IPv6 Startup

KENIC-AFRINIC IPv6 Workshop
17th – 20th June 2008

César Olvera (cesar.olvera@consulintel.es)
Jordi Palet (jordi.palet@consulintel.es)
Alvaro Vives (alvaro.vives@consulintel.es)

Agenda

1. IPv6 setup in several Platforms (Windows 2K/XP/2003/Vista, Linux, BSD)
2. Basic Configuration, Stateless/Stateful Autoconfiguration, Privacy, Static Routes
3. Transition Mechanisms Configuration
4. Examples of Applications
5. IPv6 DNS
6. Firewall IPv6
7. Enable IPv6 on Cisco Routers and IPv6 ACLs

Part 5

IPv6 DNS

IPv6 DNS (1)

- Exercise: BIND (www.isc.org) in Linux

1. Installation BIND 9.x (Download apt or red-had package)
2. Configuration
3. Tests

IPv6 DNS (2)

- BIND Configuration:

  /etc/named.conf: is the main configuration file. There are the following options:

```
options {
directory "/var/named/";
listen-on-v6 { any; };
};
```

  Which inform about the directory containing the rest of configuration files and also enables IPv6 support

IPv6 DNS (3)

- BIND Configuration:

  /etc/named.conf: includes the declaration of forward and reverse zones that the server will manage, not only as master but also as slave:

```
zone  "." {
   type hint;
   file  "named.ca";
};
zone  "localhost" {
   type master;
   file  "localhost.zone";
};
zone  "learn.example.com" {
   type master;
   file  "learn.example.zone";
};
```

IPv6 DNS (4)

- **/etc/named.conf:**

```
zone
   "0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.
   0.0.0.0.0.0.0.ip6.int" {
   type master;
   file  "::.zone";
};
zone "a.2.0.4.0.0.8.b.d.0.1.0.0.2.ip6.arpa" {
type master;
file “2001:db8:0040:2a.zone";
};
```

IPv6 DNS (5)

- **/var/named/learn.example.com:**

```
$TTL 86400
@ IN SOA ns1.example.com. dnsadmin.example.com (
    2002071901 ; serial
    28800 ; refresh
    7200 ; retry
    604800 ; expire
    86400 ; ttk
    )
   IN NS ns1.example.com.

www.learn.example.com. IN  AAAA  2001:db8:40:2a03::11
ftp.learn.example.com. IN  AAAA  2001:db8:40:2a03::11

db.learn.example.com. IN  AAAA  2001:db8:40:2a03::12
```

IPv6 DNS (6)

- **/var/named/2001:0db8:0006:2a.zone:**

```
$TTL 86400
@ IN SOA ns1.example.com. dnsadmin.example.com (
     2002071901 ; serial
     28800 ; refresh
     7200 ; retry
     604800 ; expire
     86400 ; ttk
     )

   IN NS ns1.example.com.

1.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.3.0 IN PTR
    www.learn.example.com.
```

IPv6 DNS (7)

- Tests:
- **#>dig aaaa www.learn.example.com**

```
;; QUESTION SECTION:
;www.learn.example.com.      IN      AAAA

;; ANSWER SECTION:
www.learn.example.com.  86400 IN  AAAA 2001:db8:1000:1::103
```

- **#>dig ptr -n 1.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.3.0 .a.2.0.4.0.0.f.f.f.f.e.f.f.3.ip6.arpa**

```
;; QUESTION SECTION:
; 1.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.3.0.a.2.0.4.0.0.f.f.f.f.e.f.f.3.ip6.arpa.
   IN PTR

;; ANSWER SECTION:
1.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.3.0.a.2.0.4.0.0.f.f.f.f.e.f.f.3.ip6.arpa.
   86400 IN PTR www.learn.example.com.

;; AUTHORITY SECTION:
a.2.0.4.0.0.f.f.f.f.e.f.f.3.ip6.arpa. 172800 IN NS ns1.example.com.
```

DNS IPv6: Windows 2003 dnscmd (1)

```
Usage: DnsCmd <ServerName> <Command> [<Command Parameters>]

<ServerName>:
  IP address or host name    -- remote or local DNS server
  .                          -- DNS server on local machine
<Command>:
  /Info                      -- Get server information
  /Config                    -- Reset server or zone configuration
  /EnumZones                 -- Enumerate zones
  /Statistics                -- Query/clear server statistics data
  /ClearCache                -- Clear DNS server cache
  /WriteBackFiles            -- Write back all zone or root-hint datafile(s)
  /StartScavenging           -- Initiates server scavenging
  /ResetListenAddresses      -- Set server IP address(es) to serve DNS requests
  /ResetForwarders           -- Set DNS servers to forward recursive queries to
  /ZoneInfo                  -- View zone information
  /ZoneAdd                   -- Create a new zone on the DNS server
  /ZoneDelete                -- Delete a zone from DNS server or DS
  /ZonePause                 -- Pause a zone
  /ZoneResume                -- Resume a zone
  /ZoneReload                -- Reload zone from its database (file or DS)
  /ZoneWriteBack             -- Write back zone to file
  /ZoneRefresh               -- Force refresh of secondary zone from master
  /ZoneUpdateFromDs          -- Update a DS integrated zone by data from DS
  /ZonePrint                 -- Display all records in the zone
  /ZoneResetType             -- Change zone type
  /ZoneResetSecondaries      -- Reset secondary\notify information for a zone
  /ZoneResetScavengeServers  -- Reset scavenging servers for a zone
  /ZoneResetMasters          -- Reset secondary zone's master servers
  /ZoneExport                -- Export a zone to file
  /ZoneChangeDirectoryPartition -- Move a zone to another directory partition
  /EnumRecords               -- Enumerate records at a name
  /RecordAdd                 -- Create a record in zone or RootHints
  /RecordDelete              -- Delete a record from zone, RootHints or cache
  /NodeDelete                -- Delete all records at a name
  /AgeAllRecords             -- Force aging on node(s) in zone
  /EnumDirectoryPartitions   -- Enumerate directory partitions
  /DirectoryPartitionInfo    -- Get info on a directory partition
  /CreateDirectoryPartition  -- Create a directory partition
  /DeleteDirectoryPartition  -- Delete a directory partition
  /EnlistDirectoryPartition  -- Add DNS server to partition replication scope
  /UnenlistDirectoryPartition -- Remove DNS server from replication scope
  /CreateBuiltinDirectoryPartitions -- Create built-in partitions

<Command Parameters>:
  DnsCmd <CommandName> /? -- For help info on specific Command
```

DNS IPv6: Windows 2003 dnscmd (2)

```
C:\>dnscmd  ::1 /Info
Query result:
Server info
        server name            =
    dns1.novagnet.com
        version                = 0ECE0205 (5.2
    build 3790)
        DS container           = N/A
        forest name            = N/A
        domain name            = N/A
        builtin domain partition = N/A
        builtin forest partition = N/A
        last scavenge cycle    = not since
    restart (0)
  Configuration:
        dwLogLevel             = 00000000
        dwDebugLevel           = 00000000
        dwRpcProtocol          = FFFFFFFF
        dwNameCheckFlag        = 00000002
        cAddressAnswerLimit    = 0
        dwRecursionRetry       = 3
        dwRecursionTimeout     = 15
        dwDsPollingInterval    = 180
Configuration Flags:
        fBootMethod            = 1
        fAdminConfigured       = 1
        fAllowUpdate           = 1
        fDsAvailable           = 0
        fAutoReverseZones      = 1
        fAutoCacheUpdate       = 0
        fSlave                 = 0
        fNoRecursion           = 0
        fRoundRobin            = 1
        fStrictFileParsing     = 0
        fLooseWildcarding      = 0
        fBindSecondaries       = 1
        fWriteAuthorityNs      = 0
        fLocalNetPriority      = 1
  ServerAddresses:
 Addr Count = 1
            Addr[0] => 213.172.48.139
  ListenAddresses:
        NULL IP Array.
  Forwarders:
        NULL IP Array.
        forward timeout  = 5
        slave            = 0
Command completed successfully.
```

DNS IPv6: Windows 2003 dnscmd (3)

- Enabling IPv6 in the DNS server
  - dnscmd /config /EnableIPv6 1
  - Dnscmd.exe is part of Windows Server 2003 Support Tools. These tools can be found at the Support\Tools folder of the Windows Server 2003 CD and they are installed by running suptools.msi in sucha a folder
  - Restart the DNS server
- Adding a zone
  - dnscmd serverName /ZoneAdd zoneName zoneType [options]
- Deleting a zone
  - dnsdmd serverName /ZoneDelete zoneName [/DsDel] [/f]
- Adding a record
  - dnscmd serverName /RecordAdd zoneName nodeName [/Aging] [/OpenAcl] [Ttl] typeRR dataRR
- Deleting a record
  - dnscmd serverName /RecordDelete zonceName nodeName typeRR dataRR [/f]

DNS IPv6: Exercise 1 (1)

- **Windows**

  C:\>nslookup

  >set type=a

  >www.ipv6tf.org

  Name: www.ipv6tf.org

  Address: 213.172.48.141

  >set type=aaaa

  >www.ipv6tf.org

  www.ipv6tf.org AAAA IPv6 address = 2a01:48:1:0:2e0:81ff:fe05:4658

DNS IPv6: Exercise 1 (2)

- **Linux:**

  # dig a www.ipv6tf.org

  ;; QUESTION SECTION:

  ;www.ipv6tf.org. IN A

  ;; ANSWER SECTION:

  www.ipv6tf.org. 172800 IN A 213.172.48.141

- **# dig aaaa www.ipv6tf.org**

  ;; QUESTION SECTION:

  ;www.ipv6tf.org. IN AAAA

  ;; ANSWER SECTION:

  www.ipv6tf.org. 172800 IN AAAA
  2a01:48:1:0:2e0:81ff:fe05:4658

DNS IPv6: Exercise 1 (3)

- **Linux:**

  #dig aaaa www.kame.net @
  2a01:48:1:0:2e0:81ff:fe05:4658

  ;; QUESTION SECTION:

  ;www.kame.net. IN AAAA

  ;; ANSWER SECTION:

  www.kame.net. 86400 IN AAAA
  2001:200:0:8002:203:47ff:fea5:3085

  ;; Query time: 400 msec

  ;; SERVER: 2a01:48:1:0:2e0:81ff:fe05:4658#53
  (2a01:48:1:0:2e0:81ff:fe05:4658)

  ;; WHEN: Fri Jun 24 13:49:41 2005

  ;; MSG SIZE rcvd: 107

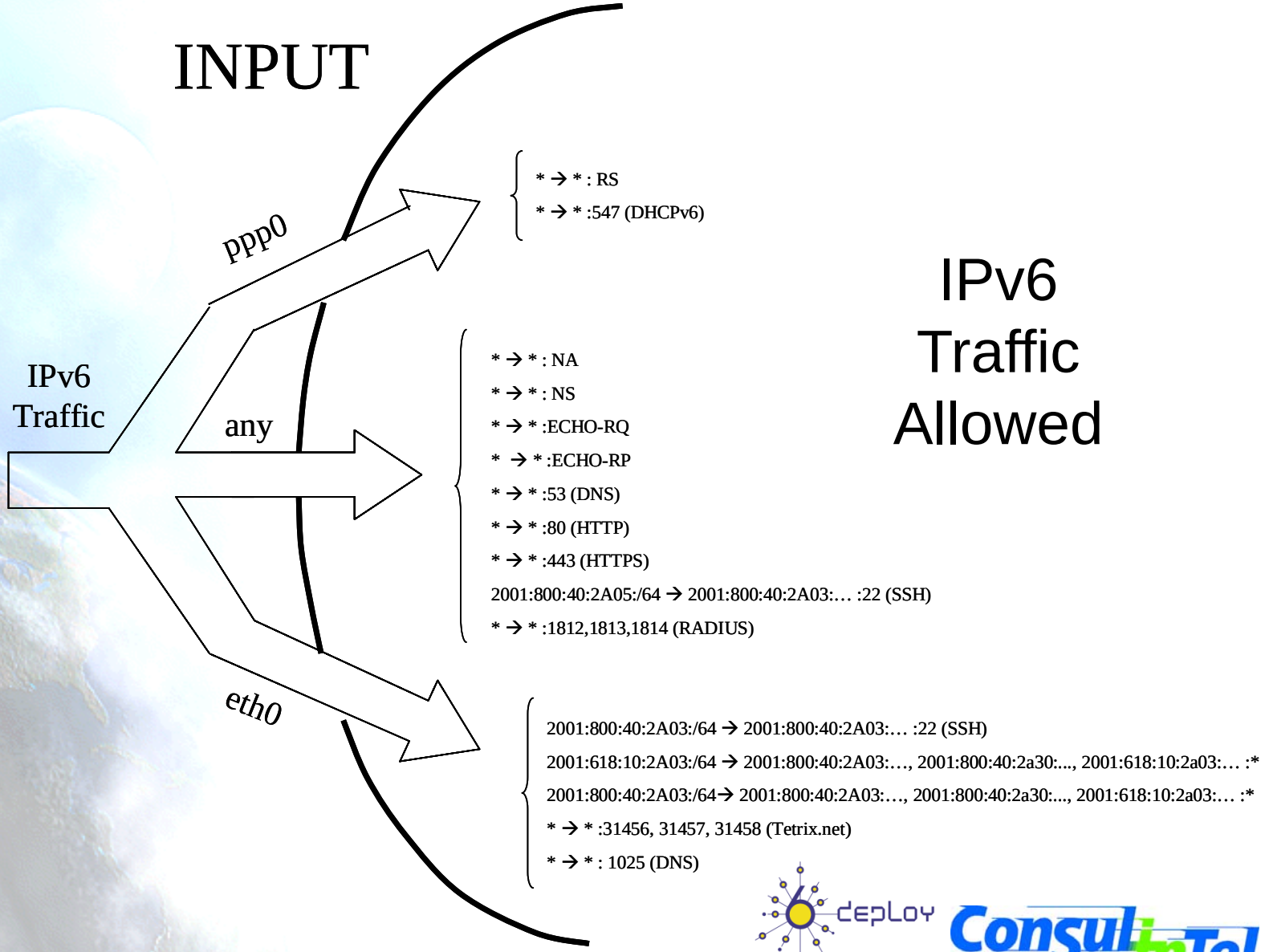
Part 7

Firewall IPv6

Firewall IPv6

- Windows XP/2003
  - Common security GUI for IPv4 and IPv6
  - Specific configurations with “netsh firewall”
    - add - add the security server configuration.
    - delete - delete the security server configuration.
    - dump - show the configuration command sequence.
    - help - show the command list.
    - reset - reset the security server configuration.
    - set - set the security server configuration.
    - show - show the security server configuration.
- Unix systems
  - ip6tables. Tool that configures and shows the kernel built-in filter tables.
  - Functionality similar to the IPv4 iptables

Firewall Example IPv6 Linux (1)



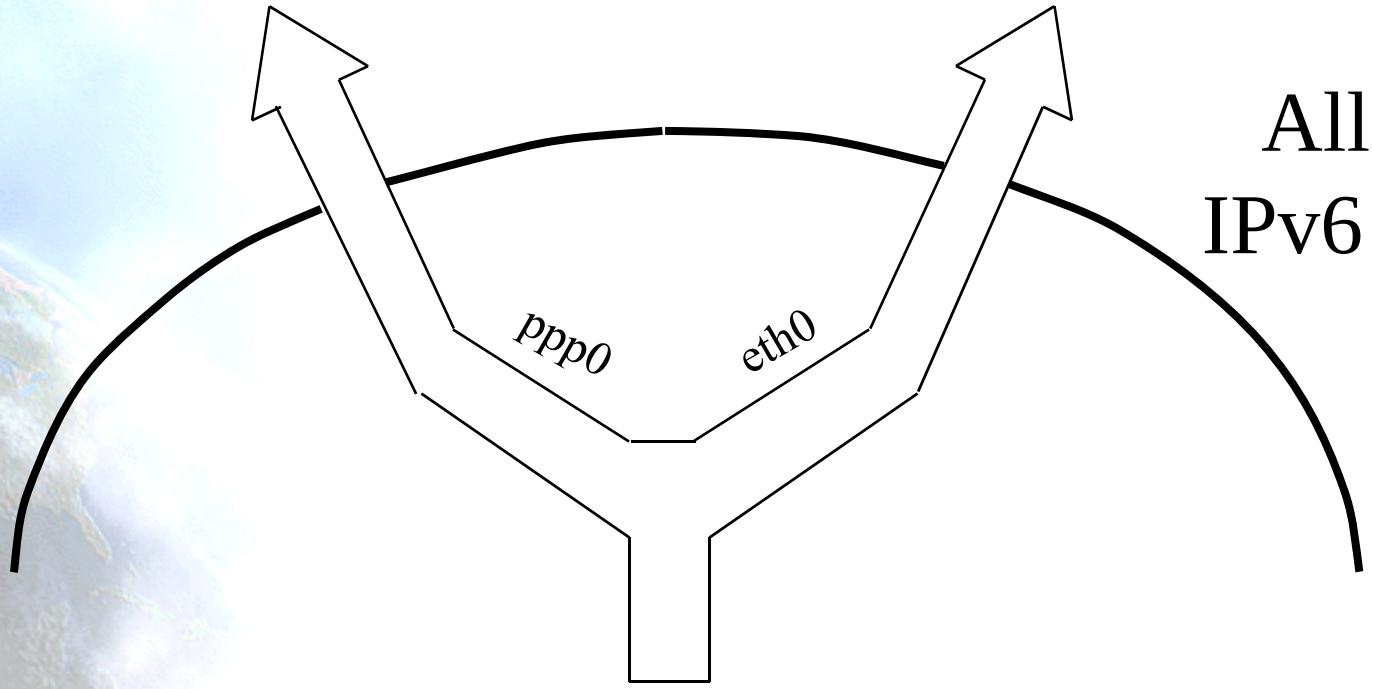
IPv6
Traffic
Allowed

Firewall Example IPv6 Linux (2)

* → * : RA
* → * : NA
* → * : NS
* → * : 546 (DHCPv6)
2001:618:10:2A03:…
2001:800:40:2A03:…
2001:618:10:2A03:…
→ 2001:800:40:2A30:/64 :*

2001:618:10:2A03:…
2001:800:40:2A03:…
2001:618:10:2A03:…
→ 2001:800:40:2A03:/64, 2001:618:10:2A03:/64 :*

2001:800:40:2A03:…, 2001:618:10:2A03:… → * :*



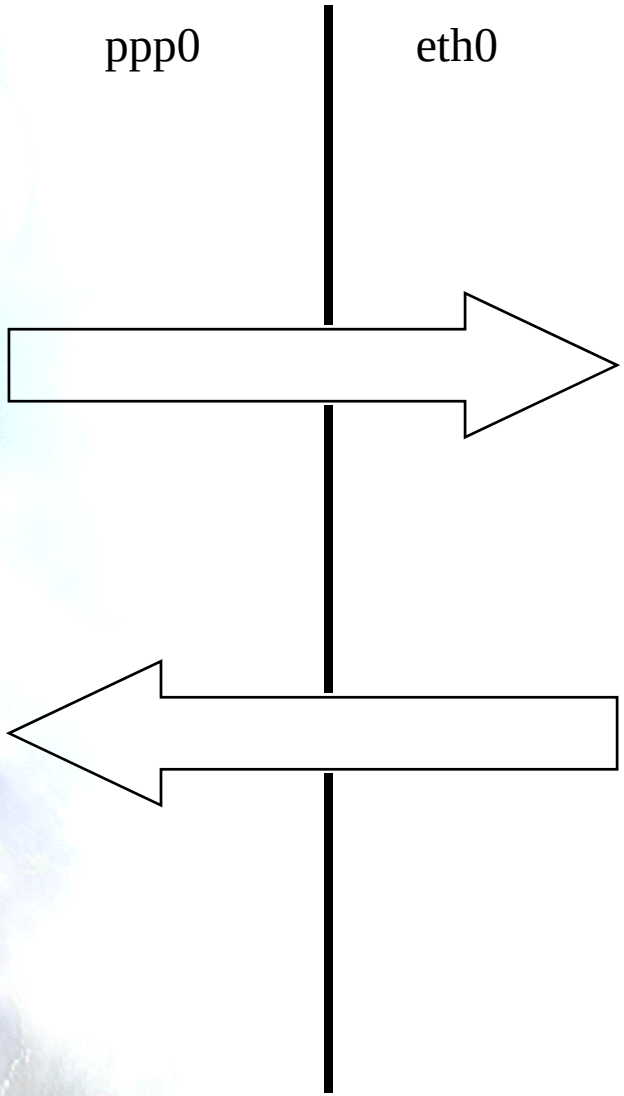
Allowed
IPv6 Traffic

OUTPUT

IPv6
Traffic

Firewall Example IPv6 Linux (3)

FORWARDING



2001:800:40:2A30:/64 → * :ECHO-RQ
2001:800:40:2A30:/64 → * :ECHO-RP
2001:800:40:2A30:/64 → * :21, 22, 23, 25 (FTP, SSH, TELNET, SMTP)
2001:800:40:2A30:/64 → * :53,80, 109, 110 (DNS, HTTP, POP-2, POP-3)
2001:800:40:2A30:/64 → * :443 (HTTPS)
2001:800:40:2A30:/64 → * :1812,1813,1814 (RADIUS)

IPv6 Traffic Allowed

Firewall Example IPv6 Linux (4)

```
#!/bin/sh
#
# rc.firewall-2.4-stronger for zafiro
#
FWVER=0.77s

echo -e "\nLoading rc.firewall - version $FWVER..\n"

IP6TABLES=/sbin/ip6tables
LSMOD=/sbin/lsmod
DEPMOD=/sbin/depmod
INSMOD=/sbin/insmod
GREP=/bin/grep
AWK=/bin/awk
SED=/bin/sed
IFCONFIG=/sbin/ifconfig

#Setting the EXTERNAL and INTERNAL interfaces for the network
EXTIF="ppp0"
INTIF="eth0"
#echo "  External Interface:  $EXTIF"
echo "  Internal Interface:  $INTIF"
echo "  ---"
```

Firewall Example IPv6 Linux (5)

```
# Specify your IP address here or let the script take care of it for you.
#
INTIPV6_1="2001:800:40:2a03:204:acff:fe77:b83d"
INTIPV6_2="2001:618:10:2a03:204:acff:fe77:b83d"
INTNETV6_1="2001:800:40:2a03::/64"
INTNETV6_2="2001:618:10:2a03::/64"
echo "  Internal IPv6 1: $INTIPV6_1"
echo "  Internal IPv6 2: $INTIPV6_2"
echo "  Internal IPv6 Network 1: $INTNETV6_1"
echo "  Internal IPv6 Network 2: $INTNETV6_2"
echo "  ---"

# Assign the external TCP/IP network and IP address
EXTNETV6="2001:800:40:2a30::/64"
EXTIPV6="2001:800:40:2a30::201"
echo "  External Network: $EXTNETV6"
echo "  External IPv6:      $EXTIPV6"
echo "  ---"


# Setting a few other local variables
#
UNIVERSE="::/0"
```

Firewall Example IPv6 Linux (6)

```
# Need to verify that all modules have all required dependencies
echo "  Verifying that all kernel modules are ok"
$DEPMOD -a

echo -en "  Loading kernel modules: "
echo -en "ip6_tables, "
#
#Verify the module isn't loaded.  If it is, skip it
#
if [ -z "` $LSMOD | $GREP ip6_tables | $AWK {'print $1'} `" ]; then
   $INSMOD ip6_tables
fi

echo "  ---"

#########################################################################################
#
#Clearing any previous configuration
#  Unless specified, the defaults for INPUT, OUTPUT, and FORWARD to DROP
#
echo "  Clearing any existing rules and setting default policy to DROP.."
$IP6TABLES -P INPUT DROP
$IP6TABLES -F INPUT
$IP6TABLES -P OUTPUT DROP
$IP6TABLES -F OUTPUT
```

Firewall Example IPv6 Linux (7)

```
$IP6TABLES -P FORWARD DROP
$IP6TABLES -F FORWARD
#
#Flush the user chain.. if it exists
if [ -n "`$IP6TABLES -L | $GREP drop-and-log-it`" ]; then
  $IP6TABLES -F drop-and-log-it
fi
#
# Delete all User-specified chains
$IP6TABLES -X
#
# Reset all IP6TABLES counters
$IP6TABLES -Z


#Configuring specific CHAINS for later use in the ruleset
#
echo "  Creating a DROP chain: 'drop-and-log-it'.."
echo "  ---"
$IP6TABLES -N drop-and-log-it
$IP6TABLES -A drop-and-log-it -j LOG --log-level info
$IP6TABLES -A drop-and-log-it -j DROP

echo -e "  Loading INPUT rulesets"
```

Firewall Example IPv6 Linux (8)

```
#############################################################################
# INPUT: Incoming traffic from various interfaces.  All rulesets are
#        already flushed and set to a default policy of DROP.
#

# loopback interfaces are valid.
#
$IP6TABLES -A INPUT -i lo -s $UNIVERSE -d $UNIVERSE -j ACCEPT

# ********** Internal specific interface rules *****************

# all trafic from local network is valid
#
$IP6TABLES -A INPUT -i $INTIF -s $INTNETV6_1 -d $INTIPV6_1 -j ACCEPT
$IP6TABLES -A INPUT -i $INTIF -s $INTNETV6_1 -d $INTIPV6_2 -j ACCEPT
$IP6TABLES -A INPUT -i $INTIF -s $INTNETV6_1 -d $EXTIPV6 -j ACCEPT
$IP6TABLES -A INPUT -i $INTIF -s $INTNETV6_2 -d $INTIPV6_1 -j ACCEPT
$IP6TABLES -A INPUT -i $INTIF -s $INTNETV6_2 -d $INTIPV6_2 -j ACCEPT
$IP6TABLES -A INPUT -i $INTIF -s $INTNETV6_2 -d $EXTIPV6 -j ACCEPT

# SSH connections from internal interface are permitted
#
$IP6TABLES -A INPUT -i $INTIF -p tcp -s $INTNETV6_1 -d $INTIPV6_1 --destination-port 22 -j ACCEPT
$IP6TABLES -A INPUT -i $INTIF -p tcp -s 2001:800:40:2a05::/64 -d $INTIPV6_1 --destination-port 22 -j ACCEPT
```

Firewall Example IPv6 Linux (9)

```
# OPEN PORTS on 'esmeralda' before start ppp link
#
$IP6TABLES -A INPUT -i $INTIF -p tcp --destination-port 31456 -j ACCEPT
$IP6TABLES -A INPUT -i $INTIF -p tcp --destination-port 31457 -j ACCEPT
$IP6TABLES -A INPUT -i $INTIF -p tcp --destination-port 31458 -j ACCEPT
$IP6TABLES -A INPUT -i $INTIF -p udp --destination-port 1025 -j ACCEPT


# ********** External specific interface rules *****************

# remote interface, claiming to be local machines, IP spoofing, get lost
#
$IP6TABLES -A INPUT -i $EXTIF -s $INTNETV6_1 -d $UNIVERSE -j drop-and-log-it
$IP6TABLES -A INPUT -i $EXTIF -s $INTNETV6_2 -d $UNIVERSE -j drop-and-log-it

# external interface, for stateless autoconfiguration traffic
#
$IP6TABLES -A INPUT -i $EXTIF -p ipv6-icmp --icmpv6-type router-solicitation -j ACCEPT

# enable internal dhcp6 server for external interface
#
$IP6TABLES -A INPUT -i $EXTIF -p tcp --destination-port 547 -j ACCEPT
$IP6TABLES -A INPUT -i $EXTIF -p udp --destination-port 547 -j ACCEPT
```

Firewall Example IPv6 Linux (10)

```
# ********** General rules for any interface ******************

# ping traffic is valid
#
$IP6TABLES -A INPUT -p ipv6-icmp --icmpv6-type echo-request -s $UNIVERSE -d $EXTIPV6 -j ACCEPT
$IP6TABLES -A INPUT -p ipv6-icmp --icmpv6-type echo-request -s $UNIVERSE -d $INTIPV6_1 -j ACCEPT
$IP6TABLES -A INPUT -p ipv6-icmp --icmpv6-type echo-request -s $UNIVERSE -d $INTIPV6_2 -j ACCEPT
$IP6TABLES -A INPUT -p ipv6-icmp --icmpv6-type echo-reply -s $UNIVERSE -d $EXTIPV6 -j ACCEPT
$IP6TABLES -A INPUT -p ipv6-icmp --icmpv6-type echo-reply -s $UNIVERSE -d $INTIPV6_1  -j ACCEPT
$IP6TABLES -A INPUT -p ipv6-icmp --icmpv6-type echo-reply -s $UNIVERSE -d $INTIPV6_2 -j ACCEPT

# external interface, for stateless autoconfiguration traffic
#
$IP6TABLES -A INPUT -p ipv6-icmp --icmpv6-type neighbour-solicitation  -j ACCEPT
$IP6TABLES -A INPUT -p ipv6-icmp --icmpv6-type neighbour-advertisement -j ACCEPT

# HTTPd - Enable the following lines if you run an EXTERNAL WWW server
#
$IP6TABLES -A INPUT -p tcp -s $UNIVERSE --destination-port 80 -j ACCEPT
$IP6TABLES -A INPUT -p tcp -s $UNIVERSE --destination-port 443 -j ACCEPT

# DNS request are attendant for any interface
#
$IP6TABLES -A INPUT -p tcp --destination-port 53 -j ACCEPT
$IP6TABLES -A INPUT -p udp --destination-port 53 -j ACCEPT
```

Firewall Example IPv6 Linux (11)

```
# RADIUS traffic is valid
#
$IP6TABLES -A INPUT -p tcp --destination-port 1812 -j ACCEPT
$IP6TABLES -A INPUT -p udp --destination-port 1812 -j ACCEPT
$IP6TABLES -A INPUT -p tcp --destination-port 1813 -j ACCEPT
$IP6TABLES -A INPUT -p udp --destination-port 1813 -j ACCEPT
$IP6TABLES -A INPUT -p tcp --destination-port 1814 -j ACCEPT
$IP6TABLES -A INPUT -p udp --destination-port 1814 -j ACCEPT

# Catch all rule, all other incoming is denied and logged.
#
$IP6TABLES -A INPUT -s $UNIVERSE -d $UNIVERSE -j drop-and-log-it

echo -e "  Loading OUTPUT rulesets"


################################################################################
# OUTPUT: Outgoing traffic from various interfaces.  All rulesets are
#         already flushed and set to a default policy of DROP.
#


# loopback interface is valid.
#
$IP6TABLES -A OUTPUT -o lo -s $UNIVERSE -d $UNIVERSE -j ACCEPT
```

Firewall Example IPv6 Linux (12)

```
# ********** Internal specific interface rules ******************

# local interfaces, any source going to local net is valid
#
$IP6TABLES -A OUTPUT -o $INTIF -s $EXTIPV6 -d $INTNETV6_1 -j ACCEPT
$IP6TABLES -A OUTPUT -o $INTIF -s $EXTIPV6 -d $INTNETV6_2 -j ACCEPT

# local interface, any source going to local net is valid
#
$IP6TABLES -A OUTPUT -o $INTIF -s $INTIPV6_1 -d $INTNETV6_1 -j ACCEPT
$IP6TABLES -A OUTPUT -o $INTIF -s $INTIPV6_1 -d $INTNETV6_2 -j ACCEPT
$IP6TABLES -A OUTPUT -o $INTIF -s $INTIPV6_2 -d $INTNETV6_1 -j ACCEPT
$IP6TABLES -A OUTPUT -o $INTIF -s $INTIPV6_2 -d $INTNETV6_2 -j ACCEPT

# anything else outgoing on internal interface is valid
#
$IP6TABLES -A OUTPUT -o $INTIF -s $INTIPV6_1 -d $UNIVERSE -j ACCEPT
$IP6TABLES -A OUTPUT -o $INTIF -s $INTIPV6_2 -d $UNIVERSE -j ACCEPT



# ********** External specific interface rules ******************

# outgoing to local net on remote interface, stuffed routing, deny
#
$IP6TABLES -A OUTPUT -o $EXTIF -s $UNIVERSE -d $INTNETV6_1 -j drop-and-log-it
$IP6TABLES -A OUTPUT -o $EXTIF -s $UNIVERSE -d $INTNETV6_2 -j drop-and-log-it
```

Firewall Example IPv6 Linux (13)

```
# enable stateless autoconfiguration
$IP6TABLES -A OUTPUT -o $EXTIF -p ipv6-icmp --icmpv6-type router-advertisement -j ACCEPT

# anything else outgoing on remote interface is valid
#
$IP6TABLES -A OUTPUT -o $EXTIF -s $EXTIPV6 -d $EXTNETV6 -j ACCEPT
$IP6TABLES -A OUTPUT -o $EXTIF -s $INTIPV6_1 -d $EXTNETV6 -j ACCEPT
$IP6TABLES -A OUTPUT -o $EXTIF -s $INTIPV6_2 -d $EXTNETV6 -j ACCEPT

# enable stateful autoconfigurtion for the remote host (DHCPv6)
#
$IP6TABLES -A OUTPUT -o $EXTIF -p tcp --destination-port 546 -j ACCEPT
$IP6TABLES -A OUTPUT -o $EXTIF -p udp --destination-port 546 -j ACCEPT


# ********** General rules for any interface ******************

# enable stateless autoconfiguration
#
$IP6TABLES -A OUTPUT -p ipv6-icmp --icmpv6-type neighbour-advertisement -j ACCEPT
$IP6TABLES -A OUTPUT -p ipv6-icmp --icmpv6-type neighbour-solicitation -j ACCEPT


# Catch all rule, all other outgoing is denied and logged.
#
$IP6TABLES -A OUTPUT -s $UNIVERSE -d $UNIVERSE -j drop-and-log-it
```

Firewall Example IPv6 Linux (14)

```
echo -e "  Loading FORWARD rulesets"

################################################################################
# FORWARD: Enable Forwarding and thus IPMASQ
#

# ********** Forwarding from ppp0 to eth0  *****************

# HTTP traffic is valid
#
$IP6TABLES -A FORWARD -i $EXTIF -o $INTIF -s $EXTNETV6 -p tcp --destination-port 80 -j ACCEPT
$IP6TABLES -A FORWARD -i $EXTIF -o $INTIF -s $EXTNETV6 -p tcp --destination-port 443 -j ACCEPT

# FTP traffic is valid
#
$IP6TABLES -A FORWARD -i $EXTIF -o $INTIF -s $EXTNETV6 -p tcp --destination-port 21 -j ACCEPT
$IP6TABLES -A FORWARD -i $EXTIF -o $INTIF -s $EXTNETV6 -p udp --destination-port 21 -j ACCEPT

# DNS request are vaild
#
$IP6TABLES -A FORWARD -i $EXTIF -o $INTIF -s $EXTNETV6 -p tcp --destination-port 53 -j ACCEPT
$IP6TABLES -A FORWARD -i $EXTIF -o $INTIF -s $EXTNETV6 -p udp --destination-port 53 -j ACCEPT

# TELNET traffic is valid
#
```

Firewall Example IPv6 Linux (15)

```
$IP6TABLES -A FORWARD -i $EXTIF -o $INTIF -s $EXTNETV6 -p tcp --destination-port 23 -j ACCEPT
$IP6TABLES -A FORWARD -i $EXTIF -o $INTIF -s $EXTNETV6 -p udp --destination-port 23 -j ACCEPT

# SSH traffic is valid
#
$IP6TABLES -A FORWARD -i $EXTIF -o $INTIF -s $EXTNETV6 -p tcp --destination-port 22 -j ACCEPT
$IP6TABLES -A FORWARD -i $EXTIF -o $INTIF -s $EXTNETV6 -p udp --destination-port 22 -j ACCEPT

# POP-2 traffic is valid
#
$IP6TABLES -A FORWARD -i $EXTIF -o $INTIF -s $EXTNETV6 -p tcp --destination-port 109 -j ACCEPT
$IP6TABLES -A FORWARD -i $EXTIF -o $INTIF -s $EXTNETV6 -p udp --destination-port 109 -j ACCEPT

# POP-3 traffic is valid
#
$IP6TABLES -A FORWARD -i $EXTIF -o $INTIF -s $EXTNETV6 -p tcp --destination-port 110 -j ACCEPT
$IP6TABLES -A FORWARD -i $EXTIF -o $INTIF -s $EXTNETV6 -p udp --destination-port 110 -j ACCEPT

# SMTP traffic is valid
#
$IP6TABLES -A FORWARD -i $EXTIF -o $INTIF -s $EXTNETV6 -p tcp --destination-port 25 -j ACCEPT
$IP6TABLES -A FORWARD -i $EXTIF -o $INTIF -s $EXTNETV6 -p udp --destination-port 25 -j ACCEPT

# RADIUS traffic is valid
#
```

Firewall Example IPv6 Linux (16)

```
$IP6TABLES -A FORWARD -i $EXTIF -o $INTIF -s $EXTNETV6 -p tcp --destination-port 1812 -j ACCEPT
$IP6TABLES -A FORWARD -i $EXTIF -o $INTIF -s $EXTNETV6 -p udp --destination-port 1812 -j ACCEPT

# RADIUS ACCOUNTING traffic is valid
#
$IP6TABLES -A FORWARD -i $EXTIF -o $INTIF -s $EXTNETV6 -p tcp --destination-port 1813 -j ACCEPT
$IP6TABLES -A FORWARD -i $EXTIF -o $INTIF -s $EXTNETV6 -p udp --destination-port 1813 -j ACCEPT

# RADIUS
#
$IP6TABLES -A FORWARD -i $EXTIF -o $INTIF -s $EXTNETV6 -p tcp --destination-port 1814 -j ACCEPT
$IP6TABLES -A FORWARD -i $EXTIF -o $INTIF -s $EXTNETV6 -p udp --destination-port 1814 -j ACCEPT



# ********** Forwarding from eth0 to ppp0 *****************

# FORWARDING traffic from anywhere to internal net is valid
#
$IP6TABLES -A FORWARD -i $INTIF -o $EXTIF -d $EXTNETV6 -j ACCEPT
```

Firewall Example IPv6 Linux (17)

```
# ********** Forwarding from any to any *****************

# Ping traffic is valid
#
$IP6TABLES -A FORWARD -p ipv6-icmp --icmpv6-type echo-request -j ACCEPT
$IP6TABLES -A FORWARD -p ipv6-icmp --icmpv6-type echo-reply -j ACCEPT


# Catch all rule, all other forwarding is denied and logged.
#
$IP6TABLES -A FORWARD -j drop-and-log-it


#############################################################################
echo -e "\nStronger rc.firewall-2.4 $FWVER done.\n"
```

Part 8

Enable IPv6 and IPv6 ACLs on Cisco Routers

Enable Telnet over IPv6 transport

- Router> enable
- Router# configure terminal
- Router(config)# ipv6 host name [port] ipv6-address1 [ipv6-address2...ipv6-address4]
  - Example: Router(config)# ipv6 host cisco-sj 2001:DB8:10:20::1
- Router(config)# line [aux | console | tty | vty] line-number [ending-line-number]
  - Example: Router(config)# line vty 0 4
- Router(config)# password password
  - Example: Router(config)# password hostword
- Router(config)# login [local | tacacs]
  - Example: Router(config)# login local
- Router(config)# ipv6 access-class acl-name (Optional: Add a host list which can access)
  - Example: Router(config)# ipv6 access-list hostlist

Enable SSH over IPv6 transport

- Router> enable
- Router# configure terminal
- Router(config)# ip ssh {[timeout seconds] | [authentication-retries integer]}
  - Example1: Router(config)# ip ssh
  - Example2: Router(config)# ip ssh timeout 100 authentication-retries 2

Enable IPv6 on interfaces (1)

- Router> enable
- Router# configure terminal
- Router(config)# interface type number
- Router(config-if)# ipv6 enable
  - Example: Router(config)# ipv6 enable
- Router(config-if)# ipv6 address
  - Example: Router(config)# ipv6 address 2001:DB8:10:20::1/64 (Configure one address and sends correspondend RA messages)
- Router(config-if)# ipv6 address autoconfig (Configure one address by autoconfiguration)

Enable IPv6 on interfaces (2)

- Is possible to configure different ND parameters
  - Router(config-if)#ipv6 nd ?

```
dad                  Duplicate Address Detection
managed-config-flag  Hosts should use DHCP for address config
ns-interval          Set advertised NS retransmission interval
other-config-flag    Hosts should use DHCP for non-address config
prefix               Configure IPv6 Routing Prefix Advertisement
ra-interval          Set IPv6 Router Advertisement Interval
ra-lifetime          Set IPv6 Router Advertisement Lifetime
reachable-time       Set advertised reachability time
suppress-ra          Suppress IPv6 Router Advertisements
```

- Is possible to configure more prefixes in the RA
  - Example: Router(config)# ipv6 nd prefix 2001:DB8:10:20::/64
- Is possible to stop the RA of certain prefix
  - Example: Router(config-if)#ipv6 nd prefix 2001:DB8:10:20::/64 no-advertise
- Is possible to suppress the RA
  - Example: Router(config)# ipv6 nd suppress-ra

Enable IPv6 on interfaces (3)

- Is possible to configure different RA parameters
  - Router(config-if)#ipv6 nd prefix 2001:DB8:10:20::/64 ?

    <0-4294967295> Valid Lifetime (secs)
    at Expire prefix at a specific time/date
    infinite Infinite Valid Lifetime
    no-advertise Do not advertise prefix
    no-autoconfig Do not use prefix for autoconfiguration
    off-link Do not use prefix for on link determination
    <cr>
- Router(config-if)#ipv6 nd ra-inteval
  - Configure the interval between RAs
- Router(config-if)#ipv6 nd ra-lifetime
  - Configure lifetime of the RA

Show IPv6 information

- Interfaces
  - Router#show ipv6 interface
- Routing table
  - Router#show ipv6 route
- Routing protocols
  - Router#show ipv6 protocols
  - Router#show ipv6 ospf

Configure 6in4 tunnel

- Router#configure terminal
  Router(config)#interface Tunnel 0
  Router(config-if)#ipv6 address <IPv6 address>/<prefix length>
  Router(config-if)#tunnel source <IPv4 address>
  Router(config-if)#tunnel source <Interface type> <Interface number>
  Router(config-if)#tunnel destination <remote IPv4 address >
  Router(config-if)#tunnel mode ipv6ip

Access Control List to filter IPv6 traffic

- General steps
  - Create an IPv6 Access Control List (ACL)
  - Configure the IPv6 ACL to permit or deny the IPv6 traffic
  - Apply the IPv6 ACL in the interface

Create and configure the IPv6 ACL (1)

Cisco IOS Release 12.2(11)T, 12.0(22)S, 12.0(21)ST

- Router> enable
- Router# configure terminal
- Router(config)# ipv6 access-list access-list-name {permit | deny} { source-ipv6-prefix/ prefix-length | any} { destination-ipv6-prefix/ prefix-length | any} [priority value]
  - Example: Router(config)# ipv6 access-list list2 deny 2001:DB8:0:0:2::/64 any

Create and configure the IPv6 ACL (2)

Cisco IOS Release 12.2(13)T, 12.0(23)S and later

- Router> enable
- Router# configure terminal
- Router(config)# ipv6 access-list access-list-name (Define the IPv6 ACL)
  - Example: Router(config)# ipv6 access-list outbound
- Router(config-ipv6-acl)# **permit** {protocol} {source-ipv6-prefix/ prefix-length | any | host source-ipv6-address} [operator [port-number]] {destination-ipv6-prefix/ prefix-length | any | host destination-ipv6-address} [operator [port-number]] [dscp value] [flow-label value] [fragments] [log] [log-input] [reflect name [timeout value]] [routing] [time-range name] [sequence value] or **deny** {protocol} {source-ipv6-prefix/ prefix-length | any | host source-ipv6-address} [operator [port-number]] {destination-ipv6-prefix/ prefix-length | any | host destination-ipv6-address} [operator [port-number]] [dscp value] [flow-label value] [fragments] [log] [log-input] [routing] [time-range name] [undetermined transport] [sequence value] (Define the behavior of the IPv6 ACL)
  - Example1: Router(config-ipv6-acl)# permit tcp 2001:DB8:300:200::/32 eq telnet any reflect reflectout
  - Example2: Router(config-ipv6-acl)# deny tcp host 1::1 any log-input

Apply the IPv6 ACL to the interface

Cisco IOS Release 12.2(11)T, 12.0(22)S, 12.0(21)ST
Cisco IOS Release 12.2(13)T, 12.0(23)S and later

- Router> enable
- Router# configure terminal
- Router(config)# interface type number
  - Example: Router(config)# interface ethernet 0
- Router(config-if)# ipv6 traffic-filter access-list-name {in | out}
  - Example: Router(config-if)# ipv6 traffic-filter outbound out

Example

- IPv6 network
- Create and apply four ACL IPv6:
  - Router(config)# ipv6 access-list inboundN
  - Router(config-ipv6-acl)#
    - deny IPv6 any {host1 destination-ipv6-address}
    - deny IPv6 any {host2 destination-ipv6-address}
    - deny udp any {host destination-ipv6-address} eq 80 log-input (HTTP)
    - deny tcp any {host destination-ipv6-address} eq 20 log-input (FTP)
  - Router(config)# interface ethernet X (Interface toward Router 1)
  - Router(config-if)# ipv6 traffic-filter inboundN in

References (1)

- [6in4] RFC1933
- [TunAut] RFC1933
- [6to4] RFC3056
- [6over4] RFC2529
- [TB] RFC3053
- [TSP] draft-vg-ngtrans-tsp-01, http://www.hexago.com/index.php?pgID=step1
- [TEREDO] RFC4380
- [TEREDOC] http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/teredo.mspx
- [ISATAP] draft-ietf-ngtrans-isatap-24
- [AYIYA] draft-massar-v6ops-ayiya-02
- [SILKROAD] draft-liumin-v6ops-silkroad-02
- [DSTM] draft-ietf-ngtrans-dstm-10
- [SIIT] RFC2765
- [NATPT] RFC2767
- [BIS] RFC2767
- [TRT] RFC3142
- [SOCKSv64] RFC3089

References (2)

- [PROTO41] draft-palet-v6ops-proto41-nat-04
- [STUN] RFC3489
- [NATPTIMPL]
  - http://www.ipv6.or.kr/english/download.htm ==> Linux 2.4.0
  - http://www.ispras.ru/~ipv6/index_en.html ==> Linux y FreeBSD
  - http://research.microsoft.com/msripv6/napt.htm Microsoft
  - ftp://ftp.kame.net/pub/kame/snap/kame-20020722-freebsd46-snap.tgz ==> KAME snapshot (22.7.2002)
  - http://ultima.ipv6.bt.com/
- [STATELESS] RFC4862
- [STATEFULL] RFC3315
- [PRIVACY] RFC4941
- Windows IPv6
  - http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/sag_ip_v6_add_utils.mspx
  - http://www.microsoft.com/technet/community/columns/cableguy/cg0902.mspx.

Thanks !

Contact:

- Jordi Palet Martínez (Consulintel): jordi.palet@consulintel.es
- Alvaro Vives Martínez (Consulintel): alvaro.vives@consulintel.es

6DEPLOY Project

http://www.6deploy.org

The IPv6 Portal:

http://www.ipv6tf.org