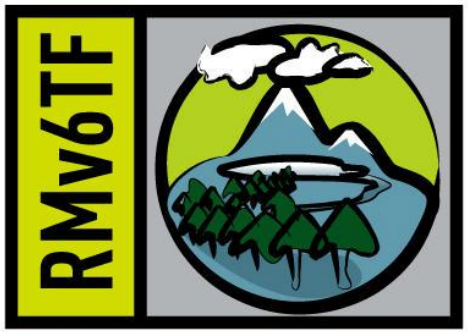
GTRI
GLOBAL TECHNOLOGY RESOURCES INC.



2013 North American IPv6 Summit
April 19, 2013

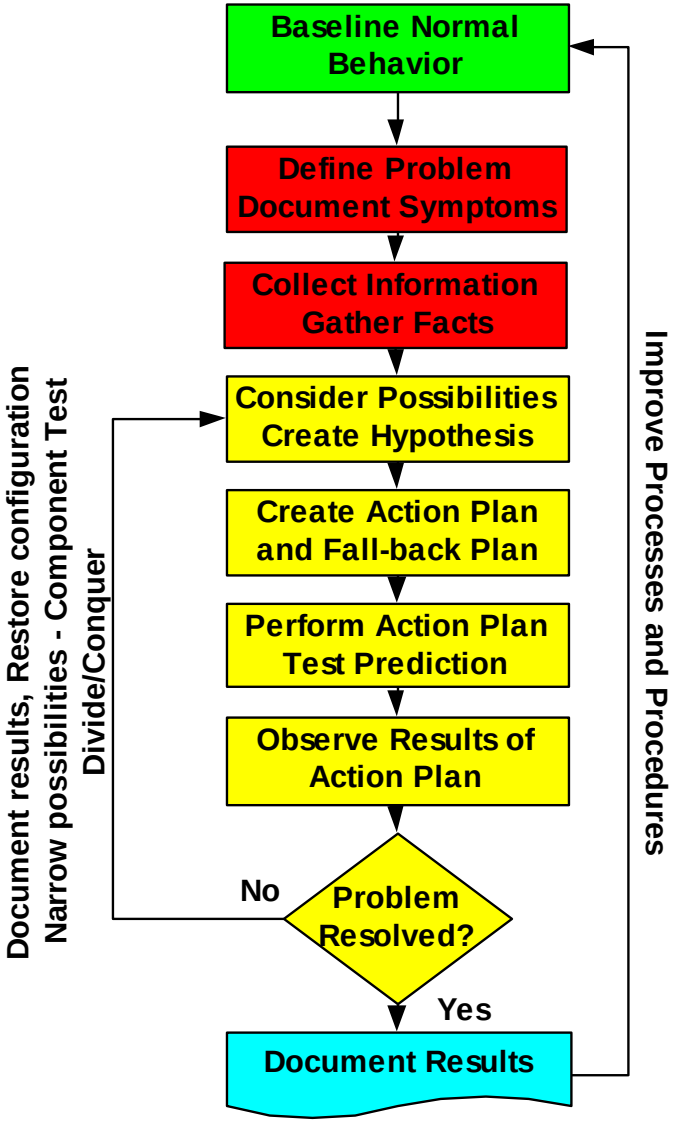
Troubleshooting Dual-Protocol Networks and Systems

Scott Hogg
GTRI - Director of Technology Solutions
RMv6TF – Chair Emeritus
CCIE #5133, CISSP #4610

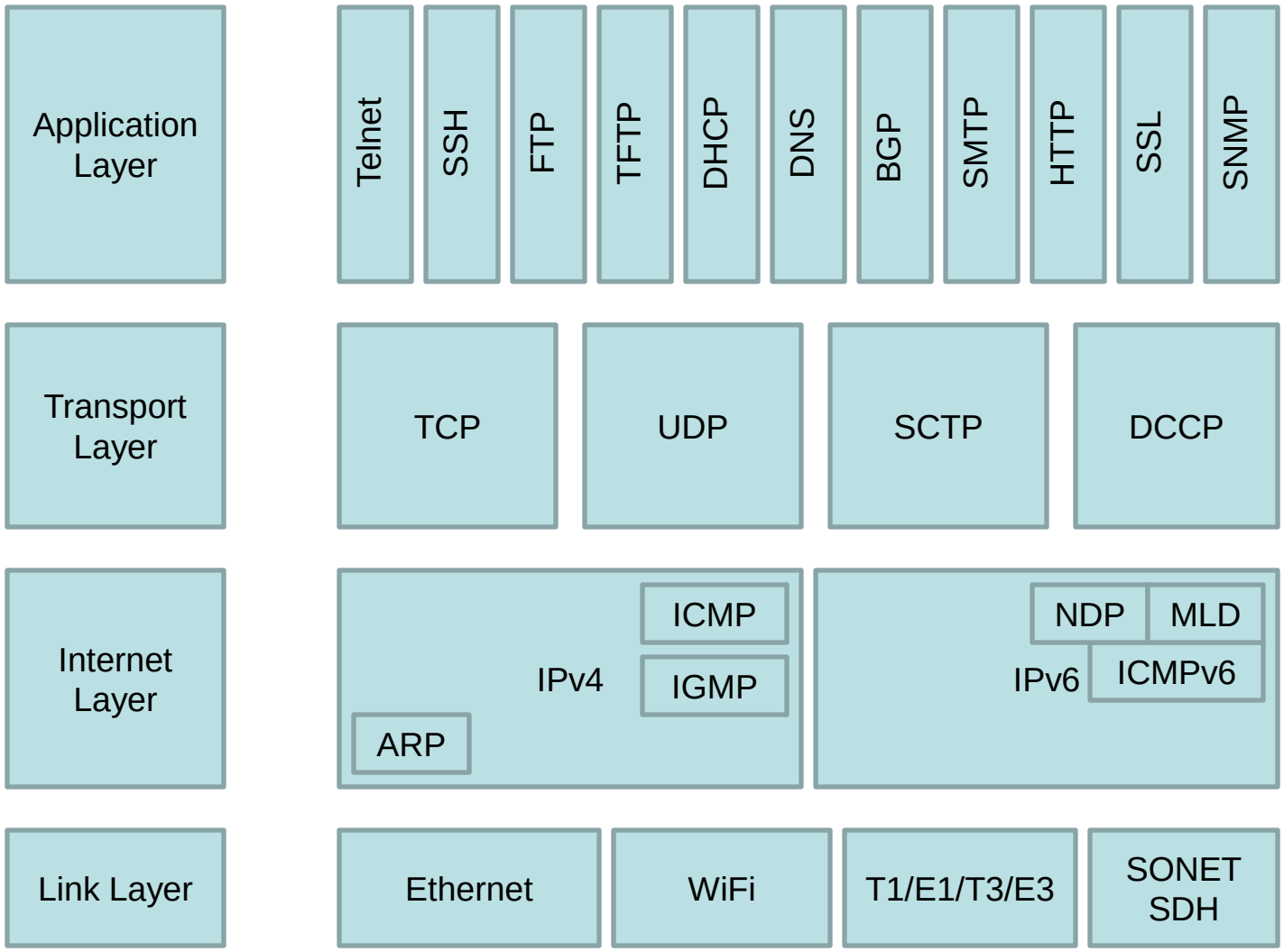
Improving Troubleshooting

- The cost of downtime can be significant, depending on the nature of your business, intangible negative reputation and customer dissatisfaction.
- Having good troubleshooting practices can help reduce MTTR, thus improving availability.
- Using a scientific troubleshooting methodology helps troubleshoot multi-part problems (like those in a dual-protocol environment).
- Network and system configurations will be changing quickly as IPv6 is deployed as change introduces more problems.
- You need to be able to troubleshoot IPv6-related problems even if you have not fully deployed IPv6.

Scientific Troubleshooting Methodology



TCP/IPv6 Troubleshooting



Node-to-Node Communications

- For two nodes to communicate they must support one common protocol
- An IPv4-only node cannot communicate with an IPv6-only node

	IPv4-Only	**Dual Protocol**	**IPv6-Only**
IPv4-Only	Yes (IPv4)	Yes (IPv4)	No
Dual Protocol	Yes (IPv4)	Yes (IPv6, IPv4)	Yes (IPv6)
IPv6-Only	No	Yes (IPv6)	Yes (IPv6)

Check TCP/IP Host Configuration

- Check that the IP address is correct
  - ifconfig, ipconfig, show ipv6 interface
- Does the host use DHCPv6?
- Check the host's default gateway
  - netstat -rn, route print
- Check DNS
  - Test forward and reverse lookups
  - Check that your resolver is good
  - Check which servers are authoritative for a domain (NS)
  - nslookup, host, dig, whois
  - Test with a protocol analyzer and inspect payload of DNS-replies
  - Consider cache poisoning as a possibility

Router Solicitations and Advertisements

Nodes send RSs (Type 133)
On bootup when they can't wait 200 seconds for the next RA

Source: FE80::/10
Link-Local address of Node
Destination: FF02::2 (all routers)

Data: Query to send RA

Routers send RAs (Type 134)
Every 200 seconds or
Responding to an RS message

Source: FE80::/10
Link-Local address of Router
Destination: FF02::1 (all nodes)

Data: Options, subnet prefix, lifetime, autoconfig flags (M&O bits)

Host IPv6 Addresses

- IPv6 nodes can have their addresses configured automatically or configured statically in various ways.
- Manually entered addresses are prone to error.
- Verify IPv6 addresses on both end hosts
  - Link-Local, GUA, ULA, etc.
- Verify IPv6 default gateway
  - Link-local next-hop address
  - Or
  - Global address for next-hop address

Neighbor Discovery Protocol (NDP)

- NDP is the IPv6 equivalent of IPv4's ARP
- Check the IPv6 Neighbor Cache (like the ARP cache) to verify mapping of IPv6 address to Layer-2 address (e.g. Ethernet MAC address)
  - Windows: netsh interface ipv6 show neighbors
  - Linux: ip neighbor show
  - BSD: ndp –a
  - Solaris: netstat -p -f inet6
  - Cisco routers: show ipv6 neighbors [statistics], show ipv6 routers
- Even though two systems have each other in their neighbor cache, they may not be able to communicate on the local LAN

Neighbor Solicitations and Advertisements

Nodes send NSs (Type 135)
When sending IPv6 packet to Another node

Source: Unicast IPv6 Address
Destination: Solicited Node Multicast Address FF02::1:FFAA:BBCC

Data: Target link-layer address
Query: What is your link-layer address?

Routers send NAs (Type 136)
Responding to an NS message

Source: Unicast IPv6 Address
Destination: Unicast Address of Requestor or FF02::1 (all nodes)

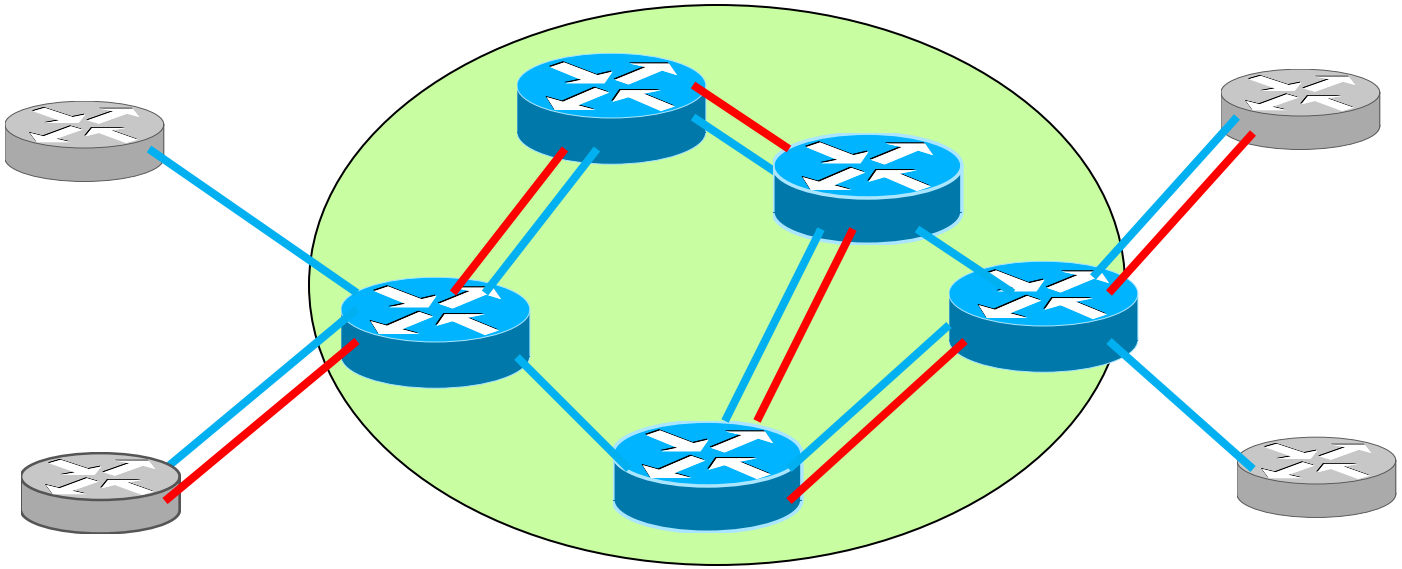
Data: R/S/O Flags, Target's Link-layer address
Response: Here is my IPv6 and link-layer address.

End-to-End Troubleshooting

- Ping (ping6) (by name, by IP addr, in both directions, specify source address, 1500-byte MTU)
  - Linux: ping6 -I eth0 fe80::1
  - Windows: ping fe80::1%12
  - Cisco: ping fe80::1%GigabitEthernet0/0
  - ping -l 1500 2001:db8:dead:c0de::1
- Traceroute (traceroute6), tracert
- Tcptraceroute6 (www.remlab.net/ndisc6/)
- Microsoft C:\>pathping -6 2001:db8:11::1
- mtr -r6 www.rmv6tf.org c100 (www.bitwizard.nl/mtr/)
- Pchar, pathchar, iperf, jperf
- Netcat (nc -6), telnet, ssh, nmap -6 -sT 2001:db8::1

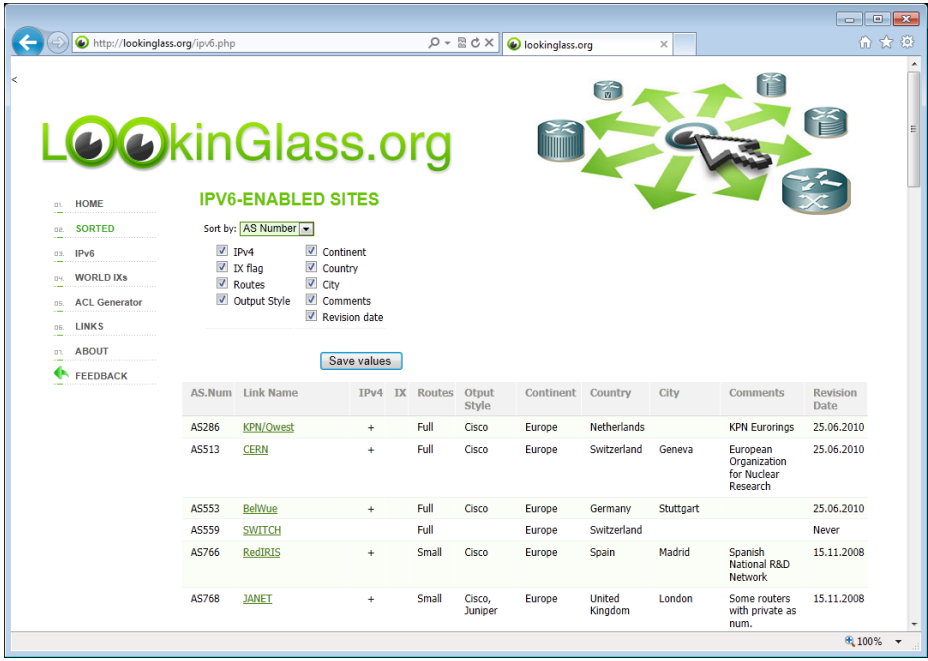
IPv4/IPv6 Topology Differences

- The IPv6 path through a network may not be the same as the IPv4 path – they may not be congruent
- Only a subset of the infrastructure may use IPv6 so IPv6 traffic may take a less optimal route than IPv4 traffic
- ISP IPv6 peering may not be as complete as their IPv4 peering



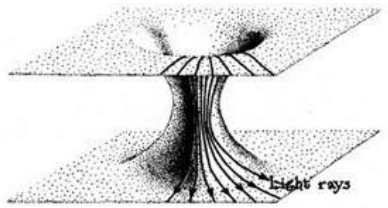
IPv6 Internet Routing

- BGP Looking glasses can be used to troubleshoot IPv6 Internet routing problems
- The looking glasses are routers or systems that are BGP-peered to other backbone routers – you can log into these and check the status of routes, ping, traceroute, etc.

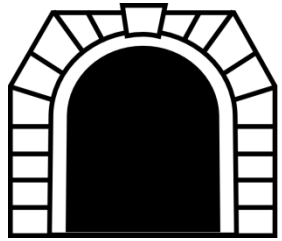


Troubleshooting IPv6 Tunnels

- Tunnels are more difficult to troubleshoot than native IPv6 connectivity
- 6-in-4 tunnels converge on IPv4 routing topology
  - How does the tunnel sit on top of the IPv4 Layer-3 topology?
  - If your IPv4 connectivity is faulty then your IPv6 connectivity will be faulty
- Tunnels can add latency (non-optimal traffic paths)
  - What if you live in NY and your IPv6 tunnel goes to LA?
- Encapsulation/Decapsulation of IPv6/IPv4 packets in a tunnel can add jitter/processing overhead



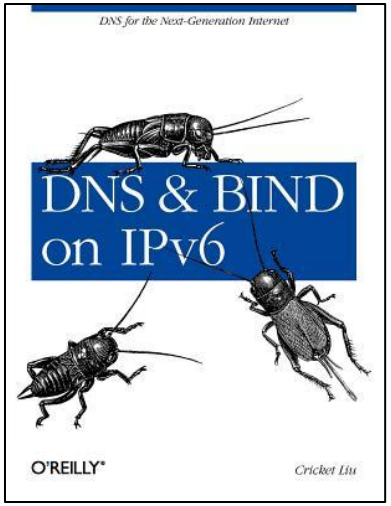
Troubleshooting IPv6 Tunnels



- Manually-configured tunnels can be misconfigured
- Automatic tunnels can fail too if relays are misconfigured (6to4 Relay, Teredo Relay, ISATAP router)
  - Look for packets that use 2002::/16 (6to4) or 2001::/32 (Teredo) addresses or have IPv6 /64 prefix followed by “0000:5EFE” followed by 32-bits of IPv4 address (ISATAP)
- Hosts using tunnels may also suffer from CPU overhead if network stack is not optimized

Check DNS Resolution

- We need to verify that DNS resolutions are indicating the correct IP version address to connect
- Different tools to check DNS resolution
  - nslookup www.rmv6tf.org –querytype=aaaa
  - nslookup
  - set type=AAAA
  - dig @4.2.2.2 www.rmv6tf.org –t aaaa
  - host www.rmv6tf.org
- The Google Public DNS IPv4 addresses:
  - 8.8.8.8 , 8.8.4.4
- The Google Public DNS IPv6 addresses:
  - 2001:4860:4860::8888 , 2001:4860:4860::8844
- Hurricane Electric Whitelisted DNS server
  - ordns.he.net (2001:470:20::2, 74.82.42.42)



IPv6 Packet Capture

- There are many different options of IPv6-capable protocol analyzers
  - These tools may require WinPcap or Libpcap
  - Wireshark, www.wireshark.org
  - TCPDump, www.tcpdump.org
  - Network Instruments Observer, www.netinst.com
  - NetScout nGenius Probes and Sniffer (Network General), www.netscout.com
  - WildPackets OmniPeek, www.wildpackets.com
  - Micorosoft Network Monitor, http://blogs.technet.com/b/netmon/

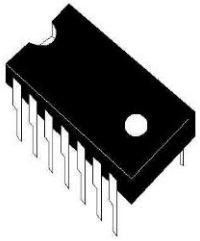
Other Protocol Analyzer Vendors

- Other protocol analyzers
- Hardware
  - Agilent (HP Test and Measurements Division) NetMetrix, Advisor
  - Spirent (Acquisition of many companies)
  - Acterna (TTC, Wandel & Goltermann DA-30c, …)
  - Cisco Network Analysis Module (NAM)
- Software:
  - Shomiti – Surveyor 4.1 – Now Finisar
  - Network Instruments Observer
  - Fluke Networks OptiView

Wireshark and IPv6

- When you capture traffic, you can perform a basic display filter “ipv6”
- After you captured the traffic then you can use capture filters
  - eth.type == 0x86dd
  - ipv6
  - host 2001:db8:11::1 && icmpv6.type == 128
  - ip proto 41
  - ipv6 and not ip proto 41
  - ipv6.addr == 2001:db8:11::1
  - ipv6.dst == 2001:db8:11::1 && tcp.port == 80
  - ipv6.src == 2001:db8:11::1

IPv6 Performance



- Some older devices may not handle IPv6 forwarding in hardware
- Software-based forwarding may cause increased CPU utilization on routers even with moderate amount of IPv6
- This results in packet loss which leads to retransmissions which leads to application issues
- We want to gather performance statistics for each hop in the end-to-end path
- Identify the device that may be contributing to slowness or creating a bottleneck, then look at the status of that device and its counters

Cisco NBAR2

- Network-Based Application Recognition (NBAR) was re-architected to work with the Service Control Engine (SCE) in ISR-G2 and ASR1K routers
- NBAR2 can classify IPv6 packets, and tunneled packets
  - NBAR2 Protocols:
    - ipv6-frag, ipv6-icmp, ipv6inip, ipv6-nonxt, ipv6-opts, ipv6-route, isatap-ipv6-tunneled, ayiya-ipv6-tunneled, sixtofour-ipv6-tunneled, teredo-ipv6-tunneled

IPv6 Service Level Agreements (SLA)

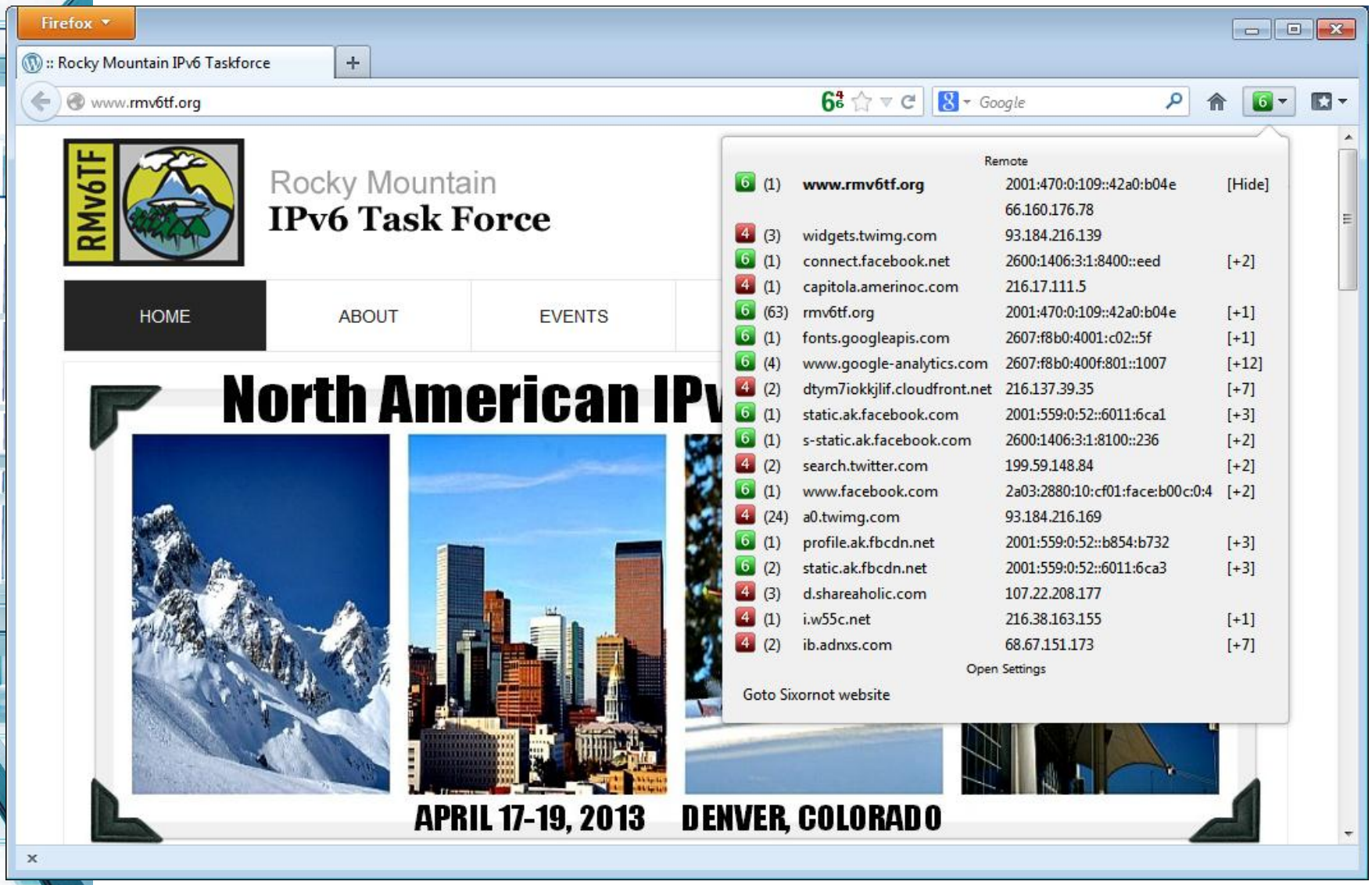
- IP SLA allows a router to perform monitoring of services or systems using active traffic monitoring and this feature is also supported for IPv6
- The following Cisco IOS IP SLAs are supported for IPv6 (ICMP, TCP Connection, UDP Connection, UDP Jitter operation)

```
#conf t
track 150 ip sla 150
exit
ip sla 150
icmp-echo 2001:DB8:11::6 source-ip 2001:DB8:4444::4444
ip sla schedule 150 life forever start-time now
end
#show track 150
#show ip sla statistics
```

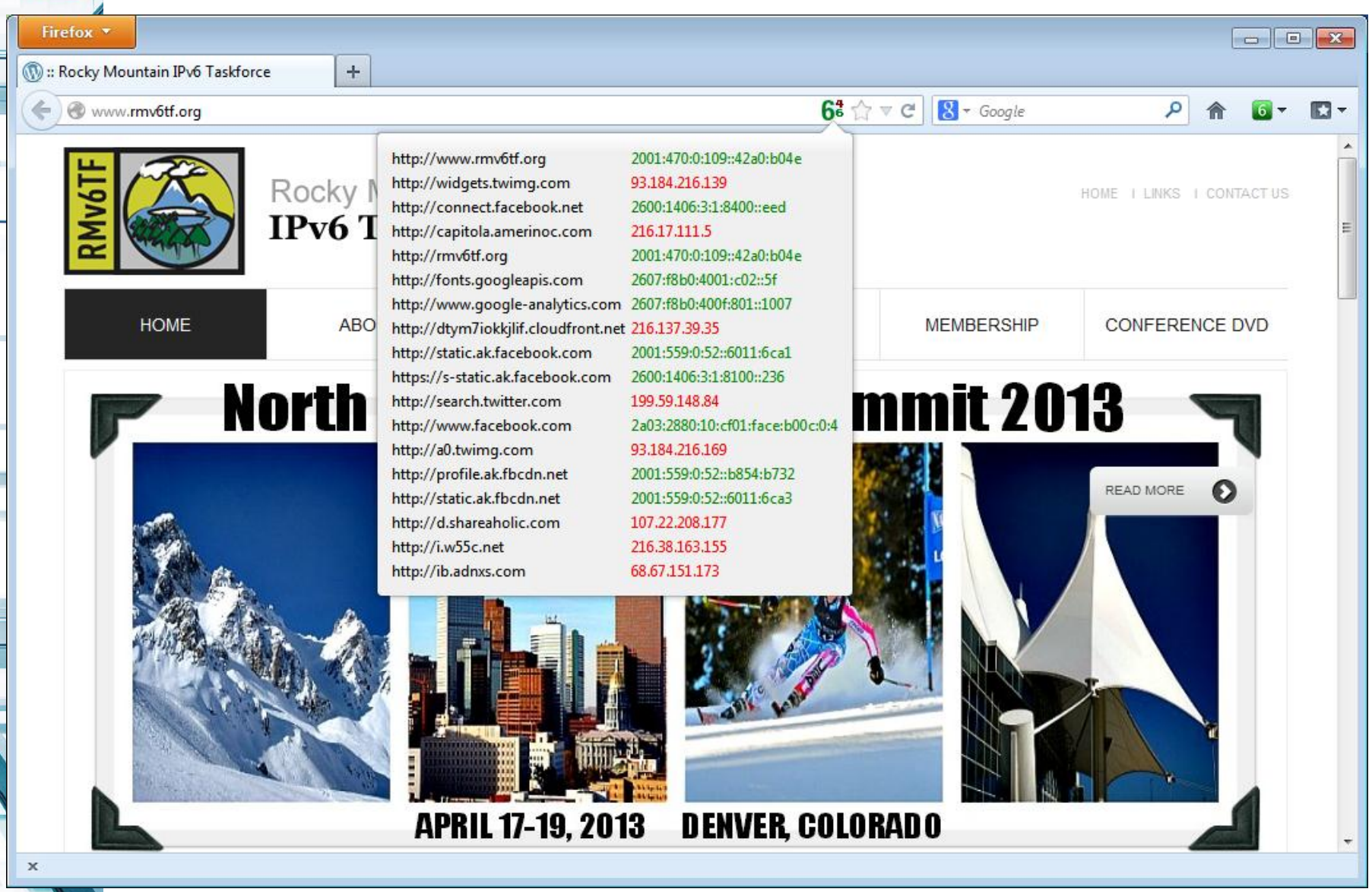
Web Browser IPv6 Support

- Most web browsers now support IPv6
  - How to tell if your browser made a v4 of v6 connection?
  - http://[2001:DB8:1003::F]:8080/index.html
  - ShowIP add-on for Firefox
  - Other plug-ins and add-ons are a available for various browsers
- Otherwise you will have to browse by IPv6 address or IPv4 or IPv6 name
- You may need to use a protocol analyzer to make absolutely sure what IP version was used to make the connection

SixOrNot Firefox Add-On

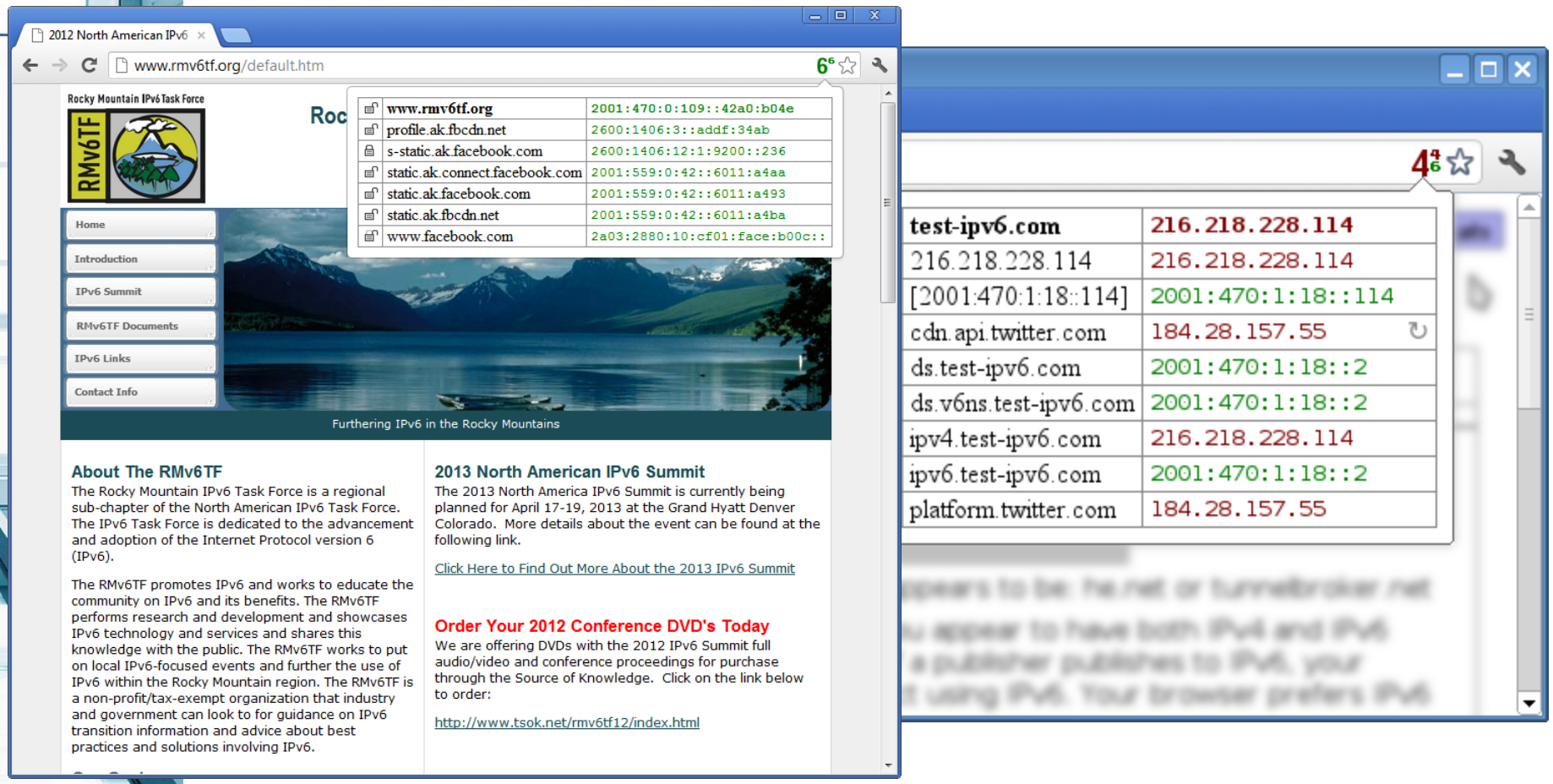


IPvFox Firefox Add-On



IPvFoo for Google Chrome

- Summarizes IPv4, IPv6, and HTTPS information for all connections made by the current webpage

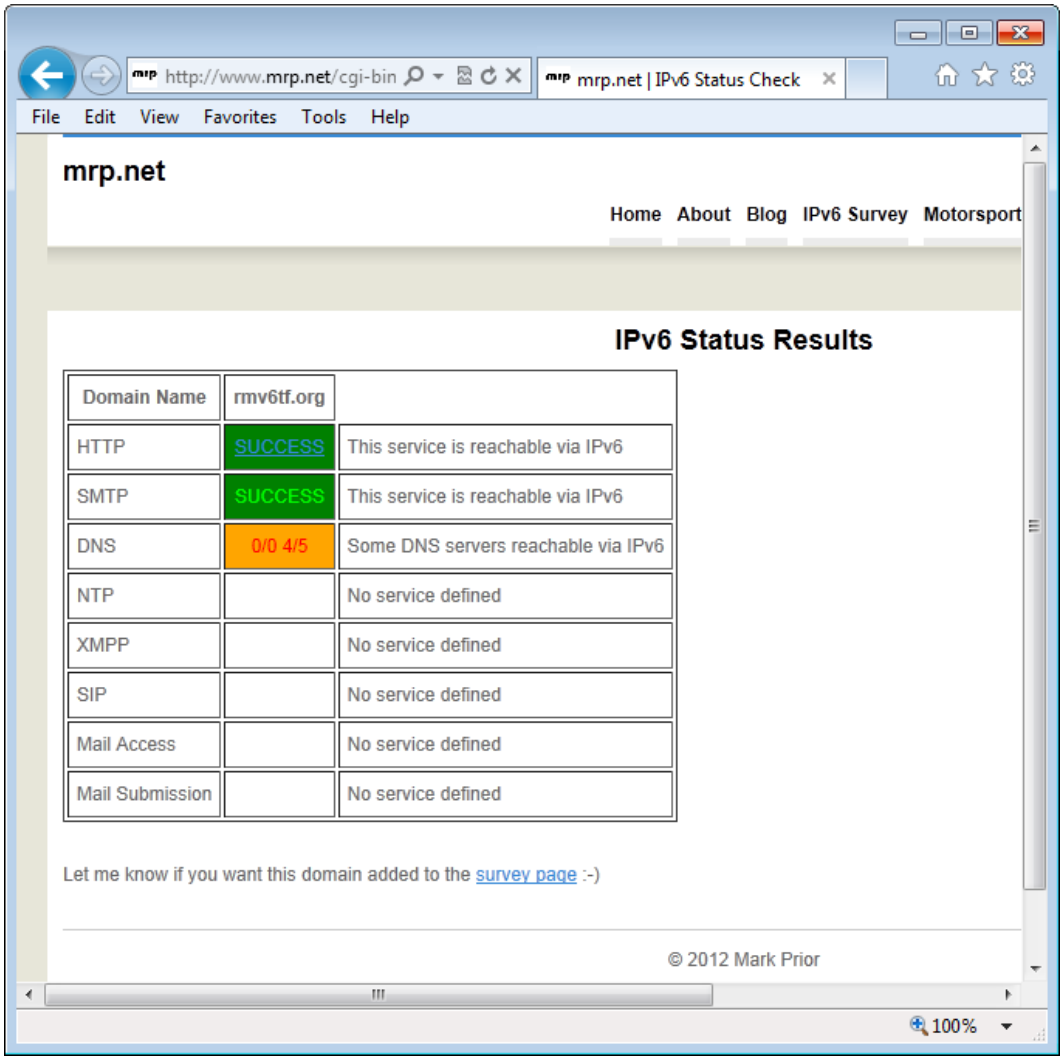


WGET

- GNU Wget is a free software package for retrieving files using HTTP, HTTPS and FTP
- IPv6-capable non-interactive command-line tool runs on UNIX-OSs and Microsoft Windows
- `[root@fez ~]# wget -6 www.rmv6tf.org`
- `--2013-01-22 17:58:43--  http://www.rmv6tf.org/`
- `Resolving www.rmv6tf.org... 2001:470:0:109::42a0:b04e`
- `Connecting to www.rmv6tf.org|2001:470:0:109::42a0:b04e|:80... connected.`
- `HTTP request sent, awaiting response... 200 OK`
- `Length: unspecified [text/html]`
- `Saving to: `index.html'`
- `    [  <=>                                  ] 42,599  175K/s   in 0.2s`
- `2013-01-22 17:58:44 (175 KB/s) - `index.html' saved [42599]`
- `[root@fez ~]# wget -6 --no-check-certificate https://www.rmv6tf.org`

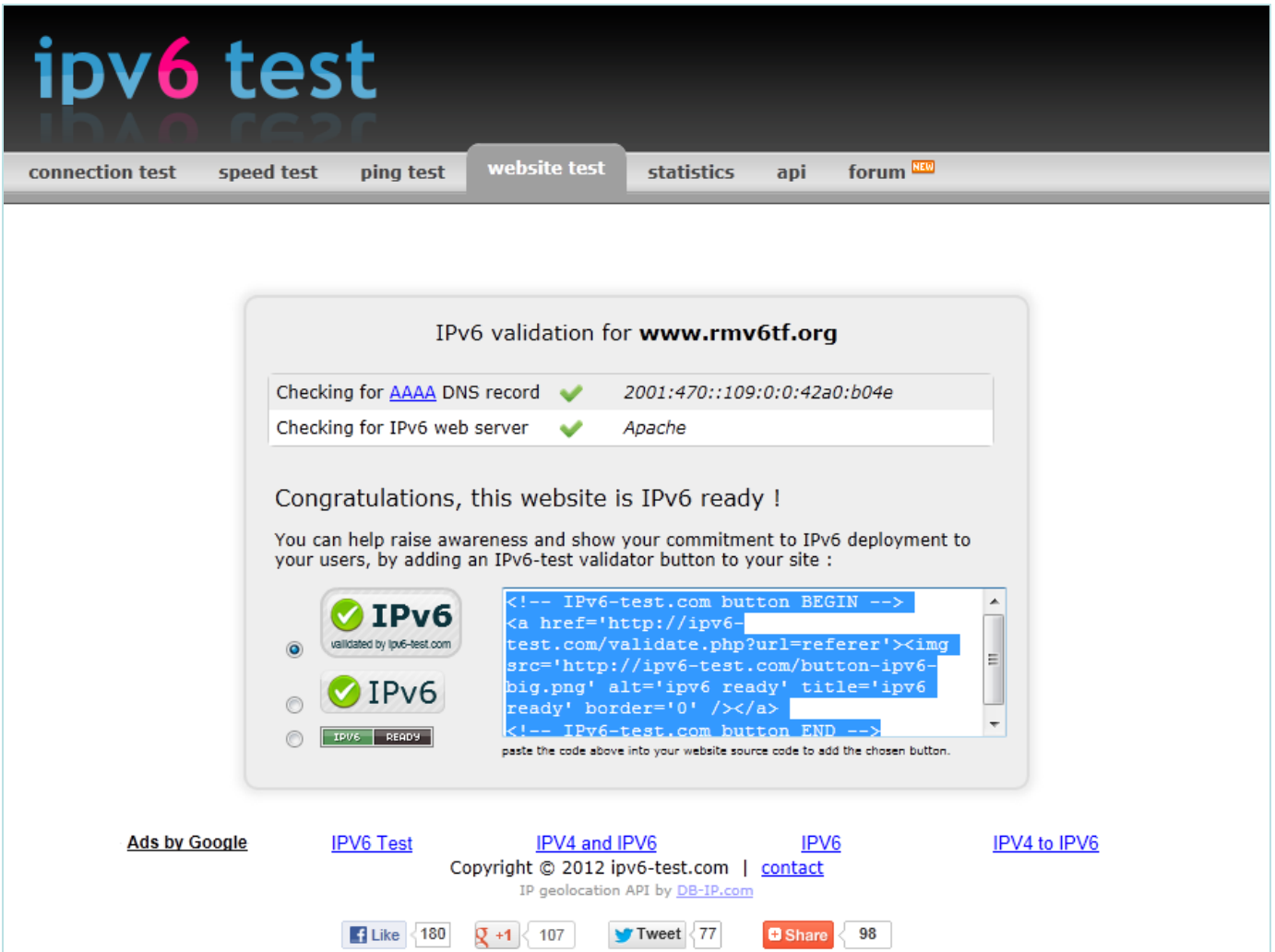
Test IPv6 From the Internet

- http://www.mrp.net/cgi-bin/ipv6-status.cgi



Test IPv6 From the Internet

- http://ipv6-test.com/validate.php



IPv6-Capable Web Monitoring

- Services that monitor your IPv6 web site
  - Keynote Internet Testing Environment (KITE)
    - keynote.com
  - Gomez (now Compuware Application Performance Management (APM))
    - http://www.compuware.com/application-performance-management/
- Other web monitoring services do not seem to have any IPv6 capabilities

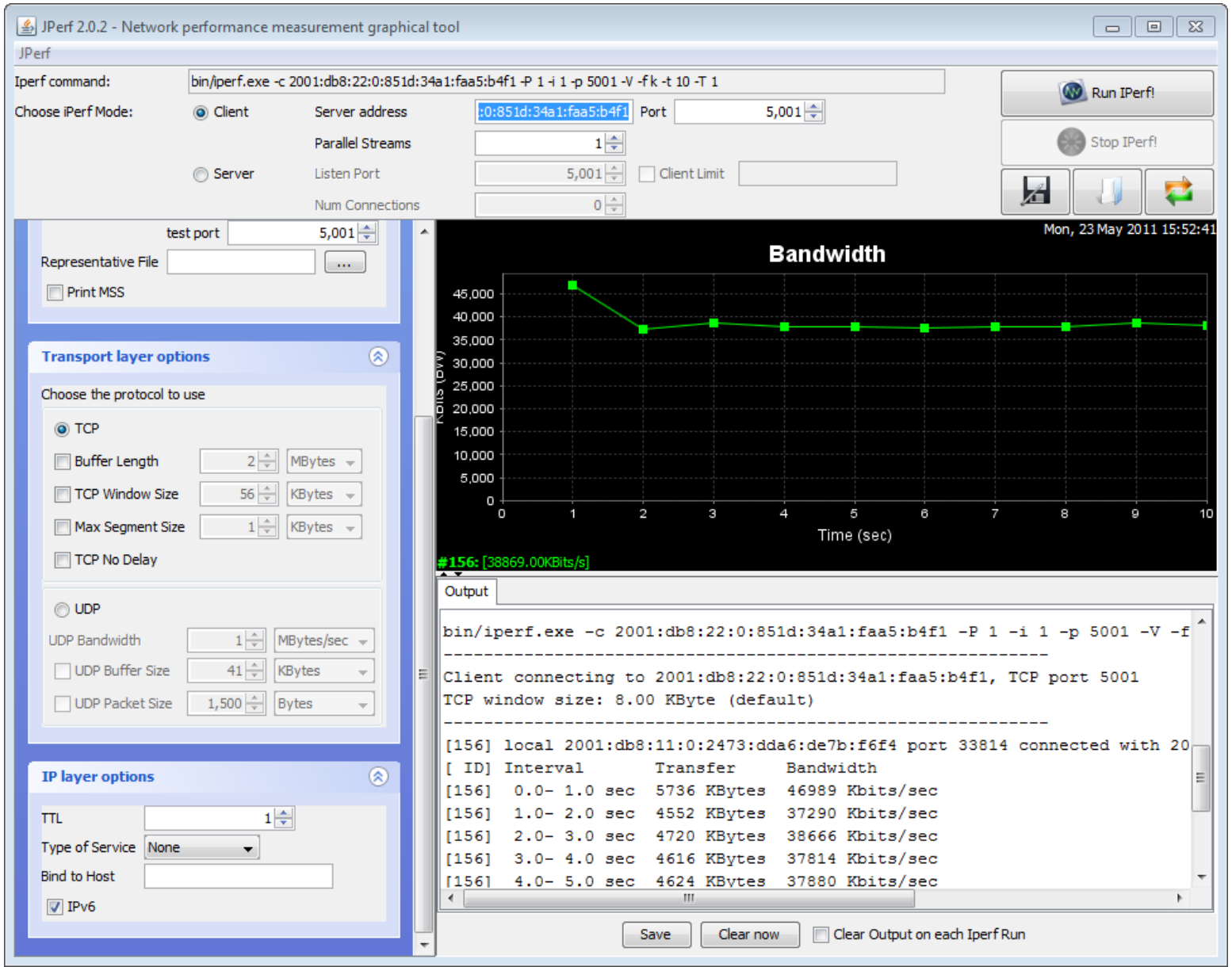
Test Network Load

- To test end-to-end network performance you will need tools that load a network with IPv6 traffic. This could be synthetic or real traffic.
- You can test the performance of your IPv6 Internet link with these services:
  - http://ipv6.speedtest.premieronline.net (Premier Communications - US)
  - http://www.burst.net/speeds.shtml (Burst.net - US)
  - http://ipv6-speedtest.net (UK)
  - http://speedtest6.com (Japan)

Iperf

- Iperf is an open-source network throughput performance utility that can generate IPv4 or IPv6 TCP or UDP packets between a client and server
- Iperf was created by the Distributed Applications Support Team (DAST) at the National Laboratory for Applied Network Research (NLANR).
  - On Server:
    - iperf –s –p 5001 -V
  - On Client:
    - iperf -c 2001:db8:22::100 -P 1 -i 1 -p 5001 -V -f k -t 10 -T 1
- Jperf (xjperf) 2.0.2 is a Google Code project java-based front end to Iperf that is IPv6-capable

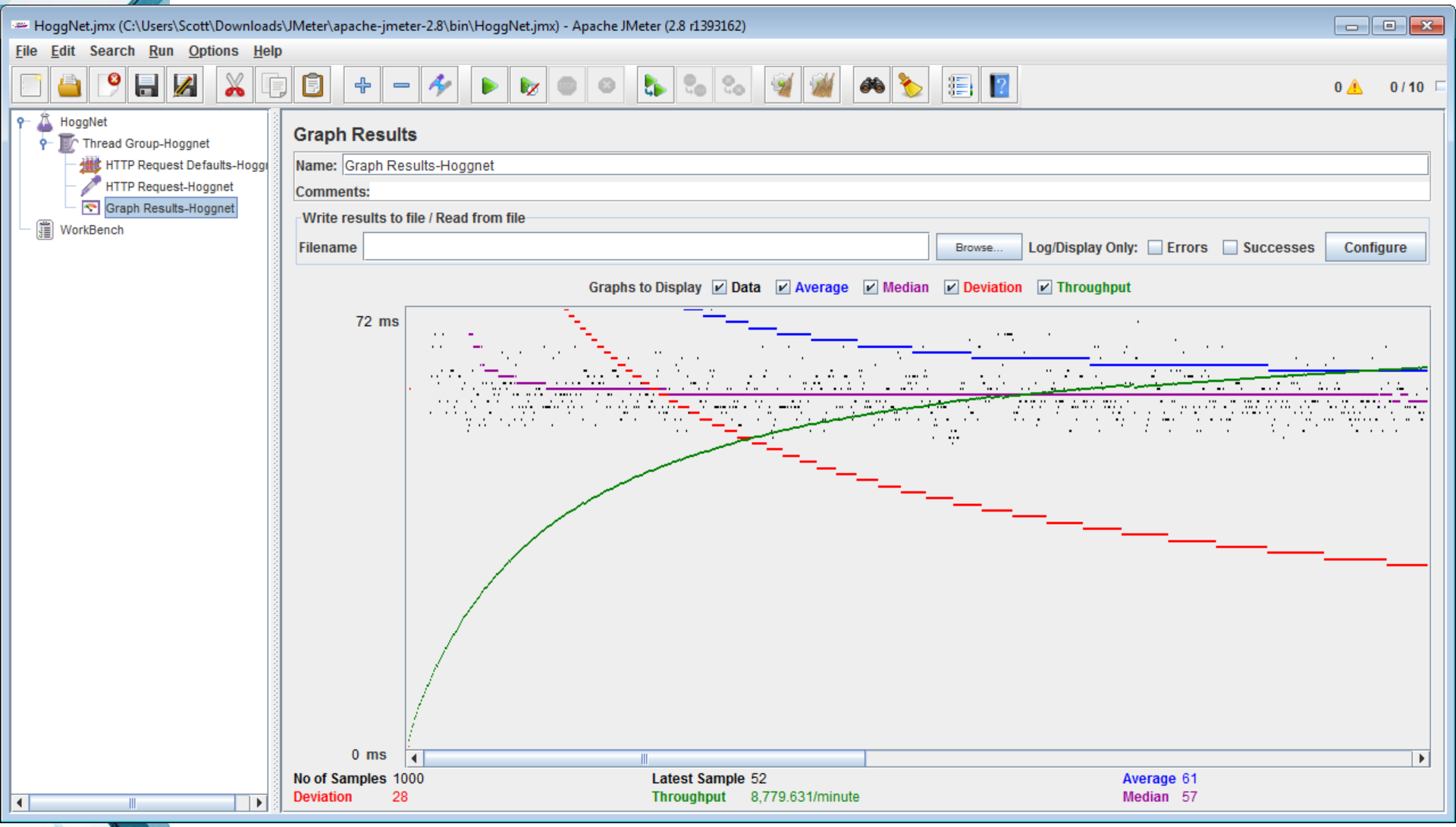
JPerf


JPerf 2.0.2 - Network performance measurement graphical tool
JPerf
Iperf command:
bin/iperf.exe -c 2001:db8:22:0:851d:34a1:faa5:b4f1 -P 1 -i 1 -p 5001 -V -f k -t 10 -T 1
Choose iPerf Mode:
Client
Server address
:0:851d:34a1:faa5:b4f1
Port
5,001
Parallel Streams
1
Server
Listen Port
5,001
Client Limit
Num Connections
0
Run IPerf!
Stop IPerf!
test port
5,001
Representative File
Print MSS
Transport layer options
Choose the protocol to use
TCP
Buffer Length
2
MBytes
TCP Window Size
56
KBytes
Max Segment Size
1
KBytes
TCP No Delay
UDP
UDP Bandwidth
1
MBytes/sec
UDP Buffer Size
41
KBytes
UDP Packet Size
1,500
Bytes
IP layer options
TTL
1
Type of Service
None
Bind to Host
IPv6
Mon, 23 May 2011 15:52:41
Bandwidth
KBits (BW)
45,000
40,000
35,000
30,000
25,000
20,000
15,000
10,000
5,000
0
0
1
2
3
4
5
6
7
8
9
10
Time (sec)
#156: [38869.00KBits/s]
Output
bin/iperf.exe -c 2001:db8:22:0:851d:34a1:faa5:b4f1 -P 1 -i 1 -p 5001 -V -f
Client connecting to 2001:db8:22:0:851d:34a1:faa5:b4f1, TCP port 5001
TCP window size: 8.00 KByte (default)
[156] local 2001:db8:11:0:2473:dda6:de7b:f6f4 port 33814 connected with 20
[ID] Interval Transfer Bandwidth
[156] 0.0- 1.0 sec 5736 KBytes 46989 Kbits/sec
[156] 1.0- 2.0 sec 4552 KBytes 37290 Kbits/sec
[156] 2.0- 3.0 sec 4720 KBytes 38666 Kbits/sec
[156] 3.0- 4.0 sec 4616 KBytes 37814 Kbits/sec
[156] 4.0- 5.0 sec 4624 KBytes 37880 Kbits/sec
Save
Clear now
Clear Output on each Iperf Run

Apache JMeter

- JMeter is a simple open-source Java app designed to load test functional behavior and measure performance of web and other applications
- Download Jmeter 2.8 to a directory, unzip
- Run bin/Jmeter.bat
- Created a Threat Group with HTTP Request Defaults for www.hoggnet.com, HTTP Request for /, Graph Results
- Changed bin/system.properties files to:
  - java.net.preferIPv4Stack=false
  - java.net.preferIPv6Addresses=true

Jmeter Results – IPv6



Check Your IPv6 Address

- http://whatismyv6.com, http://ipv6.whatismyv6.com, http://whatismyipv6address.com, http://ip6.me (for mobile devices)
- http://whatsmyipv6.org
- http://www.myipv6address.com
- http://www.v6address.com (v4address.com)
- http://ip6tools.com, http://www.my-ip6.com
- http://www.runningipv6.net/what-is-my-ipv6-address.php
- http://www.ipv6chicken.com (uses large MTU size)
  - http://www.ipchicken.com

Check Your IPv6 Connectivity

- http://www.kame.net
- http://6to4test7.runningipv6.net
- http://test-ipv6.comcast.net
- http://test-ipv6.com
- http://ipv6-test.com
- http://onlyv6.com (IPv6-only web site)
- http://www.traceroute6.net
- http://s.a.ak6i.net/a1/results/demo.html (Akamai AK6I IPv6 Connectivity check)
- http://ipv6eyechart.ripe.net (RIPE's dual-stack connectivity chart)

Port Scan Yourself

- Tim's Free Online IPv6 Port Scanner (Firewall Tester)
  - http://ipv6.chappell-family.com/ipv6tcptest/index.php
  - http://ipv6.chappell-family.com/timswiki/index.php5/IPv6
- SubnetOnline.com Online Port Scanner IPv6
  - http://www.subnetonline.com/pages/ipv6-network-tools/online-ipv6-port-scanner.php
- Qualys FreeScan
  - https://freescan.qualys.com
- L'Altro Mondo Free Online Opensource IPv6 TCP Port Scanner
  - http://laltromondo.dynalias.net/~ipv6/
- VikingScan - Portscan your IP for Free!
  - •http://miniscan6.vikingscan.org
- http://www.scanipv6.com free IPv6-capable nmap scanner

IPv6 and PMTUD

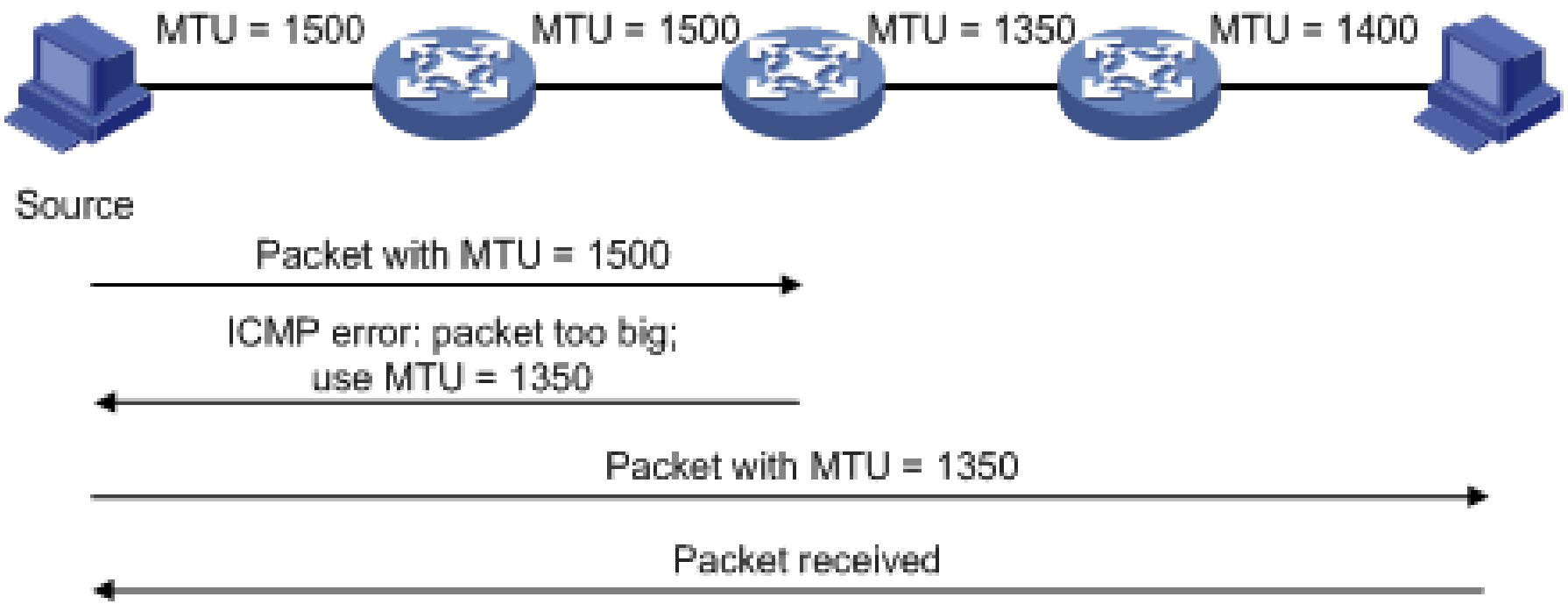
- IPv6 routers do not perform fragmentation of IPv6 packets (Minimum IPv6 Link MTU=1280 bytes)
  - Routers drop the packet and send back ICMPv6 Packet Too Big message (Type 2) to the source
- Hosts must perform Path MTU Discovery (PMTUD) and reduce packet size and cache new size
- Fragmentation Extension Header will be added to fragmented packets (next-header 44)
- Tunnels are pervasive for IPv6, tunnel overhead reduces effective MTU, PMTUD needed more frequently with IPv6 networks due to tunnel usage
- Firewalls should not filter PMTUD messages, if they do, then PMTUD will not work

IPv6 and PMTUD (Cont.)

- Many applications today do not perform PMTUD properly and this will need to change with the introduction of IPv6 (most web servers set DF=1)
- Application may complete initial connection (smaller packets) then hang when larger data is sent by server
- Turning down TCP Maximum Segment Size (MSS) to 1220 bytes only works for TCP, but may not work in all cases
- Turning down interface MTU to 1280 bytes is far less than ideal, someday we will want jumbo frames

IPv6 and PMTUD (Cont.)

- You can test PMTUD with ping
- ping -l 1500 2001:DB8:DEAD:C0DE::1
- netsh int ipv6 show destinationcache

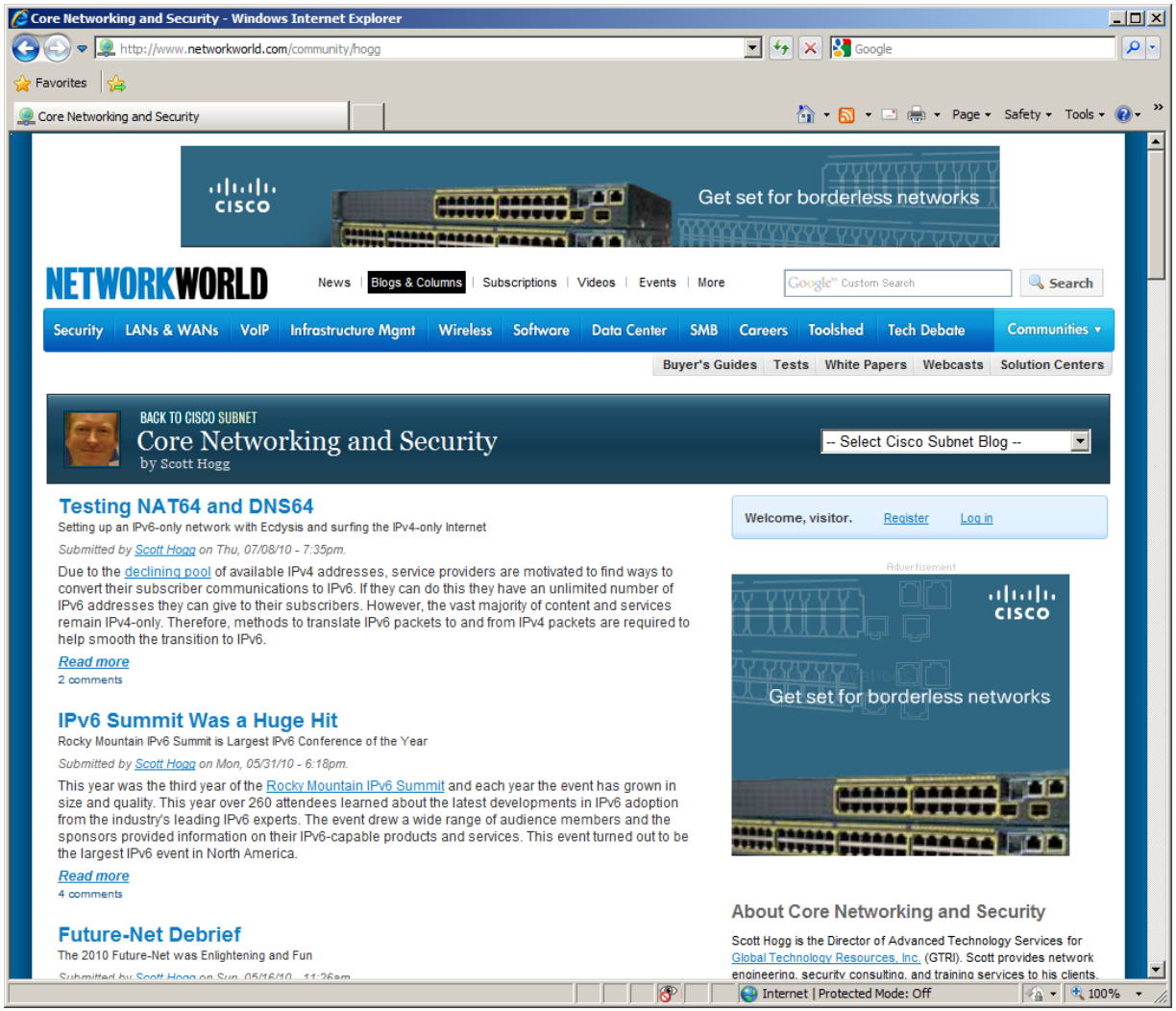


The Bottom Line

- ***Use good methodology***
- ***Document actions and results***
- ***Leverage all tools to gather information***
- ***Use protocol analyzer to help troubleshoot problems***
- ***Understand protocols you are troubleshooting***

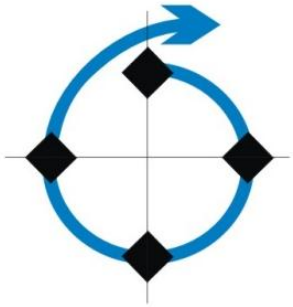
NetworkWorld Blog

http://www.networkworld.com/community/hogg



GTRI's IPv6 Transition Services

- IPv6 Inventory
  - Documentation of your current inventory and determination of IPv6 compatibility
  - Data gathering expertise (manual, data calls, automated utilities)
  - Cisco and GTRI automated tools
  - Inventory data aggregation and review
- IPv6 Training
  - Education for your teams to help them learn IPv6 technologies
  - Classroom and hands-on training
- IPv6 Impact Analysis
  - IPv6 Risk Assessment using OMB's own Risk Analysis Methodology
  - Custom-tailored transition planning for your IPv6 migration, tied to your enterprise architecture
- IPv6 Application Assessment
  - Software assessments leveraging COTS tools and our extensive experience
  - Review of your operating system constraints for IPv6 adoption
- IPv6 Experimentation and Testing
  - Systems testing in our IPv6 lab (DNS, routing, security, applications)
- IPv6 Deployment
  - Deployment of dual-stack and other IPv6 transition techniques
  - Dual Stack DNS servers and IPv6 security deployment



Question and Answer

Q:

&

A:

SHogg@GTRI.com
Scott@HoggNet.com

Mobile: 303-949-4865