Department of Defense

High Performance Computing Modernization Program

Defense Research and Engineering Network IPv6 Pilot --

3 years of IPv6 in the real world

Sept 19, 2006

baird@hpcmo.hpc.mil

Outline

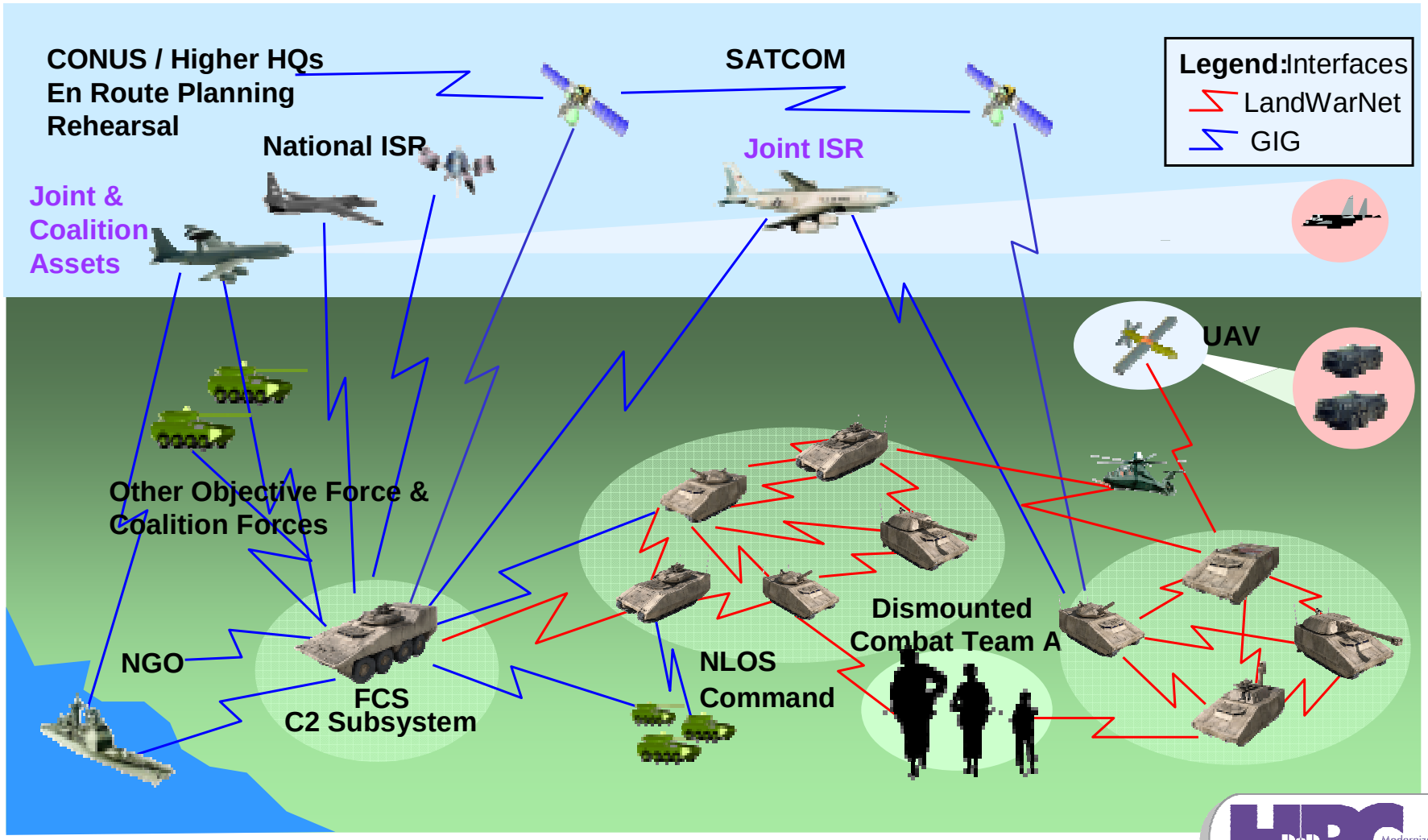
- Introduction
- The DoD High Performance Computing (HPC) Modernization Program
- The Defense Research and Engineering Network (DREN)
- DREN IPv6 pilot
- Some Lessons Learned
  - Why we were successful
  - How we measured success
  - DREN IPv6 pilot goals accomplished
- Final Thoughts

Introduction

In the U.S. consumer market, IPv6 Leads To…

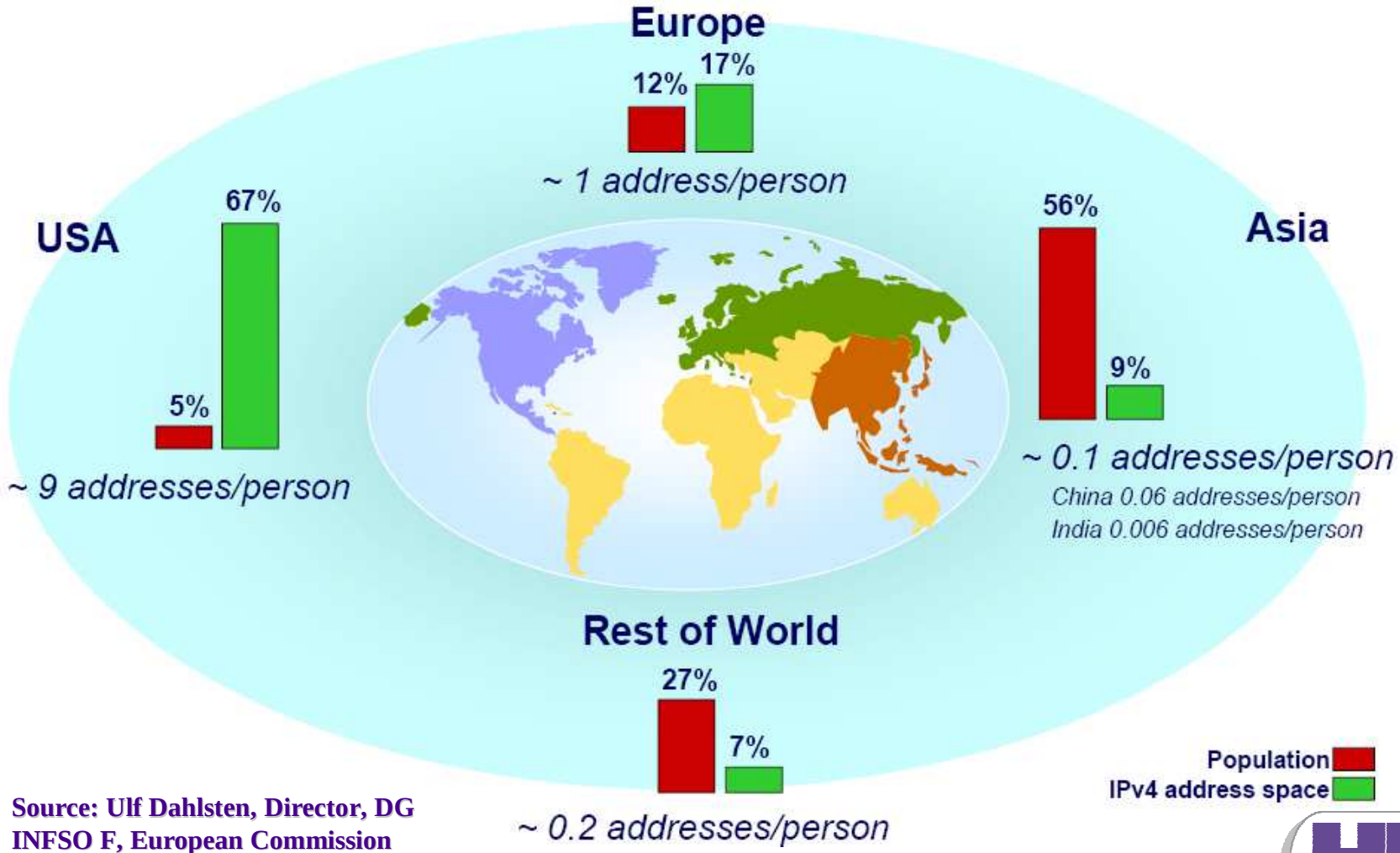
Introduction

In the U.S. DoD, IPv6 Leads To…



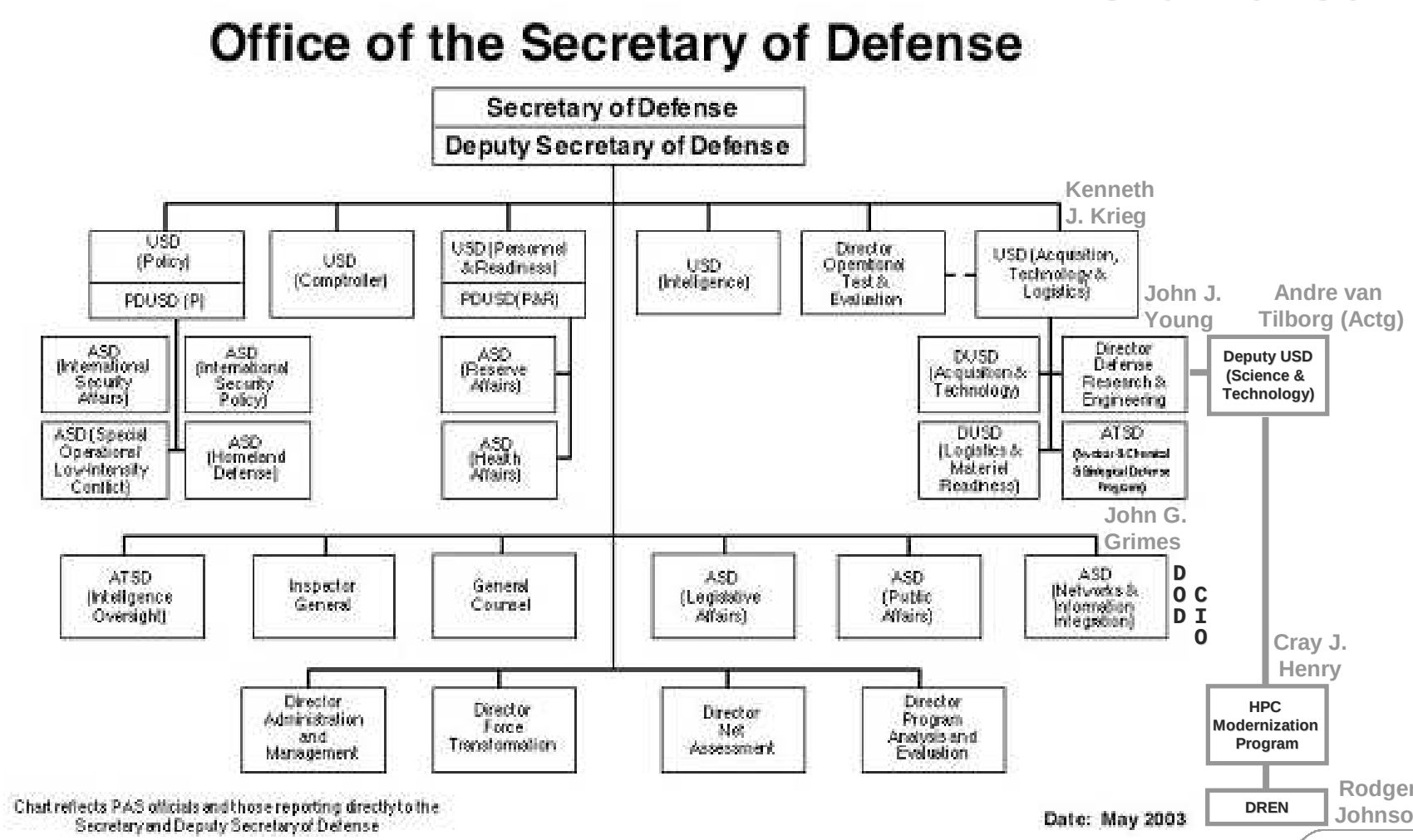
Introduction

While outside the U.S., IPv6 Leads To…

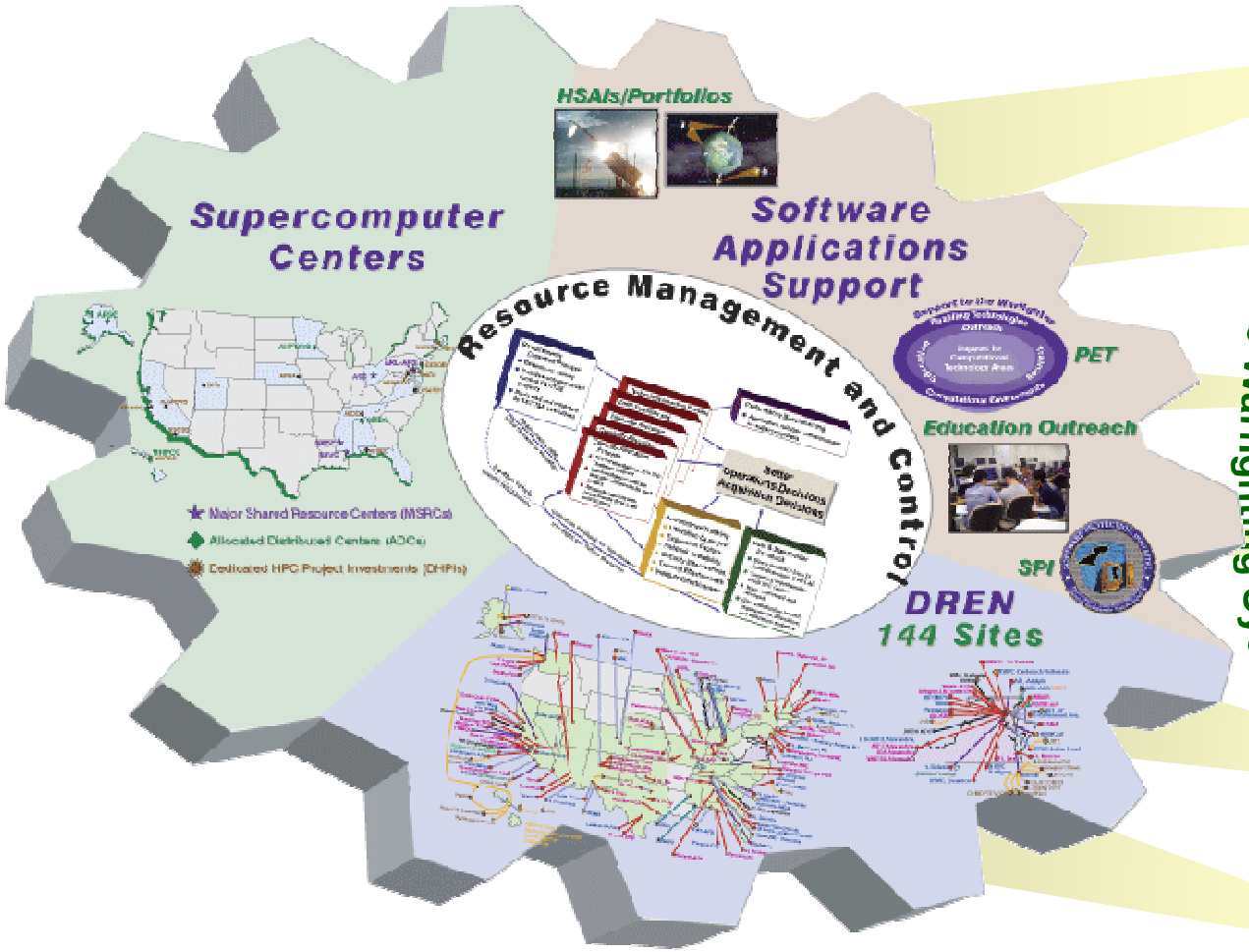


Source: Ulf Dahlsten, Director, DG INFSO F, European Commission

HPCMP
Chain of Command



HPCMP Summary



Transferring Technology into Future Warfighting Systems

Army HPCMP Resource

- *ARL & ERDC MSRCs*
- *AHPCRC & SMDC ADCs*
- *ATC, DPG & CERDEC DHPIs*
- *1,350 Users/25 Locations/122 Projects*
- *51 DREN Sites*
- *10 Challenge Projects*
- *3 Institutes/1 Portfolios*

Navy HPCMP Resource

- *NAVO MSRC*
- *FNMOC, SSCSD, NAWCWD, NSWCCD & NUWC DHPIs*
- *1,645 Users/25 Locations/234 Projects*
- *30 DREN Sites*
- *10 Challenge Projects*
- *1 Institute/2 Portfolios*

Air Force HPCMP Resource

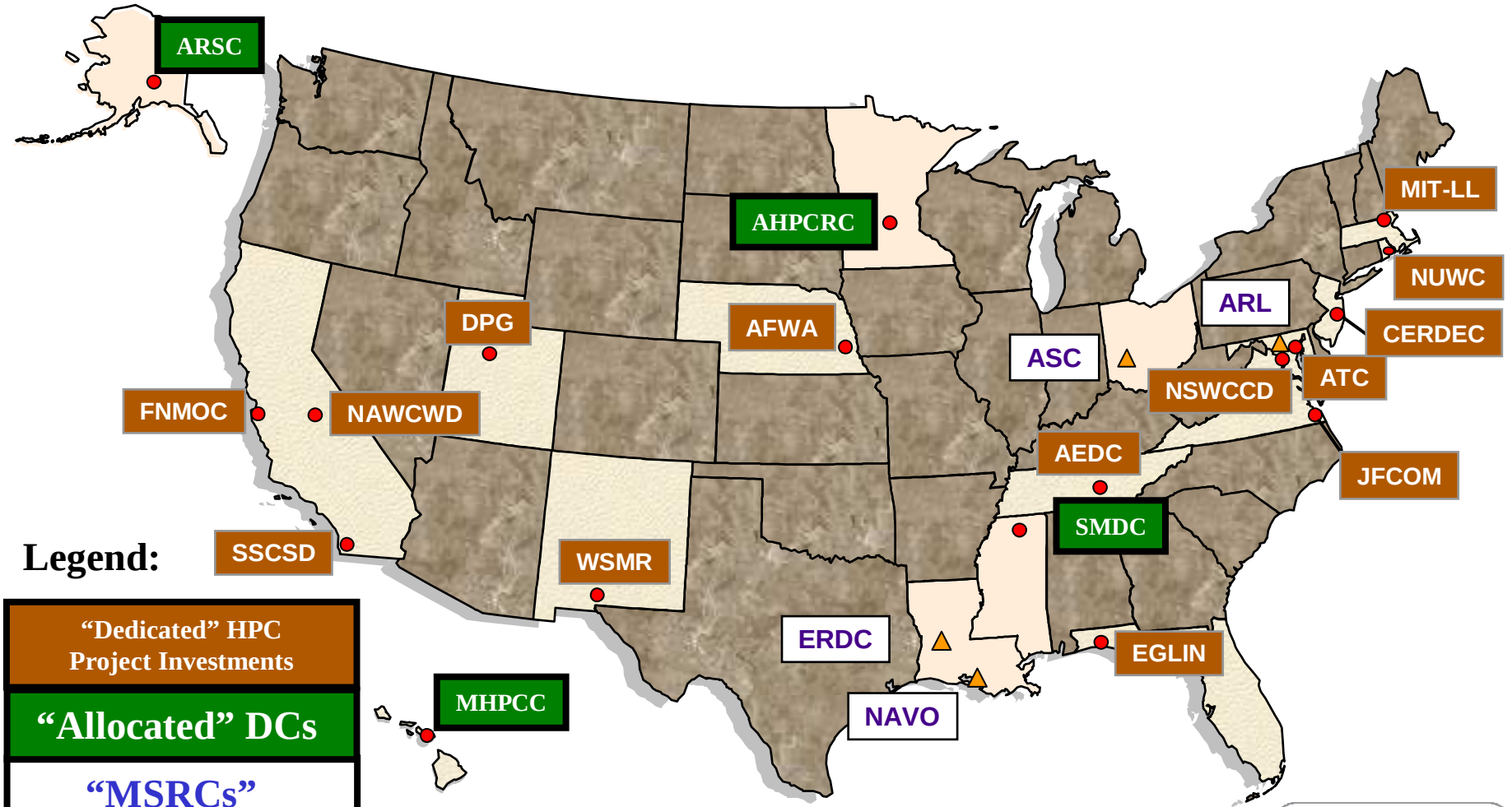
- *ASC MSRC*
- *MHPCC ADC*
- *AEDC/AFSEO, AFWA & MHPCC DHPIs*
- *1,222 Users/36 Locations/207 Projects*
- *20 DREN Sites*
- *14 Challenge Projects*
- *2 Institutes/1 Portfolio*

Defense Agencies/Other

- *DARPA, DTRA, JNIC, JFCOM, MDA, DMSO, & OTE*
- *JFCOM DHPI*
- *400 Users/4 Locations/24 Projects*
- *29 DREN Sites*
- *3 Challenge Projects*

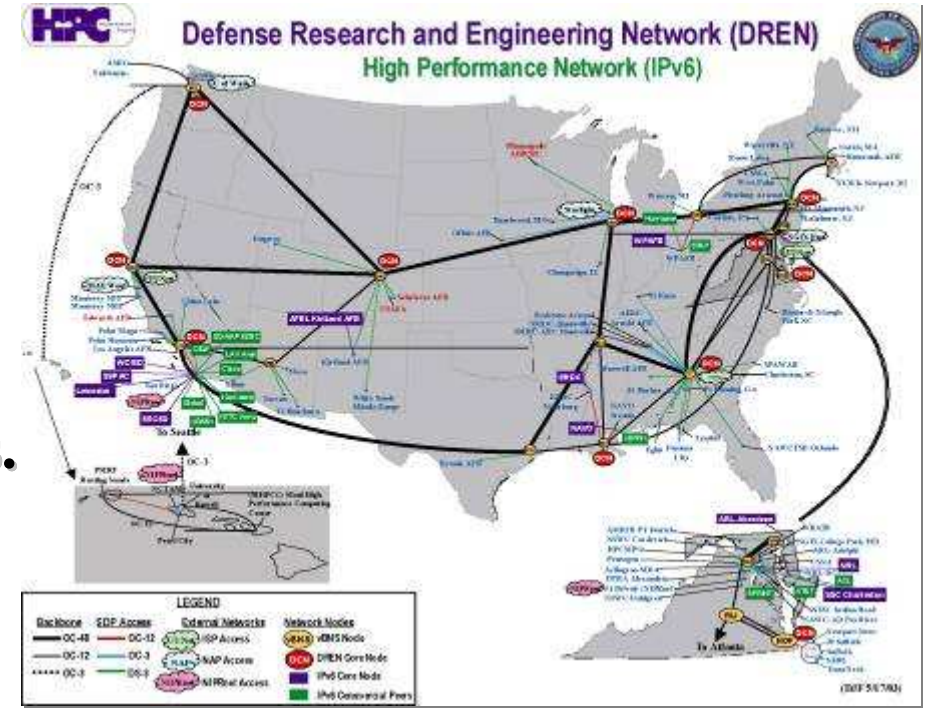
HPCMP

Supercomputer Centers



DREN
Summary

- "Defense Research and Engineering Network"
  - A DoD network supporting the Research, Engineering, Modeling and Simulation, and related communities.
  - Major thrusts are high performance, security, and support of new technologies.
  - High capacity, low latency, predominately unclassified.
  - Peers with the Internet, numerous commercial, and other DoD networks.
  - A commercial service provided by Verizon Business.



DREN
Capabilities

- High speed backbone, OC-192c (10 Gb/s) backbone (CONUS), OC-12c (622 Mb/s) extensions to Hawaii and Alaska.
- 140+ Service Delivery Point (SDP) sites, connected at DS-3 (45 Mb/s) to OC-48c (2.488 Gb/s) rates.
- Internet Protocol version 4 (IPv4) unicast, multicast, and Asynchronous Transfer Mode (ATM) services provided since 1992.
- IPv6 unicast services provided since late 2003.
- IPv6 multicast “soon.”

DREN

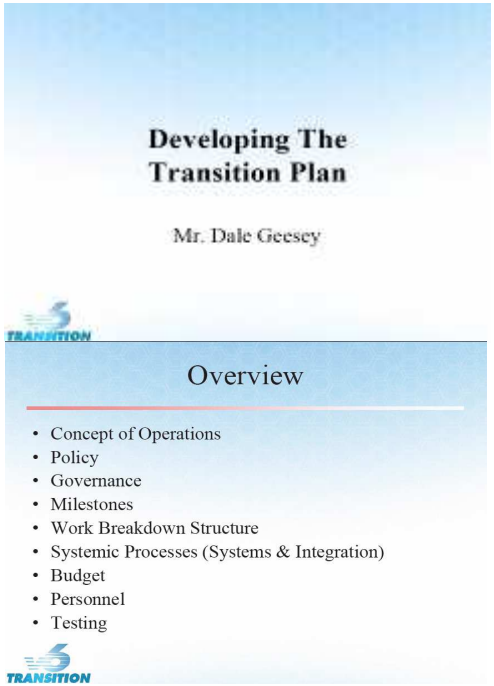
IPv6 History

- 2001
  - Feb – DRENv6 test bed activated.
  - June – Received address allocation from American Registry for Internet Numbers (ARIN).
- 2003
  - June – DoD CIO issues DoD transition memorandum.
  - July – DREN chosen as first DoD IPv6 pilot.
  - Oct – First DREN IPv6 Pilot sites exchange IPv6 packets.
    – MoonV6 begins first interoperability event.
- 2005
  - Aug – OMB issues Federal transition memorandum.
- 2006
  - Aug – DoD, GSA, NASA propose Federal Acquisition Regulation changes for IPv6.

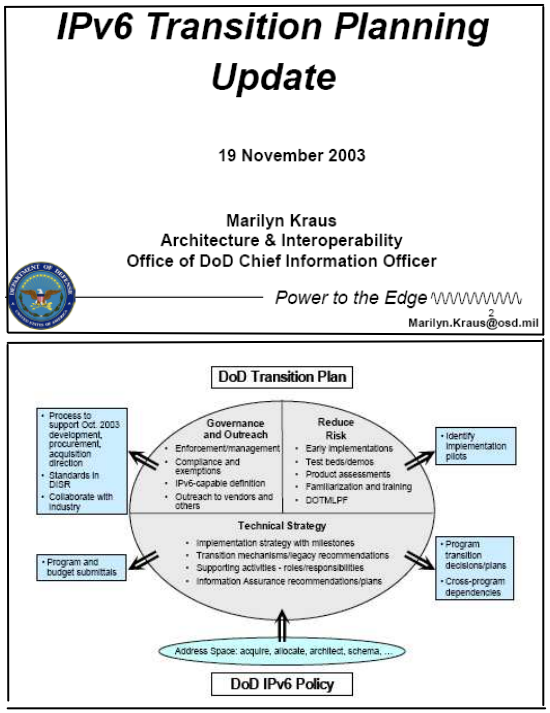
DREN IPv6 Pilot

A different perspective…

- **The perspective of many agencies:**



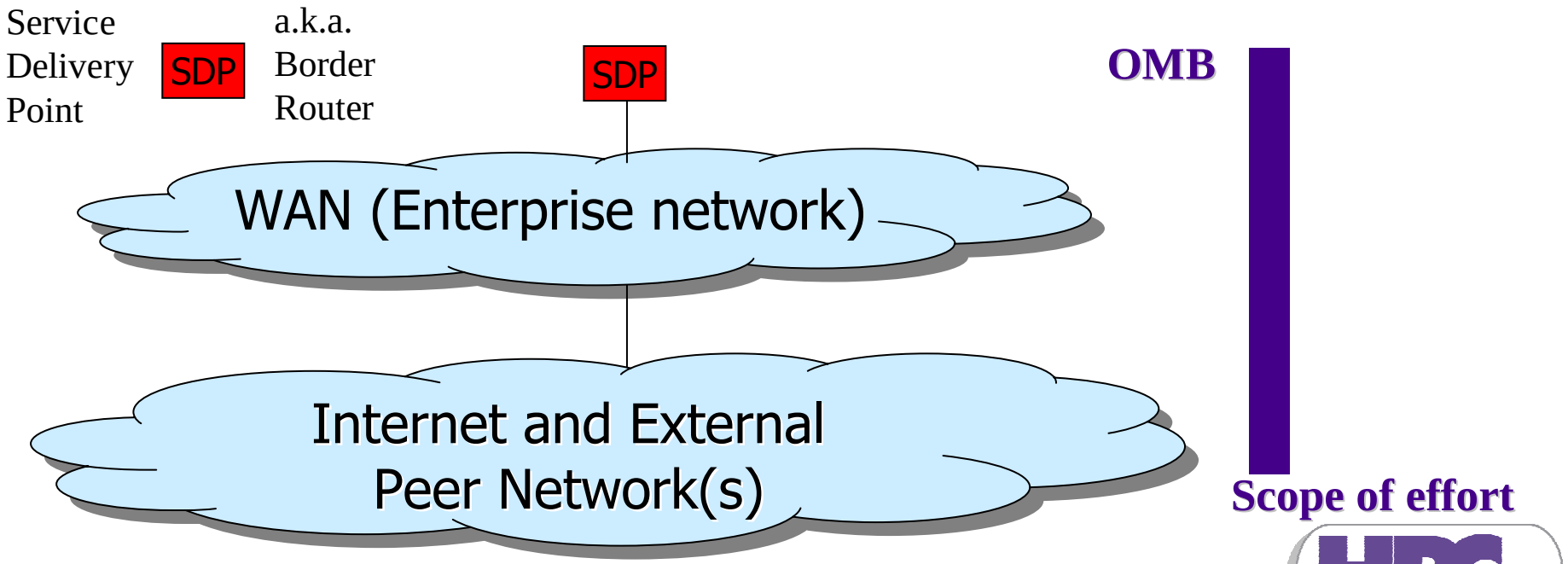
(source: Mr. Dale Geesey, Federal IPv6 Summit, May 17-19, 2006, Reston, VA)



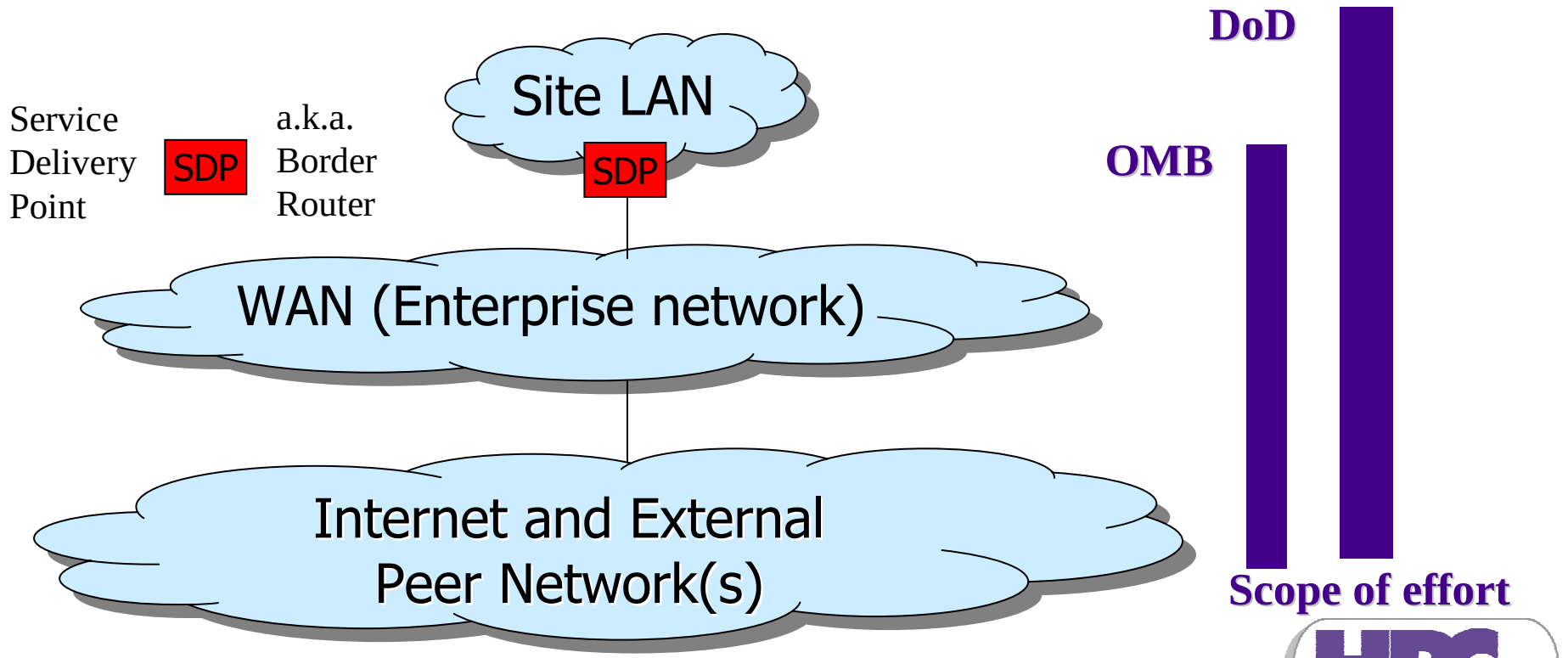
(source: Ms. Marilyn Kraus, ASD/NII, DoD IPv6 Working Group, Nov 19, 2003)

- **The DREN IPv6 Pilot perspective:**
  - **How quickly can we make IPv6 happen?**

DREN IPv6 Pilot

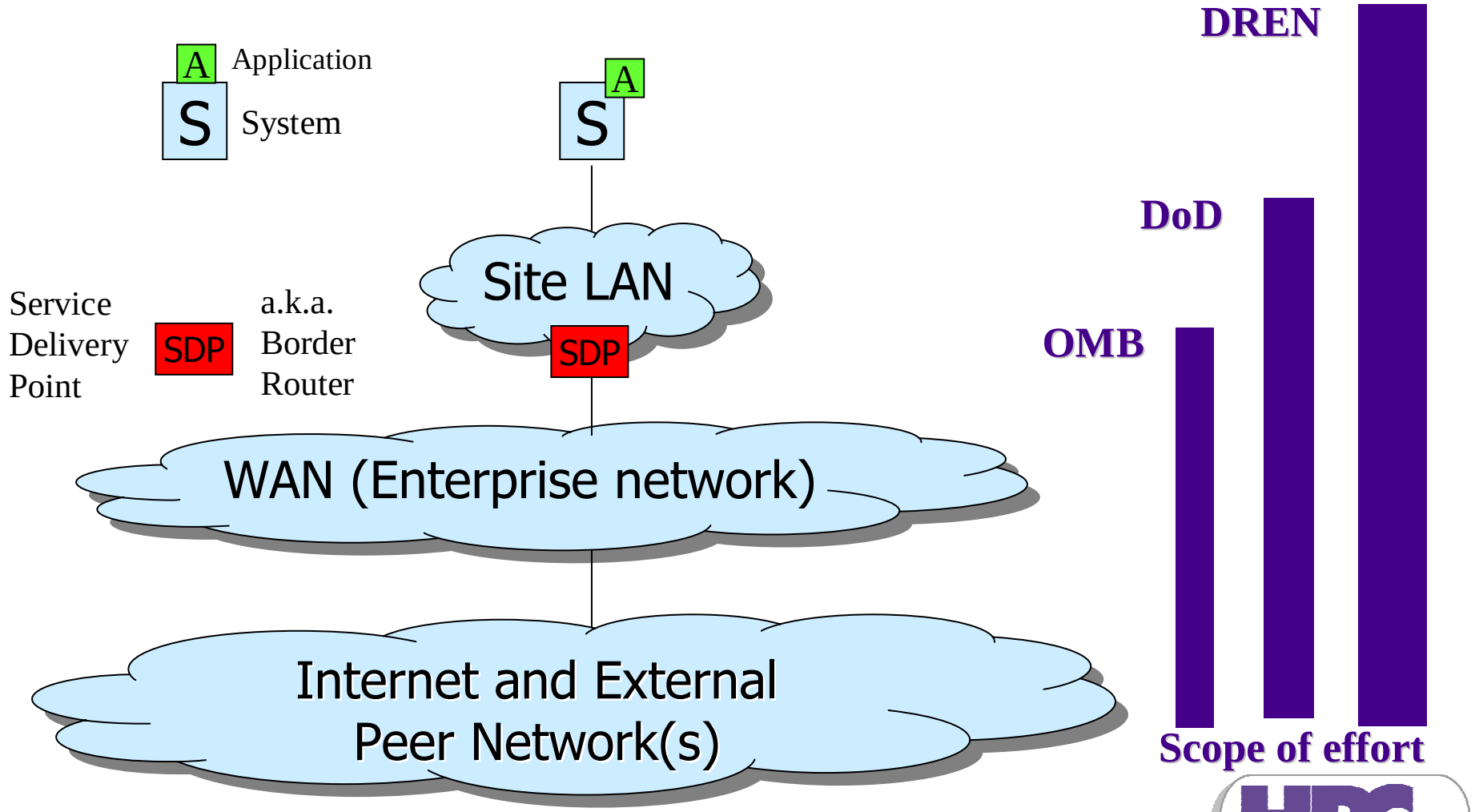


DREN IPv6 Pilot



DREN IPv6 Pilot

Pioneers are the ones with the arrows in their backs



DREN IPv6 Pilot

Accomplishments

DREN IPv6 Pilot FY2003 Goals:

1. **IPv6 enabled WAN infrastructure: border routers (called SDPs), the Verizon-provided backbone, and the Network Operations Center (NOC). Complete**
2. **Security and Performance as good as existing IPv4-only network. Complete**
3. **Facilitate IPv6 deployment into HPCMP funded sites' infrastructures. Complete**
4. **IPv6 enabled:**
   - **HPCMP funded sites' infrastructures. Mostly complete**
   - **HPCMP provided applications. Complete**
   - **COTS applications at HPCMP sites. Ongoing**
   - **Selected user application candidates. Outside scope**
5. **Provide equipment feedback, lessons learned, via web and via briefings. Complete**

Some Lessons Learned

- **Why we were successful**
  - Personality profile
  - Process
  - People
  - Procurement practice (not policy)
- **DREN IPv6 Pilot FY2003 Goals**
  - Goal 1: IPv6 enabled WAN infrastructure
  - Goal 2: Security and Performance
    - Security
    - Performance
  - Goal 3: IPv6 enabled: facilitate deployment at HPCMP sites
  - Goal 4: IPv6 enabled: COTS applications at HPCMP sites
  - Goal 5: Provide equipment feedback, lessons learned, via web and via briefings
- **How we measured "success"**

Why we were successful

Personality Profile

- DREN in a unique position to be DoD's first IPv6 pilot.
  - A history of supporting new technology.
    - Familiar with insertion process, and with being a pioneer.
    - Experience with IPv6 from running DRENv6 test bed.
  - Provided as a service by ~~MCI~~ Verizon Business over their VBNS+ network, which includes:
    - Recent, homogeneous, high-end equipment.
    - Highly skilled network management personnel.
    - Option to support IPv6 in existing contract.
  - Chain of Command supportive, even without additional funding.

Why we were successful

Personality Profile

- DREN is not a typical DoD network.
  - DREN supports the R&E community rather than operational missions. DoD policy prohibits the presence of IPv6 packets on operational networks "at this time."
- Push the "I believe" button, and turn on IPv6 everywhere in the WAN to see what worked (and what didn't).
- Dual stack everywhere (no tunnels).
- We strived for functional equivalence with IPv4.
  - We didn't plan to use new features of IPv6 (until later).
  - We insisted on the same functionality in IPv6 that was available in IPv4 (or the functional equivalent where they differ). If you can't do the basics well, new features hardly matter.

Why we were successful

Process

- Adapt the Carnegie-Mellon Software Engineering Institute's (SEI) enterprise TransPlant technology transition planning process. Program planning steps include:
  1. Define problem, solution, and scope.
  2. Decide on transition strategy.
  3. Characterize adopters.
  4. Define whole products and commitment process to identify mechanisms.
  5. Define desired end state; synthesize and select.
  6. Prepare to manage risk.
  7. Document the plan.
- Execute the plan during Q3 FY03 – Q4 FY04.

Source: the Carnegie-Mellon Software Engineering Institute (SEI), see http://www.sei.cmu.edu/news-at-sei/features/2001/4q01/feature-4-4q01.htm

Why we were successful

Process

Enclave level TransPlant technology deployment steps include:

1. Learn the terminology and technology*
2. Establish the Change Team
3. Describe Desired State
4. Baseline Current State
5. Analyze the Gap
6. Develop the Solution(s)
7. Trial the Solution(s) (testing by another name)
8. Roll Out the Solution(s)
9. Analyze Lessons Learned

Source the Carnegie-Mellon Software Engineering Institute (SEI), see http://www.sei.cmu.edu/pub/documents/98.reports/pdf/98tr004.pdf

*Shown in grey since not in the SEI steps

Why we were successful

People

- **Enterprise level DREN IPv6 pilot implementation**

Functional Areas (FA)	Team Lead
– FA01 IP transport	Navy (also IPv6 pilot chief engineer)
– FA02 Infrastructure services	contractor
– FA03 Network Management	Army
– FA04 Security	OSD
– FA05 Applications	Air Force
– FA06 Planning for the Future	IPv6 pilot chief engineer
– FA07 HPC Community Involvement*	OSD (also HPCMP IPv6 implementation manager)

> "Technology makes change possible, or even necessary, but people make it happen"
> – David S. McIntosh, CBI Network

*only full-time position, all others were part-time positions

Why we were successful

People

- Without mission critical urgency, we needed to encourage enclave level personnel to make IPv6 transition a priority.
  - "If you decree it, they won't necessarily build it."
- Personal touch in motivating enclave level IPv6 transition paid off.
  - Kick-off on-site visits and presentations.
  - Executives, Management, and technicians have different interests and motivations – needed separate presentations to engage them.
  - Frequent follow-up phone calls and emails were necessary to maintain motivation, interest, and progress.

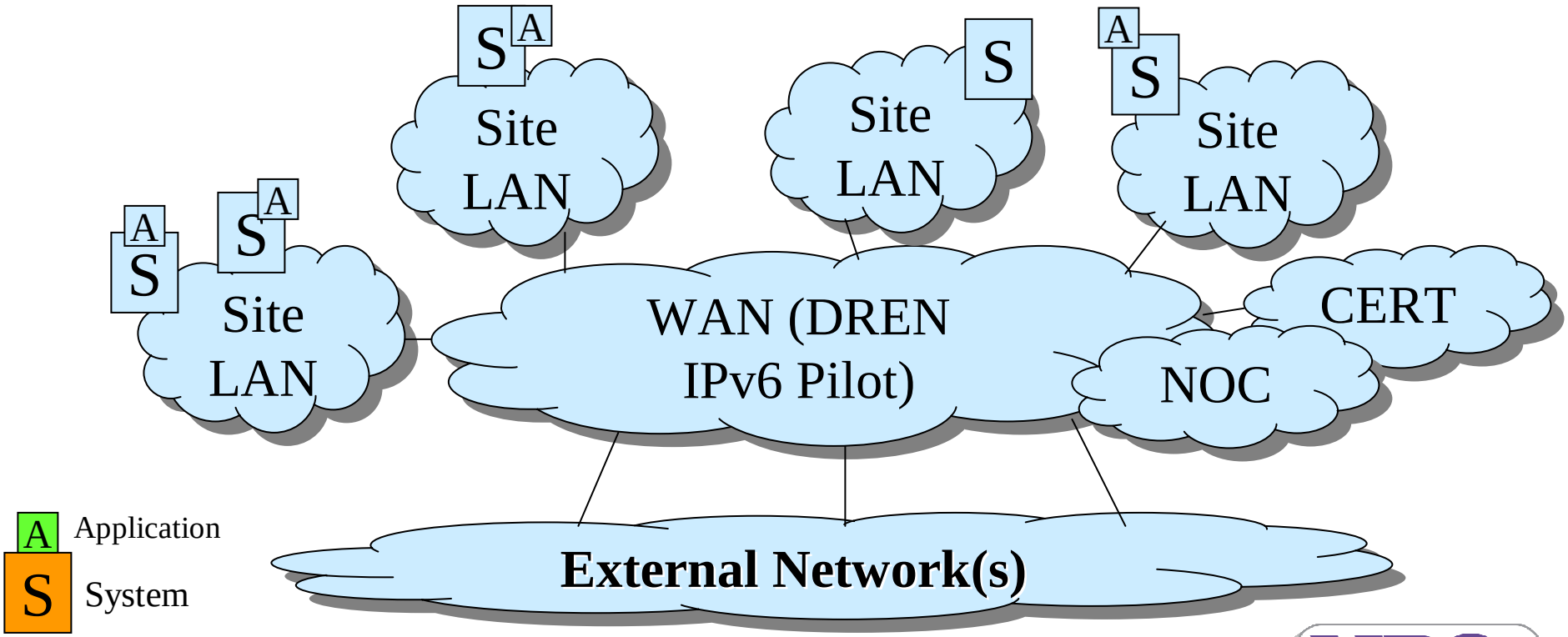
Why we were successful

Procurement practice (not policy)

- **DREN IPv6 Pilot**
  - **Wide-Area Network runs over vBNS+ equipment**
    - **Which is owned by Verizon Business.**
    - **Which they update regularly to keep pace with the rapidly evolving requirements of the DREN customer base.**
  - **At the HPCMP sites, equipment life is ~3 ½ years.**
    - **These are HPC centers – not data centers.**
- **DoD in general**
  - **Predicated on low- or no-cost transition primarily through technology-refresh cycles.**
    - **Excellent approach except that 2003-2008 sometimes too short a cycle.**

Goal #1: IPv6 enabled WAN infrastructure

- Start with network core, and work out to the edges.
- Dual Stack throughout WAN and sites' infrastructures.
- Minimal use of tunnels, translators, and other transition schemes.



Goal #1: IPv6 enabled WAN infrastructure

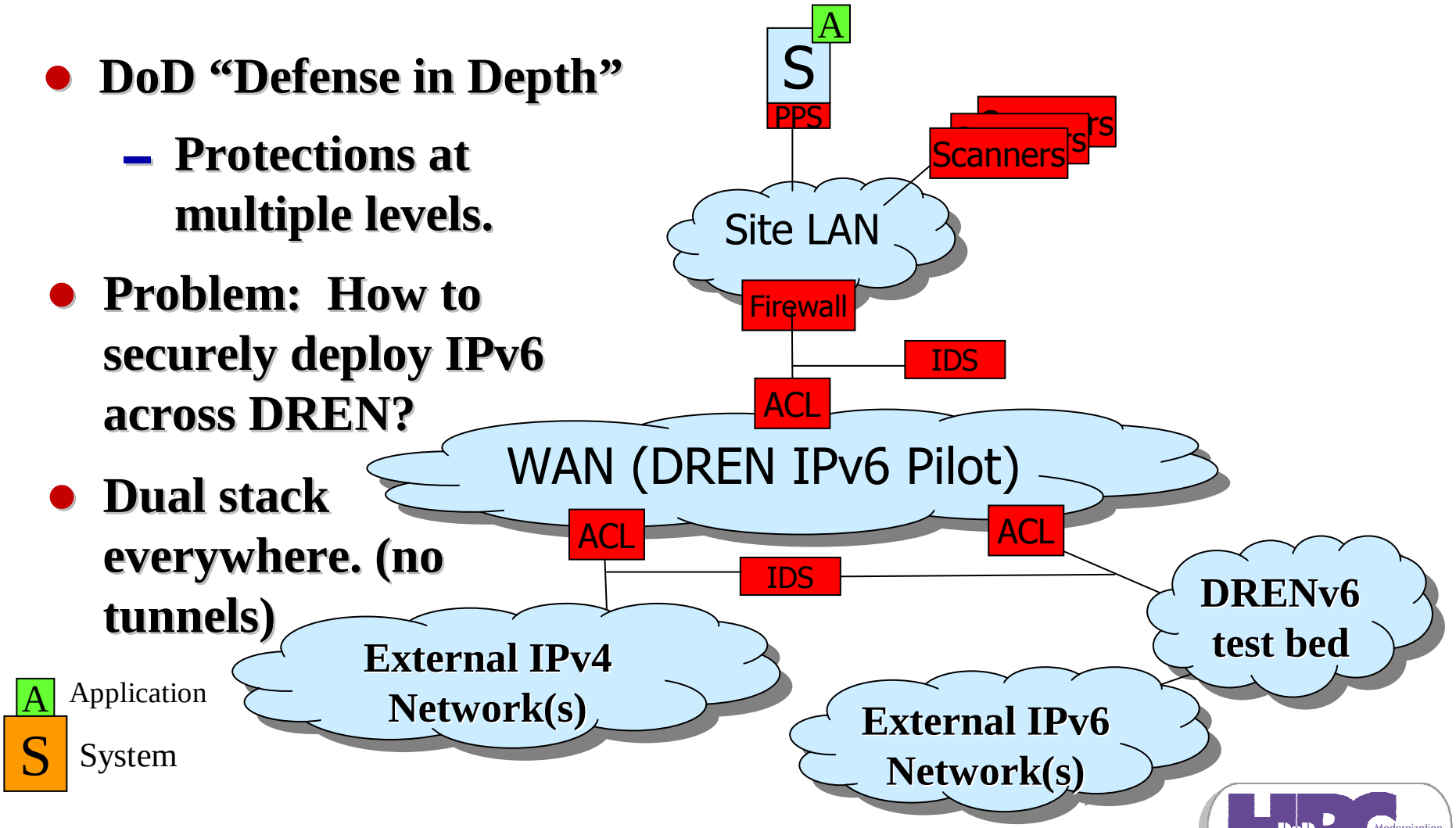
- The initial DREN routing of IPv6 sites was static
  - Static routing is not scalable – It is hard to maintain past a dozen or so sites.
  - But, it was the simplest way to get started (Jul-Oct 2003).
- Long term solution required establishment of Border Gateway Protocol (iBGP intra-DREN) and eBGP between router confederations and externally, plus OSPFv3.
  - This was fairly complex to set up, but scales well.
  - There were other ways to solve our routing problems, but since DREN supports multiple protocols, this was the best choice.
- 1 + 1 > 2
  - Designing 2 IP networks (new IPv6 overlay on existing IPv4) can at least double the complexity due to new interactions.
  - Making topologies congruent can minimize such impact.
  - But – managing the results need not be more difficult (no more people added to DREN or site LAN staffs).

Goal #2: Security and Performance: Equivalent Security

- "We have met the enemy and he is us" – Pogo (Walt Kelly)
  - Problem: Ignoring IPv6 on the LAN, ~~may~~ will not make it go away.
    - Microsoft Windows server 2003/Vista (native) and Vista (tunneled) – on by default.
    - Some versions of UNIX/Linux (Fedora, Ubuntu, Apple Mac OS X) – on by default.
    - Intentionally turned on by intruders of compromised hosts for stealth networking.
      - » Windows XP, most implementations of UNIX/Linux.
  - Catch 22: Most security and management products (IDS, IPS, scanners, and the like) with IPv6 capabilities are not as mature nor as widely available as they are for IPv4. Hence, even minimal IPv6 protection can require care and some extra effort.
  - Solution: Act to make it "IPv6 incapable," since it isn't so by default.
    - Step 1: Border routers and firewalls should have minimal changes to detect and block propagation of native IPv6 packets and IPv6-specific tunneling protocols.
    - Step 2: Local systems should be assessed, and simple configuration changes made to turn off IPv6 support when it is found to be enabled.

Goal #2: Security and Performance: Equivalent Security

- DoD "Defense in Depth"
  - Protections at multiple levels.
- Problem: How to securely deploy IPv6 across DREN?
- Dual stack everywhere. (no tunnels)



Goal #2: Security and Performance: Intrusion Detection Systems (IDS)

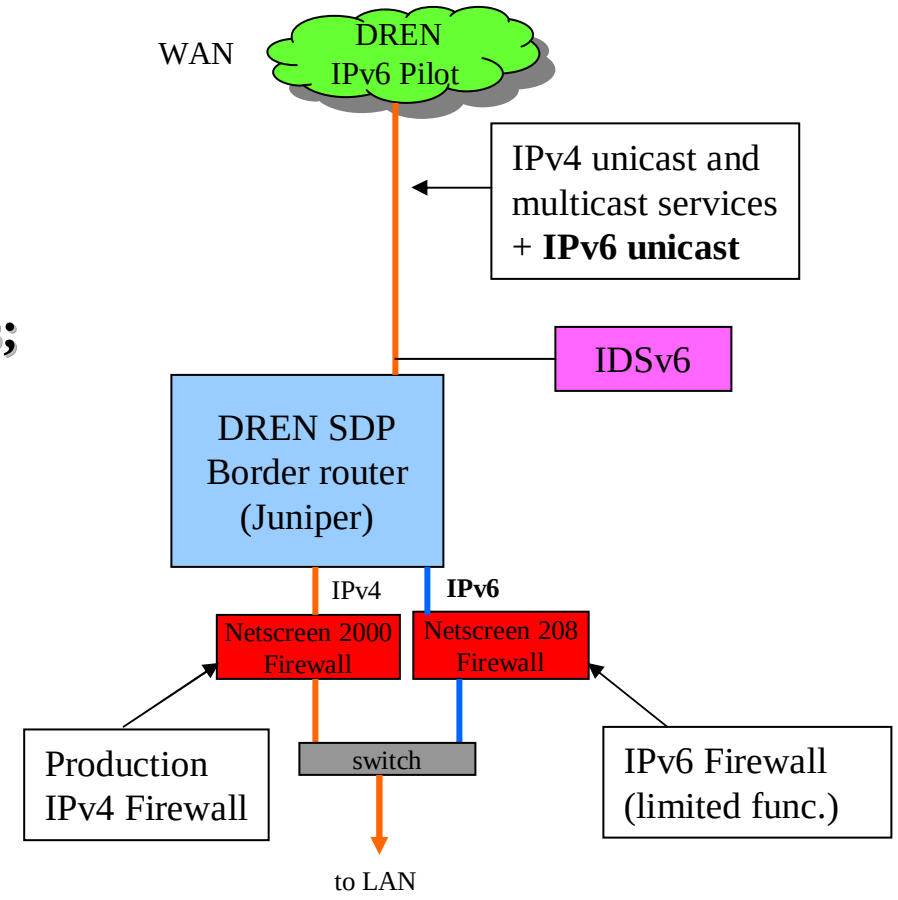
- Isolate IPv6 traffic on DREN IPV6 Pilot from all external networks save one.
  - Continue operation of DRENv6 test bed as an "untrusted" IPv6 network.
  - Establish trusted gateways to DRENv6 test bed as the only external IPv6 peering. Do not route/tunnel IPv6 with other peering networks (until later).
  - Peer DRENv6 test bed with Internet2, MoonV6, and other IPv6 enabled networks.
- Upgrade HPCMP Intrusion Detection Systems (IDS) installed at these trusted gateways to be v6-capable.
- Monitor IDS at these trusted gateways and selected other points across DREN by the HPC Computer Emergency Response Team (CERT).

Goal #2: Security and Performance: Access Control Lists (ACLs)

- At trusted gateways to DRENv6 test bed:
  - Adapt standard DREN IPv4 Access Control List (ACL) to create equivalent IPv6 version. (DREN IPv4 ACL is a superset of DoD compliant ACL.)
  - Maintain ACLs and monitor trusted gateways and other selected points across DREN by DREN Network Operations Center (NOC).
- Result: Sites connected to DREN continue to receive "safe" IPv4 service via dual-stacked WAN, in parallel with new IPv6 service
  - Of course, IPv6 service only upon site request!

Goal #2: Security and Performance: Site Firewalls

- 2003
  - Very few firewalls available.
  - Limited functionality.
  - Some sites used their own software-based firewalls.
- Beginning in 2005
  - Cisco PIX, Check Point offerings; Netscreen offers IPv6-capable firewalls (but so far IPv6 only).
  - Mixed results in using these.
    - Small sites with limited requirements may be OK.
    - HPC Centers need to spread traffic across several boxes, because no one box can meet all site requirements.
- 2006
  - DREN IPv6 pilot beta testing Netscreen ISG-2000 at 10 sites.



Goal #2: Security and Performance: Scanners and other Security Software

- **Vulnerability Assessment (Scanners)**
  - ISS doesn't support IPv6 and has no announced plans to do so.
  - NESSUS hasn't support IPv6, but after years of urging has promised support in 3.2 (est. Dec 2006).
- **Open source and European tools exist but are not widely known, nor trusted by site security personnel. DREN IPv6 Pilot sites made limited use of them.**
  - NMAP extended to do UDP scans, for example.
  - Tools are listed in the IPv6 product information article on DREN IPv6 pilot knowledge base.
- **IPsec**
  - Incomplete in most OS implementations (true for IPv4 as well).
  - Still lacking hardware support in some routers.
  - New standards emerging, so no commercial products.

Goal #2: Security and Performance: Protocols Ports and Services (PPS)

Recommendations for DREN IPv6 pilot sites:

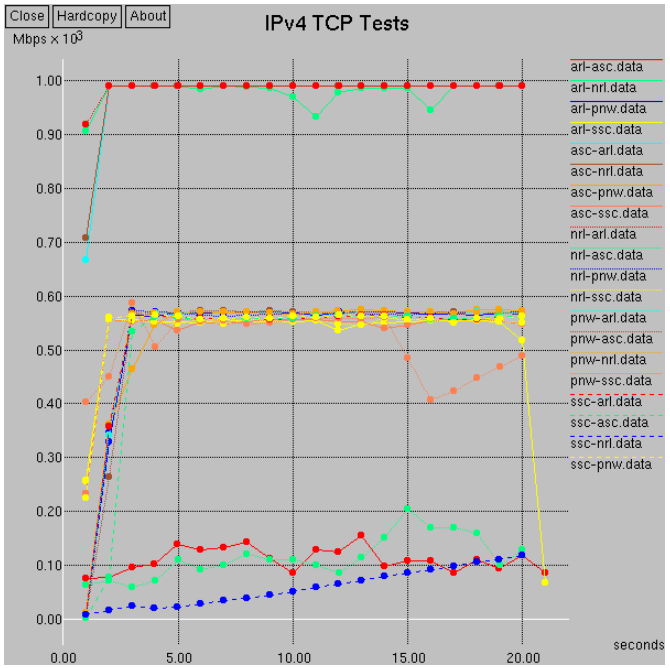
- **Protocols**
  - Only support protocols by conscious decision.
- **Ports**
  - Deny by default, permit by exception.
    - Only open ports needed by supported protocols.
    - Only open a port if a service is listening/may listen on it.
- **Services**
  - Do not implement an IPv4 service unless:
    - You can scan it for vulnerabilities.
    - It has been assessed and found to be an acceptable risk.
  - Do not implement a service for IPv6 unless the service is also running for IPv4 on the same system.

Goal #2: Security and Performance: Equivalent Performance

- DREN rides on an MPLS backbone, consequently:
  - IPv6 is routed in the same way as IPv4, using 6PE.
  - Somewhat surprising if performance were not equivalent.
- 2003 tests between Linux systems in California and Maryland connected to DREN OC-12 (622Mbps) sites.
  - about 567 Mbps with IPv4, 565 Mbps with IPv6.
- 2003 tests internal to an HPC Center, sending a 4 Gb/s stream between Linux systems with 10Gb-E NIC.
  - 3939.8044 Mbps UDP single stream (IPv4)
  - 3930.6234 Mbps UDP single stream (IPv6)
- 2005 tests between DREN OC-48 (2.4Gbps) sites.
  - About 990 Mbps with IPv4, 988 Mbps with IPv6.
  - Speed limited by Gigabit I/F on end systems, not by DREN
- Performance nearly identical, allowing for header overhead.

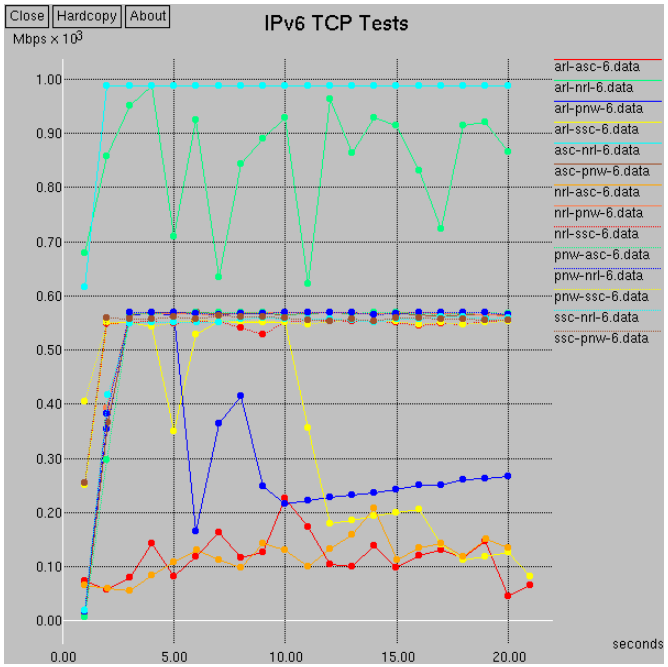
Goal #2: Security and Performance: Equivalent Performance

- **Performance is ~~no longer~~ not usually an IP issue. It is now a network provider and application developer issue (for IPv4 as well as IPv6)**



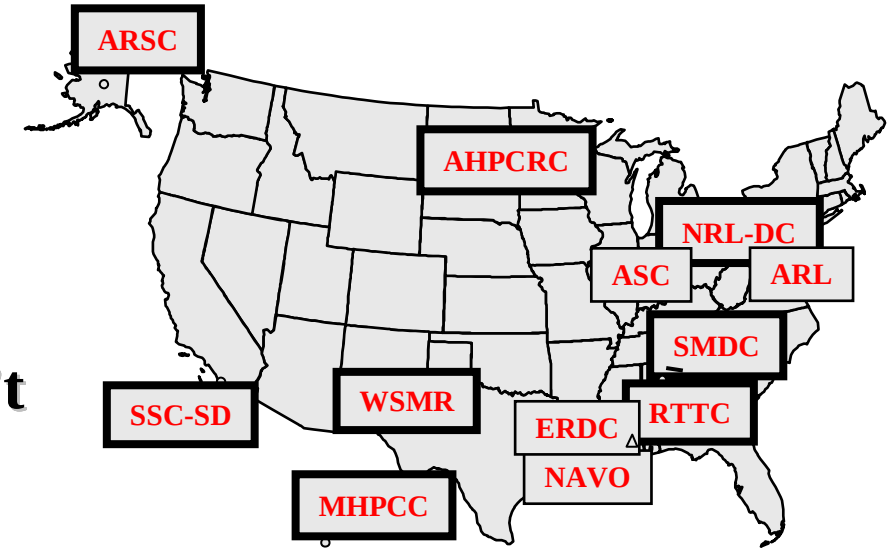
The graphs show TCP throughput second by second for 20 seconds. After typical 1-2 second slow TCP start up, equi-librium occurs.

The 1 Gig & 622 Meg line rate tests stand out. Observe the greater stability or robustness of IPv4 over IPv6 on some paths. Reason(s) for this are TBD.



Goal #3: IPv6 enabled: Facilitate deployment at HPCMP sites

- Visit participating sites and conduct briefings.
- Offer follow-up assistance, resources, training.
- Result: 12 sites transitioned to dual-stack environment.
  - Surprisingly few acquisitions, little training required.
  - Few technical challenges or surprises.
  - Security approval to "go live" always the last hurdle.
- "After you build it, they won't necessarily maintain it."
  - Once an IPv6 capability is in place, it must then be monitored, or else it will become a source of future security compromises.

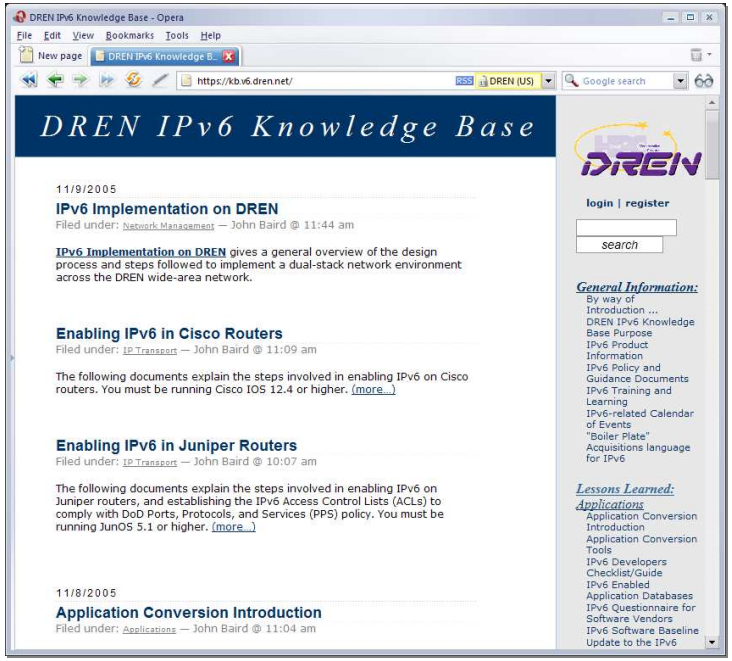


Goal #4: IPv6 enabled: COTS applications at HPCMP sites

- HPC Center supercomputers mostly run user-written programs (~70% of utilization).
- ~ 350 Commercial or Government Off-The Shelf (COTS/GOTS) applications are installed at one or more HPC Centers. Of these:
  - ~2/3 of the applications just compute, no inter-computer communications is involved. (Probably not typical)
  - ~1/3 of the applications do some sort of inter-computer communications.
    - ~50 of these use Macrovision's FlexLM license manager.
    - ~5 are currently IPv6 capable.
    - Of the remaining 60, ~½ the vendors are aware of DoD and OMB policy, have evaluated its impact, and are ready to supply an IPv6 capable version when they receive an order, ~¼ don't intend to comply, ~¼ are clueless.
      - » Big change in this regard over 3 years.
      - » In 2003 most were clueless.

Goal #5: Provide equipment feedback, lessons learned, via web and via briefings

- **Web: DREN IPv6 knowledge base**
  - **https://kb.v6.dren.net (v4/v6 capable)**
    - **Open to DoD (CAC enabled) or upon special request**
  - **Includes IPv6 product information, lessons learned, configuration, implementation guides, DoD policy, Pilot PoCs, TransPlant briefings, et cetera**
- **Briefings:**
  - **Conferences: Army, DoE, Internet2, JET, JITC Interop, NAv6TF, Navy, Super Computing, U.S. IPv6 Summit**
  - **Agencies: DISA, GAO, NIST, NRO, NSA, OMB, WHCA, Federal IPv6 TWG**
  - **Military Academies and Institutes**
  - **Academic HPC Centers**
  - **Numerous Service-specific site visits**



How we measured "success"

- At each of the 12 sites, IPv6 transition was done:
  - By a small number of part-time technical personnel,
  - As an additional duty, and
  - Without any additional funding.
- Consequently,
  - Detailed tracking of expenses attributable to IPv6 transition was not performed.
  - Most sites did provide anecdotal and summary data.
  - At the time of information collection, none of the sites had completed IPv6 transition, so estimates to complete the effort were included.
- Information was collected in 3 broad categories:
  - Purchases necessary to enable IPv6 transition.
  - Training of site personnel to enable IPv6 transition.
  - Time and effort by site personnel to enable IPv6 transition.
- Additional details are provided in the Lessons Learned slides.

How we measured "success"

- Regarding site purchases to enable IPv6 transition
  - Hardware: remarkably few purchases were necessary
    - Only 2 of the Pilot sites had to buy a router, which was scheduled to be replaced anyway (@ $25,000 and $8,200 each)
    - Some sites with Cisco routers chose to replace their Supervisor Blade with newer ones that did IPv6 in hardware rather than software (avg =$25,000). At a site with lesser bandwidth requirements, the old Blades would have been OK as is
    - It was fairly typical to expand the memory on routers, at a cost of $500 to $2,000 per router
    - No site had to replace any computers for the IPv6 transition
  - System Software:
    - Upgrades from Windows 2000 to Windows XP operating system and from Windows 2000 server to 2003 server were common
    - All other necessary software upgrades were covered under maintenance contracts at no additional cost

How we measured "success"

- Regarding training of site personnel to enable IPv6 transition
  - Commercial training
    - 2 sites purchased 3 – 5 day training from NativeV6 @ $2250/person
    - 1 site sent people to Internet2/Abilene 2 day workshop @ $600/person
  - HPCMP provided training
    - Many personnel at each Pilot site attended a ½ day on-site IPv6 orientation/IPv6 transition planning seminar as part of the pilot
    - At last four DREN Networkers conferences, a ½ day IPv6 seminar
  - Self-training (books and Internet accessible information)
    - Most personnel at all Pilot sites either bought at least one IPv6 book (avg = $30), or viewed at least one recommended webinar or video (avg = ~3 hours), or both

How we measured "success"

- **Regarding time and effort spent by site personnel to enable IPv6 transition over a period of 6 to 9 months**
  - **Context: Each site in the Pilot is primarily a computer center, with a few (1 – 6) HPC computers, massive file servers, a couple of high speed networks, and a small number (15 – 80) of desktop/laptop computers and visualization workstations. Total number of sites = 12**
    - **At the smaller sites, 100 to 200 hours (aggregate) were spent by a team of 2 – 4 part time people**
    - **At the medium sites, 200 to 400 hours (aggregate) were spent by a team of 4 – 7 part time people**
    - **At the larger sites, 400 to 600 hours (aggregate) were spent by a team of 5 – 7 part time people.**

Remember: times are only for infrastructure, no applications!

How we measured "success"

- Regarding initial DREN Wide Area Networking IPv6 infrastructure transition by Verizon Business:
  - Purchases: No hardware was purchased, but numerous router software upgrades were made (and are being made).
  - Training: ½ day on-site IPv6 orientation/IPv6 transition planning seminar for Network Operations Center (NOC) personnel (similar to the site seminar) was held.
  - Time and effort over a period of 4 months:
    - vBNS+ design, testing and implementation - 100 hours.
    - NOC:
      - » Workstation with Linux to support IPv6 - 20 hours.
      - » IPv6 address plan - 50 hours.
      - » Implementation at initial 12 IPv6 sites - 100 hours.
      - » IPv6 design testing and troubleshooting - 150 hours.

Final Thoughts I

How to get started

- Work from outside in, then bottom-up
  - WAN/ISP, border, DMZ, firewall, enclave
  - LAN interfaces, desktops, servers, apps
- Focus first on your public facing services
  - www, DNS, MX
- Establish a corporate culture to include IPv6 in all IT plans and activities
  - from CIO down to all technical staff
- Take the long view
  - get there via normal tech refresh, not forklift upgrade during crisis
- Don’t be afraid to try new things, take calculated risks

Final Thoughts II

How Hard is it?

- Easy parts of the IPv6 transition:
  - Dual-stacking the networks (WANs, LANs)
  - Enabling IPv6 functionality in modern operating systems
  - Establishing basic IPv6 services (DNS, SMTP, NTP)
  - Enabling IPv6 in some commodity services (HTTP)
- A little more challenging:
  - Getting the address plan right
  - Operating and debugging a dual stack environment
  - Multicast (though easier than in IPv4)
- Hard parts:
  - Creating and maintaining a security infrastructure
    - firewalls, IDS, proxys, IDP/IPS, VPNs, ACLs
  - Working around missing or broken functionality
  - DHCPv6 (in conjunction with IPv4, rather than in isolation)
  - Creating incentives to upgrade and try IPv6
  - Getting the vendors to fix bugs or incorporate missing features
    - Not enough market pressure, so other activities take priority

Final Thoughts III

On-going Challenges

- Keeping security policies consistent across dual stacks.
  - ACLs, Firewall policies, et cetera.
- Adversaries now have a new entry vector.
  - Don't allow IPv6 path to become a new weakest link.
- Diagnosing network problems.
  - Especially where the routing topology isn't congruent across protocols.
  - Confusion over which protocol is broken, and what protocol is being tested using diagnostic tools.
- Trying to outlaw NAT.
  - Some still believe that it brings important features (i.e. "security" rather than "obscurity").

Final Thoughts IV

- These are necessary but not sufficient to show functional equivalence:
  - Standards activities (IETF, DISR), theoretical analysis of standards (NSA), test equipment (Agilent, Ixia, Spirent), JITC generic test plans and approved product lists, and test beds (DRENv6, MoonV6).
- These are sufficient but not conclusive to show equivalence:
  - Extended use in real networks to expose and fix remaining errors (Internet2, DREN IPv6 pilot, still more would be nice).
- To really determine IPv6 support for your needs, query the vendor for specific features that matter to you. Be careful in evaluating their response. Try not to let your expectations dictate the results you find, or you will overlook/misinterpret results that contradict those expectations.

*It is **crucial** that IPv6 products have **functional parity** with IPv4 products!*