



# IPv6 Deployment Lessons-Learned and Keys to Success

# Background

- **14 years of active IPv6 deployment activities on various DOD networks, on wide-area and enterprise scales**
- **With that experience, we have learned:**
  - There are some key factors to success
  - There are some common mistakes that everyone makes

# Various Initiatives

- **2001 – Defense Research and Engineering Network (DREN) IPv6 Testbed**
  - “If you build it, they will come” (NOT!)
  - In operation until 2009 – now done with testbeds
- **2003 – DOD IPv6 “pilot”, using DREN**
  - Take an existing WAN, and make it dual-stack
  - Full-production operation
- **2004 – IPv6-enabling local enclaves (like SPAWAR and HPC sites)**
  - The network was easy, the computers were much more work
- **2008 – Taking it to the next level**
  - Management LANs IPv6-only
  - Initiative to make one enterprise network 100% dual-stack
  - All public-facing services IPv6-enabled (first “all green”)
- **2010 – Enterprise network 98% dual-stack (took 2 years)**
- **2013 – Next-generation DREN**
  - An IPv6 network, with legacy support for IPv4
  - All customer connections MUST be dual-stack

*Met the Federal Milestones – 4 years ahead of schedule in some cases!*

# Steps Taken to Achieve This

- **For each network where IPv6 was deployed**
  - There was long-term vision, with near-term goals and milestones
  - There was at least one “champion” that drove the initiative, and had support from the rest of the organization
  - Leadership supported the goal
    - Authorization to make network changes
    - Capital funding for technical refresh of equipment
- **External mandates and pressure not sufficient**

# IPv6 Today

- **IPv6 is mainstream, and has reached significant maturity**
  - But we have not yet reached full parity with IPv4
- **Security and performance of IPv6 is equivalent to IPv4**
- **IPv6 deployment does not have to be costly**
  - If you start early and use an incremental approach, and use technical refresh, there is almost no cost to deployment
  - If you procrastinate, it will be costly
  - If you haven't started, you may be too late

# Key Factors to Success

- **Have the right perspective and the correct paradigms**
- **Have a corporate IPv6 culture, with proper vision and leadership**
- **Keep it simple**
- **Employ good mandates and incentives**
- **Measure and share progress**

# Incorrect Perspective

- **Experience has shown that most organizations that plan to deploy IPv6, or IPv6-enable their products, initially have an incorrect perspective on how to get there**
- **Typical errors in thinking:**
  - “What’s the business case or Return on Investment (ROI) if I spend money and effort on deploying IPv6 now?”
  - “How can I charge more money for IPv6, since it is a feature?”
  - “I can’t do IPv6 because things will break when I turn off IPv4”
  - “I can’t do IPv6 because it costs too much. It is not a high-priority”
  - “I don’t need IPv6, because I have plenty of IPv4 addresses”
  - Thinking that you need to be conservative with IPv6 addresses, like we have been with IPv4

# Proper Perspective

- **What is it you are trying to do?**
  - Add full support for IPv6 everywhere in your network, your products and services, wherever you have IPv4 today; and continue to support IPv4 in parallel for the next decade or more. You will know when and where to shut off IPv4, so don't worry about it now
  
- **Why are you doing this?**
  - The future of the Internet is at stake. It cannot grow without ubiquitous IPv6. You are part of "ubiquitous"
  - If we don't get on with it, bad things will happen (Carrier-Grade Network Address Translation (CGN))



# Proper Perspective

- **What is the business case for IPv6?**
  - There is no early return on investment
  - The benefit is long-term, once the rest of the Internet reaches critical mass of IPv6-deployment
  - Soon, some of the rest of the world will not have IPv4, so how will you communicate to them?

# Benefits of IPv6 Today (Examples)

- **Addressing**
  - Can better map subnets to reality
  - Can align with security topology, simplifying Access Control Lists (ACLs)
  - Sparse addressing (harder to scan/map)
  - Never have to worry about “growing” a subnet to hold new machines
  - Auto-configuration, plug-n-play
  - Universal subnet size, no surprises, no operator confusion, no bitmath
  - Shorter addresses in some cases
  - At home: multiple subnets rather than single IP that you have to Network Address Translation (NAT)
- **Link Local implemented on every interface**
- **Multicast is simpler**
  - Embedded Rendezvous Point (RP)
  - No Multicast Source Distribution Protocol (MSDP)
- **Mobile IPv6 is cleaner/simpler than in IPv4**

# Proper Perspective

- **What will it take in time and resources?**
  - You have a choice:
    - Use normal technical refresh cycles to roll out IPv6, over 5+ years at almost no extra cost
    - Wait until it is really necessary or mandated, then do it quickly at very high-cost (think “forklift upgrades”)
  - Lesson: If you haven’t started yet, you are probably too late to take the inexpensive path. Delaying any longer will just make it worse

# Culture, Vision, Goals

- **Successful enterprise IPv6 deployments require:**
  - Clear vision and goals, set and communicated from the top (CIO/CEO)
  - There needs to be one or a few individuals leading the charge, in a full-time role
  - The IT staff must be enabled (given authority) to make it happen
  - The whole organization (everyone involved in IT) must embrace an IPv6 culture
  - Status and progress must be measured and published
- **It is much more than just an IP networking issue**

# Keep it Simple

- **Common Problem:**

- I have seen agencies get bogged down in years of planning, before passing a single IPv6 packet
  - It is mostly a waste because they have the wrong mindset and worldview, and are thinking IPv4 paradigms (address conservation for example)
- Agencies can be overwhelmed by not knowing what to do or where to start

- **A Simpler Approach:**

- Start early to gain operational experience
- (For 2012 objective): Can you get to my website via IPv6? If not, fix that
- (For 2014 objective): Can my users get a good score at <http://test-ipv6.com>? If not, fix that

# Keep it Simple

- Example: (from an earlier presentation to this forum):

## Your assignment

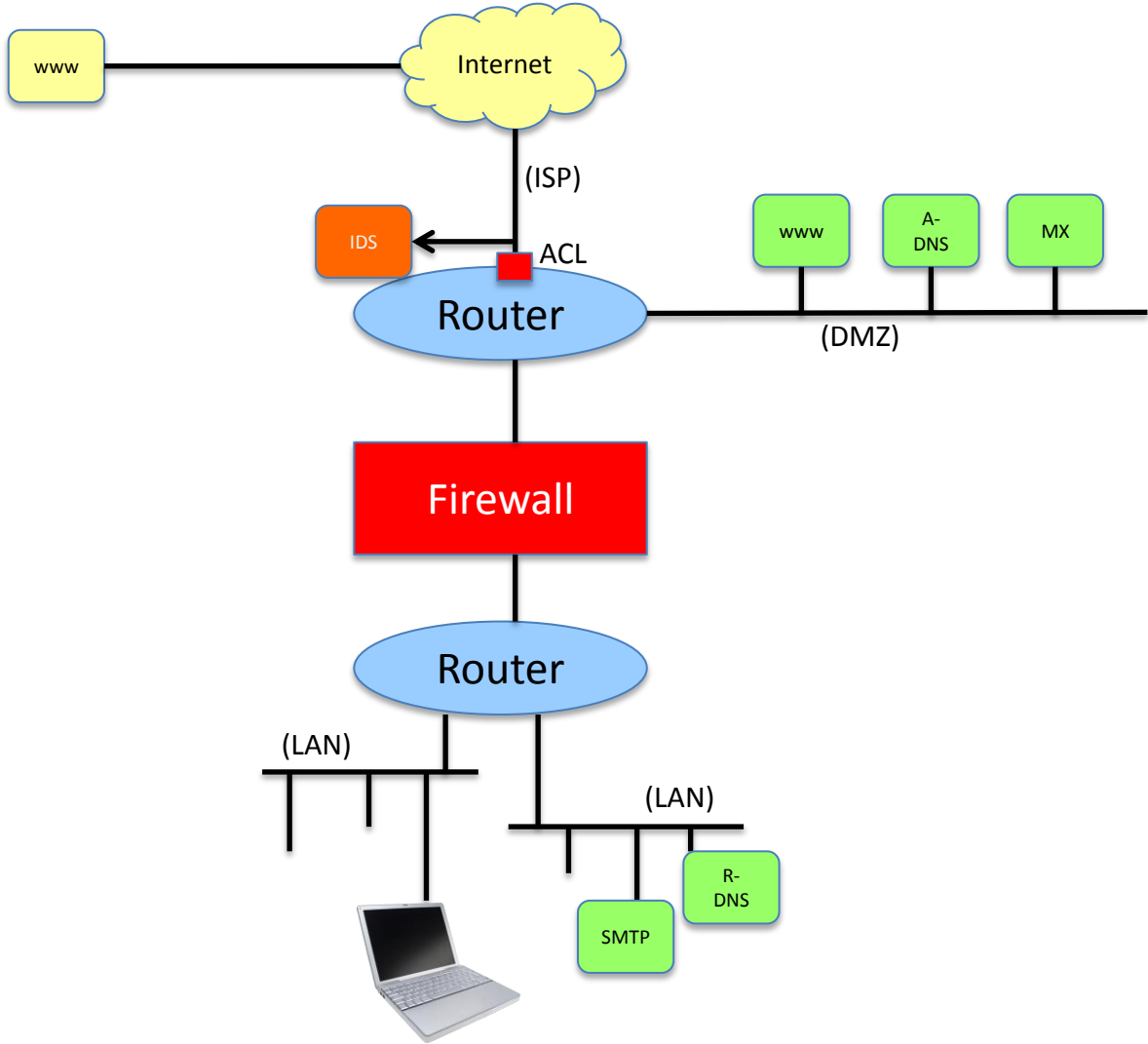
- From your office desktop computer, go to <http://test-ipv6.com>
  - If you don't have 10/10, report the problem to your IT help desk, network staff, and others as appropriate.
- With the help of your network operations folks, map out every single device that a packet needs to go through to get from your desktop to a website out on the Internet, and back again.
  - For every device and link in that path, ask:
    - Is it capable of supporting IPv6 today?
    - if not then what will it take to upgrade it (software, hardware)?
    - When can you turn on IPv6? What is stopping you?
- Don't let IT marketers in the door, unless their corporate web site is IPv6-enabled.

10/10

# Example Goal: Meet the 2014 Milestone

- **To start with, from your desktop web browser you must be able to open any IPv6-only web page out on the Internet**
- **To do this, an IPv6 packet from your desktop must be able to reach that remote website, and the IPv6 packets from that website need to be able to reach your desktop, preferably as native end-to-end**
- **What are the things you need to do to make this possible?**

# Let's Walk Through the Pieces

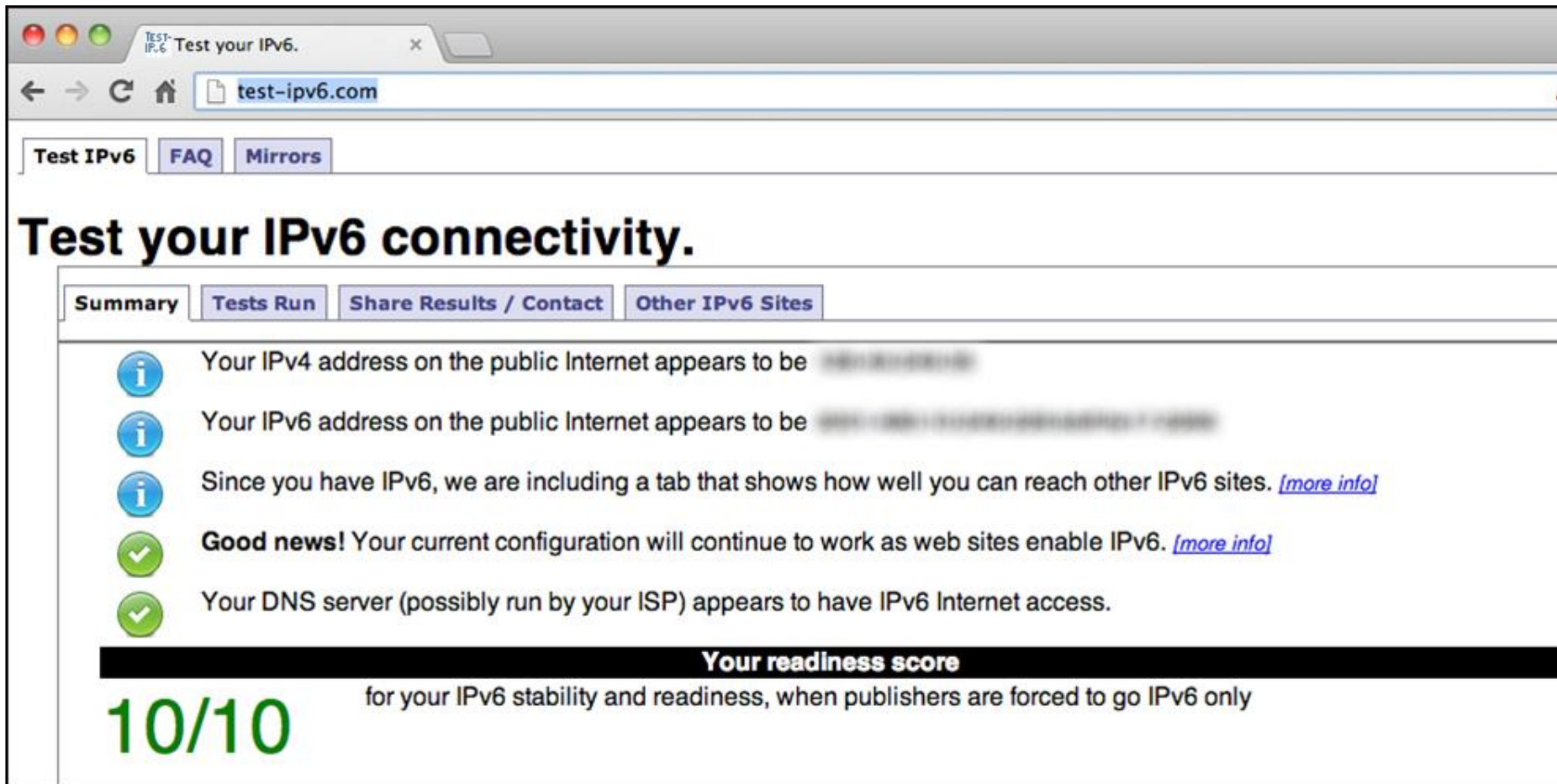




# Native IPv6 from your Desktop

- **Inventory of Activities**
  - Configure your border router to route IPv6 packets to/from your ISP
  - Make sure IPv6 packets will make it through your firewall, and other components of your security stack
    - This can be VERY hard, so start on this early
  - Put an IPv6 address on all your internal router interfaces
    - This is VERY simple, once you have your addressing plan
  - If you disabled IPv6 in your PC for some reason, turn it back on
  - Test: Browse to <http://test-ipv6.com>

# Verify Success








TEST IPv6 Test your IPv6. x

test-ipv6.com

Test IPv6 FAQ Mirrors

## Test your IPv6 connectivity.

Summary Tests Run Share Results / Contact Other IPv6 Sites

-  Your IPv4 address on the public Internet appears to be **192.168.1.100**
-  Your IPv6 address on the public Internet appears to be **2001:db8:1:1::1**
-  Since you have IPv6, we are including a tab that shows how well you can reach other IPv6 sites. [\[more info\]](#)
-  **Good news!** Your current configuration will continue to work as web sites enable IPv6. [\[more info\]](#)
-  Your DNS server (possibly run by your ISP) appears to have IPv6 Internet access.

**Your readiness score**

**10/10** for your IPv6 stability and readiness, when publishers are forced to go IPv6 only

# Addressing Plans

- **A key early requirement to any IPv6 deployment effort is to obtain IPv6 address space, and come up with a plan as to how it will be allocated**
- **Without sufficient operational experience with IPv6 deployment, you WILL get it wrong at first**
  - Usually takes the 3<sup>rd</sup> time to get it right
- **Planners are hindered by IPv4-thinking**
  - Being conservative with address space
  - Thinking “hosts” instead of “subnets”

# Addressing Plans

- **Common Mistakes:**
  - Doing other than /64 for subnets
    - Didn't read RFC 4291 or 5375
  - Thinking that the addressing plan has to be perfect the first time
    - Because you “believe” you can't afford to re-address
  - Choosing allocations for sites based on size of site
    - Because /48 for all sites is too wasteful
  - Justification “upwards”, instead of pre-allocation “downwards”
  - Host-centric allocation instead of subnet-centric

# The Problem with Addressing Plans

- Everyone makes the same common mistakes
- It comes from “IPv4 thinking”. You have to make a major paradigm shift
- We say:

*“Anyone who says that using /64s for subnets or using /48s for sites is wasteful, is unqualified for developing your IPv6 addressing plan.”*

# Deploy “Native” IPv6

- **Common misunderstanding that native IPv6 implies IPv6-only (turning off IPv4)**
  - We can’t turn off IPv4, yet
- **When we say “native”, we mean:**
  - Not translated
  - Not tunneled
- **“native” is really short for “native end-to-end”**
  - The goal is to have communications paths where IPv6 packets are transported “natively” from client to server (end-to-end), without going through translators (like today’s NAT devices), and without being “tunneled” inside IPv4 networks

Saltzer, J. H., D. P. Reed, and D. D. Clark (1981) "End-to-End Arguments in System Design"

# Summary Do's and Don't's

## Do:

- **Get buy-in from corporate leadership, especially CIO**
- **Develop a corporate culture for IPv6**
  - Involve all parts of the organization, not just the network guys
  - Have a local champion
  - Include IPv6 in every IT initiative
- **Take baby steps**
  - Go for the low-hanging fruit
  - Get experience along the way
- **Leverage tech refresh rather than spend \$\$\$ on fork-lift upgrades out-of-cycle**
  - It doesn't have to be very expensive
- **Start now**
  - If you haven't, you are already quite late to the game
- **Start by IPv6-enabling your public-facing services**
  - Work from outside-in, and from bottom-up
- **Go native**
  - Avoid translators, tunnels, and other transition schemes
- **Only choose suppliers that have a good IPv6 story**

# Summary Do's and Don't's

## Don't:

- **Waste time developing a complete transition plan with no operational experience**
- **Base your addressing plan on conservative IPv4 practices**
- **Waste time on a comprehensive addressing plan without operational experience**
  - Consider the first one a throw-away
- **Waste time trying to develop a business case (ROI) for deploying IPv6**
  - It is a matter of business survival
- **Be afraid to break some glass**
  - World IPv6 day validated that



# Acquiring IPv6 Capable Products

- **Vendors will say that their products support IPv6, or are IPv6-capable.**
  - This means nothing
- **Lessons-learned over 14 years:**
  - All products lack IPv4/IPv6 feature parity
  - Vendors aren't "eating their own dog food"
  - IPv6 bugs and missing features do not get resolved unless the company has a strong corporate commitment to IPv6, or there is airtight contractual language that requires it

# Lessons from Recent DREN III Acquisition

# DREN IPv6 Contractual Requirements

- **DREN III is an IPv6 network, with legacy support for IPv4**
  - Establish the vision
- **IPv6 must work as good as, or better than, IPv4**
  - This is measurable, and enforceable
- **Must not deploy anything in the network that does not comply with this requirement**
  - Non-compliant components can be rejected
- **All network management functions are IPv6-only (no IPv4)**
  - No cheating

# How Well did this Approach Work?

- **During acceptance testing, lack of IPv6 support was identified in various products and services. Examples:**
  - Large network management product was missing IPv6 support, and had to be replaced
  - 2-factor authentication lacking IPv6 support, will need to be replaced
  - And many others
- **All exceptions are tracked, and must be resolved**
- **All use of IPv4 on the management network is tracked until removed**
- **Summary: The approach works very well**

# Observations

- **DREN III requires that all customers connect with dual-stack (IPv4 + IPv6), run BGP, support jumbo frames, and support 802.1q “tagging”**
- **We thought the big problem for some customers was going to be routers and other Customer Premise Equipment (CPE) that didn’t support IPv6**
- **Surprisingly, IPv6 was supported in all customer products we interfaced with**
  - Even if those customers didn’t care about IPv6, had never tried to make their network support IPv6, nor tried to purchase IPv6-capable products
- **Lesson: Mainstream products have basic IPv6 support today**

# Other Observations

- **We encountered significant apathy towards IPv6 at many customer locations**
  - Most had no knowledge of the Federal or DOD mandates
  - Without some incentive, IPv6 does not get turned on
  - Too many other priorities, and no perceived benefit
- **But, there was no resistance to enabling it on the CPE router**
  - A few tried to quote the STIGs or other policies that appear to say IPv6 must be disabled
- **Lesson: We need to provide more incentives**

# Evaluating New Products

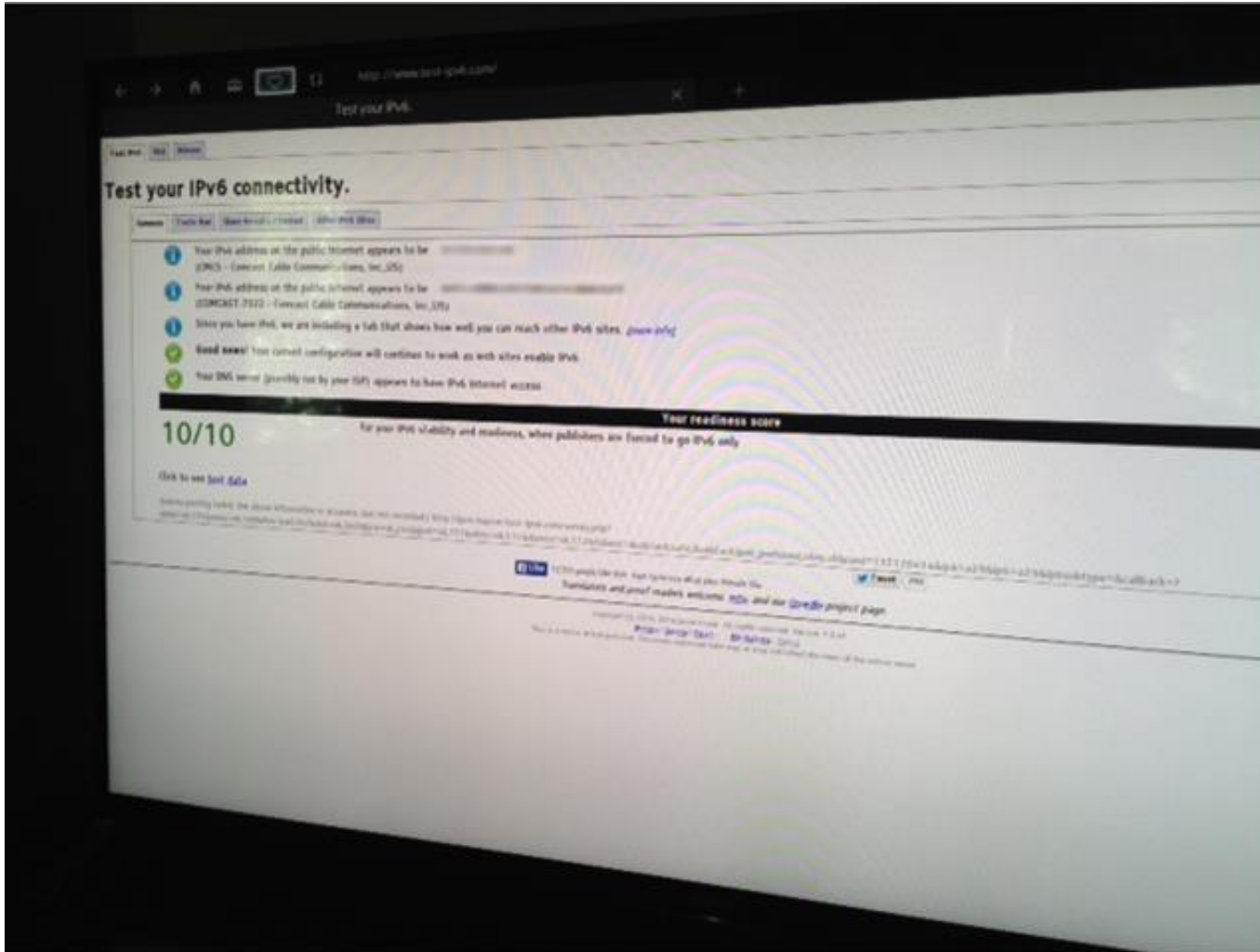
- **Our #1 Rule:**
  - If we can't get to the company or product website via IPv6, we won't consider such products
  
- **Why this hard line?**
  - We learned the hard way that without strong corporate commitment to IPv6 support, it will take forever to get IPv6 bugs fixed or features added
  - We learned that the corporate website being IPv6-enabled was a good indicator of corporate commitment to IPv6
  - This has been tested many times, and it works
  - In the process, we encourage industry to IPv6-enable their public-facing services
  
- **Examples**
  
- **#2 Rule:**
  - Verify “eating your own dog food”
  - Test product in production IPv6 network

# My Own Current Efforts

- **Achieve stable addressing for enterprise networks**
  - Make Dynamic Host Configuration Protocol for IPv6 (DHCPv6) work (harder than you think)
  - Eliminate StateLess Address AutoConfiguration (SLAAC) where possible
- **Still trying to make network management IPv6-only**



# Even my TV does IPv6



# Questions?

Ron Broersma  
DREN Chief Engineer  
[ron@dren.hpc.mil](mailto:ron@dren.hpc.mil)