IPv6 tunnel discovery

Lorenzo Colitti

Roma Tre University

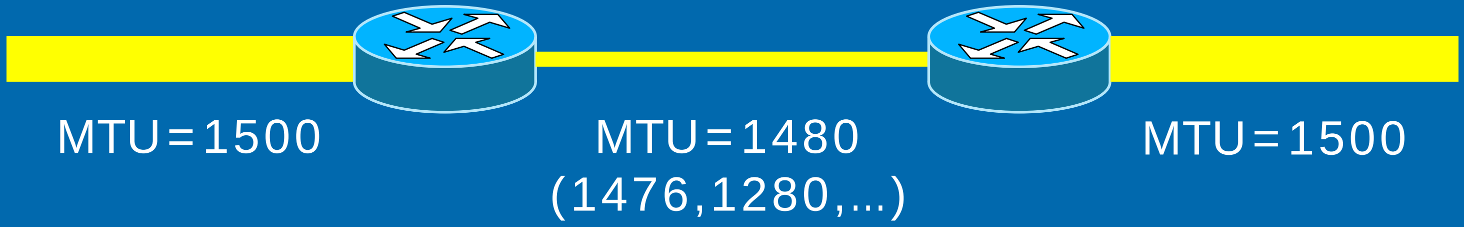
RIPE NCC

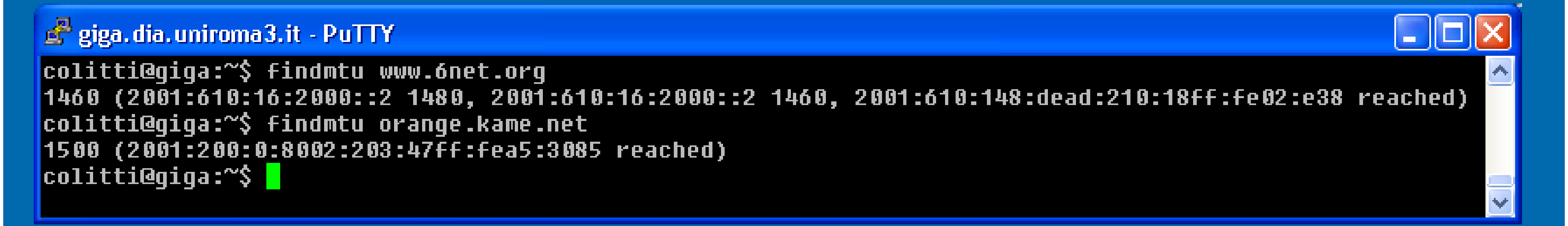
Tunnel avoidance

- Low performance
  - Heavy on routers
  - Encourage inefficient routing
- Difficult to troubleshoot
- Security!
- To avoid them we must know they’re there
  - Transparent to IPv6, “single-hop”
  - What can we do?
  - (What we can’t do: DNS)

Tunnel detection

- Path MTU discovery can spot a tunnel
  - MTU of tunnel usually lower than native links
  - Certain MTU values typical of tunnels
- Allows us to find first tunnel in a path
  - Often we only want to see if there is a tunnel or not
- Tool: `findmtu` (linux, freebsd)

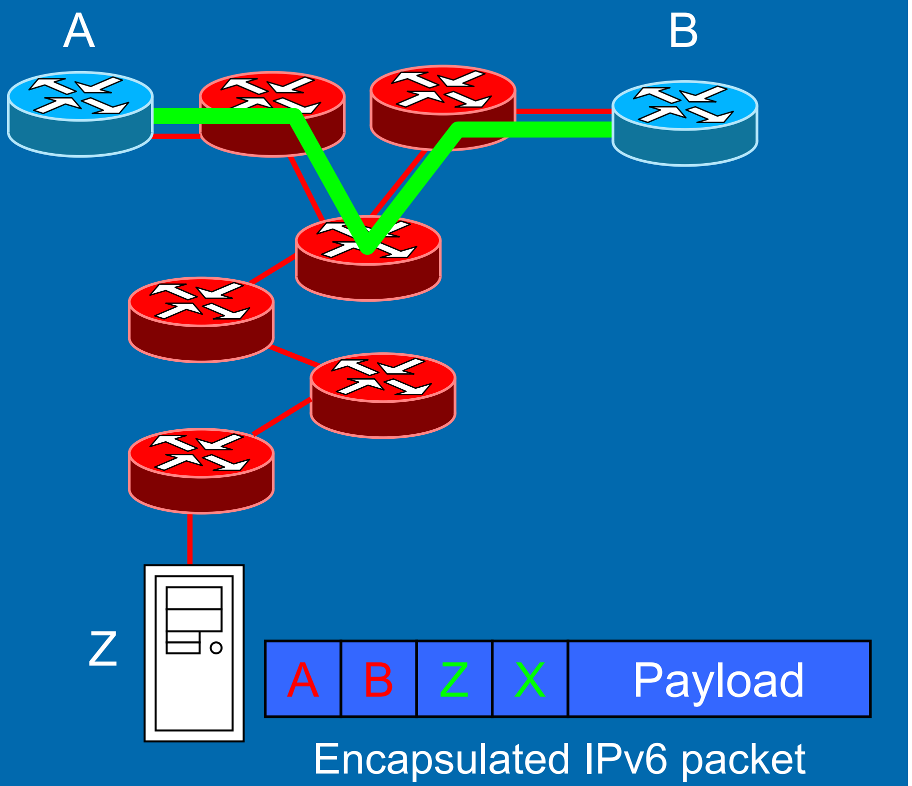




```
colitti@giga:~$ findmtu www.6net.org
1460 (2001:610:16:2000::2 1480, 2001:610:16:2000::2 1460, 2001:610:148:dead:210:18ff:fe02:e38 reached)
colitti@giga:~$ findmtu orange.kame.net
1500 (2001:200:0:8002:203:47ff:fea5:3085 reached)
colitti@giga:~$ 
```

Tunnel confirmation

- Tunnels provide no authentication mechanism
- Any host that knows the endpoints can “inject” packets into the tunnel
- Allows Z to confirm the presence of a tunnel
- Also allows Z to:
  - Source IPv6 traffic from B, bypassing routing
  - Find more tunnels from B with MTU discovery (frag)
  - Find v6 address of B (TTL=1)



A	B	Z	X	Payload

Encapsulated IPv6 packet

A = IPv4 address of A

A = IPv6 address of A

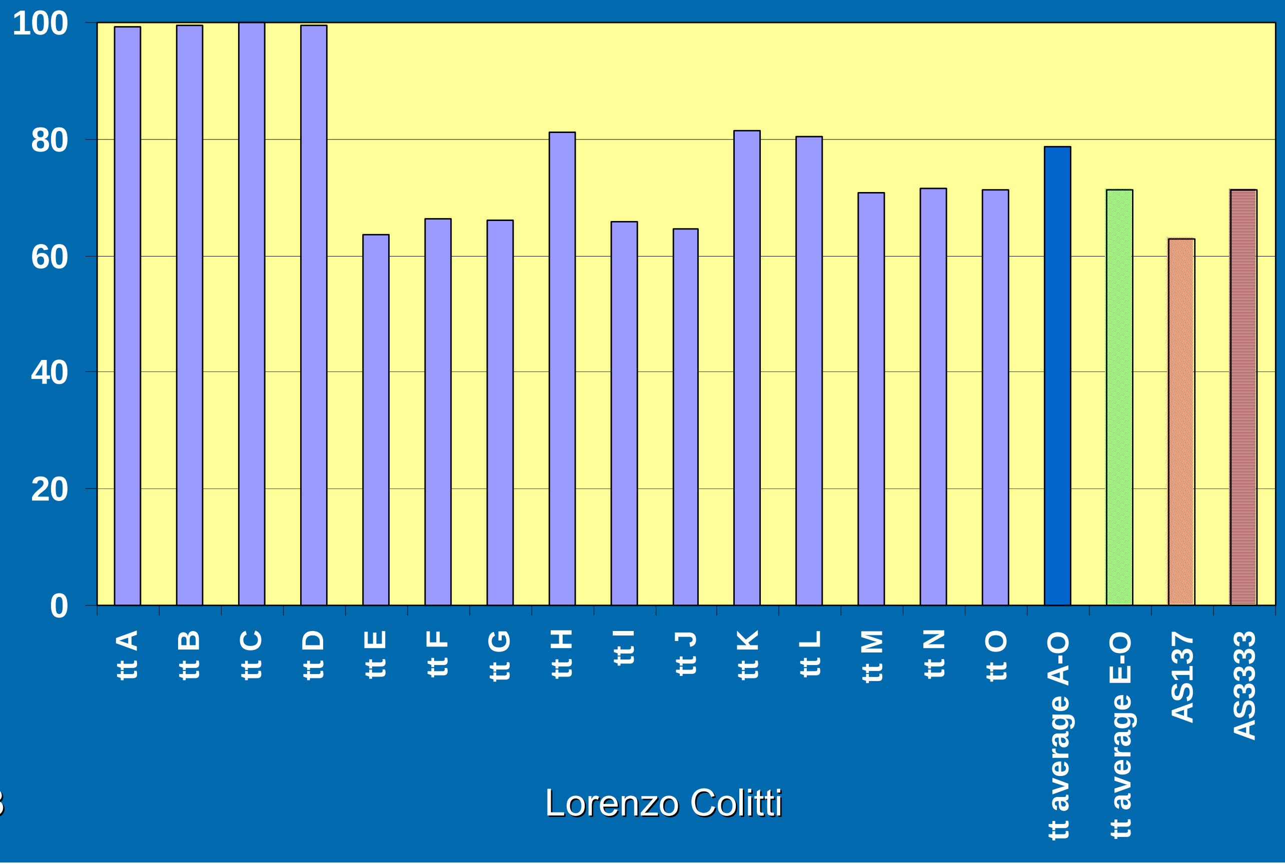
How many tunnels?

- The 6bone registry contains >1000 “spoofable” tunnels (~25%)
- The rest nonexistent (~50%), down or filtered
- We measured the MTU from each endpoint to all BGP prefixes
- Results: native paths only ~ 8% of total

MTU	# paths	%
1480	150946	39.4
1280	138358	36.1
1476	44404	11.6
1500	31525	8.2
1428	13619	3.6
Other	4104	1.1
Total	382956	100.0

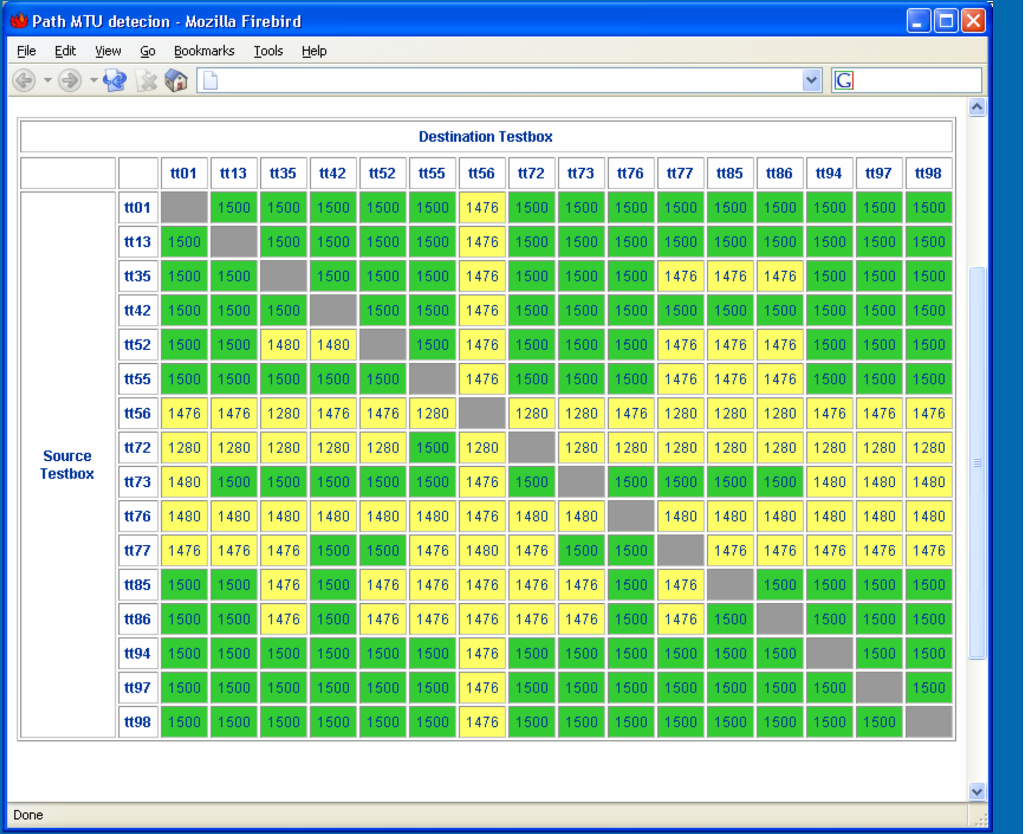
How native are we?

Percentage of BGP prefixes reached through tunnel(s) from TT boxes, GARR, RIPE NCC. Even the “best” are ≥ 62%



Conclusions

- IPv6 largely relies on tunnels
  - In total, 8% of paths native
  - Native networks don't do better than 40%
- Tunnels can be detected with Path MTU discovery
  - This lets us avoid them where possible
- In the future:
  - Tunnel detection coming to RIPE TTM service
  - Tunneltrace
    - Like traceroute, gives information on tunnels
    - Works, but not yet ready for distribution


Path MTU detecion - Mozilla Firebird
File Edit View Go Bookmarks Tools Help
Done

		Destination Testbox															
		tt01	tt13	tt35	tt42	tt52	tt55	tt56	tt72	tt73	tt76	tt77	tt85	tt86	tt94	tt97	tt98
Source Testbox	tt01		1500	1500	1500	1500	1500	1476	1500	1500	1500	1500	1500	1500	1500	1500	1500
	tt13	1500		1500	1500	1500	1500	1476	1500	1500	1500	1500	1500	1500	1500	1500	1500
	tt35	1500	1500		1500	1500	1500	1476	1500	1500	1500	1476	1476	1476	1500	1500	1500
	tt42	1500	1500	1500		1500	1500	1476	1500	1500	1500	1500	1500	1500	1500	1500	1500
	tt52	1500	1500	1480	1480		1500	1476	1500	1500	1500	1476	1476	1476	1500	1500	1500
	tt55	1500	1500	1500	1500	1500		1476	1500	1500	1500	1476	1476	1476	1500	1500	1500
	tt56	1476	1476	1280	1476	1476	1280		1280	1280	1476	1280	1280	1280	1476	1476	1476
	tt72	1280	1280	1280	1280	1280	1500	1280		1280	1280	1280	1280	1280	1280	1280	1280
	tt73	1480	1500	1500	1500	1500	1500	1476	1500		1500	1500	1500	1500	1480	1480	1480
	tt76	1480	1480	1480	1480	1480	1480	1476	1480	1480		1480	1480	1480	1480	1480	1480
	tt77	1476	1476	1476	1500	1500	1476	1480	1476	1500	1500		1476	1476	1476	1476	1476
	tt85	1500	1500	1476	1500	1476	1476	1476	1476	1476	1500	1476		1500	1500	1500	1500
	tt86	1500	1500	1476	1500	1476	1476	1476	1476	1476	1500	1476	1500		1500	1500	1500
	tt94	1500	1500	1500	1500	1500	1500	1476	1500	1500	1500	1500	1500	1500		1500	1500
	tt97	1500	1500	1500	1500	1500	1500	1476	1500	1500	1500	1500	1500	1500	1500		1500
	tt98	1500	1500	1500	1500	1500	1500	1476	1500	1500	1500	1500	1500	1500	1500	1500	