucaid.edu 29.402 ms 21.303 ms 25.059 ms
6 snvang-dnvrng.abilene.ucaid.edu 47.596 ms 46.697 ms 47.369 ms
7 losang-snvang.abilene.ucaid.edu 59.969 ms 56.496 ms 56.979 ms
8 3ffe:8140:101:1::2 162.123 ms 165.666 ms 160.905 ms
9 hitachi1.otemachi.wide.ad.jp 161.746 ms 162.355 ms 161.763 ms
10 pc3.yagami.wide.ad.jp 160.792 ms 161.377 ms 161.129 ms
11 gr2000.k2c.wide.ad.jp 162.913 ms 163.35 ms 163.567 ms
12 orange.kame.net 163.24 ms 163.757 ms 162.71 ms
```