ERNW
providing security.

IPv6 Security in Enterprise LANs

Enno Rey &
Christopher Werny
{erey,cwerny}@ernw.de

Who we are

ERNW
providing security.

- **Old-school network security guys from**
- **Germany based ERNW GmbH**
  - Independent
  - Deep technical knowledge
  - Structured (assessment) approach
  - Business reasonable recommendations
  - We understand corporate
- **Blog: www.insinuator.net**
- **Conference: www.troopers.de**

© ERNW | Breslauer Str. 28 | GmbH D-69124 Heidelberg | www.ernw.de

Some unordered preliminary notes

ERNW
providing security.

- **This talk assumes you already have some knowledge as for the way IPv6 works.**
  - Unfortunately, we won‘t have the time to give introductory explanations.
  - All discussions of $TECH will happen from a security point of view.

- **This talk has an “enterprise perspective“.**
  - As opposed to a “consumer perspective“.
    Or the one of a smartphone,
    a car, a smart meter or a fridge...
  - Large organizations might have very different needs wrt IPv6.

- **Last but not least, for the record: whenever we use terms like “sysadmin“ or “security practitioner“ etc., these may designate female persons or male ones.**

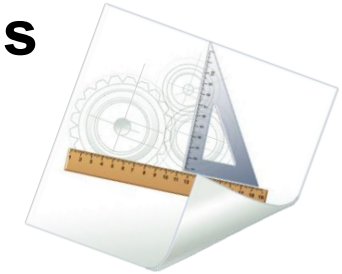
© ERNW | Breslauer Str. 28 | GmbH D-69124 Heidelberg | www.ernw.de

Agenda

ERNW
providing security.

- **Right now: the big illusion.**
  - “We do not yet use IPv6.“

- **Very soon: some challenges waiting for you.**
  - Planning for “full IPv6“.



- **And then: life doesn‘t get easier ;-)**
  - More security challenges...

© ERNW | Breslauer Str. 28 | GmbH D-69124 Heidelberg | www.ernw.de

IPv6 basic security assumptions

ERNW
providing security.

- **“The local network is trustworthy.”**
  - Ha Ha!
  - And: what’s “local” anyway?

- **“If there are threats, we can address them with crypto.”**
  - Ever heard of “operational overhead” (caused by crypto)?

- **“Everybody will use IPsec (that’s why we’ve built it in).”**
  - Well, IPsec is a success story in itself, isn’t it? ;-)
  - Unfortunately this has lead to a number of debatable protocol decisions.
    - OSPFv3 without MD5 (or SHA-x for that matter) is … crazy…

© ERNW | Breslauer Str. 28 | GmbH D-69124 Heidelberg | www.ernw.de

Strong misconception as for IPv6

“IPv6 is a well-defined set of completed standards.”

- **It’s not!**
- **Still big debates as for major fundamental elements.**
- **Lots of RFCs, both “standard track” and informational, and IETF drafts floating around.**
- **Vendors may implement fundamental stuff quite differently**
  - E.g. how to get host part of address.

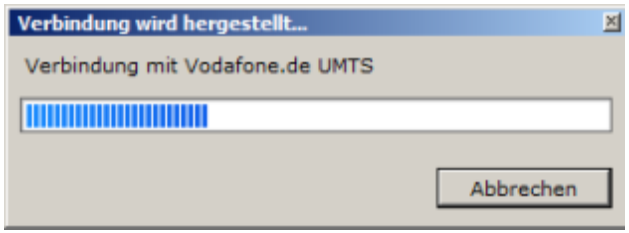
© ERNW | Breslauer Str. 28 | GmbH D-69124 Heidelberg | www.ernw.de

The big illusion (“We don‘t use IPv6“)

ERNW
providing security.

- **O rly?**

```
Connection-specific DNS Suffix  . : c.hospitality.swisscom.com
   Link-local IPv6 Address . . . . . : fe80::f1e7:4925:ba11:4bec%10
   IPv4 Address. . . . . . . . . . . : 192.168.48.120
   Subnet Mask . . . . . . . . . . . : 255.255.252.0
   Default Gateway . . . . . . . . . : 192.168.48.1
```




```
Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::ac3f:4615:1db2:2988%17
   IPv4 Address. . . . . . . . . . . : 2.204.240.146
   Subnet Mask . . . . . . . . . . . : 255.255.255.252
   Default Gateway . . . . . . . . . : 2.204.240.145
```

```
Tunnel adapter 6TO4 Adapter:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2002:2cc:f092::2cc:f092
   Default Gateway . . . . . . . . . : 2002:c058:6301::c058:6301
```

```
tracert -6 ipv6.google.com

Tracing route to ipv6.l.google.com [2a00:1450:8004::93]
over a maximum of 30 hops:

  1    52 ms    69 ms    59 ms  2002:c058:6301::1
  2    72 ms    59 ms    49 ms  gige-g2-6.core1.fra1.he.net
[2001:470:0:150::1]
  3    56 ms    69 ms    59 ms  de-cix10.net.google.com
[2001:7f8::3b41:0:1]
```


© ERNW | Breslauer Str. 28 | GmbH D-69124 Heidelberg | www.ernw.de

The big illusion — What's behind this?

ERNW
providing security.

- **Transition technologies present in all current $WIN_OS.**
- **Somehow implement "their own approach of dual-stack".**
- **Implications not fully understood in many environments.**
- **They may be responsible for a large part of "the latent threat".**

© ERNW | Breslauer Str. 28 | GmbH D-69124 Heidelberg | www.ernw.de

ERNW
providing security.

Dual-Stack & Tunnel/Transition Technologies

Dual-Stack Mode

- **Dual-stack mode (sometimes: *DSM*) just means: a node has both IPv4 and IPv6 “present”.**
  - Where “present” might mean:
    - IPv4 enabled and IPv6 “dormant”
    - IPv4 enabled and IPv6 “active on local-link”
    - IPv4 enabled and IPv6 fully active in parallel. Both are used for “respective communication”.

- **Often DSM can be found together with tunnel technologies…**
- **DSM might be susceptible to “the latent threat”.**

© ERNW | Breslauer Str. 28 | GmbH D-69124 Heidelberg | www.ernw.de

The *latent threat*

ERNW
providing security.

- **Term designates all types of threats that arise of DSM, in particular if sysadmins (or ISOs) don't even know that IPv6 is somehow present.**
  - All Windows OS since Win Vista have IPv6 enabled by default…
- **It might happen that IPv6 gets "active" by receiving a RA.**
  - E.g. when client connects to hotspot with Wifi device emitting RAs.
- **IPv6 packets might (then) not get treated with "the same security scrutiny" as IPv4 packets.**
  - E.g. (disabled) split tunneling of Cisco VPN client only applies to IPv4.

© ERNW | Breslauer Str. 28 | GmbH D-69124 Heidelberg | www.ernw.de

The 30 sec version: How to address the *latent threat*

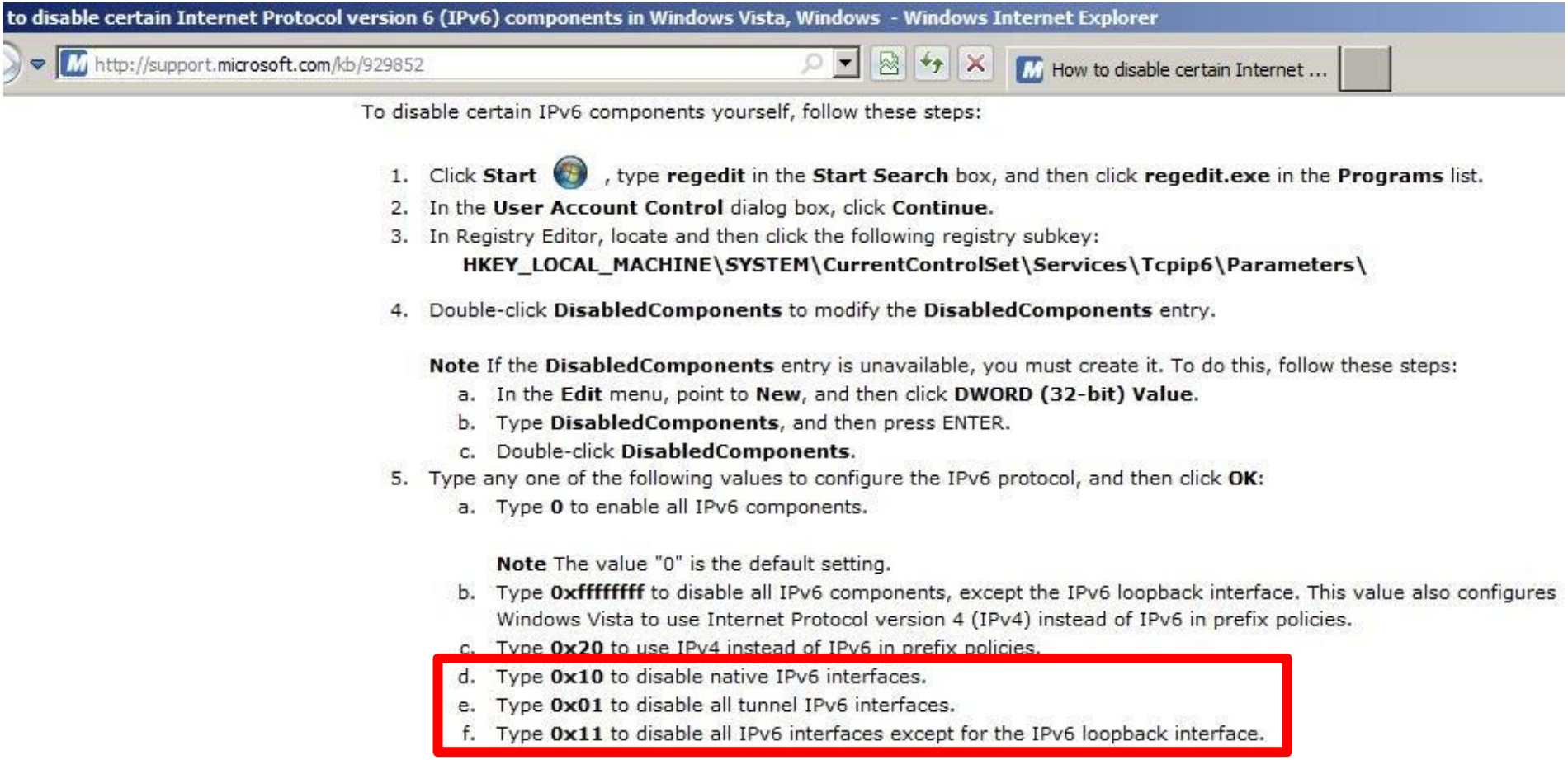
ERNW providing security.

- **Always assume that IPv6 is present on boxes.**

- **Control its behavior by**
  - Either providing full-blown, well-defined IPv6 connectivity for all hosts.
    - Unrealistic in the short term.
  - Or disabling explicitly IPv6 (or parts of it, like tunnel techs) on all managed hosts.
    - In Windows world this usually can be done by one registry key (→ doable w/ GPOs).
  - Try to monitor if application installation magically enables IPv6 (or parts).
    - E.g. MS Meeting Space & its successors.

© ERNW | Breslauer Str. 28 | GmbH D-69124 Heidelberg | www.ernw.de

DisabledComponents RegKey



to disable certain Internet Protocol version 6 (IPv6) components in Windows Vista, Windows - Windows Internet Explorer

http://support.microsoft.com/kb/929852

How to disable certain Internet ...

To disable certain IPv6 components yourself, follow these steps:

1. Click **Start** , type **regedit** in the **Start Search** box, and then click **regedit.exe** in the **Programs** list.
2. In the **User Account Control** dialog box, click **Continue**.
3. In Registry Editor, locate and then click the following registry subkey:
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters
4. Double-click **DisabledComponents** to modify the **DisabledComponents** entry.

   Note If the **DisabledComponents** entry is unavailable, you must create it. To do this, follow these steps:
   a. In the **Edit** menu, point to **New**, and then click **DWORD (32-bit) Value**.
   b. Type **DisabledComponents**, and then press ENTER.
   c. Double-click **DisabledComponents**.
5. Type any one of the following values to configure the IPv6 protocol, and then click **OK**:
   a. Type **0** to enable all IPv6 components.

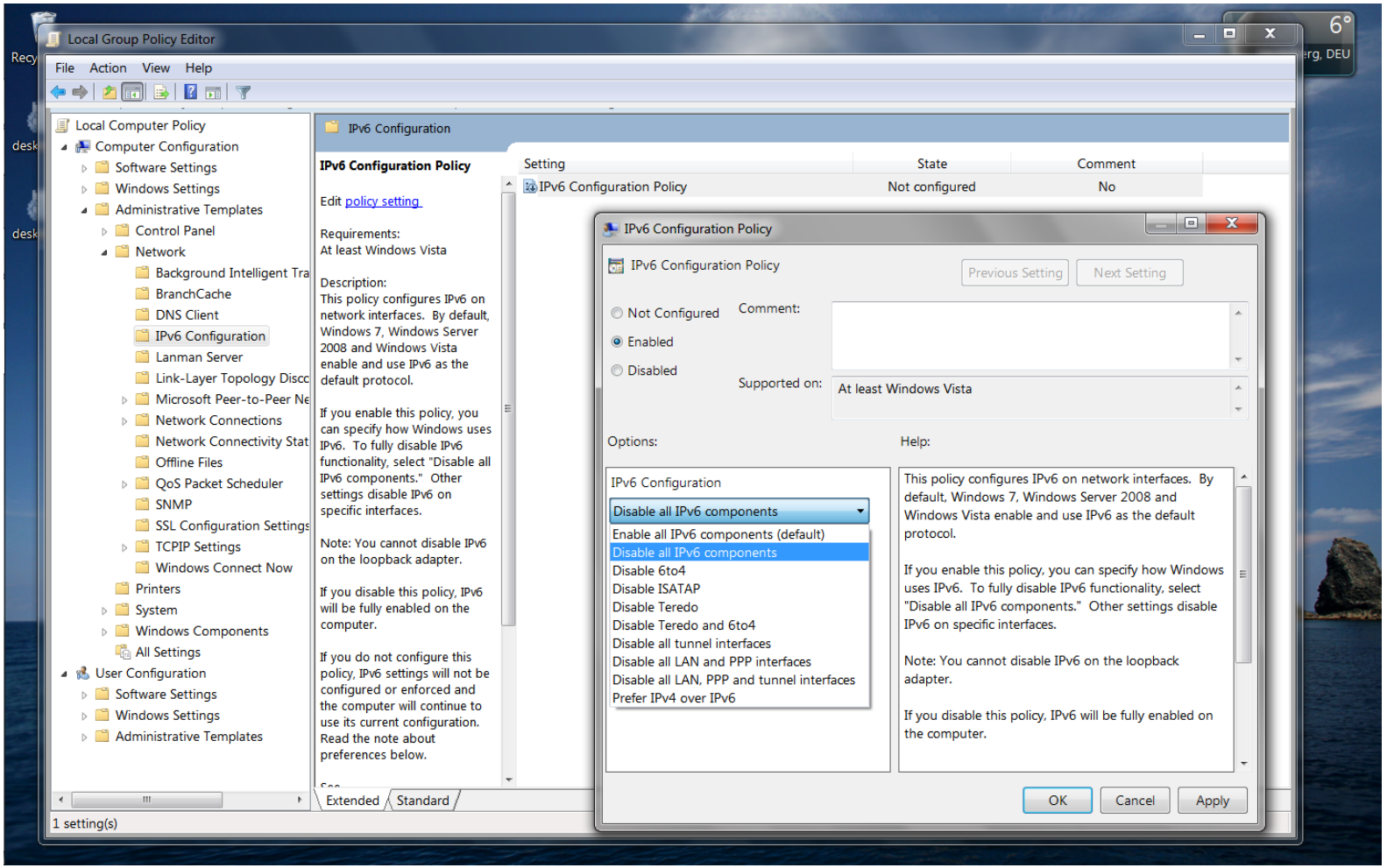
      Note The value "0" is the default setting.
   b. Type **0xffffffff** to disable all IPv6 components, except the IPv6 loopback interface. This value also configures Windows Vista to use Internet Protocol version 4 (IPv4) instead of IPv6 in prefix policies.
   c. Type **0x20** to use IPv4 instead of IPv6 in prefix policies.
   d. Type **0x10** to disable native IPv6 interfaces.
   e. Type **0x01** to disable all tunnel IPv6 interfaces.
   f. Type **0x11** to disable all IPv6 interfaces except for the IPv6 loopback interface.

© ERNW | Breslauer Str. 28 | GmbH D-69124 Heidelberg | www.ernw.de

Can be done by (3rd party) GPO as well

[http://www.expta.com/2009/02/how-to-configure-ipv6-using-group.html]

ERNW
providing security.



© ERNW | Breslauer Str. 28 | GmbH D-69124 Heidelberg | www.ernw.de

Be aware

- **Microsoft strongly recommends against disabling IPv6 and somehow threatens "you'll lose support if you do so".**
  - Personally I see no reason to disable at least some tunneling prots. And I've not experienced any problems with this, so far.
  - Most cautious approach: deactivate tunnel interf. with netsh commands.

- **See also:**
  - http://blogs.technet.com/b/netro/archive/2010/11/24/arguments-against-disabling-ipv6.aspx

- **Funnily enough…**
  - *Windows Update* does not work over IPv6 as of April 2011.

© ERNW | Breslauer Str. 28 | GmbH D-69124 Heidelberg | www.ernw.de

A further note on dual-stack hosts

ERNW
providing security.

- **When both active, usually IPv6 is preferred over IPv4.**
- **Typical behavior goes like**
  - Dual-stack host performs DNS request for www.example.com
  - DNS reply might contain A and AAAA records
  - If AAAA record was provided client takes IPv6

- **But the behavior might heavily depend on the application**
  - … with all the consequences this has, e.g. for troubleshooting…

© ERNW | Breslauer Str. 28 | GmbH D-69124 Heidelberg | www.ernw.de

Tunnels & Transition Tools, Variants

ERNW
providing security.

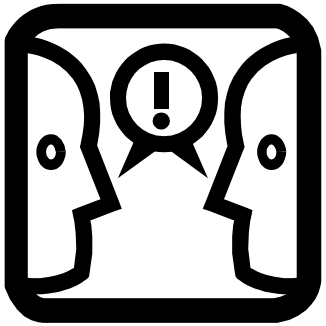
- **Static / configured tunnels**
  - See also RFC 4213
- **Automatic Tunnels**
  - 6to4
  - ISATAP
  - Teredo
- **Other**
  - Proxy-like stuff / Application Layer
  - NAT
  - Tunneling IPv4 over IPv6 (starting in 2015 ;-)

© ERNW | Breslauer Str. 28 | GmbH D-69124 Heidelberg | www.ernw.de

Static / configured tunnels (6in4)

ERNW
providing security.

- **RFC 3056, overall very similar to GRE**
- **Protocol type 41 (0x29)**
- **Usually don’t work across NAT**
- **Keep MTU (20 extra bytes needed) in mind…**
- **Security discussion: as they have to be configured manually you should know what you do anyway ;-)**
  - Always be aware: there’s no more NAT (around)…



© ERNW | Breslauer Str. 28 | GmbH D-69124 Heidelberg | www.ernw.de

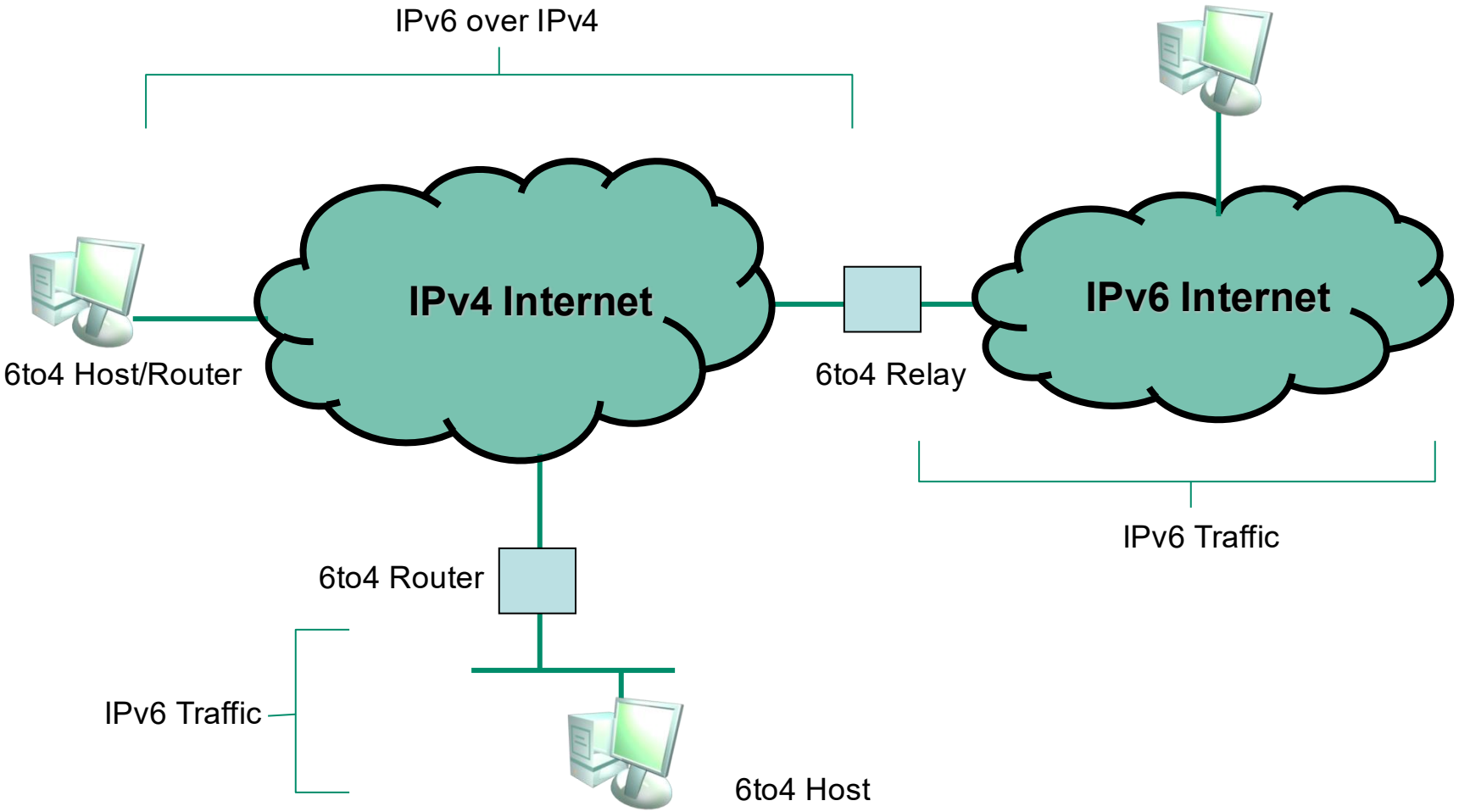
6to4

- **6to4 [RFC 3056] is a router-to-router, host-to-router and router-to-host automatic tunneling technology.**
- **6to4 tunneling interface treats the entire IPv4 Internet as a single link layer. In this case the link layer encapsulation is IPv4.**

- **Uses IP protocol 41**
  - → Usually does not work across NAT.
  - Requires public IP address on hosts.
- **Oldest & subsequently “most widely deployed“ tech.**

© ERNW | Breslauer Str. 28 | GmbH D-69124 Heidelberg | www.ernw.de

6to4 components

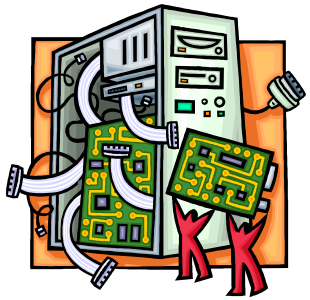


© ERNW | Breslauer Str. 28 | GmbH D-69124 Heidelberg | www.ernw.de

6to4 components

ERNW
providing security.

- **6to4 host**
  - Native IPv6 host with at least one 6to4 address (global).
  - Creates 6to4 address(es) using standard address autoconfiguration.
  - Does not have a 6to4 tunneling interface and doesn‘t perform tunneling.



- **6to4 router**
  - Uses a 6to4 tunneling interface to forward 6to4 traffic between the 6to4 hosts within its network and other 6to4 routers across the IPv4 Internet.
  - On Windows systems usually enabled once *Internet Connection Sharing* (ICS) is configured.
  - Sends router advertisements!

© ERNW | Breslauer Str. 28 | GmbH D-69124 Heidelberg | www.ernw.de

6to4 components

ERNW
providing security.

- **6to4 host/router**
  - Default behavior for Windows OS if public IP address available!
    - At least for Windows Server 2008 R2, Vista, Win 7.
  - Assigns itself address from 2002:*WWXX*:*YYZZ*::/64 type (+ route).
  - Tries to resolve 6to4.ipv6.microsoft.com to get “nearest relay“.
  - Does not forward traffic for other (6to4) hosts.

- **6to4 relay**
  - IPv6/IPv4 router that forwards 6to4 traffic between 6to4 routers and 6to4 host/routers on the IPv4 internet and hosts on the IPv6 internet.
  - Microsoft has deployed a 6to4 relay on the IPv4 Internet
    - At DNS name 6to4.ipv6.microsoft.com.

© ERNW | Breslauer Str. 28 | GmbH D-69124 Heidelberg | www.ernw.de

Deactivating 6to4, Windows

ERNW
providing security.

- `netsh interface 6to4 set state disabled`

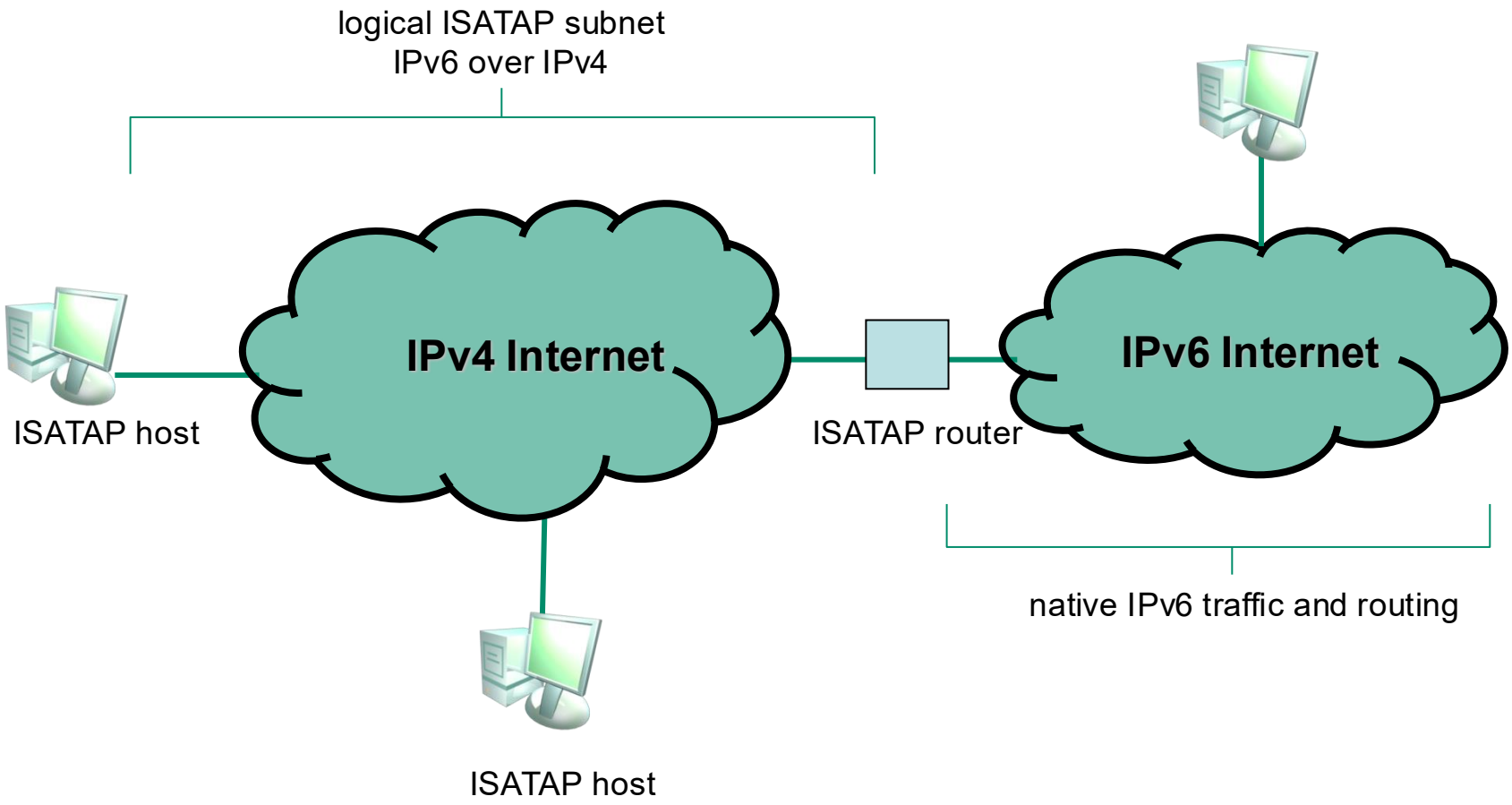
© ERNW | Breslauer Str. 28 | GmbH D-69124 Heidelberg | www.ernw.de

ISATAP Overview

- ***Intra-Site Automatic Tunnel Addressing Protocol***
- **Specified in RFC 5214**
- **Address assignment and tunneling technology**
- **Allows unicast network communication between IPv6/IPv4 nodes over IPv4 Internet or backbone.**
- **Allows connections:**
  - router-to-router
  - host-to-router
  - host-to-host

© ERNW | Breslauer Str. 28 | GmbH D-69124 Heidelberg | www.ernw.de

ISATAP Components

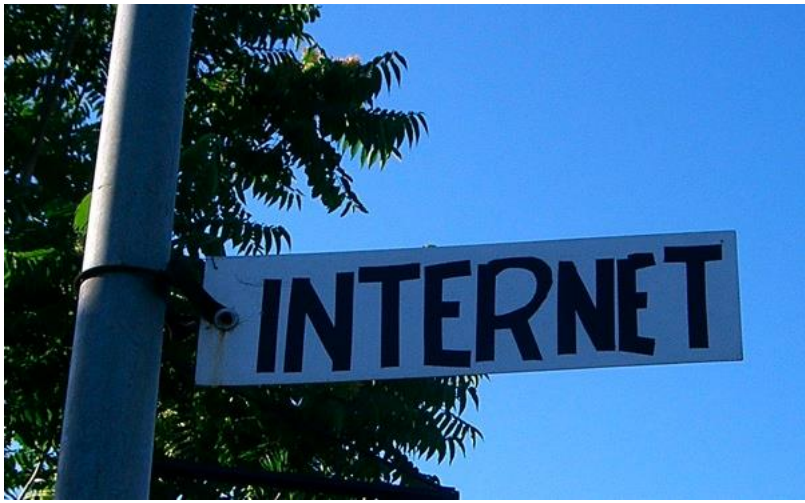


© ERNW | Breslauer Str. 28 | GmbH D-69124 Heidelberg | www.ernw.de

ISATAP Address Format

ERNW
providing security.

- **ISATAP has an own address format:**
  - [*64-bit unicast prefix*]:0:5EFE:*w.x.y.z*
    - *If w.x.y.z is a private IPv4 address*
  - [*64-bit unicast prefix*]:200:5EFE:*w.x.y.z*
    - *If w.x.y.z is a public IPv4 address*
    - Example: FE80::200:5EFE:157.59.137.133



© ERNW | Breslauer Str. 28 | GmbH D-69124 Heidelberg | www.ernw.de

ISATAP, Windows

```
Tunnel adapter isatap.{3BEF8F2E-AA12-4FD0-8E4C-72ABABD9D3D4}:

   Connection-specific DNS Suffix  . : ernw.de
   IPv6 Address. . . . . . . . . . . : 2001:db8:1234:1234:0:5efe:10.0.0.37
   Link-local IPv6 Address . . . . . : fe80::5efe:10.0.0.37%22
   Default Gateway . . . . . . . . . : fe80::5efe:10.0.0.5%22
```


© ERNW | Breslauer Str. 28 | GmbH D-69124 Heidelberg | www.ernw.de

ISATAP Support

- **Windows XP since Service Pack 2**
- **Windows Vista**
- **Windows 7**
- **Windows Server 2003**
- **Windows Server 2008**
- **Linux**
  - Since 2.6.25
- **Cisco IOS**

© ERNW | Breslauer Str. 28 | GmbH D-69124 Heidelberg | www.ernw.de

ISATAP Tunneling – Server 2003 and XP

- **The ISATAP tunneling interface is automatically created.**

- **The name of the interface is “Automatic Tunneling Pseudo-Interface“.**
- **The interface index is typically set to 2.**

© ERNW | Breslauer Str. 28 | GmbH D-69124 Heidelberg | www.ernw.de

Windows Server 2008 /Vista; Server 2008 R2 /Windows 7

ERNW providing security.

- **Without Service Pack**
  - The IPv6 protocol creates a separate ISATAP tunneling interface for each LAN interface installed on the host that has a different DNS suffix.
  - On the ISATAP tunneling interface the link-local address is automatically configured with the corresponding IPv4 address of the LAN interface.

- **With SP1**

  - The ISATAP tunneling interfaces are installed as “media disconnected“ unless the name “ISATAP“ can be resolved.
  - Also the link-local ISATAP address is only configured if the name “ISATAP“ can be resolved.
  - The behavior in W7/W7-SP1 is the same as in Vista with SP1.

© ERNW | Breslauer Str. 28 | GmbH D-69124 Heidelberg | www.ernw.de

Resolving the name “ISATAP“

- **For resolving the name “ISATAP“ standard Windows TCP/IP host name resolution techniques are used.**
- **If resolving the hostname is successful, the host unicasts an IPv4-encapsulated router solicitation message to the ISATAP router at the resolved address.**
- **The router responds with an IPv4-encapsulated unicast router advert. message.**
  - The message contains prefixes to use for autoconfiguration of additional ISATAP addresses.

© ERNW | Breslauer Str. 28 | GmbH D-69124 Heidelberg | www.ernw.de

What does this mean security-wise?

ERNW
providing security.

- **“Injecting” the name “ISATAP” might allow for traffic redirection.**

- **[NISTSP800-119] therefore recommends**
  - “Thus, even if an organization has not enabled ISATAP it might be useful to have a static DNS entry for isatap.company.com pointing to the loopback address 127.0.0.1, thus disabling ISATAP.”

- **Still, if you don’t need ISATAP (which is very probable for an enterprise environment), disabling ISATAP at all might be a better idea…**

© ERNW | Breslauer Str. 28 | GmbH D-69124 Heidelberg | www.ernw.de

Handling ISATAP, Windows

ERNW
providing security.

- **Deactivation on an individual system:**
  - `netsh interface isatap set state disabled`

- **Remove name *isatap* from DNS query blocklist on server:**
  - `dnscmd /config /globalqueryblocklist [wpad]`
  - `dnscmd /info  /globalqueryblocklist`
- **See also:**
  - http://technet.microsoft.com/en-us/library/cc772069(WS.10).aspx

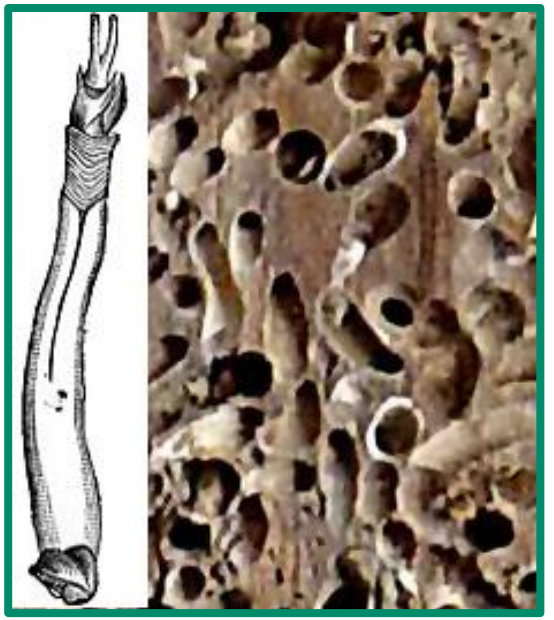
© ERNW | Breslauer Str. 28 | GmbH D-69124 Heidelberg | www.ernw.de

Teredo Overview

ERNW
providing security.

- **Specified in RFC 4380**
- **Similar to the functions of 6to4.**
  - BUT: does not use IP Prot 41. Teredo uses UDP encapsulation.

- **Subject of heavy debates after MS enabled Teredo in Vista.**
  - http://www.symantec.com/avcenter/reference/Teredo_Security.pdf



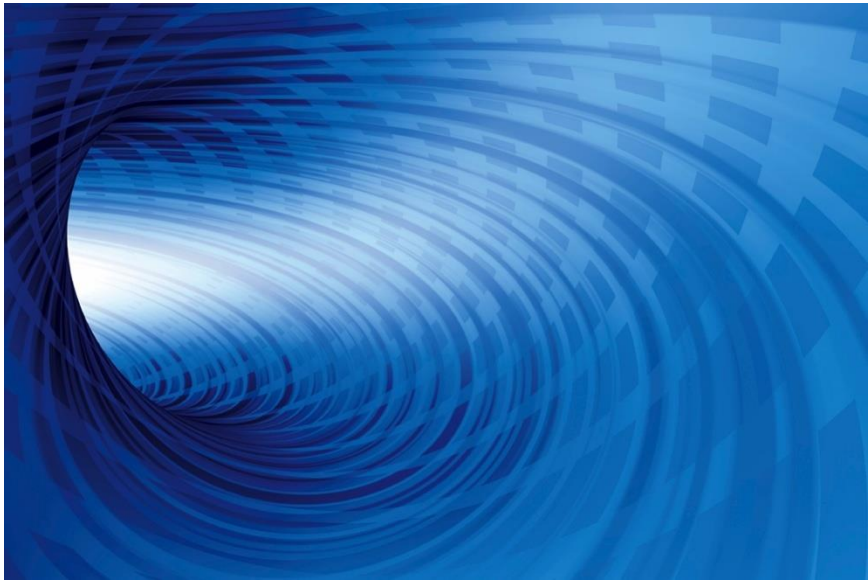
Work done by the teredo worm

© ERNW | Breslauer Str. 28 | GmbH D-69124 Heidelberg | www.ernw.de

Teredo Overview

- **With a huge difference: Teredo can build up tunnels out of networks which are using NAT.**

- **Teredo was designed as interim solution and is supposed to disappear after migration.**
- **Allows connections:**
  - host-to-router
  - host-to-host



© ERNW | Breslauer Str. 28 | GmbH D-69124 Heidelberg | www.ernw.de

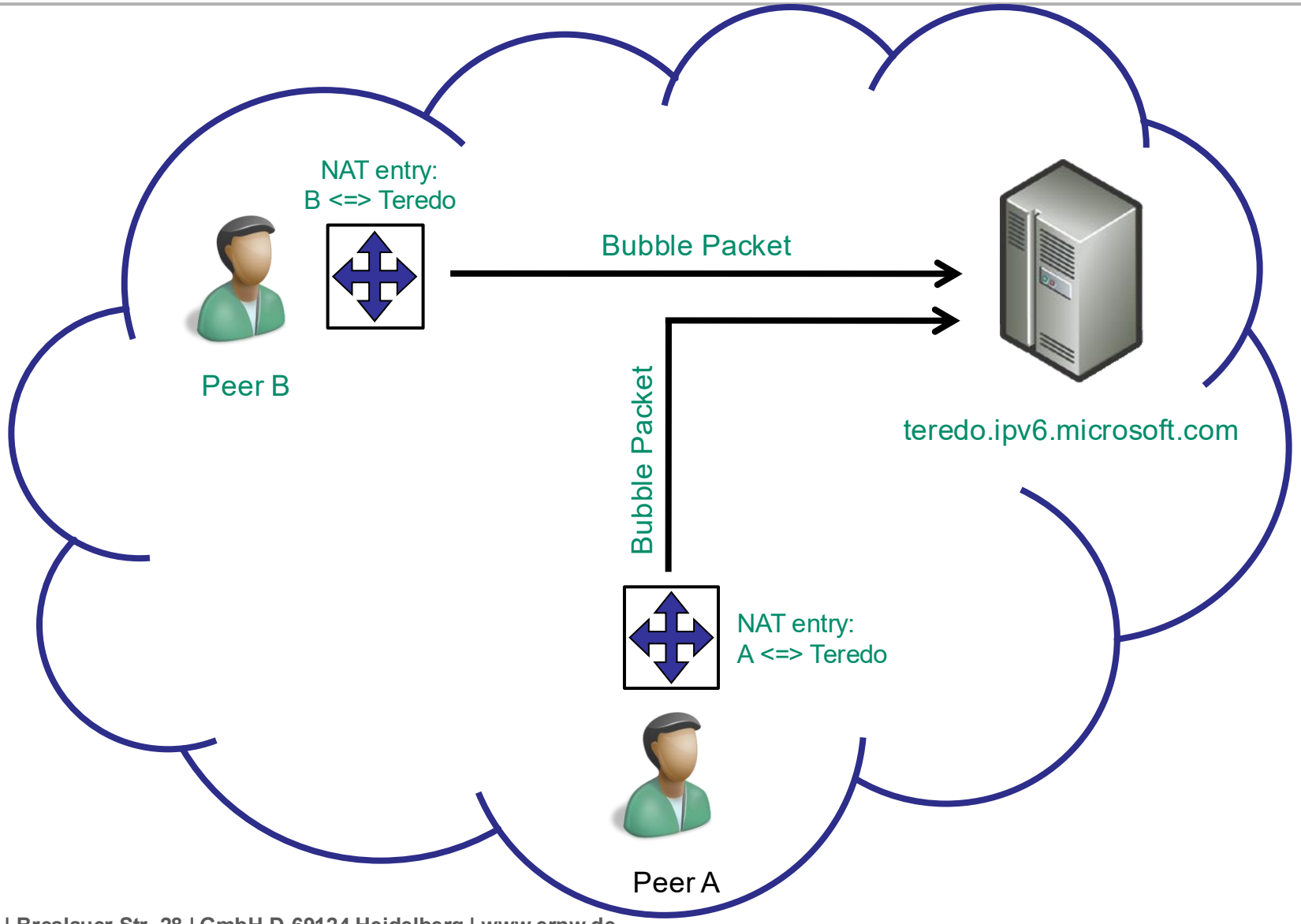
Teredo Address Format

- **RFC 4380 defines the prefix 2001::/32**

- **Until 2006 the address format 3ffe:831f::/32 was used by Windows XP und Server 2003.**

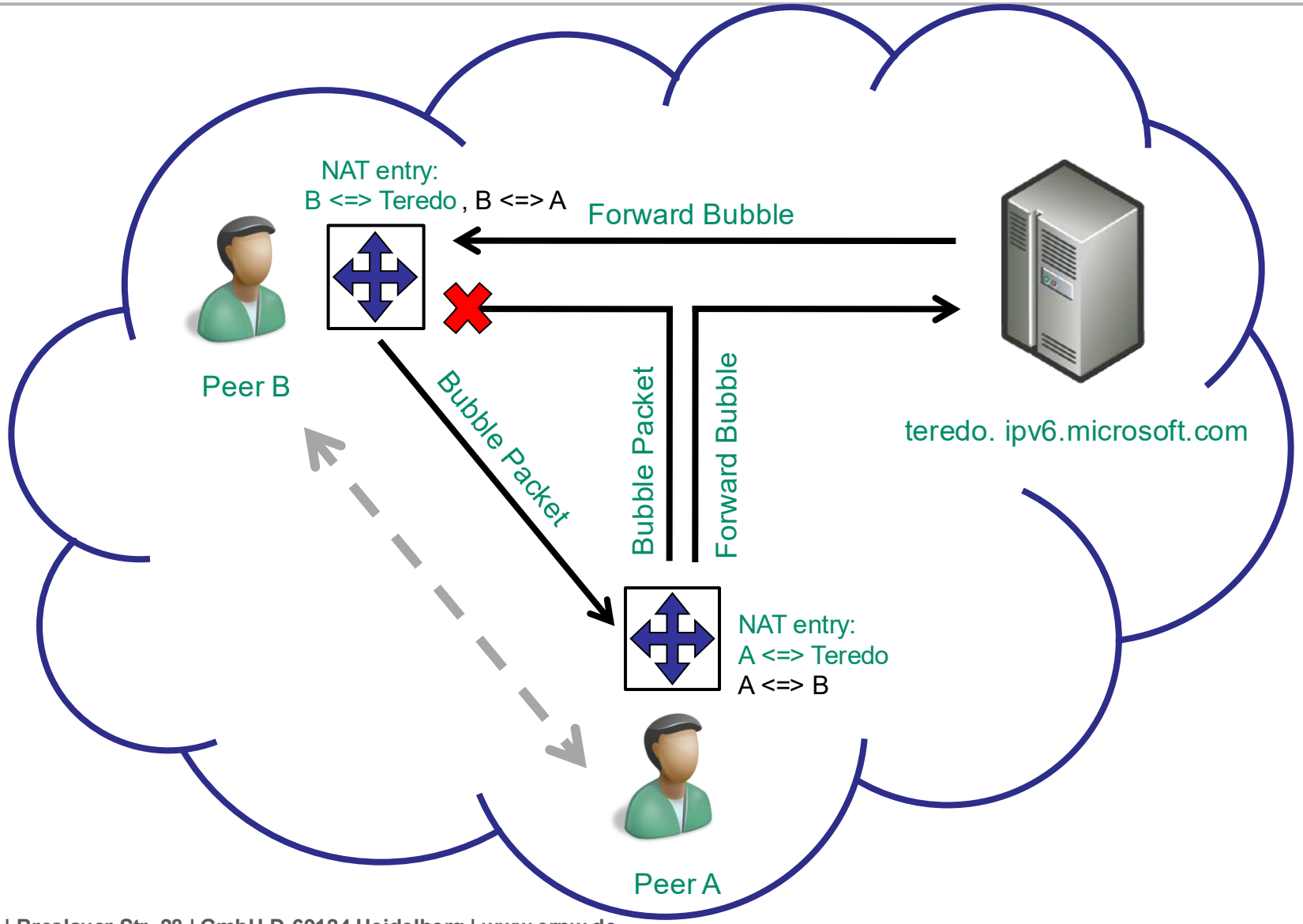
© ERNW | Breslauer Str. 28 | GmbH D-69124 Heidelberg | www.ernw.de

Teredo – Initial Setup



© ERNW | Breslauer Str. 28 | GmbH D-69124 Heidelberg | www.ernw.de

Teredo – NAT Traversal



© ERNW | Breslauer Str. 28 | GmbH D-69124 Heidelberg | www.ernw.de

Teredo Support

ERNW
providing security.

- **Windows XP since Service Pack 2**
- **Windows Vista**
- **Windows Server 2003**
- **Windows Server 2008**
- **Linux**
  - Miredo
- **FreeBSD**
  - ng_teredo

© ERNW | Breslauer Str. 28 | GmbH D-69124 Heidelberg | www.ernw.de

Teredo, Windows default behavior

ERNW providing security.

- **Client checks if it belongs to an AD domain**
  - If yes, Teredo is disabled
  - If not, Teredo is enabled
- **If no local firewall is enabled, Teredo is disabled**

- **When enabled two Teredo states possible**
  - Dormant
  - Qualified
  - Client tries to reach Teredo server every 30 seconds
  - Teredo goes to *qualified* state in case an application needs Teredo
    - A number of BitTorrent clients is able to use IPv6/Teredo. ! MS Meeting Space!
- **The current Teredo State can be viewed with netsh**
  - *netsh interface teredo show state* [slightly different approach on next slide]

© ERNW | Breslauer Str. 28 | GmbH D-69124 Heidelberg | www.ernw.de

This happens more often than you think ;-)

ERNW
providing security.

```
G:\>netsh int ipv6 sh ter
Teredo Parameters
---------------------------------------------
Type                    : client
Server Name             : teredo.ipv6.microsoft.com.
Client Refresh Interval : 30 seconds
Client Port             : unspecified
State                   : qualified
Client Type             : teredo client
Network                 : unmanaged
NAT                     : restricted
NAT Special Behaviour   : UPNP: No, PortPreserving: Yes
Local Mapping           : 192.168.48.120:56328
External NAT Mapping    : 213.61.186.250:56328
```

© ERNW | Breslauer Str. 28 | GmbH D-69124 Heidelberg | www.ernw.de

Teredo, Security Discussion

ERNW
providing security.

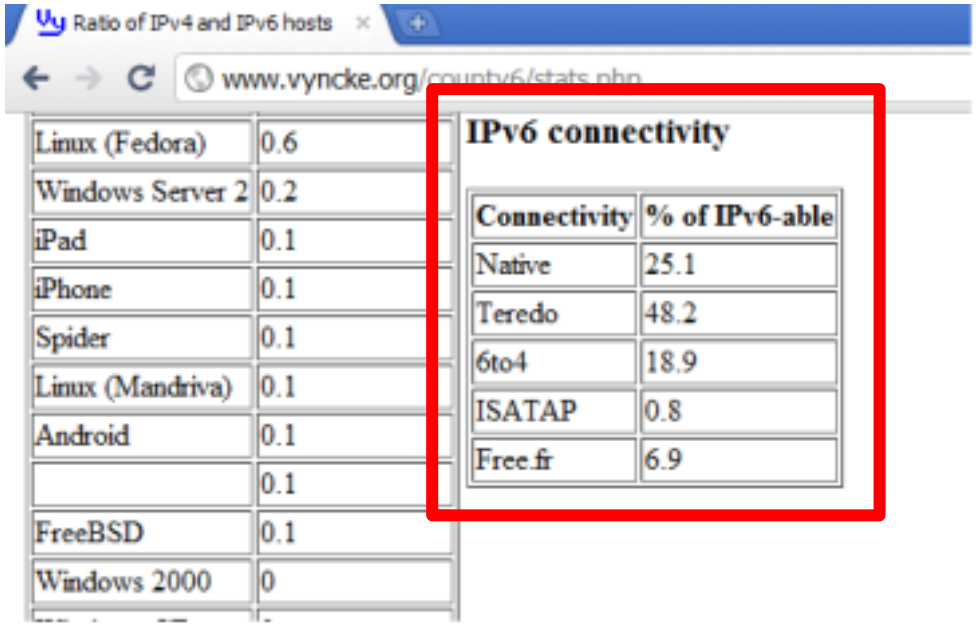
- **Teredo can drill holes in firewalls and provide unwanted connectivity/reachability of clients.**

- **All controls to address the *latent threat* come into play.**
  - Disable if not needed (by *DisabledComponents* reg key).
  - Systems belonging to AD domain have Teredo disabled by default
    - Still, can be enabled by application installation. Be aware of this!

- **By default, Teredo uses UDP port 3544**
  - As a last resort blocking this port on SOHO devices might be an idea.
  - Obviously only allowing desired communication would be better ;-)
  - Port can be modified by user or application.

© ERNW | Breslauer Str. 28 | GmbH D-69124 Heidelberg | www.ernw.de

Some statistics



Linux (Fedora)	0.6
Windows Server 2	0.2
iPad	0.1
iPhone	0.1
Spider	0.1
Linux (Mandriva)	0.1
Android	0.1
	0.1
FreeBSD	0.1
Windows 2000	0

IPv6 connectivity

Connectivity	% of IPv6-able
Native	25.1
Teredo	48.2
6to4	18.9
ISATAP	0.8
Free.fr	6.9

© ERNW | Breslauer Str. 28 | GmbH D-69124 Heidelberg | www.ernw.de

Small tunneling security checklist

ERNW
providing security.

- **6to4 clients might become active once they have a global address (e.g. via dial-in).**
- **6to4 can‘t work across NAT and needs IP procotol 41.**

- **ISATAP clients might become active once they can resolve DNS name “ISATAP“.**
- **ISATAP can‘t work across NAT and needs IP procotol 41.**

- **Teredo mostly becomes active by “application needs“.**
- **Teredo *can* work across NAT & needs $SOME_UDP_PORT.**

© ERNW | Breslauer Str. 28 | GmbH D-69124 Heidelberg | www.ernw.de

ERNW
providing security.

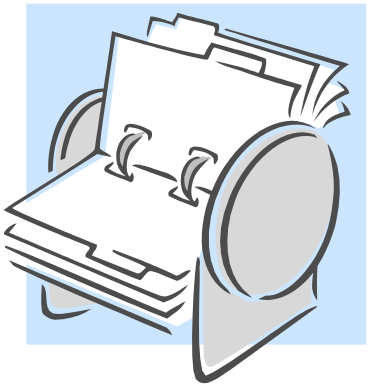
Some challenges waiting for you.

Planning for “full IPv6“.

Addressing & its sec implications

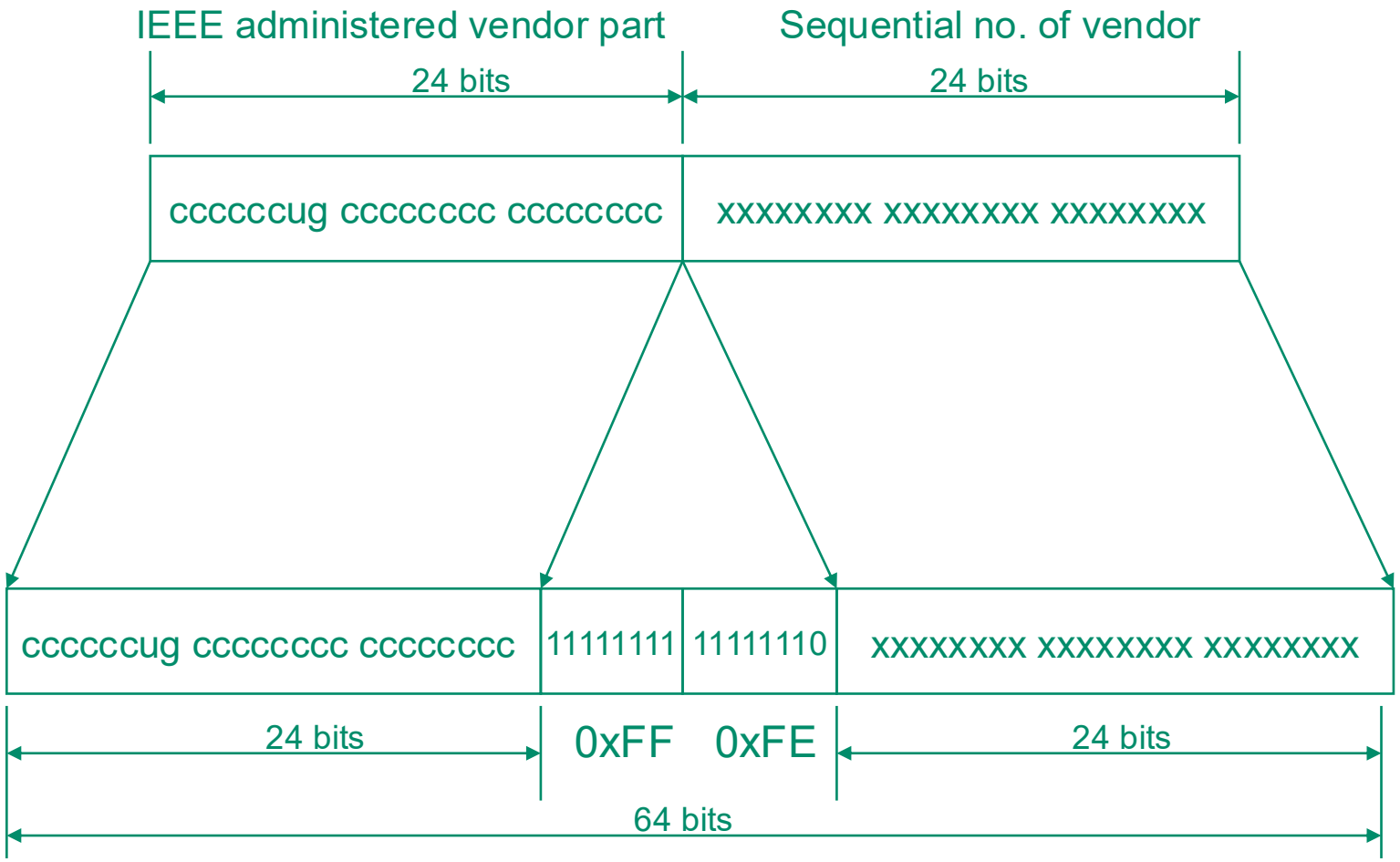
ERNW
providing security.

- **(Main) Variants as for the generation of the host part**
  - EUI-64
  - Privacy extensions
- **Main types of addresses**
  - Link-local (unicast)
  - Global unicast
  - Unique local (unicast)
  - Multicast



© ERNW | Breslauer Str. 28 | GmbH D-69124 Heidelberg | www.ernw.de

EUI-64 address, based on IEEE 802



© ERNW | Breslauer Str. 28 | GmbH D-69124 Heidelberg | www.ernw.de

Privacy Extensions

- **Potential approaches for more privacy**
  - Using DHCPv6 (?)
  - Changing MAC address over time
  - Using Privacy Extensions

- **Privacy Extensions**
  - Specified in RFC 4941
  - Might provide “anonymity“ similar to IPv4
  - Using randomly generated ‘‘Interface Identifier“
  - Might only be valid for a specific time-interval
    - i.e. for each initiation of a new communication

© ERNW | Breslauer Str. 28 | GmbH D-69124 Heidelberg | www.ernw.de

Privacy extensions, Sec Discussion

ERNW
providing security.

- **Might heavily impact traceability or forensics.**

- **Windows default behavior can be changed via**
  - `netsh interface ipv6 set global randomizeidentifiers=disabled`

© ERNW | Breslauer Str. 28 | GmbH D-69124 Heidelberg | www.ernw.de

Unique Local Addresses (ULA)

ERNW
providing security.

- **ULA is divided into two groups, identified by the prefixes**

- **fc00::/8**
  - Can be centrally assigned by some sort of registrar (router)
  - One gets FCxx:xxxx:xxxx:yyyy:zzzz:zzzz:zzzz:zzzz

- **fd00::/8**
  - Not assigned by central authority/entity
  - (“Pseudo“) Randomly generated number
  - One gets FDxx:xxxx:xxxx:yyyy:zzzz:zzzz:zzzz:zzzz

© ERNW | Breslauer Str. 28 | GmbH D-69124 Heidelberg | www.ernw.de

ULA, Security Discussion

ERNW
providing security.

- **ULA widely regarded as successor to RFC 1918 addresses**
  - Will potentially be used (mostly) the same way

- **RFC 4193, section 4.1 *Routing* clearly states:**

"The default behavior of exterior routing protocol sessions between administrative routing regions must be to ignore receipt of and not advertise prefixes in the FC00::/7 block."

- **Still it's a bit unclear today what will happen exactly…**

- **Advice: filter (or better: null-route) FC00::/7 on borders.**

© ERNW | Breslauer Str. 28 | GmbH D-69124 Heidelberg | www.ernw.de

A word on NAT in IPv6

ERNW
providing security.

- **Initially NAT was unwanted.**
  - End-to-end principle! one of the main architecture goals of IPv6.
- **But: many people like NAT for security reasons.**
  - Heavy debates within IPv6 community.

- **Problem: there's still no standardized NAT approach… and we'll (hopefully) not see any soon…**
-
  - IETF *BEHAVE* wg, http://datatracker.ietf.org/wg/behave
  - Yes, we're aware that just recently some RFCs (in the 6144 to 6156 range) were published… we just don't "believe in them" ;-)

© ERNW | Breslauer Str. 28 | GmbH D-69124 Heidelberg | www.ernw.de

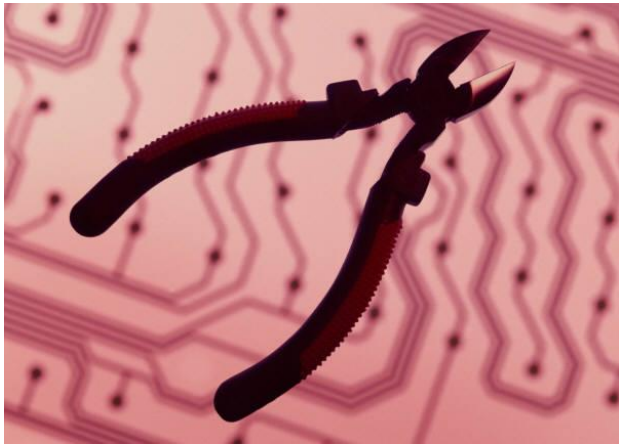
Some words in link-local addresses

ERNW
providing security.

- **Might have huge security benefits in some cases**
  - Cannot be routed.
  - Can not!

- **Think about isolating certain boxes by just giving them a LL address.**

- **Still too early to really understand use cases.**

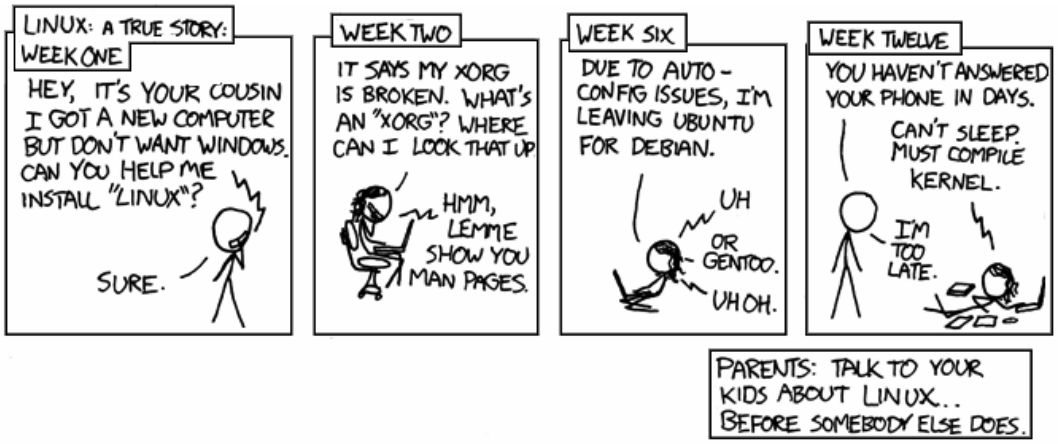


© ERNW | Breslauer Str. 28 | GmbH D-69124 Heidelberg | www.ernw.de

ERNW
providing security.

So now you have IPv6... ... what should you care about most?

ERNW
providing security.



Source: xkcd.com

Some Very Quick Refresher on Autoconfiguration

Autoconfiguration, Variants

ERNW
providing security.

- **Stateless**
  - Router Advertisements play a major role here.

- **Stateful**
  - DHCPv6
  - Please note: even here “initial stuff” *can* happen by RAs
    - Some OS (Windows) might try DHCPv6 immediately.

© ERNW | Breslauer Str. 28 | GmbH D-69124 Heidelberg | www.ernw.de

1-Slide Sec Discussion of DHCPv6

ERNW
providing security.

- **As in v4 *rogue DHCP servers* can cause harm.**
  - Nothing new here.
  - We'll probably release a *LOKI* module for this soon…
- **Overall risk pretty much the same as in v4.**
  - Might be even smaller as link-local address not deployed by DHCP.
- **Same mitigation techniques (if any) will probably apply.**
  - Certainly some "DHCP snooping successor" will be available.

© ERNW | Breslauer Str. 28 | GmbH D-69124 Heidelberg | www.ernw.de

1-Slide on Neighbor Cache Entries

ERNW
providing security.

State	Description
INCOMPLETE	Neighbor Solicitation has been sent, but no Neighbor Advertisement has been retrieved.
REACHABLE	Positive confirmation was received within the last *ReachableTime* milliseconds, no special actions necessary.
STALE	ReachableTime milliseconds have elapsed, no actions takes place. This is entered upon receiving an unsolicited Neighbor Discovery message → entry must actually be used.
DELAY	ReachableTime milliseconds have elapsed and a packet was sent within the last *DELAY_FIRST_PROBE_TIME* seconds. If no message was sent → change state to PROBE.
PROBE	A reachability confirmation is actively sought by retransmitting Neighbor Solicitations every *RetransTimer* milliseconds until reachability confirmation is received.

© ERNW | Breslauer Str. 28 | GmbH D-69124 Heidelberg | www.ernw.de

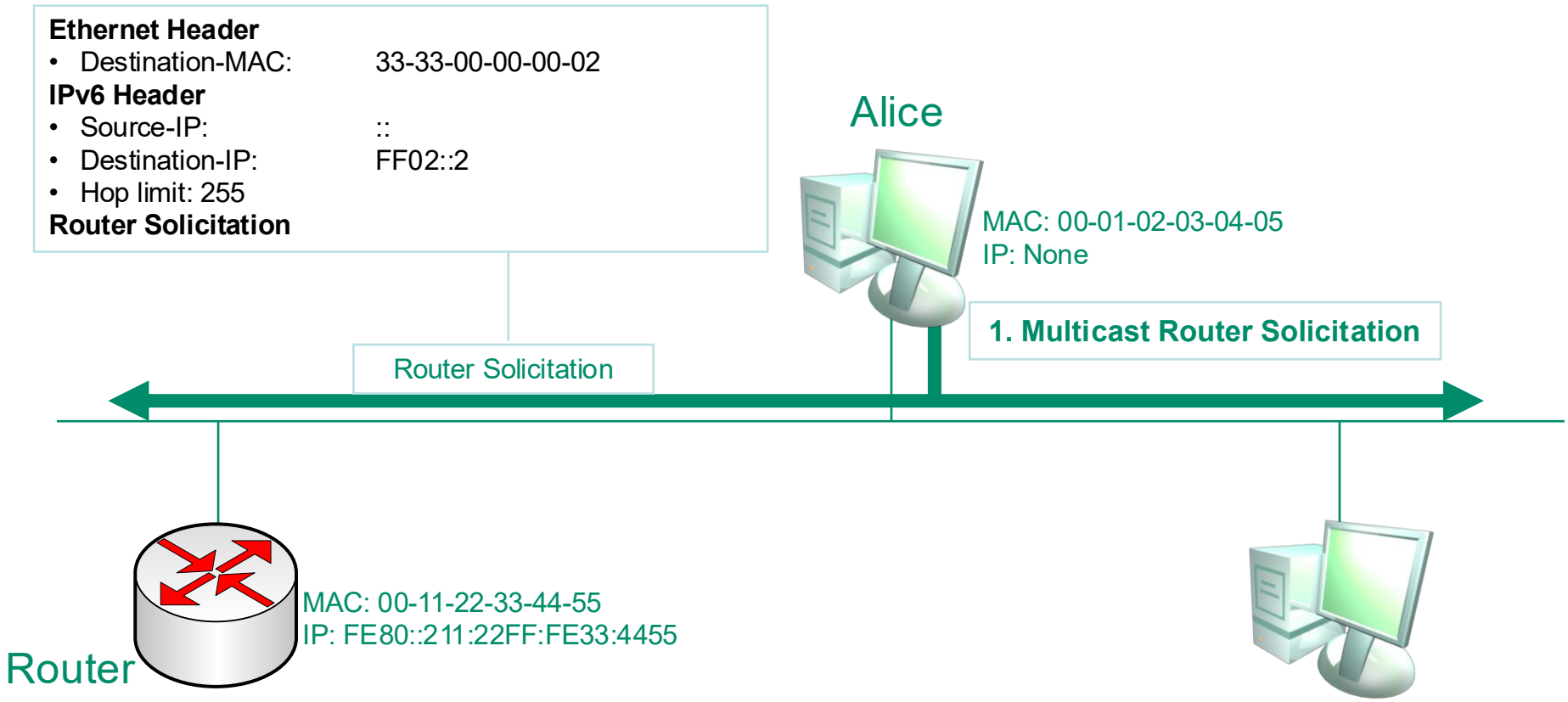
Router Discovery

- **Locate routers on local-link and get some config info from them.**

- **Furthermore, IPv6 Router Discovery provides:**
  - Standard-value for the ”Hop-Limit“-field
  - If additionally a “stateful“ address protocol (DHCPv6) should be used.
  - Time configuration for ”Retransmission Timer“
  - Potentially network-prefix for the local network
  - MTU of the network
  - Mobile IPv6 informations
  - “Routing information”

© ERNW | Breslauer Str. 28 | GmbH D-69124 Heidelberg | www.ernw.de

Multicast Router Solicitation Message



© ERNW | Breslauer Str. 28 | GmbH D-69124 Heidelberg | www.ernw.de

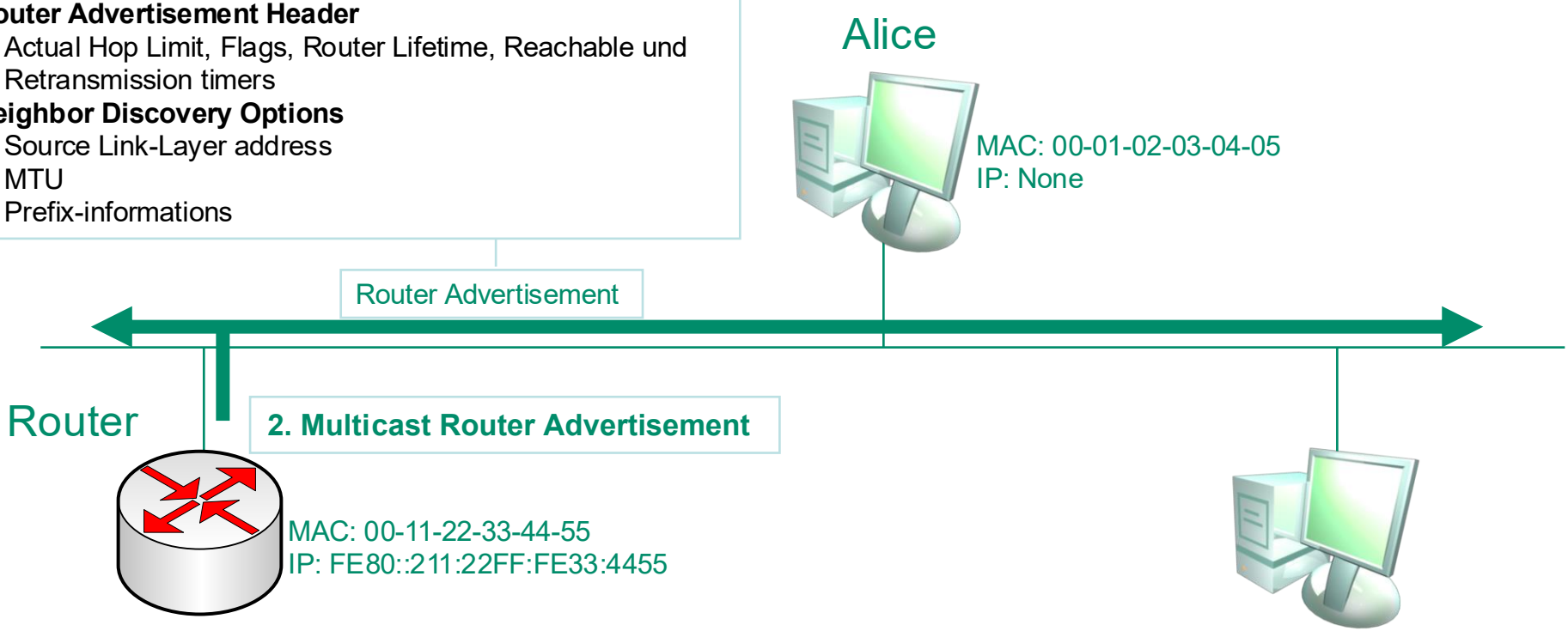
Multicast Router Advertisement Message

Ethernet Header
- Destination MAC: 33-33-00-00-00-01

IPv6 Header
- Source-IP: FE80::211:22FF:FE33:4455
- Destination-IP: FF02::1
- Hop limit: 255

Router Advertisement Header
- Actual Hop Limit, Flags, Router Lifetime, Reachable und Retransmission timers

Neighbor Discovery Options
- Source Link-Layer address
- MTU
- Prefix-informations

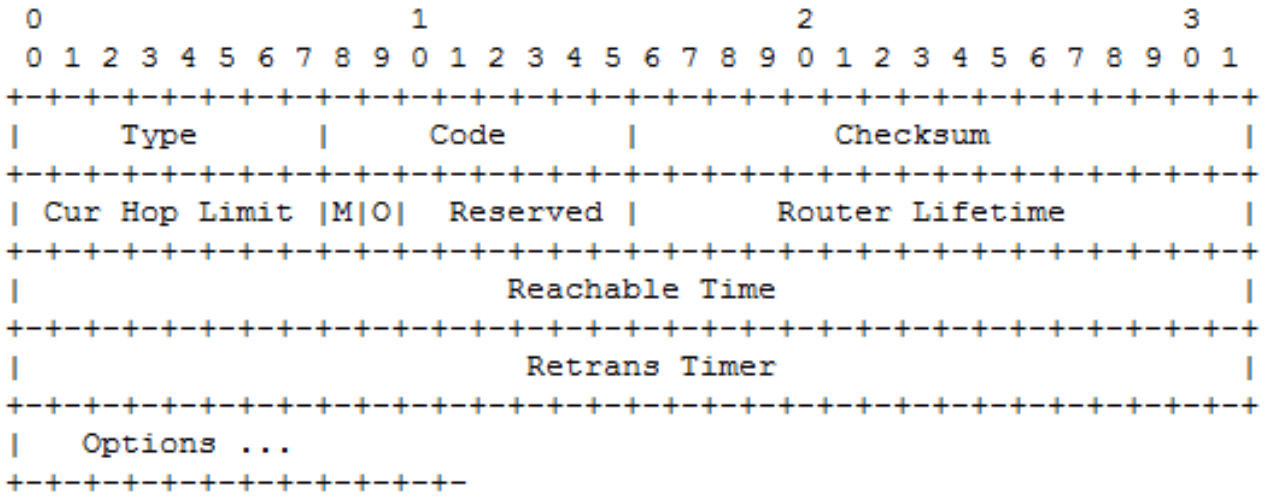


© ERNW | Breslauer Str. 28 | GmbH D-69124 Heidelberg | www.ernw.de

Router Advertisements, Flags

- **Routers can inform the adjacent clients that additional configuration parameters (like a DNS Server) are available over a stateful configuration protocol (DHCPv6).**

- **In the Router Advertisement Header are two flags (M and O) which can be set to inform the clients that additional configuration parameters are available.**



© ERNW | Breslauer Str. 28 | GmbH D-69124 Heidelberg | www.ernw.de

O-Flag

- **1-bit ”other configuration“ flag**

- **When set, it indicates that other configuration information is available via DHCPv6.**
- **Examples of such information are DNS-related information (DNS Server, DNS Suffix).**
- **Both flags are defined in RFC 4861 (Section 4.2).**

© ERNW | Breslauer Str. 28 | GmbH D-69124 Heidelberg | www.ernw.de

M-Flag

- **1-bit "Managed address configuration" flag.**
- **When set, it indicates that addresses are available through DHCPv6.**
- **If the M flag is set, the O flag is redundant and can be ignored because DHCPv6 will return all available configuration information.**
- **If neither M nor O flags are set, this indicates that no information is available via DHCPv6.**

© ERNW | Breslauer Str. 28 | GmbH D-69124 Heidelberg | www.ernw.de

Message Validation

ERNW
providing security.

- **Validation of Router Solicitation Messages**
  - Hosts MUST silently discard any received Router Solicitation Messages.
  - A router MUST silently discard any received Router Solicitation messages that do not satisfy all of the following validity checks:
    - IP Hop Limit field has a value of 255
    - ICMP Checksum is valid
    - ICMP Code is 0
    - ICMP length is 8 or more octets
    - All included options have a length greater than zero
    - If IP source address is the unspecified address
      → there is no source link-layer address option in the message

© ERNW | Breslauer Str. 28 | GmbH D-69124 Heidelberg | www.ernw.de

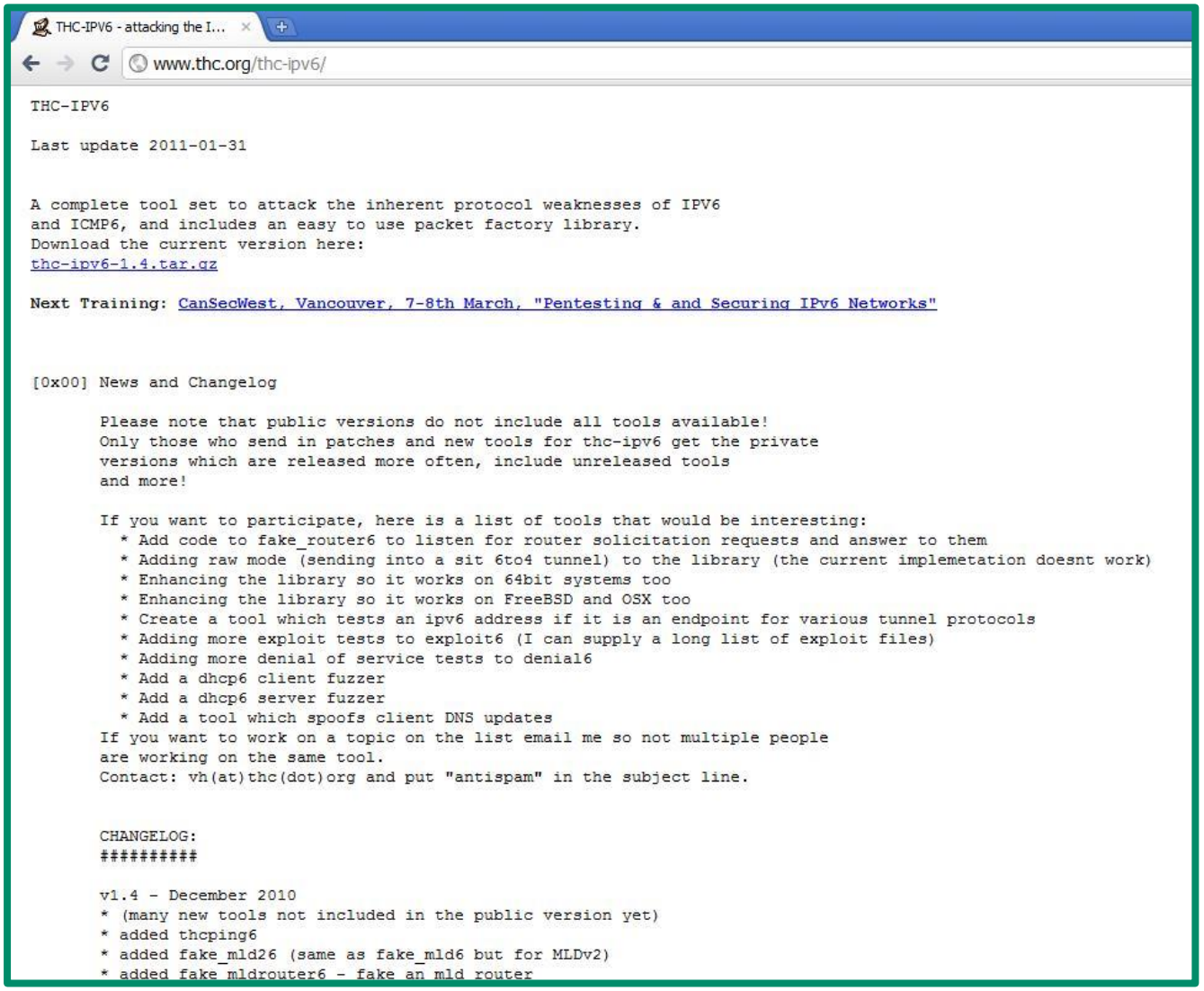
Bad things that can happen

ERNW
providing security.

- **Some RA-generating entity accidentally active in your network**
  - IPv6 capable SOHO device connected by user.
  - Windows system with ICS enabled (see above).
  - Virtual machine running sth emitting RAs…
- **Attacker interferes with router discovery**
  - Denial-of-service by sending many bogus RAs
  - Traffic redirection by spoofed RAs

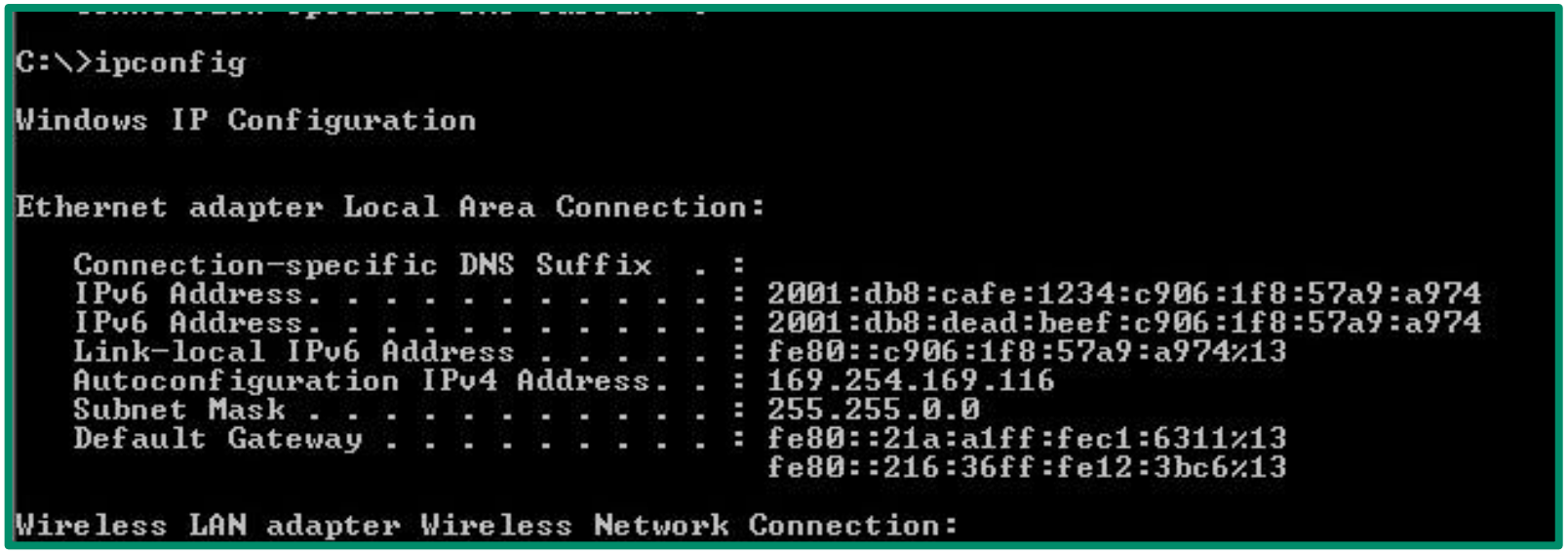
© ERNW | Breslauer Str. 28 | GmbH D-69124 Heidelberg | www.ernw.de

RA based attacks with THC-IPV6



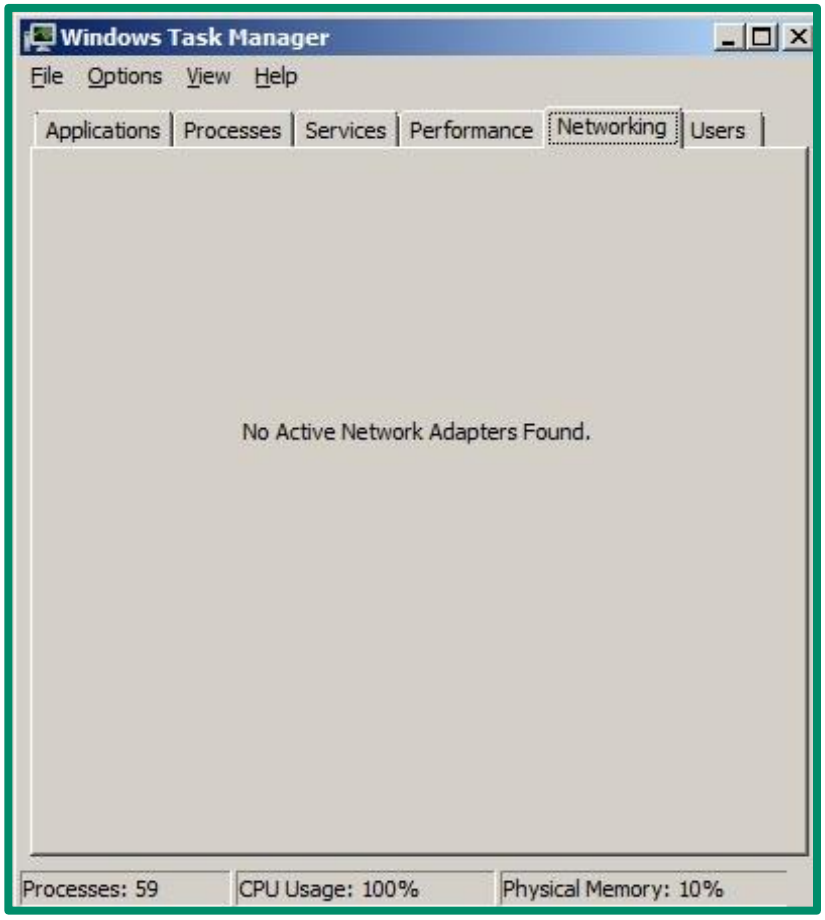
© ERNW | Breslauer Str. 28 | GmbH D-69124 Heidelberg | www.ernw.de

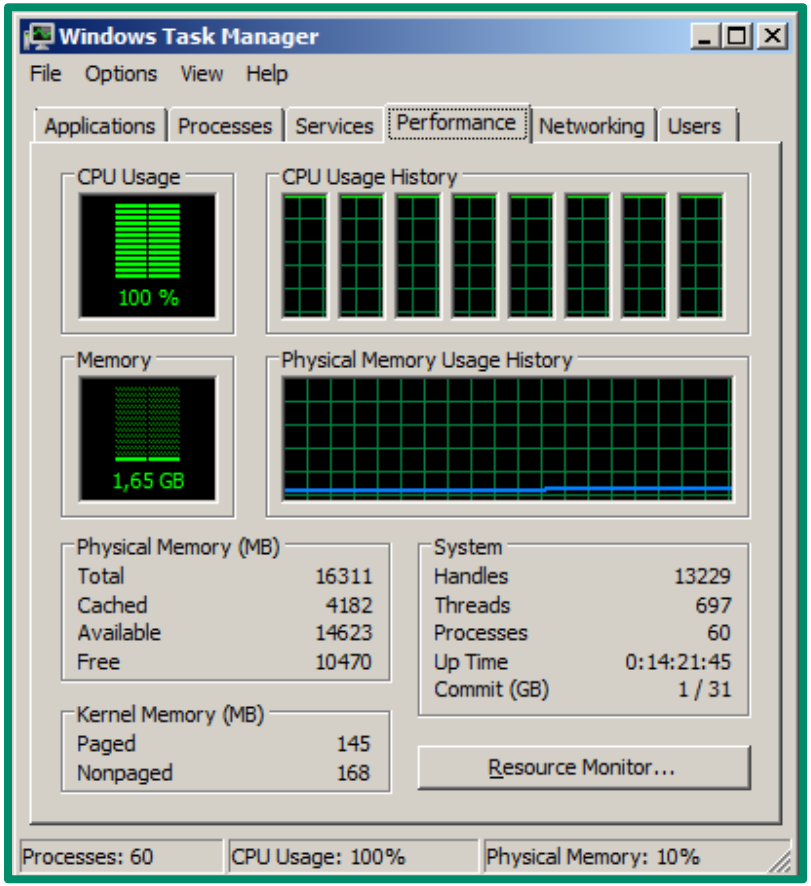
fake_router6, Impact



© ERNW | Breslauer Str. 28 | GmbH D-69124 Heidelberg | www.ernw.de

flood_router6, Impact





© ERNW | Breslauer Str. 28 | GmbH D-69124 Heidelberg | www.ernw.de

Did you note?

- **This is EVIL stuff!**

© ERNW | Breslauer Str. 28 | GmbH D-69124 Heidelberg | www.ernw.de

Spoofed RA protection as of RFC 6104

- **Manual configuration**
- **RA Snooping (RA Guard)**
- **Using ACLs**
- **SEcure Neighbor Discovery (SEND)**
- **Router Preference**
- **Relying on Layer 2 Admission Control**
- **Host-Based Packet Filters**
- **Using an “Intelligent” Deprecation Tool**
  - E.g. NDPMon
- **Using Layer 2 Partitioning**

© ERNW | Breslauer Str. 28 | GmbH D-69124 Heidelberg | www.ernw.de

This can be broken down to the “ERNW Seven Sisters of Infrastructure Sec”

Access Control

Restriction (Filtering)

Segmentation/Isolation

Encryption

Hardening

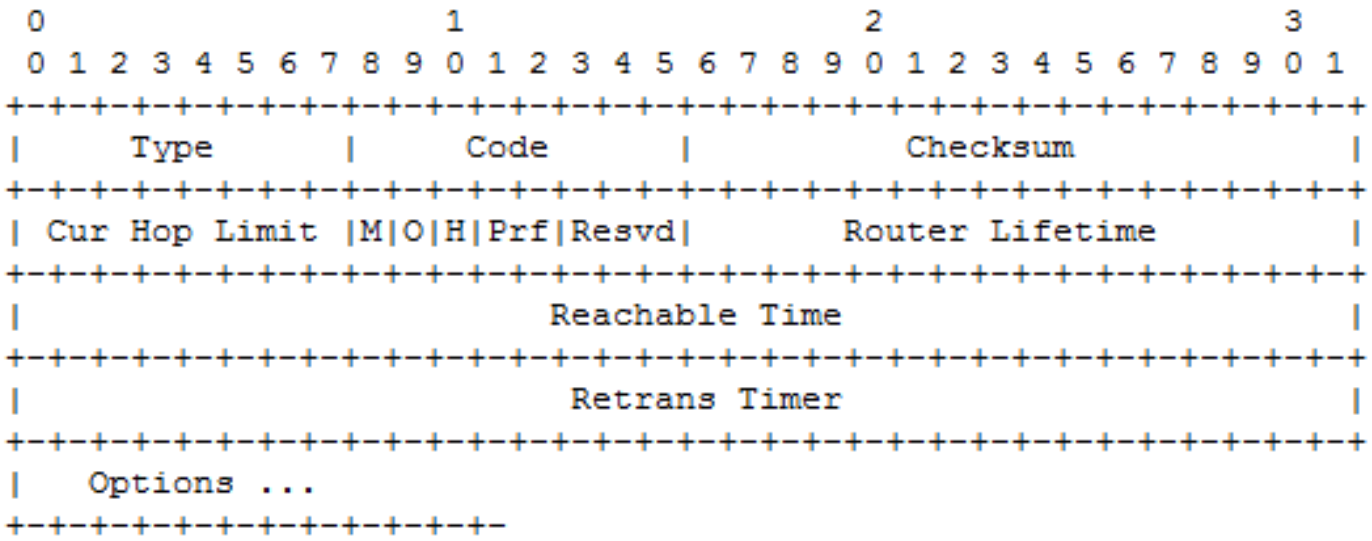
Secure Management

Visibility

© ERNW | Breslauer Str. 28 | GmbH D-69124 Heidelberg | www.ernw.de

Default Router Preference

- **In RFC 4191 an additional flag was introduced within RA messages to indicate the preference of a default router in case more than one are present on the local link.**



© ERNW | Breslauer Str. 28 | GmbH D-69124 Heidelberg | www.ernw.de

Router Preference Values

- **The *preference* values are encoded as a two-bit signed integer with the following values:**
  - 01 High
  - 00 Medium (default)
  - 11 Low
  - 10 Reserved

© ERNW | Breslauer Str. 28 | GmbH D-69124 Heidelberg | www.ernw.de

RA Messages

- **When the *preference* is set, the RA messages look like:**

```
Internet Control Message Protocol v6
    Type: 134 (Router advertisement)
    Code: 0
    Checksum: 0xded0 [correct]
    Cur hop limit: 64
  Flags: 0x08
      0... .... = Not managed
      .0.. .... = Not other
      ..0. .... = Not Home Agent
      ...0 1... = Router preference: High
    Router lifetime: 1800
    Reachable time: 0
    Retrans timer: 0
  ICMPv6 Option (Source link-layer address)
  ICMPv6 Option (MTU)
  ICMPv6 Option (Prefix information)
```

```
Internet Control Message Protocol v6
    Type: 134 (Router advertisement)
    Code: 0
    Checksum: 0xcdc6 [correct]
    Cur hop limit: 64
  Flags: 0x00
      0... .... = Not managed
      .0.. .... = Not other
      ..0. .... = Not Home Agent
      ...0 0... = Router preference: Medium
    Router lifetime: 1800
    Reachable time: 0
    Retrans timer: 0
  ICMPv6 Option (Source link-layer address)
  ICMPv6 Option (MTU)
  ICMPv6 Option (Prefix information)
```


© ERNW | Breslauer Str. 28 | GmbH D-69124 Heidelberg | www.ernw.de

Configuration (Cisco)

- **The configuration of the preference is done with the following command:**

  - `Router(config)# interface f0/1`
  - `Router(config-if)# ipv6 nd router-preference {high | medium | low}`

- **If the command is not configured, the default value of medium will be used in the RA messages.**

- **Command available since IOS Version 12.4(2)T**

© ERNW | Breslauer Str. 28 | GmbH D-69124 Heidelberg | www.ernw.de

Deactivation of RA processing on *Windows* Hosts (e.g. within DMZ)

- **`netsh int ipv6 set int [index] routerdiscovery=disabled`**

```
C:\>netsh int ipv6 sh int 11

Interface Local Area Connection Parameters
----------------------------------------------
IfLuid                                 : ethernet_6
IfIndex                                : 11
State                                  : connected
Metric                                 : 5
Link MTU                               : 1500 bytes
Reachable Time                         : 38500 ms
Base Reachable Time                    : 30000 ms
Retransmission Interval                : 1000 ms
DAD Transmits                          : 1
Site Prefix Length                     : 64
Site Id                                : 1
Forwarding                             : disabled
Advertising                            : disabled
Neighbor Discovery                     : enabled
Neighbor Unreachability Detection      : enabled
Router Discovery                       : enabled
Managed Address Configuration          : enabled
Other Stateful Configuration           : enabled
Weak Host Sends                        : disabled
Weak Host Receives                     : disabled
Use Automatic Metric                   : enabled
Ignore Default Routes                  : disabled
Advertised Router Lifetime             : 1800 seconds
Advertise Default Route                : disabled
Current Hop Limit                      : 0
Force ARPND Wake up patterns           : disabled
Directed MAC Wake up patterns          : disabled
```


© ERNW | Breslauer Str. 28 | GmbH D-69124 Heidelberg | www.ernw.de

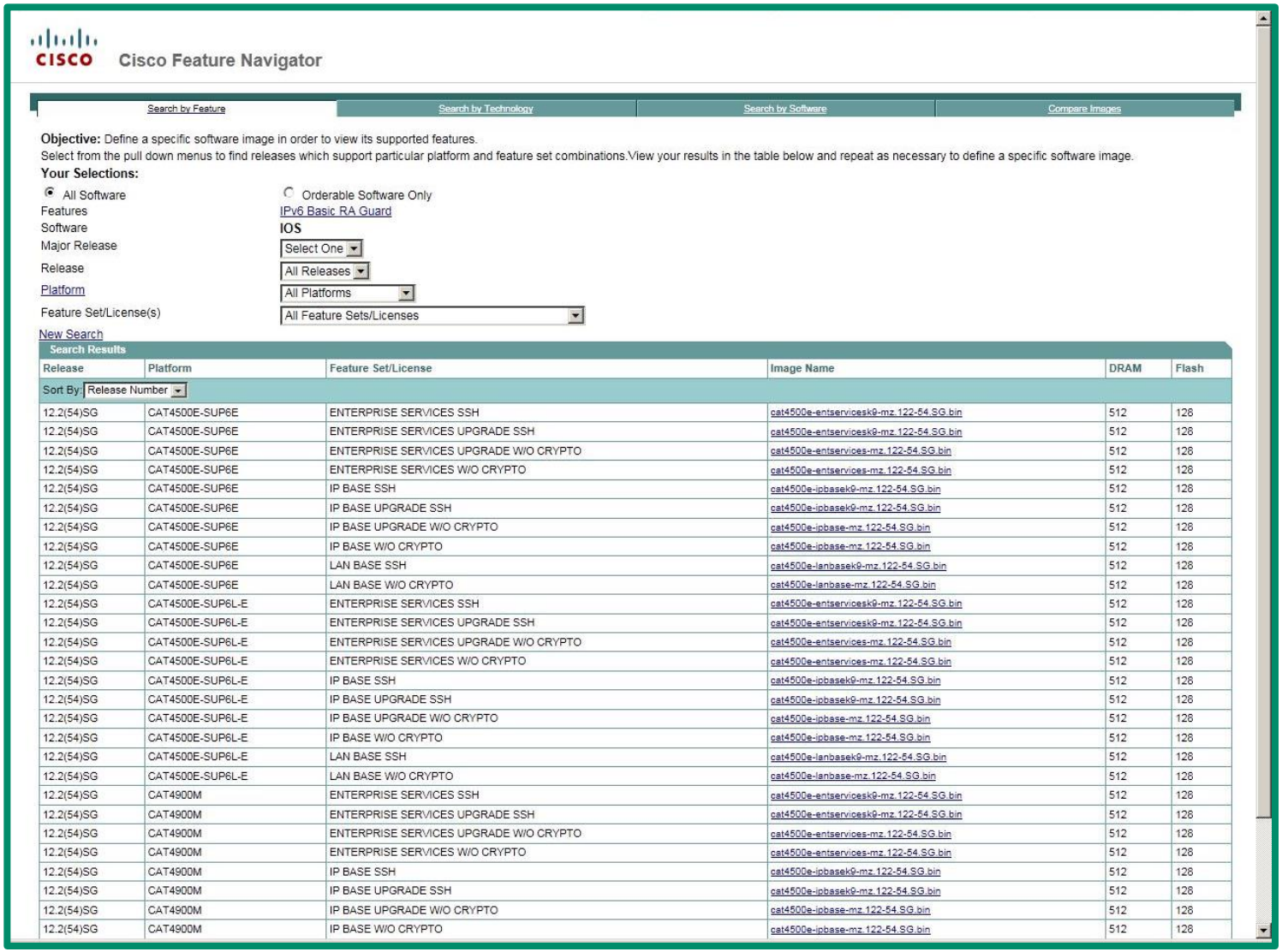
RA Guard

- **Implements *isolation* principle similar to other L2 protection mechanisms already deployed in v4 world.**
- **RFC 6105**

- **Works like a charm!**
  - But it seems currently no logging or port deactivation can be implemented. RA packets are just dropped.
- **UNFORTUNATELY as of 05/2011 only available on quite few platforms in Cisco space.**

© ERNW | Breslauer Str. 28 | GmbH D-69124 Heidelberg | www.ernw.de

RA Guard availability (05/2011)



Cisco Feature Navigator

Search by Feature | Search by Technology | Search by Software | Compare Images

Objective: Define a specific software image in order to view its supported features.
Select from the pull down menus to find releases which support particular platform and feature set combinations.View your results in the table below and repeat as necessary to define a specific software image.

Your Selections:

All Software / Orderable Software Only
Features: IPv6 Basic RA Guard
Software: IOS
Major Release: Select One
Release: All Releases
Platform: All Platforms
Feature Set/License(s): All Feature Sets/Licenses

New Search

Search Results

Release	Platform	Feature Set/License	Image Name	DRAM	Flash
Sort By: Release Number					
12.2(54)SG	CAT4500E-SUP6E	ENTERPRISE SERVICES SSH	cat4500e-entservicesk9-mz.122-54.SG.bin	512	128
12.2(54)SG	CAT4500E-SUP6E	ENTERPRISE SERVICES UPGRADE SSH	cat4500e-entservicesk9-mz.122-54.SG.bin	512	128
12.2(54)SG	CAT4500E-SUP6E	ENTERPRISE SERVICES UPGRADE W/O CRYPTO	cat4500e-entservices-mz.122-54.SG.bin	512	128
12.2(54)SG	CAT4500E-SUP6E	ENTERPRISE SERVICES W/O CRYPTO	cat4500e-entservices-mz.122-54.SG.bin	512	128
12.2(54)SG	CAT4500E-SUP6E	IP BASE SSH	cat4500e-ipbasek9-mz.122-54.SG.bin	512	128
12.2(54)SG	CAT4500E-SUP6E	IP BASE UPGRADE SSH	cat4500e-ipbasek9-mz.122-54.SG.bin	512	128
12.2(54)SG	CAT4500E-SUP6E	IP BASE UPGRADE W/O CRYPTO	cat4500e-ipbase-mz.122-54.SG.bin	512	128
12.2(54)SG	CAT4500E-SUP6E	IP BASE W/O CRYPTO	cat4500e-ipbase-mz.122-54.SG.bin	512	128
12.2(54)SG	CAT4500E-SUP6E	LAN BASE SSH	cat4500e-lanbasek9-mz.122-54.SG.bin	512	128
12.2(54)SG	CAT4500E-SUP6E	LAN BASE W/O CRYPTO	cat4500e-lanbase-mz.122-54.SG.bin	512	128
12.2(54)SG	CAT4500E-SUP6L-E	ENTERPRISE SERVICES SSH	cat4500e-entservicesk9-mz.122-54.SG.bin	512	128
12.2(54)SG	CAT4500E-SUP6L-E	ENTERPRISE SERVICES UPGRADE SSH	cat4500e-entservicesk9-mz.122-54.SG.bin	512	128
12.2(54)SG	CAT4500E-SUP6L-E	ENTERPRISE SERVICES UPGRADE W/O CRYPTO	cat4500e-entservices-mz.122-54.SG.bin	512	128
12.2(54)SG	CAT4500E-SUP6L-E	ENTERPRISE SERVICES W/O CRYPTO	cat4500e-entservices-mz.122-54.SG.bin	512	128
12.2(54)SG	CAT4500E-SUP6L-E	IP BASE SSH	cat4500e-ipbasek9-mz.122-54.SG.bin	512	128
12.2(54)SG	CAT4500E-SUP6L-E	IP BASE UPGRADE SSH	cat4500e-ipbasek9-mz.122-54.SG.bin	512	128
12.2(54)SG	CAT4500E-SUP6L-E	IP BASE UPGRADE W/O CRYPTO	cat4500e-ipbase-mz.122-54.SG.bin	512	128
12.2(54)SG	CAT4500E-SUP6L-E	IP BASE W/O CRYPTO	cat4500e-ipbase-mz.122-54.SG.bin	512	128
12.2(54)SG	CAT4500E-SUP6L-E	LAN BASE SSH	cat4500e-lanbasek9-mz.122-54.SG.bin	512	128
12.2(54)SG	CAT4500E-SUP6L-E	LAN BASE W/O CRYPTO	cat4500e-lanbase-mz.122-54.SG.bin	512	128
12.2(54)SG	CAT4900M	ENTERPRISE SERVICES SSH	cat4500e-entservicesk9-mz.122-54.SG.bin	512	128
12.2(54)SG	CAT4900M	ENTERPRISE SERVICES UPGRADE SSH	cat4500e-entservicesk9-mz.122-54.SG.bin	512	128
12.2(54)SG	CAT4900M	ENTERPRISE SERVICES UPGRADE W/O CRYPTO	cat4500e-entservices-mz.122-54.SG.bin	512	128
12.2(54)SG	CAT4900M	ENTERPRISE SERVICES W/O CRYPTO	cat4500e-entservices-mz.122-54.SG.bin	512	128
12.2(54)SG	CAT4900M	IP BASE SSH	cat4500e-ipbasek9-mz.122-54.SG.bin	512	128
12.2(54)SG	CAT4900M	IP BASE UPGRADE SSH	cat4500e-ipbasek9-mz.122-54.SG.bin	512	128
12.2(54)SG	CAT4900M	IP BASE UPGRADE W/O CRYPTO	cat4500e-ipbase-mz.122-54.SG.bin	512	128
12.2(54)SG	CAT4900M	IP BASE W/O CRYPTO	cat4500e-ipbase-mz.122-54.SG.bin	512	128

© ERNW | Breslauer Str. 28 | GmbH D-69124 Heidelberg | www.ernw.de

RA Guard

ERNW providing security.

```
Router(config-if)#ipv6 nd ?
  raguard  RA_Guard Configuration Command
Router(config-if)#ipv6 nd raguard ?
  <cr>
Router(config-if)#switchport mode access
Router(config-if)#ipv6 nd raguard
Router(config-if)#exit
Router(config)#exit
```


```
Router# show version
Cisco IOS Software, s3223_rp Software (s3223_rp-IPBASEK9-M),
Version 12.2(33)SXI5, RELEASE SOFTWARE (fc2)
```


© ERNW | Breslauer Str. 28 | GmbH D-69124 Heidelberg | www.ernw.de

When thinking about security controls...

- **Two essential factors must be evaluated:**
  - *Security benefit*
    - "How much do we gain, security-wise?"
    - "What's the risk reduction of this control?"

  - Operational feasibility
    - "What's the **operational** effort to do it?"
    - Pls note: *opex*, not *capex*, counts!

- **For some more discussion on these see also:**
  - http://www.insinuator.net/2011/05/evaluating-operational-feasibility/
  - http://www.insinuator.net/2010/12/security-benefit-operational-impact-or-the-illusion-of-infinite-resources/

© ERNW | Breslauer Str. 28 | GmbH D-69124 Heidelberg | www.ernw.de

Evaluating *operational effort*

ERNW providing security.

- **For each potential control the following points should be taken into account**
  - How many lines of code/configuration does it need?
    - Can it be implemented by means of templates or scripts? Effort needed for this?
  - To what degree does the implementation differ in different scenarios?
    - Per system/subnet/site?
    - Can “the difference” be scripted?
      - Taken from another source (e.g. central database)
      - “Calculated” (e.g. neighboring routers on local link)

  - How much additional configuration is needed for previous functionality?
    - E.g. to pass legitimate traffic in case of (“new”) application of ACLs?
  - “Business impact” incl. number of associated support/helpdesk calls.
  - Cost for deployment of additional hardware/licenses.
    - Cost for their initial procurement is *capex*.

© ERNW | Breslauer Str. 28 | GmbH D-69124 Heidelberg | www.ernw.de

Applying this approach to RFC 6104
[devices capable of RA guard assumed]

ERNW
providing security.

Control	Sec Benefit	Operational Feasibility
Manual configuration	4	1
RA Snooping (RA Guard)	5	4
Using ACLs	5	3
SEcure Neighbor Discovery (SEND)	5	1
Router Preference	3	4
Relying on Layer 2 Admission Control	5	2
Host-Based Packet Filters	3	1
Using an “Intelligent” Deprecation Tool	2	1
Using Layer 2 Partitioning	4	3

© ERNW | Breslauer Str. 28 | GmbH D-69124 Heidelberg | www.ernw.de

Summary / Main recommendations

ERNW
providing security.

- **Use RA Guard wherever possible!**
  - Start including it in your network equipment RFIs/RFPs _tomorrow_...

- **Deactivate tunnel technologies on all corporate desktops**
  - By netsh approach.
  - Most probably you don't need them in corporate space anyway.

© ERNW | Breslauer Str. 28 | GmbH D-69124 Heidelberg | www.ernw.de

There’s never enough time…

ERNW
providing security.

THANK YOU…

...for yours!

© ERNW | Breslauer Str. 28 | GmbH D-69124 Heidelberg | www.ernw.de

Appendix: Tools

ERNW providing security.

- **scapy6 [http://namabiiru.hongo.wide.ad.jp/scapy6/]**
- **ip6sic [http://ip6sic.sourceforge.net/]**
- **THC IPv6 [http://freeworld.thc.org/thc-ipv6/]**
- **ERNW fuzzing toolkit**
  - http://www.insinuator.net/2011/05/update-for-your-fuzzing-toolkit/
- **LOKI**
  - http://www.insinuator.net/2010/08/try-loki/

- ***nmap* can't v6-scan subnets, but individual hosts**

© ERNW | Breslauer Str. 28 | GmbH D-69124 Heidelberg | www.ernw.de