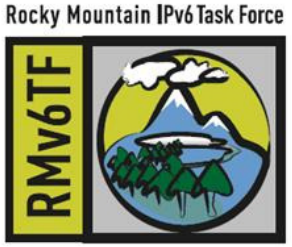


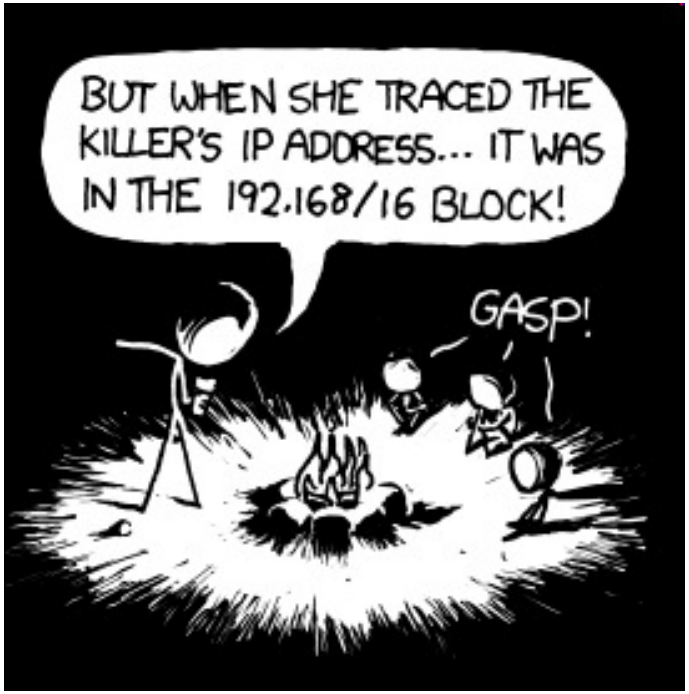
The Importance of IPv6 Test & Evaluation in the Enterprise

April 27, 2011

Jeremy Duncan
Senior Director & IPv6 Network Architect
Cyber Security Solutions

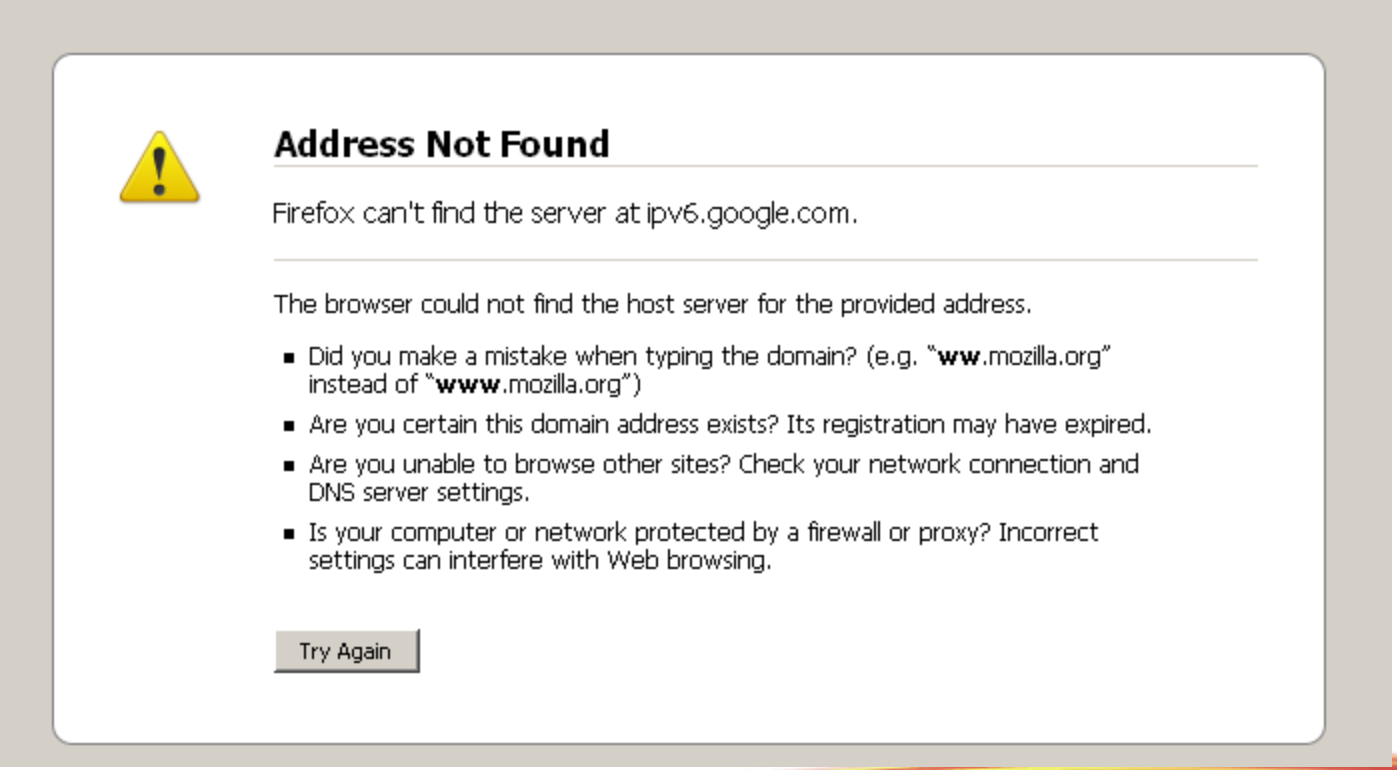
Overview

- Why Enterprise-level IPv6 integration testing is needed
- When this testing must happen
- What type of testing must be done
- How to develop a test and evaluation master plan for your enterprise



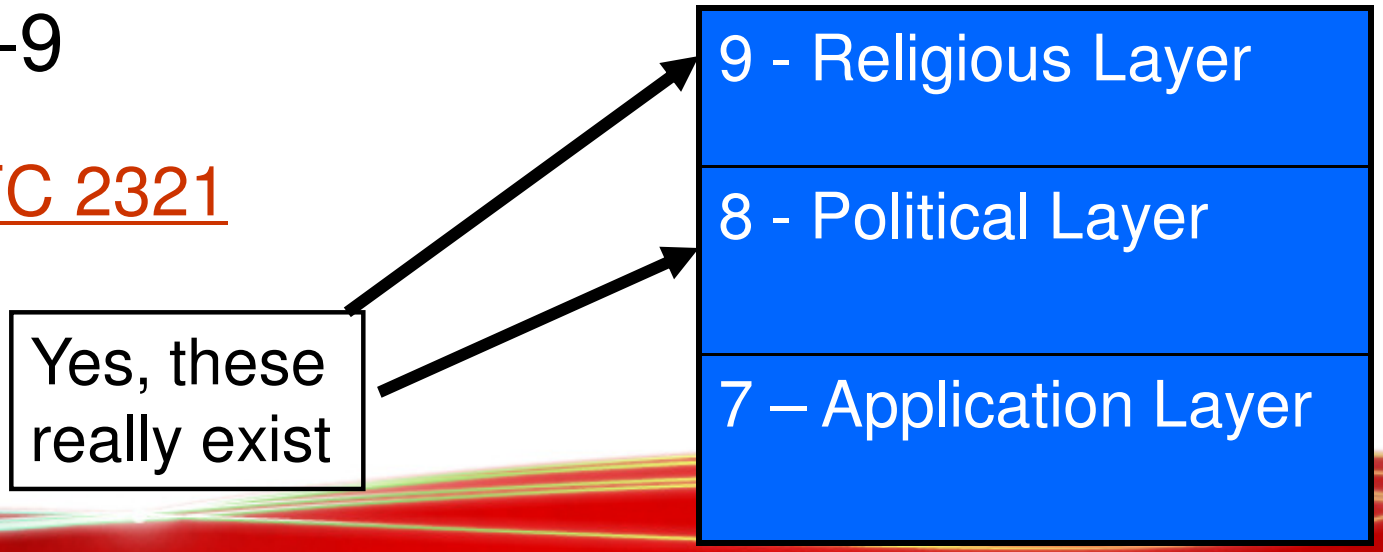
Why IPv6 Integration Testing is Needed

- Reason# 1: You don't want this to happen to your live business applications….



Why IPv6 Integration Testing is Needed

- IPv6 testing on individual networking devices is well established (IPv6 Ready, DoD, NIST, etc.)
  - The Internet "plumbing" will work
- IPv6 has strong integration impacts on OSI Layers 7-9
  - See RFC 2321



Some Real-World Scenarios from Today

- Windows XP and IPv4-only AAAA DNS requests
- Windows 7 defaulting to IPv6 for Home Groups
- Web-based Java application not listening on IPv6 even if the server is IPv6 enabled
- Home grown C+/.NET/Java business applications can't configure IPv6 address or accept IPv6 connection
- Database connections only in IPv4
- Some SNMPv3 implementations only done in IPv4

Some Real-World Scenarios from Today (cont.)

- Firewalls not firing on identical IPv4 rules for IPv6
- IDS not picking up on simple attacks over IPv6
  - DDoS, SYN-flood, malware, tunneling
- IPv6 network infrastructure may need Stateless Address Autoconfiguration ***and*** DHCPv6
- Architectural support for Secure Neighbor Discovery
  - Windows client support not quite available

Some Real-World Scenarios from Today (cont.)

- Network layer “gaps”
  - Cisco VRF-Lite & OSPFv3
  - RA Guard for non-Cisco switches
  - IPSec isn’t automatically there
- Firewalls and IPv6
  - McAfee Sidewinders won’t do High Available (HA) clustering when IPv6 is enabled
  - Cisco ASAs won’t do OSPFv3

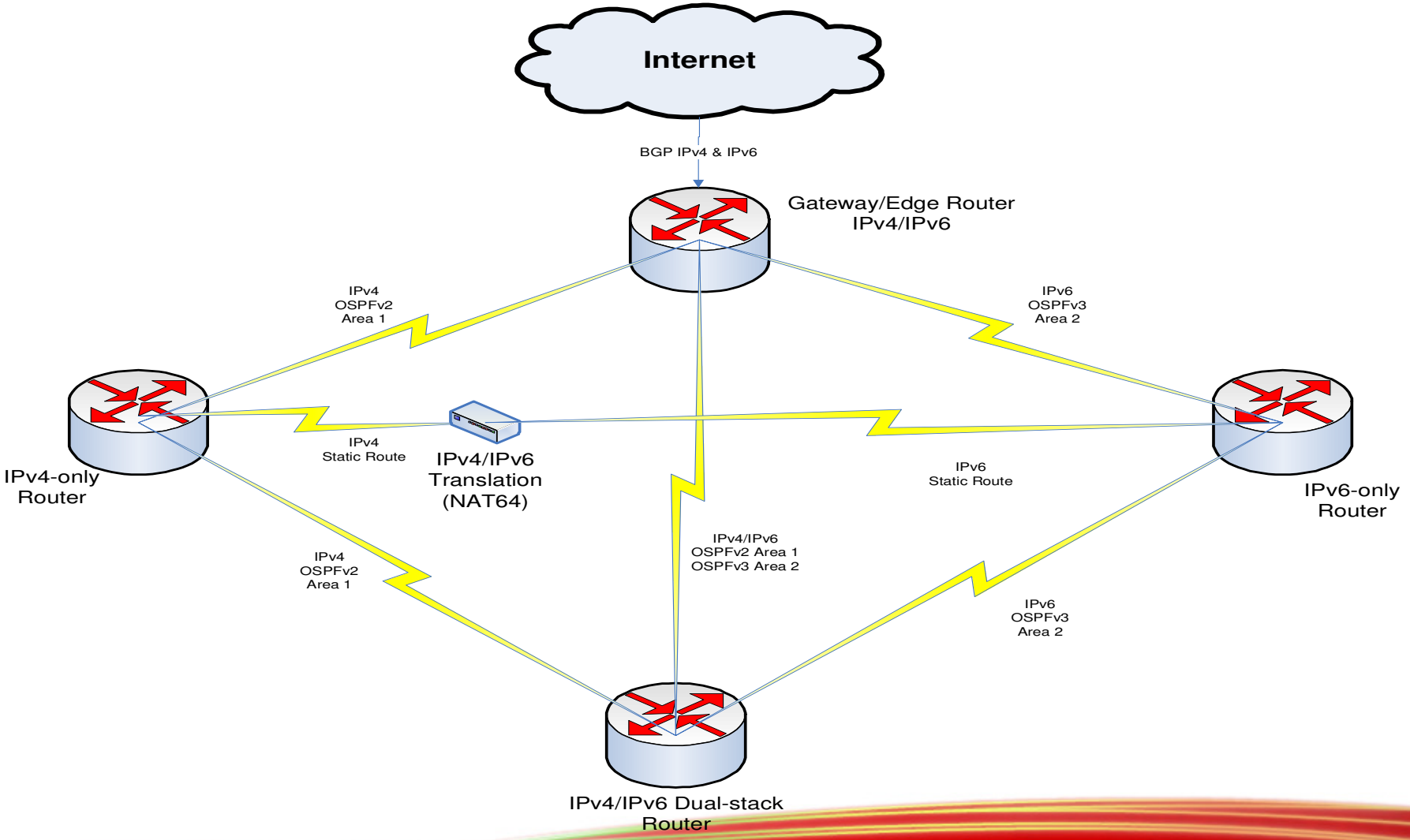
When Should this Testing Occur?

- Develop an IPv6 Architecture for your enterprise that answers how IPv6 affects routing, switching, security, mail, DNS, directory services, web applications, and home-grown applications
- Develop an IPv6 transition and technical implementation plan
- Write and communicate your test and evaluation master plan to your application and system owners
- Now test…

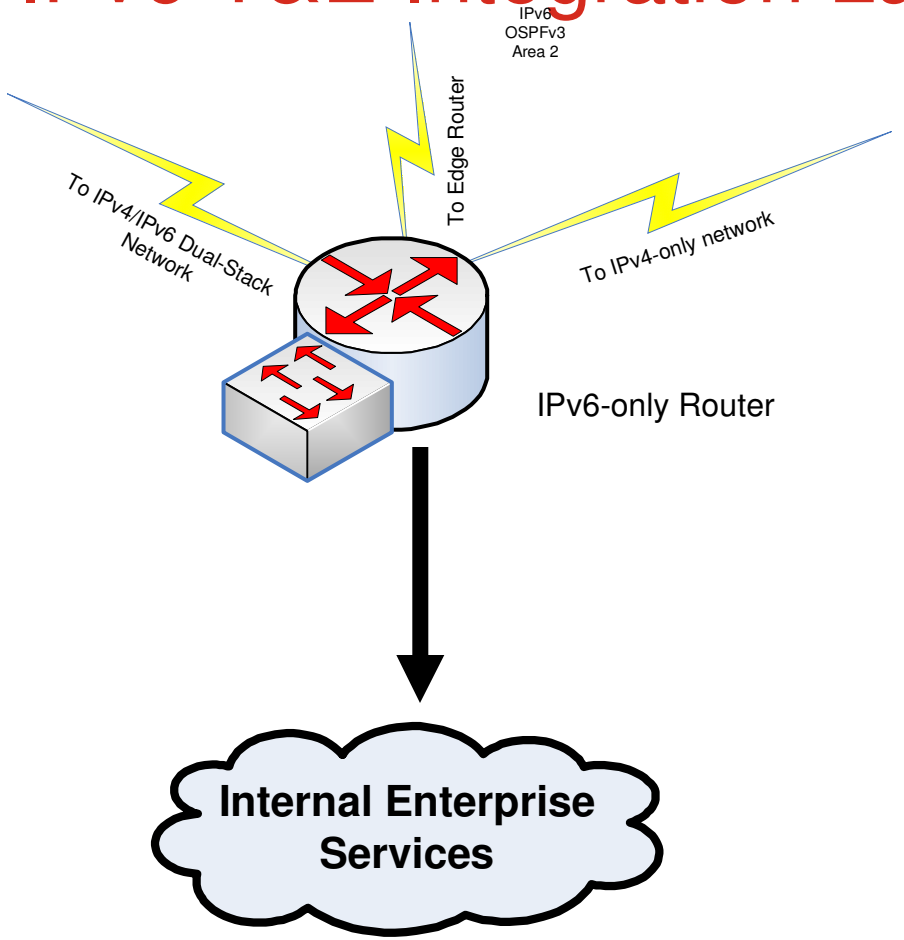
Build an IPv6 T&E Integration Lab

- IPv6-only
  - Should mirror your IPv4-only test network in devices and applications. However, disable all IPv4 addressing, routing and management.
- Dual-Stack
  - Enable IPv6 on a mirrored IPv4 test network keeping IPv4 as a duplicate network protocol
- As-is IPv4 only
  - Must be provided for legacy users and systems in IPv4-only. Provide a translation gateway between the other networks.

Build an IPv6 T&E Integration Lab (cont.)



Build an IPv6 T&E Integration Lab (cont.)



What kind of testing should I do?

- Pre-Test Assessment
- Functionality & Interoperability
- Performance
- Security
- Post-Test Documentation

Pre-Test Assessment

- Gather your COTS vendors, test engineers, and system engineers in a room
  - Communicate your test strategy & plan
  - Solicit capability statements on how their systems meet the organization's IPv6 architecture
- Talk-through test procedures and methodology
  - Document IPv4 dependencies
- Identify success criteria
  - Pass/Fail or Information only?

Functionality & Interoperability Testing

- Focus all your tests and user stories on end-to-end operation of the system and application only over IPv6 first (on the IPv6-only infrastructure).
- Document failures
- Repeat failed test cases in the Dual-Stack network
- Ensure IPv4-only users still have functional use of system over IPv4 (test done on IPv4-only network)

System Performance Testing

- Benchmark the system/application in the IPv4-only infrastructure
  - Capture concurrent TCP sessions
  - Capture latency
  - Capture throughput on intermediate devices in system
- Repeat benchmark the system/application in the IPv6-only and Dual-Stack infrastructure
  - Capture concurrent TCP sessions
  - Capture latency
  - Capture throughput on intermediate devices in system
- Document differences and variations

Security Testing

- The most involving assessment
- Your current auditing tools may not help you much
  - Retina – No IPv6 support
  - Nessus – Limited IPv6 capabilities
  - OpenVAS – No IPv6 support
- Some better tools
  - Mu Dynamics – great IPv6 capabilities
  - Open Source always wins (NMAP, Scapy, NetCat, John the Ripper, etc.)
  - Spirent ThreatEx

Security Testing, etc.

- Mirror scans, intrusion and detection tests in IPv6
- Test new threats for IPv6
  - IPv6 in IPv4 tunneling (in UDP, etc.)
  - Extension header complexities
- Document the results

Post-Assessment Documentation

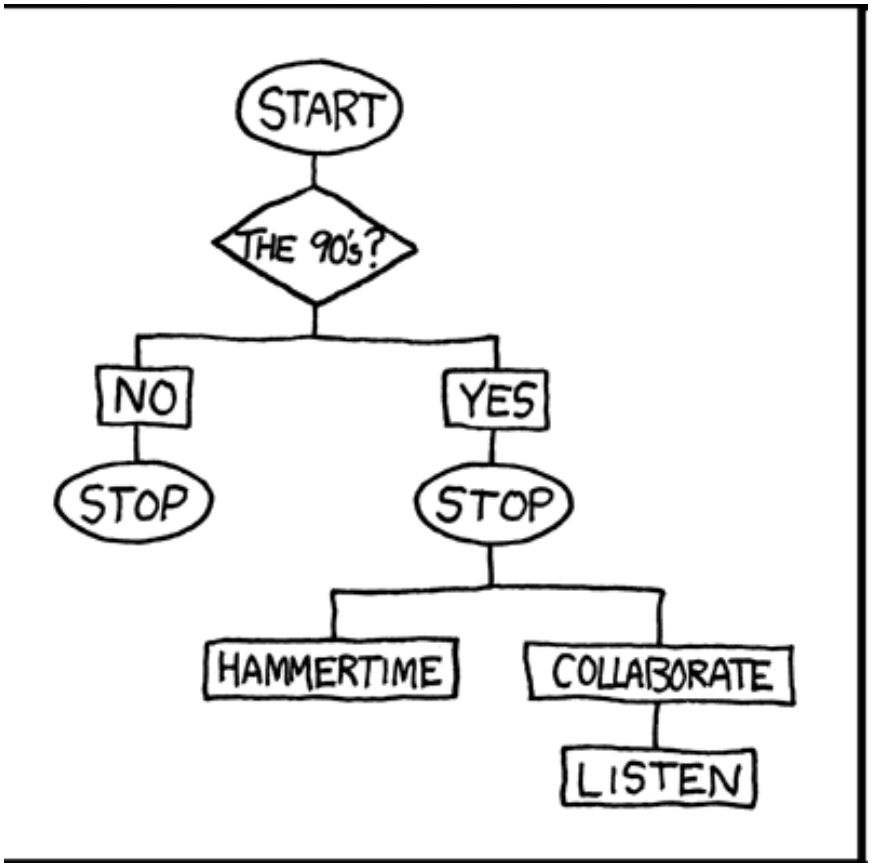
- Have a “hot wash” or after-action with the test and system engineers
  - IPv4 functional dependencies
  - IPv6 performance metrics
  - IPv6 security issues
- Pass/Fail ***or*** document and mitigate
  - Your choice

Test & Evaluation Master Plan Strategy

- Design it with all stakeholder input
- Know your organization
- Develop a simple process
- Integrate it into working evaluation process

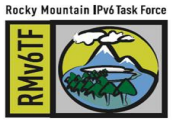
Test & Evaluation Master Plan

- Define the roles and responsibilities
  - Who approves results
  - Who tests
  - Who schedules
- Develop the test architecture
- Design the process



Test & Evaluation Master Plan, cont

- Define high-level success criteria
- Write your generic test procedures
- Communicate it!



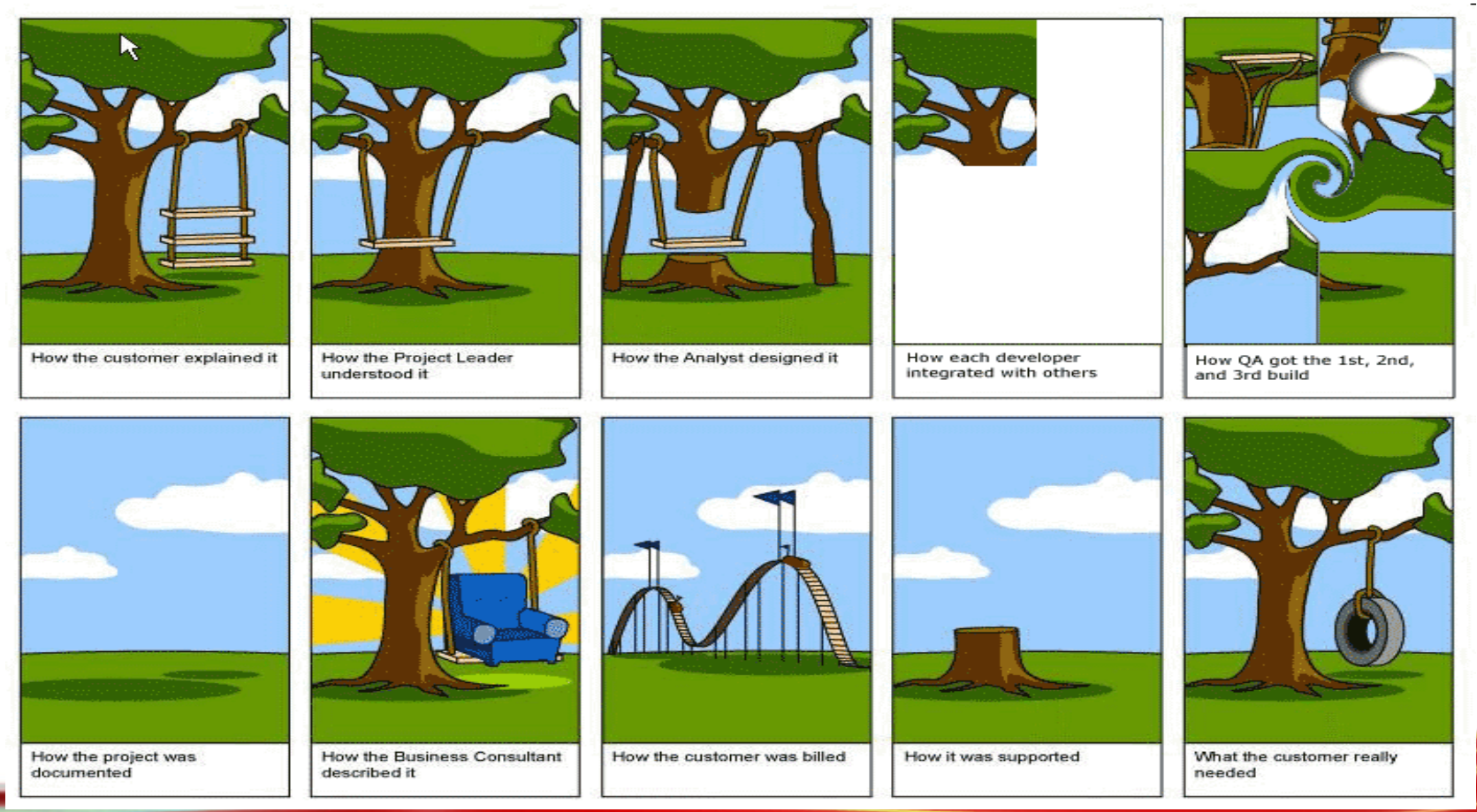
COMMAND INFORMATION

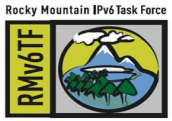
Summary

- Why Enterprise-level IPv6 integration testing is needed
- When this testing must happen
- What type of testing must be done
- How to develop a test and evaluation master plan for your enterprise
  - For all you .mil engineers, talk to me later….

Conclusion

- What you don't want in your IPv6 deployment is **more** frustrated users





COMMAND INFORMATION

Thank You

Jeremy Duncan

Command Information

Email: Jeremy.Duncan@commandinformation.com

Twitter: Command_Info

Facebook: Command Information

Google Voice: 540.440.1193