IPv6 Security Aspecten

KIVI NIRIA
IPv6 themabijeenkomst

Frans van Leuven

29/05/2013

Atos
Worldwide IT Partner

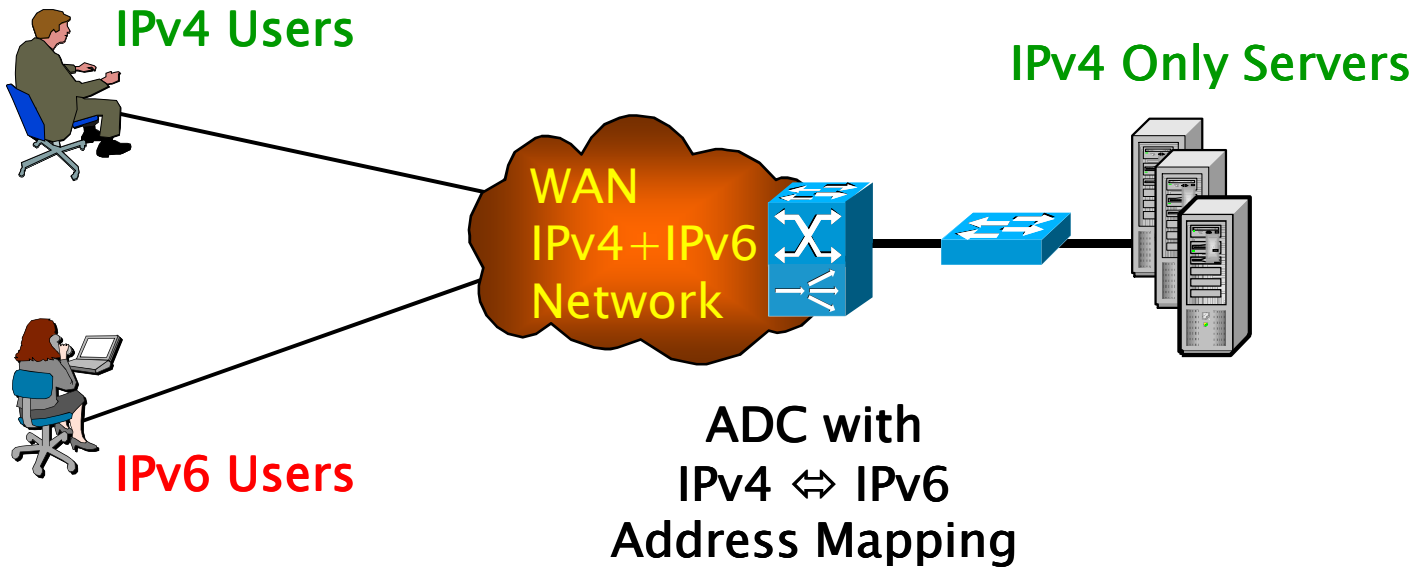
Content

- Introduction to IPv6
  - Basics and terminology
  - Common misperceptions
- Required knowhow
  - What's new with IPv6
  - Something about transition technologies
- IP-security and mitigation
    - Disabling IPv6?
    - Controlling deployments of transition technologies
    - New technology aspects requiring mitigation
- Question time

Ways how IPv6 can be implemented
Also essential for used terminology

- Single Stack implementation
  - Closed community IT applications may be kept on IPv4 till End Of Live
- Dual Stack implementation
  - This is the way to go where possible
  - Main disadvantage is duplication of various network tasks and activities.
- Encapsulating IPv6 in IPv4 or vice versa for transport (=Transition technologies)
  - Essential for migration and should be understood very well by many
- Supporting Network Address Translation including Protocol Translation
  - If all other options are not possible
  - Using a Load Balancer may be a better alternative

Using ADC's for IPv4 <=> IPv6
Quick solution for External/Internet access

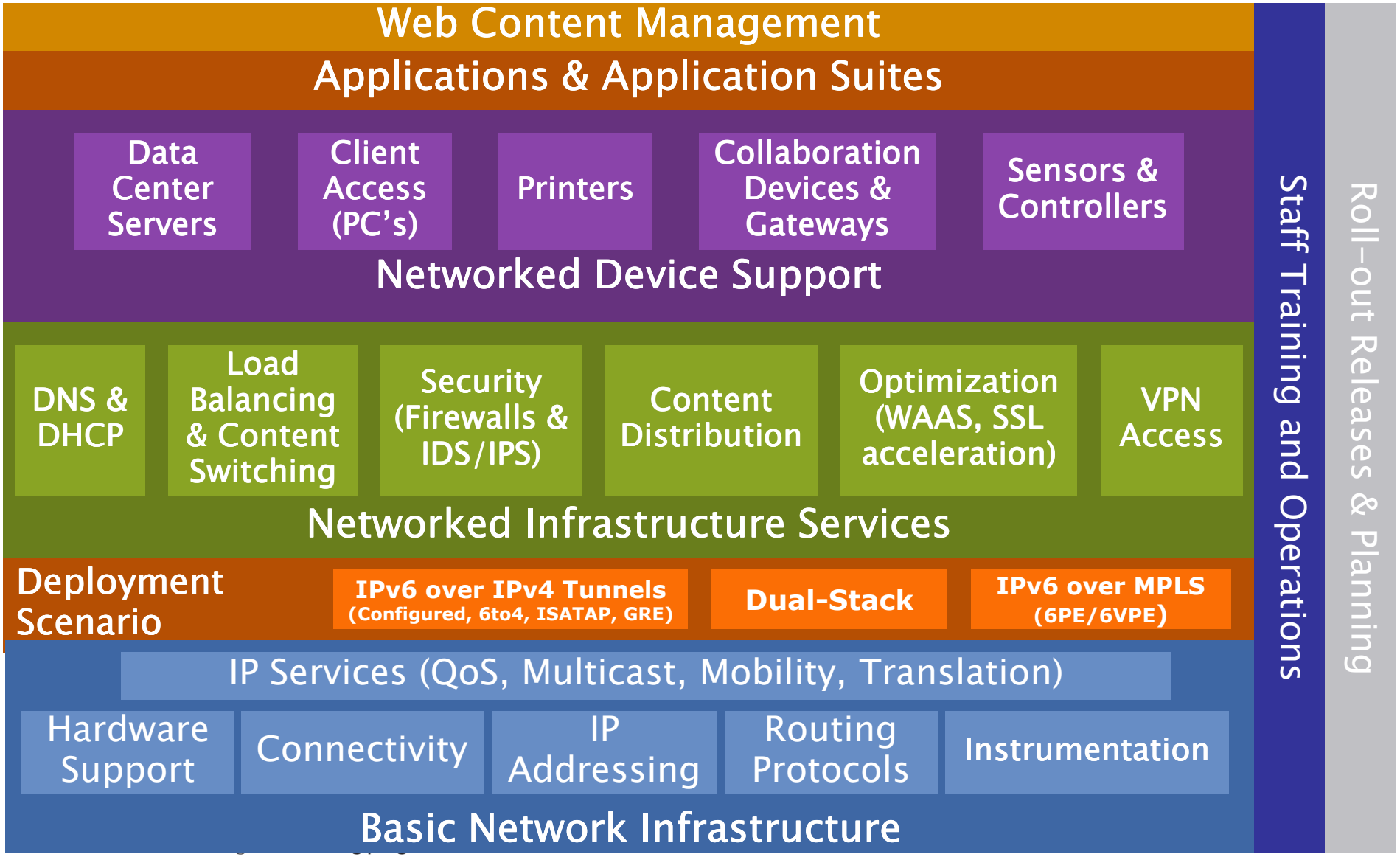


Positive effects of using IPv6
More than just a bigger address space

- There are several structural improvements coming with IPv6
  - It solves the IP-space scalability problem (32 bits ➔ 128 bits addressing)
  - It effectively deals with MTU and Fragmentation problems
    - Potential for dynamic deployment of Jumbo Frames
  - It avoids duplicated IP-addresses
  - It avoids problems related to subnet masks
  - Multicast replaced Broadcast and Anycast is a standard functionality now
  - Address assignment has improved and was simplified operationally
    - New options for privacy versus traceability and dynamic subnet allocation
  - IPsec is integral part of the IPv6 stack now
  - Provisions for extensions (cloud computing could make use of this e.g.)
- It does not improve the scalability of the Internet as such
  - Potentially many more routes to be processed (being a real challenge)
  - Higher router resource utilization to process 128 bits instead of 32

The Scope of Enterprise IPv6
Source: Cisco Systems

29/05/2013
Frans van Leuven



Common misperceptions about IPv6

1. A market will arise for IPv4 space solving imminent shortage
2. We use Private IPv4 space therefore we won't need IPv6
   - Only valid living on an island in splendid isolation
3. IPv6 improves security of IP networks
   - In fact it has initially more new challenges than really new goodies
4. IPv6 will simplify the network and will lower TCO
   - Potentially very true on the long term (=IPv6 only)
   - Dual Stack will raise costs for both management and resource utilization
5. The preparation for IPv6 readiness is a job for the network boys & girls
   - Applications and Tooling are main attention areas
   - Between 8% and 20% of all current applications are incompatible with IPv6
6. If I keep using IPv4 only then nothing needs to be done by me (now)
   - Security aspects of recent Operating Systems require countermeasures today!

IPv6 transition technologies
Protocol Translations and Encapsulations

- A universal NAT-PT standard was an original goal (RFC2766 / RFC 4966)
  - Did prove not the be achievable for multiple reasons and is obsolete now
  - NAT-PT was replaced by NAT64 and NAT46 standards
- IPv6 over IPv4 Networks connectivity (enabled by most OS versions)
  - ISATAP (Intra-Site Tunneling Addressing Protocol)
    - Meant for testing and validation, very quick deployments are possible
  - 6in4 (=Generic Routing Encapsulation for IPv6)
    - Implemented standard on Unix next to traditional support on routers
    - Not implemented or used by Microsoft (use 6to4 host-mode instead)
  - 6to4 (offered as a service by ISP's to interconnect IPv6 Islands)
    - Uses 6to4 Relay routers via well-known anycast addresses (e.g. 192.88.99.1)
    - IPv4 address is prepended with 2002::/16
  - 6rd (Rapid Deployment) used by ISP's as a closed community alternative for 6to4
  - Teredo (Host based tunneling method over IPv4 using UDP Port Translation)
    - Supports ISP connection point based on IPv4+NAT i.c.w. a Dual Stack PC
    - Teredo addresses are prepended with 2001::/32 and crafted by the Relay
  - DA (Microsoft Direct Access) merging multiple technologies and other goodies

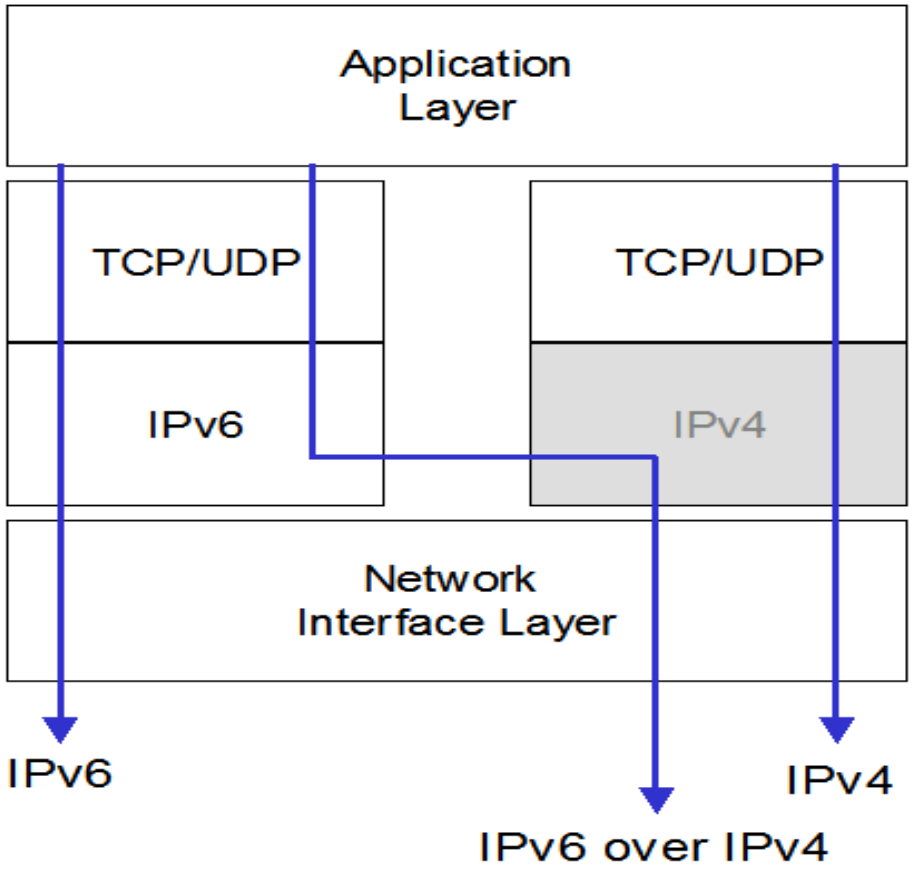
IPv6 security aspects
Doing nothing is never an option

- FW's should be IPv6 capable including unique IPv6 functionalities
  - Must also analyze IPv6 wrapped in IPv4 (=Protocol Type 41 packets)
  - Must check for protocol extensions
  - Validate PMTU behavior (Path MTU discovery, Fragmentation)
  - Fine grain selective ICMP filtering
  - Be aware PT=41 decimal in a filter/trace this is 29 HEX
- Perimeter control of Migration Protocols
  - Filter ISATAP, 6over4, Teredo and Microsoft IP-HTTPS where desired
  - Teredo (= a shipworm) was named so for its FW penetrating capabilities
- LAN setup needs to control roque SLAAC / DHCpv6 Routers/Servers
  - In its simples form this is L2 MAC based selective ICMP filtering
  - Network manufactures/specialists often unfamiliar with Transition Protocols
    - A draft standard is in the make with late/slow development
    - Manufactured are late/slow to deliver remedies

Security vulnerabilities
Differences per OS

- Weaknesses coming with new technologies
  - ICMPv6 including SLAAC and DHCPv6 has many new features
  - Transition Protocols are new and complex
- Specifics of Microsoft environments
  - Uses Dual Stack as the default with preference for IPv6
  - Transition technologies made active by default
    - ISATAP, 6to4 host-mode, 6to4 tunnel-mode, Teredo and IP-HTTPS
    - Used today actively for various purposes
    - Activated automatically under water in multiple cases
- Specifics of Unix / Linux / MAC environments
  - Uses Dual Stack as the default with preference for IPv6
  - Transition technologies are available but mostly not a default
    - ISATAP, 6in4 (=GRE), 6to4 Tunnel-Mode and Miredo (=Teredo)
- The combination of new functions and defaults main cause of vulnerabilities
  - Microsoft deployments are a concern, but also consistent
  - Unix/Linux have similar features. Packaging may result in potential obscured vulnerabilities and potential exploits being distributed

Microsoft IP stack
IPv4 and IPv6 have been integrated



Security exposures doing nothing
(Temporary) disabling IPv6 on Windows a good idea?

- **On a coporate PC within an IPv4 only environment**
  - Done via policy settings and distributed automatically
  - This may be a good idea but consequences are to be well investigated
    - Microsoft assumes IPv6 is enabled and uses it where possible
    - Preference for IPv6 may influence performance negatively if unavailable
    - Security aspects are plenty and result in many choices
- **On a private PC if you don't need IPv6 yet (use at your own risk !)**
  - *On Individual Interfaces via the control panel*
    No way to disable tunnel and loopback interfaces!
  - *Manually via netsh commands*

    netsh int ipv6 isatap set state disabled
  - *Manually via Registry (Disable IPv6 on all interfaces and prefer IPv4 to IPv6)*
    set
    KEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters\DisabledComponents
    to
    DWORD to 0xFF

Typical Dual Stack View?
Or is something very wrong?!

29/05/2013

Frans van Leuven

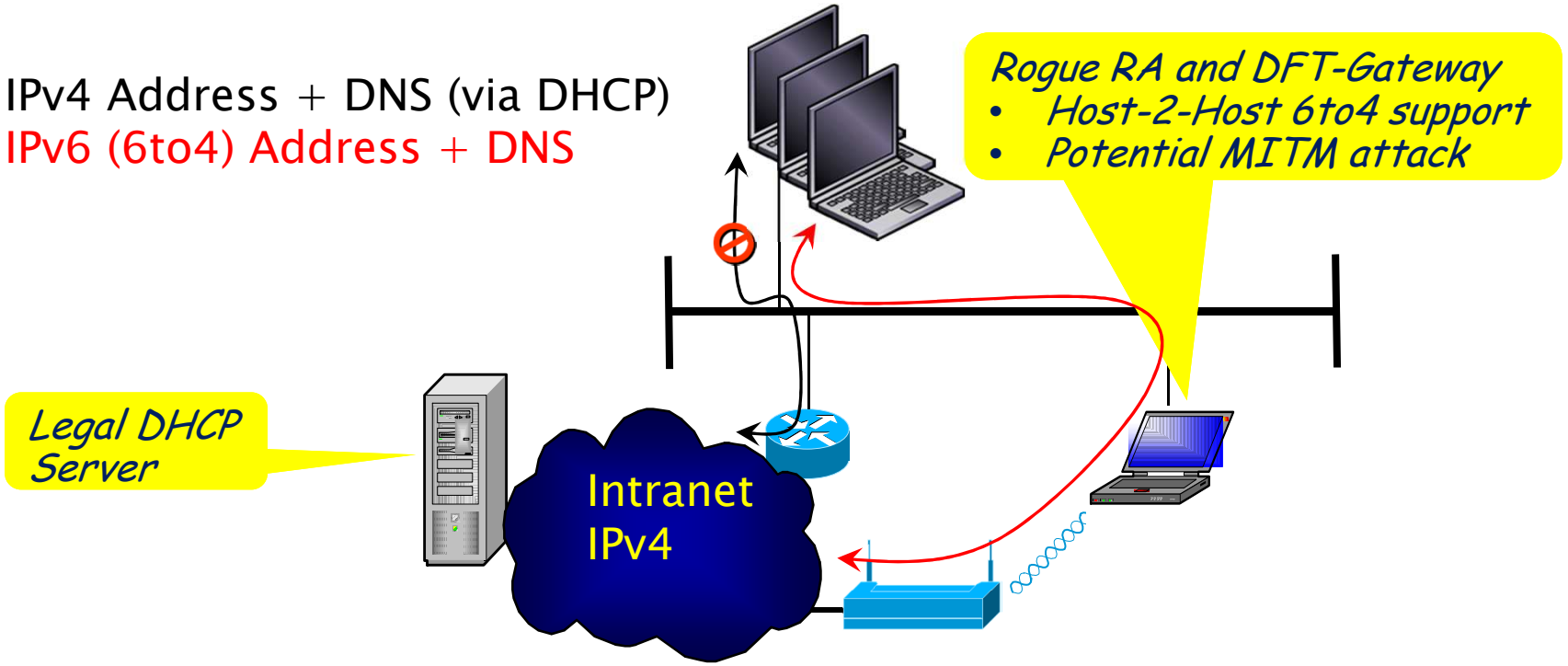
```
Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : europe.nl.intra
   Description . . . . . . . . . . . : Marvell Yukon 88E8055 PCI-E Gigabit Ether
net Controller
   Physical Address. . . . . . . . . : 00-A0-D1-CD-EC-60
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : 2002:a15a:1279:a:b8db:9f47:af7e:468d(Pref
erred)
   IPv6 Address. . . . . . . . . . . : 2002:a15a:1628:a:b8db:9f47:af7e:468d(Pref
erred)
   IPv6 Address. . . . . . . . . . . : 2002:a15a:2684:a:b8db:9f47:af7e:468d(Pref
erred)
   Site-local IPv6 Address . . . . . : fec0::a:b8db:9f47:af7e:468d%1(Preferred)

   Temporary IPv6 Address. . . . . . : 2002:a15a:1279:a:816e:540d:b980:75f7(Pref
erred)
   Temporary IPv6 Address. . . . . . : 2002:a15a:1628:a:816e:540d:b980:75f7(Pref
erred)
   Temporary IPv6 Address. . . . . . : 2002:a15a:2684:a:816e:540d:b980:75f7(Pref
erred)
   Link-local IPv6 Address . . . . . : fe80::b8db:9f47:af7e:468d%11(Preferred)
   IPv4 Address. . . . . . . . . . . : 161.90.39.36(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.252.0
   Lease Obtained. . . . . . . . . . : donderdag 27 oktober 2011 8:50:18
   Lease Expires . . . . . . . . . . : vrijdag 28 oktober 2011 1:20:19
   Default Gateway . . . . . . . . . : fe80::ec2b:bda0:bc2c:ff83%11
                                       161.90.36.1
   DHCP Server . . . . . . . . . . . : 161.90.122.217
   DHCPv6 IAID . . . . . . . . . . . : 335585489
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-13-FC-91-B3-00-13-E8-F8-83-09

   DNS Servers . . . . . . . . . . . : 161.90.126.110
                                       161.90.126.112
   Primary WINS Server . . . . . . . : 161.90.126.110
   Secondary WINS Server . . . . . . : 161.90.126.112
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Rogue Router Advertisements
Exploit using W7 standard features



Windows ICS "Internet Connection Sharing" will send Router Advertisements!

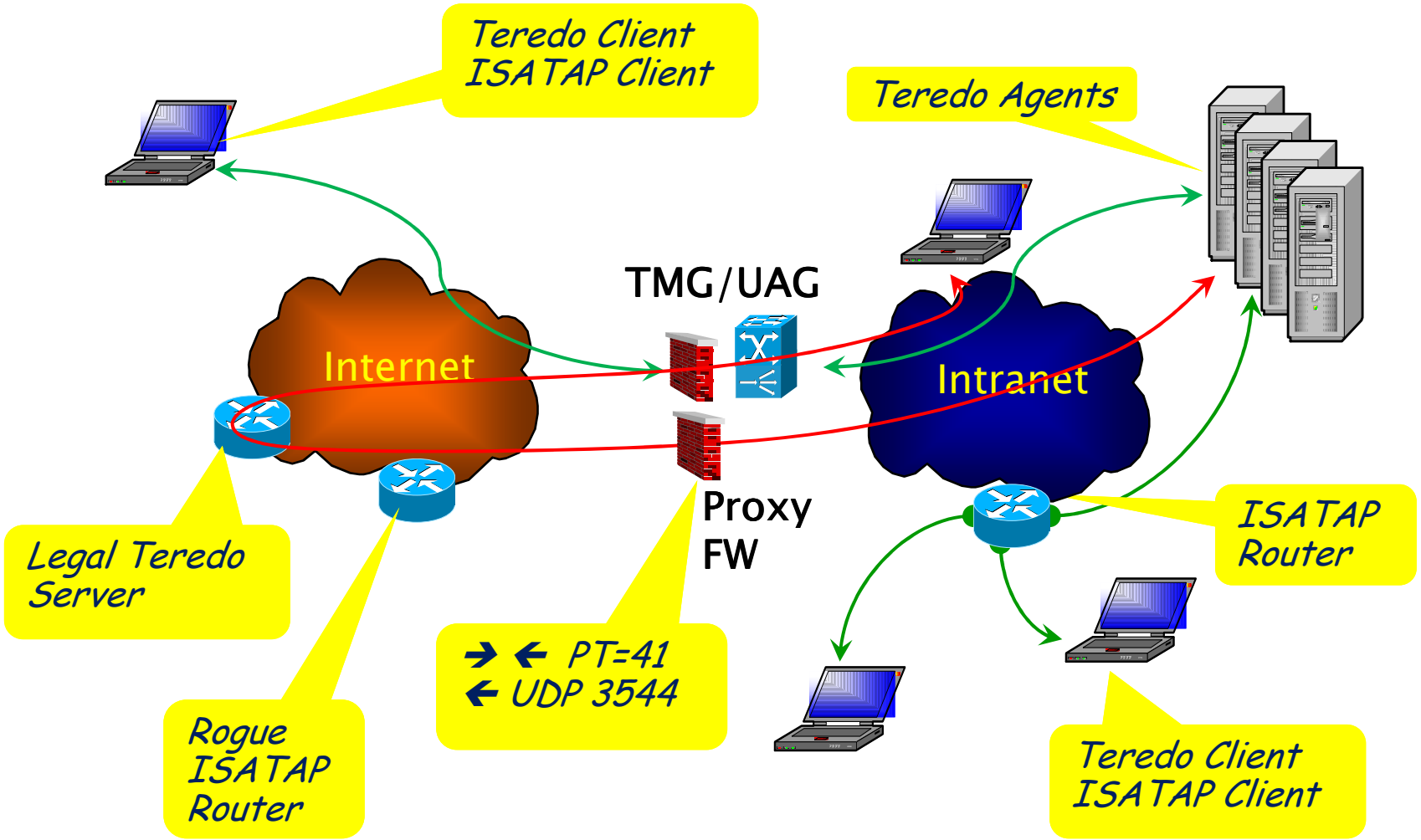
- It will advertise 6to4 addresses if both IPv4 and IPv6 is enabled
- All hosts will use IPv6 as a better path (even when IPv6 is based on 6to4)
- Man In The Middle attacks may use it as a basis

Microsoft Direct Access
Simple for the user but complex under the hood

29/05/2013
Frans van Leuven

- DA is auto launching when Native Intranet connectivity is not detected
  - Works via IPv6 only (native or ISATAP)
  - Will use 6to4 via a Provider Proxy Router as 2nd choice
  - 3rd choice Teredo to find the DA Server using a well known DA Proxy on the Internet
  - After session loss a re-connection is tried. A new path may use alternate methods
- Will next do 2 IPsec ESP Authentications and encrypt these sessions with TLS
  - Using Machine Certificates for the first session (=used for DNS + Mgt)
  - Uses User Credentials for the second session (=used for User Flows)
- If IPsec SEC Authentication is blocked by a FW then it will try Internet Protocol over Secure Hypertext Transfer Protocol (IP-HTTPS
- Internet Access remains local by default
  - Split Brain DNS + Name Resolution Policy Table (NRPT) enable policies for DNS resolution

Blocking Transition Protocols
Also if you don't have, need, want IPv6



Recommended material

- Cisco presentations: BRKSEC-2003 and BRKSEC-2603

- http://www.ipv6ready.org
  - What is going on with IPv6?
  - IPv6 Ready Logo Program Approved List

- http://www.ipv6forum.com
  - Testing and Certification
  - Qualification for an IPv6 Ready logo

- Want to learn more about IPv6?
  - Get an excellent 306 page free book from Lawrence Hughes!
    - http://www.ipv6forum.com/dl/books/the_second_internet.pdf

Other sources and material

- Cisco presentations:
  - Security during Networkers 2012: BRKSEC-2003 and BRKSEC-2603
- RIPE http://www.ipv6actnow.org/
- IPv4 Address Exhaustion: An Inconvenient Truth
  - Source : http://www.burtongroup.com/research/PublicDocument.aspx?cid=1534
  - In this Burton Group report, Senior Analyst Jeff Young looks at issues that surround Internet Protocol version 4 (IPv4) and Pv6 as the last IPv4 address is consumed.
- EC Factsheet 066-ipv6
  - EC directive stating that within the EC the usage of IPv6 should be promoted.
  - By 2010, the Commission wants to see at least 25% of users able to connect to the Internet using IPv6
- The Choice: IPv4 Depletion or Transition to IPv6?
  - Source: Jordi Palet
  - Extensive document describing different strategies
- IPv6 Essentials by Silvia Hagen
  - Source: O'Reilly ISBN -13: 978-0-596-10058-2
  - Extensive document describing IPv6 (Second Edition)

It’s Question Time!

Frans van Leuven

Atos Managed Services – Business Development
Eindhoven – The Netherlands
+31(0)8826 56477
+31(0)622407123

frans.vanleuven@atos.net

How big is the application challenge?

- On average 12% of all current applications is incompatible
  - Organizations may have from hundreds to several thousands of applications
  - For Business applications like ERP and CRM this is about 8%
  - For homebrew applications and tooling this can amount up to 20%
- The Stipv6 white paper 'IP Version Dependency in Application Software – Preparing source code for IPv6' can be downloaded free of charge at www.stipv6.nl
- The time to fix a problem will vary
  - An update/upgrade may take several weeks
  - Application fixing and testing may already take several months
  - But a total application replacement may even take multiple years