



Torino
Technologies
Group

ICT  POWER.IT

Incontro TTG 26 settembre 2019

Fondamenti e utilizzo del protocollo IPv6
in ambiente Windows

Ermanno Goletto

Microsoft MVP Reconnect

@ermannog

www.devadmin.it

Roberto Massa

Microsoft MVP Reconnect

@robi_massa

massarobi.wordpress.com

Agenda



Torino
Technologies
Group



- Perchè preoccuparsi dell'IPv6?
- IPv6 Nozioni base
- Supporto all'IPv6 in Windows
- Gestione IPv6 tramite PowerShell
- Considerazioni sull'adozione dell'IPv6



Torino
Technologies
Group

ICT  POWER.IT

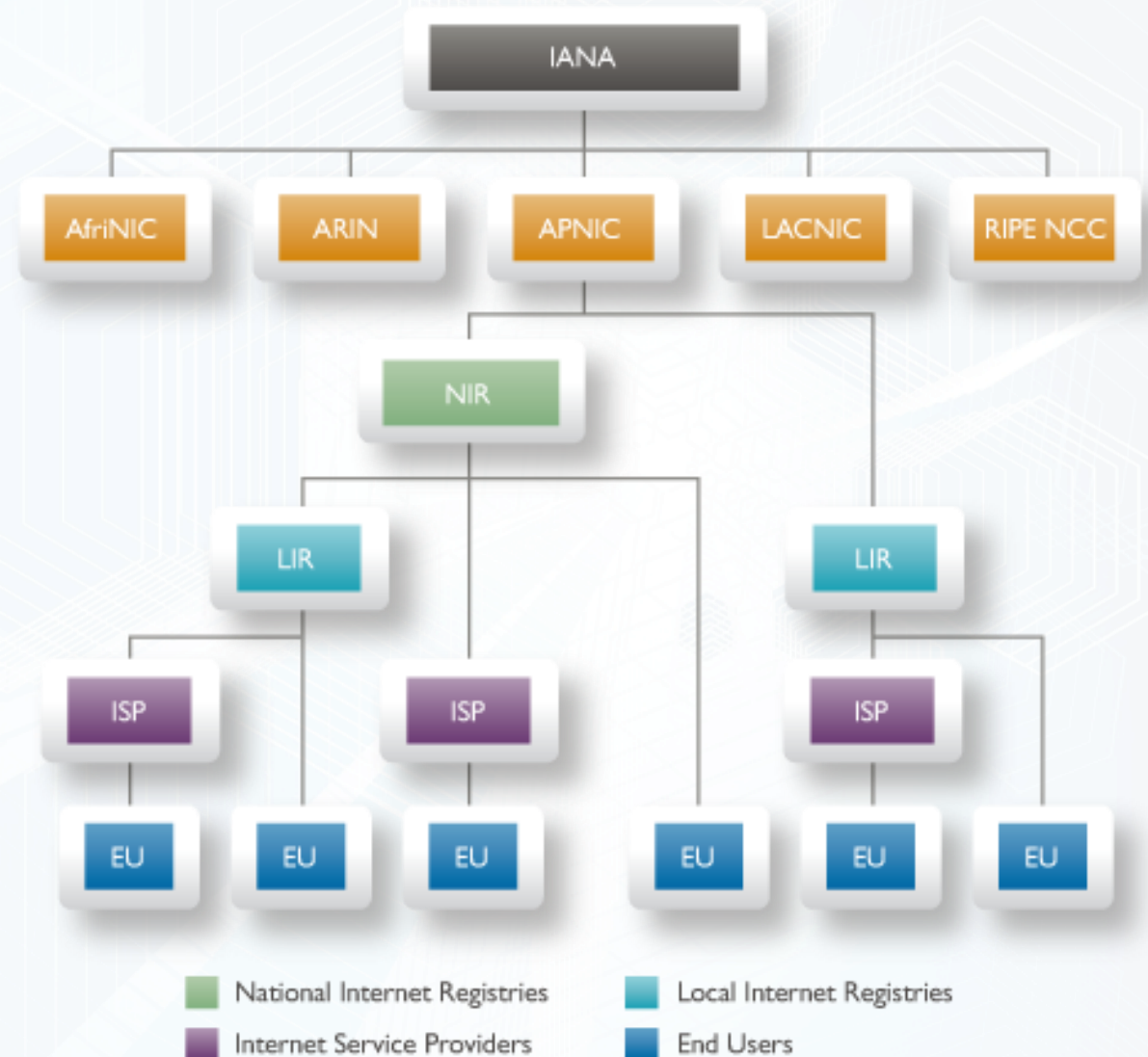
Perchè preoccuparsi dell'IPv6?

Fondamenti e utilizzo del protocollo IPv6 in ambiente Windows

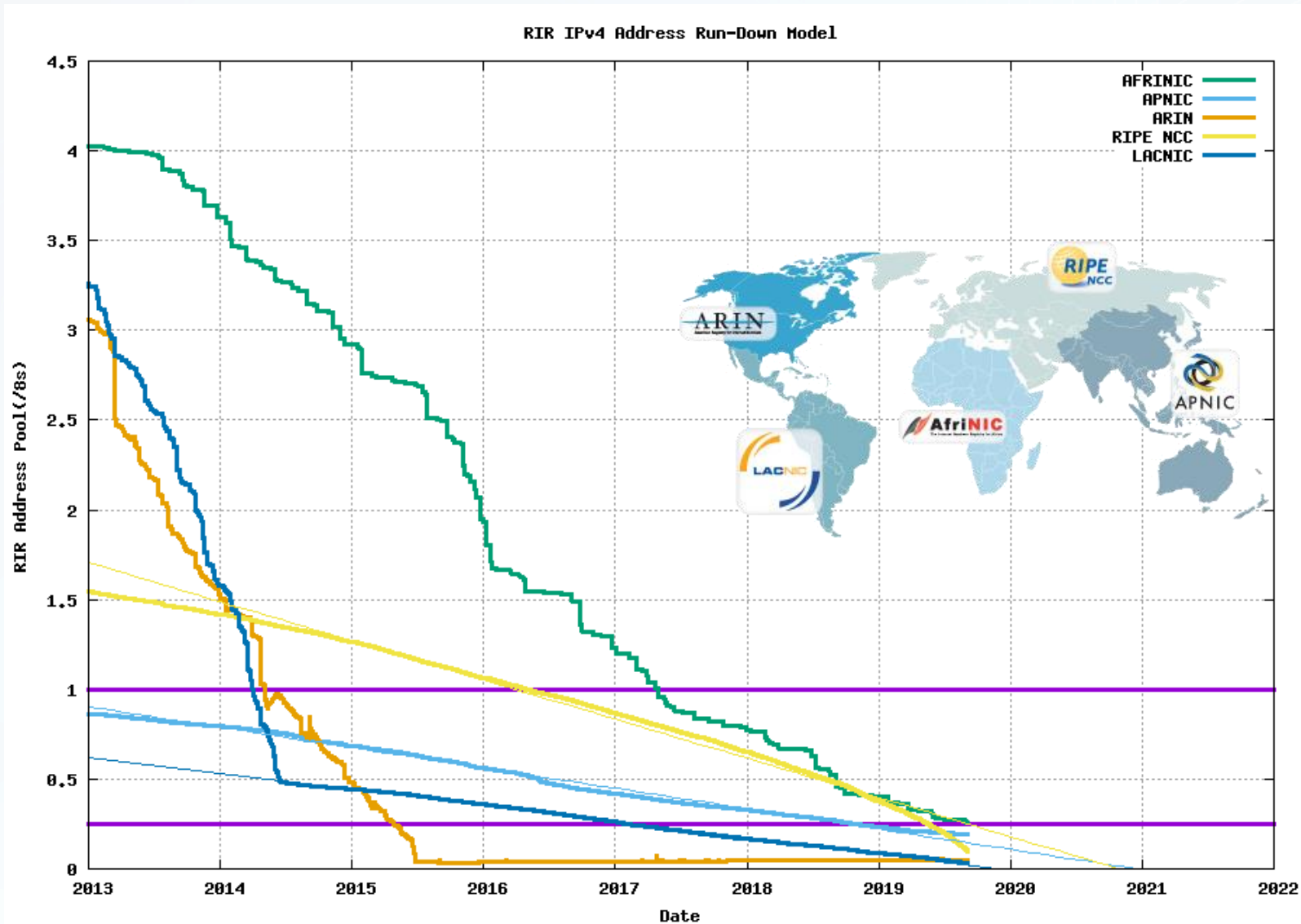
Gestione assegnazione indirizzi IPv4

Saturazione indirizzi IPv4

- IPv4 usa 32 bit permettendo circa 4 miliardi di indirizzi
- L'IPv4 è stato sviluppato nel 1978 con ARPANET
- L'IPv4 è stato pubblicato con l'RFC 791 nel 1981
- Feb 2011: IANA assegna gli ultimi blocchi /8 di IP
- Apr 2011: APNIC inizia ad allocare l'ultimo blocco /8 di IP
- Set 2012: RIPE NCC inizia ad allocare l'ultimo blocco /8 di IP
- Apr 2014: IANA inizia una politica di recupero degli indirizzi
- Giu 2014: LACNIC inizia ad allocare l'ultimo blocco /8 di IP
- Set 2015: ARIN inizia ad allocare l'ultimo blocco /8 di IP
- Apr 2017: AFRINIC inizia ad allocare l'ultimo blocco /8 di IP



Situazione IPv4 a settembre 2019



Giugno 2015

APNIC:	19-Apr-2011 (actual)	0.7098
RIPE NCC:	14-Sep-2012 (actual)	1.0097
LACNIC:	10-Jun-2014 (actual)	0.1739
ARIN:	20-Jul-2015	0.1500
AFRINIC:	07-Mar-2019	2.5993

Settembre 2019

APNIC:	19-Apr-2011 (actual)	0.1920
RIPE NCC:	14-Sep-2012 (actual)	0.0986
LACNIC:	10-Jun-2014 (actual)	0.0302
ARIN:	24-Sep-2015 (actual)	0.0002
AFRINIC:	09-Feb-2020	0.2566

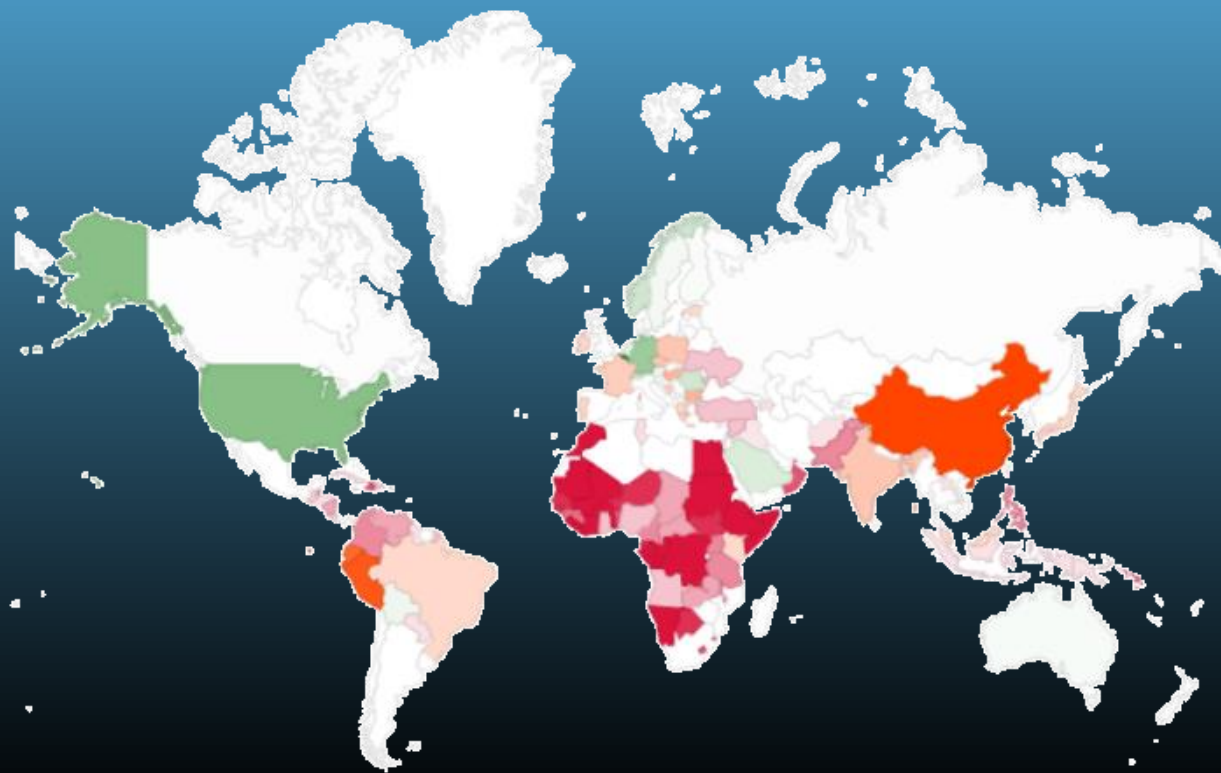
Previsione esaurimento indirizzi IPv4

- ARIN e LACNIC (America) e RIPE NCC (Europa) rischiano di esaurire gli IP entro il 2020
- APNIC (Asia) rischia di esaurire gli IP entro il 2021

Diffusione IPv6

Maggio 2015

7,12 %

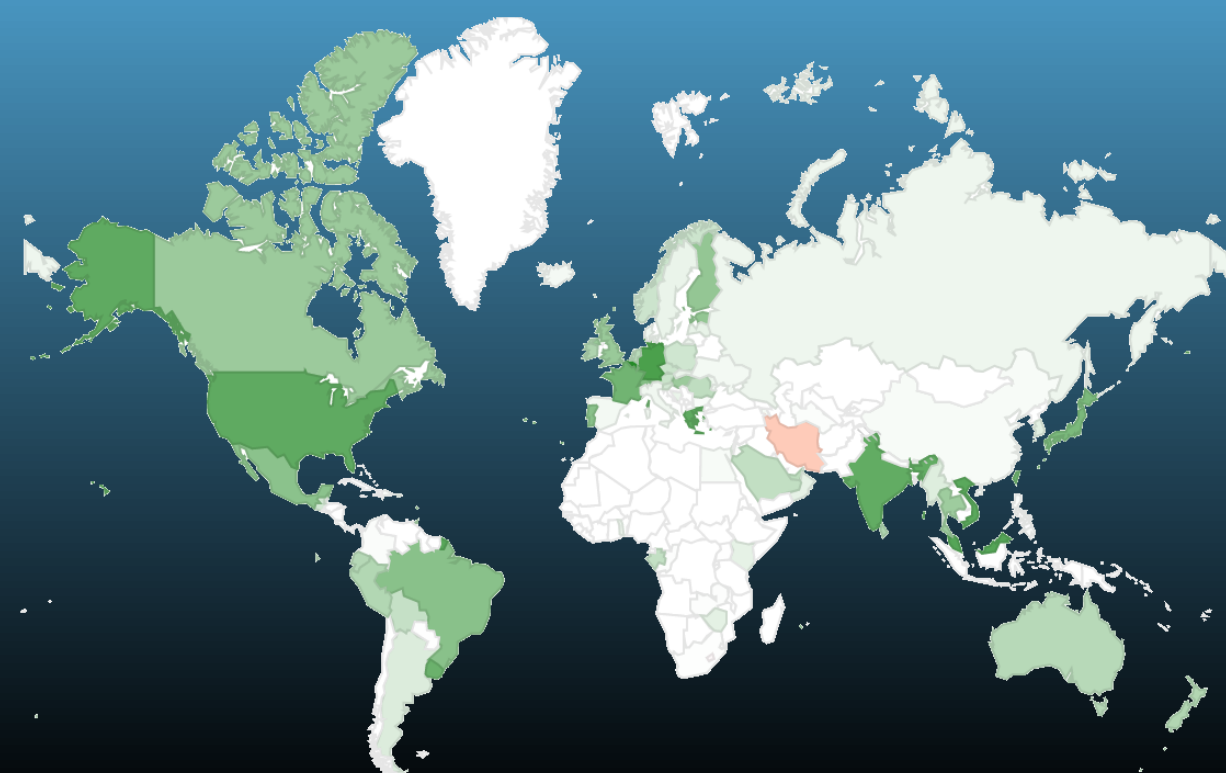


<http://www.google.com/intl/it/ipv6/statistics.html>

Belgio 33,53%	Norvegia 7,11%	Francia 5,6%
Stati Uniti 18,12%	Grecia 8,22%	Cina 2,71%
Germania 14,75%	Arabia Saudita 7,11%	Inghilterra 0,31%
Svizzera 9,57%	Romania 6,67%	Italia 0,05%
Ampia diffusione e connessioni affidabili		
Buona diffusione, ma con issues(*)		

Settembre 2019

26,26 %



<http://www.google.com/intl/it/ipv6/statistics.html>

Belgio 52,05%	Francia 33,68%	Russia 3,91%
Germania 42,84%	Svizzera 29,5%	Italia 3,59%
Grecia 38,14%	Inghilterra 24,3%	Iran 2,64%
Stati Uniti 37,92%	Ungheria 23,6%	Cina 1,95%
Scarsa diffusione con issues (*)		

(*) affidabilità e/o latenza

Perché occorre adottare l'IPv6

IPv4



Nonostante NAT (Network Address Translation), NAPT (Network Address and Port Translation), CIDR (Classless Inter-Domain Routing), vendita e trasferimento gestiti dai RIR gli IPv4 si stanno esaurendo



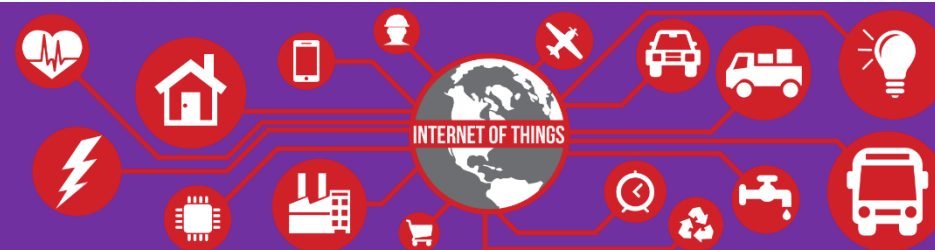
IPv6

I RIR che esauriscono gli IPv4 rilasceranno a ISP e organizzazioni che richiedono IP nella loro area necessariamente allocazioni di spazio d'indirizzamento IPv6



"Our job is to ensure that Microsoft thrives in a mobile and cloud-first world"

Satya Nadella
CEO, Microsoft



"Cloud services and mobile devices cannot scale without either IPv6 addresses or an evolved best-practice to manage them effectively"

Tom Coffeen
Chief IPv6 Evangelist, Infoblox



Torino
Technologies
Group

ICT  POWER.IT

IPv6 nozioni base

Fondamenti e utilizzo del protocollo IPv6 in ambiente Windows

Formato dell'indirizzo IPv6 (RFC 5952)

Indirizzo IPv6: **fe80:0000:0000:0000:0290:27ff:0077:de97**

8 campi di 4 cifre esadecimali (16 bit) con lettere minuscole

Leading zero trimming: **fe80:0:0:0:290:27ff:77:de97**

Gli zeri iniziali sono opzionali, i campi composti da tutti zeri possono essere contratti ad un solo zero

Zero group compression: **fe80::290:27ff:77:de97**

Uno o più gruppi consecutivi di zero possono essere sostituiti da ::, tale notazione può essere utilizzata una sola volta in modo da ridurre la lunghezza dell'indirizzo il più possibile partendo da sinistra

- Per specificare IPv6 in un URL occorre racchiuderlo tra parentesi graffe: `http://{fe80::290:27ff:77:de97}:8888/index.html`
- La rappresentazione di una rete IPv6 è basata sulla notazione prefisso/lunghezza prefisso (notazione CIDR)
 - Nel caso in cui la lunghezza del prefisso non sia un multiplo di 16 bit va completato con zeri
 - IPv6 non supporta le subnet mask, ma solo la notazione lunghezza del prefisso

Proprietà - Protocollo Internet versione 6 (TCP/IPv6)

Generale

Le impostazioni IPv6 possono essere configurate automaticamente, se la rete in uso supporta tale funzionalità. In caso contrario è necessario richiedere all'amministratore della rete le impostazioni IPv6 appropriate.

☐ Ottieni automaticamente un indirizzo IPv6

☒ Usa l'indirizzo IPv6 seguente:

Indirizzo IPv6:

Lunghezza prefisso subnet:

Gateway predefinito:

☐ Ottieni indirizzo server DNS automaticamente

☒ Utilizza i seguenti indirizzi server DNS:

Server DNS preferito:

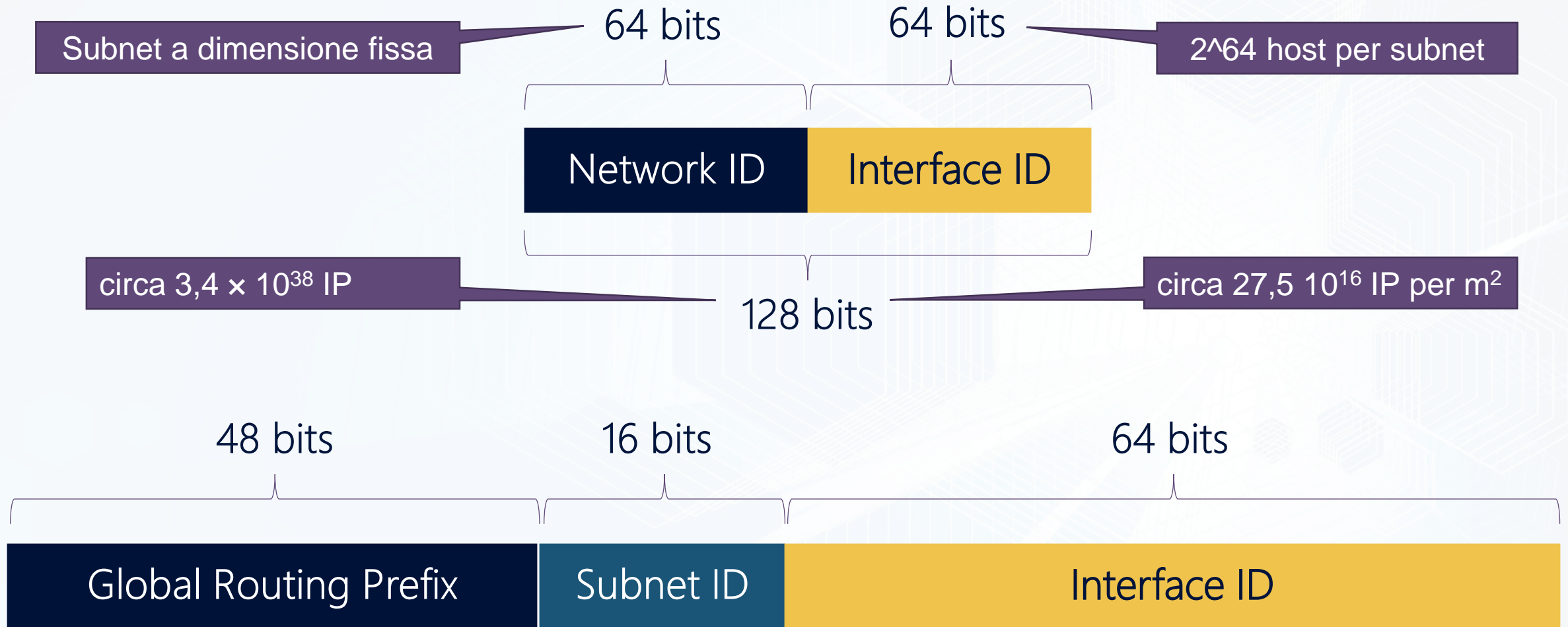
Server DNS alternativo:

☐ Convalida impostazioni all'uscita

Avanzate...

OK Annulla

Struttura indirizzo IPv6



I RIR richiedono un blocco ogni 18 mesi esaurendo il primo blocco assegnato da IANA (1/8 del totale) nel 2158

Tipi di indirizzo IPv6 (RFC 3513)

Unicast

- Identifica una singola interfaccia di rete di un host
- Un pacchetto con indirizzo IP unicast è inviato solo all'interfaccia con tale indirizzo
- Per gestire i sistemi di bilanciamento di carico l'RFC 3513 consente a più interfacce di usare lo stesso indirizzo

- Global
- Link-local
- Site-local [deprecati]
- Unique Local (ULA) [sostituiscono i Site-Local]
- Speciali [Unspecified, Loopback]
- Indirizzi di compatibilità

Multicast

- Identifica un insieme d'interfacce di rete, tipicamente di host diversi
- Un pacchetto con indirizzo IP multicast è inviato a tutte le interfacce con tale indirizzo
- Non supporta il broadcast

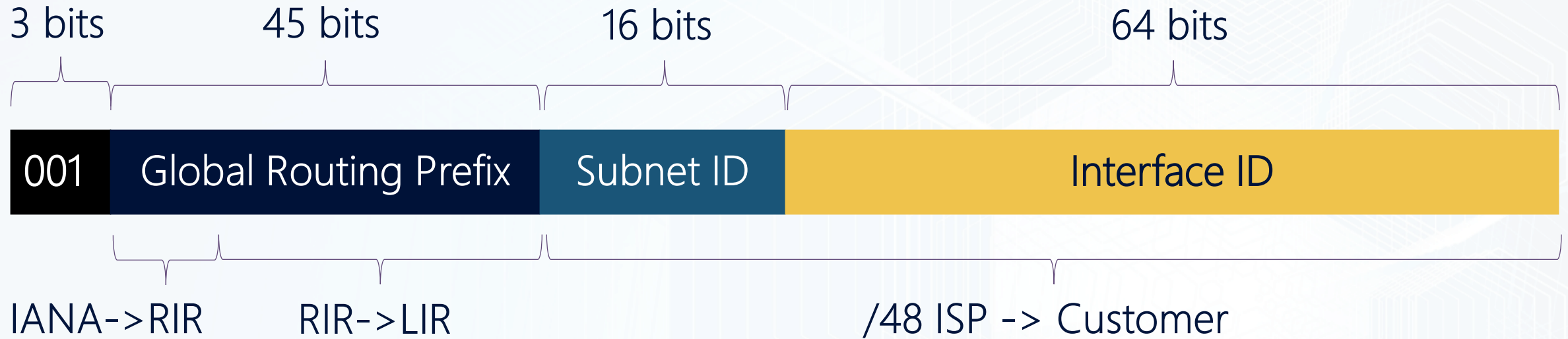
Gli indirizzi broadcast non sono più utilizzati
L'RFC 3513 non definisce un indirizzo di broadcast

Anycast

- Identifica un insieme d'interfacce di rete, tipicamente di host diversi
- Un pacchetto con indirizzo IP anycast è inviato ad una sola interfaccia con tale indirizzo, quella più vicina in termini di routing

Gli indirizzi anycast vengono attualmente utilizzati solo come indirizzi di destinazione e assegnati solo ai router

Indirizzi unicast Global (RFC 3587, RFC 4291)



Instradabili e raggiungibili a livello globale nella rete Internet

- **Prefisso 2000::/3**
- Il Global Routing Prefix individua un Site di un'organizzazione
- La Subnet ID viene utilizzata all'interno del Site dell'organizzazione per creare fino a 65.536 subnet

Indirizzi unicast Unique Local Addresses (RFC 4193)



Instradabili e raggiungibili a livello di Site in una Intranet, non instradabili e raggiungibili a livello globale nella rete Internet

- **Prefisso fc00::/7**
- L=1 indica prefisso locale (L=0 non è al momento definito) quindi **gli ULA hanno prefisso fd00::/8**
- Il Global ID identifica il Site di un'organizzazione impostato in modo pseudo casuale (RFC 4193 ora+EUI-64 NIC)
- La Subnet ID viene utilizzata all'interno del Site dell'organizzazione per creare fino a 65.536 subnet
- Equivalenti allo spazio private IPv4 (10.0.0.0/8, 172.16.0.0/12 e 192.168.0.0/16)
- Sostituiscono gli indirizzi unicast Site Local (RFC 3879)

Indirizzi unicast Link Local (RFC 4862)



Utilizzati dai nodi per comunicare con nodi adiacenti sullo stesso Link e non sono instradabili

- **Prefisso fe80::/64**
- Equivalenti agli indirizzi IPv4 APIPA (169.254.0.0/16)
- Necessario per i processi di individuazione dei router adiacenti
- Viene sempre configurato automaticamente anche in assenza di tutti gli altri indirizzi unicast
- Interface ID generato automaticamente dal MAC Address tramite l'algoritmo EUI-64 (IEEE 64-bit Unique Identifier)
- Un router IPv6 non inoltra il traffico Link Local oltre il link stesso

Indirizzi unicast speciali (RFC 5156)

Indirizzo Unspecified

0:0:0:0:0:0:0:0 oppure :: oppure ::/128

Utilizzato come indirizzo origine per pacchetti che tentano la verifica dell'univocità di un indirizzo provvisorio (richiesta iniziale DHCP o durante il processo DAD)

Equivale
all'indirizzo
IPv4
0.0.0.0



Indirizzo di Loopback

0:0:0:0:0:0:0:1 oppure ::1 oppure ::1/128

Utilizzato per consentire ad un nodo di inviare pacchetti a se stesso, i pacchetti destinati all'indirizzo di loopback non possono essere inviati tramite un link o inoltrati da un router

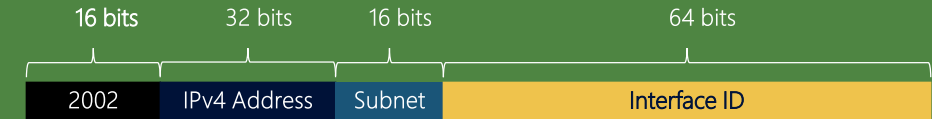
Equivale
all'indirizzo
IPv4
127.0.0.1



Indirizzi unicast di compatibilità



Indirizzo 6to4 (RFC 3056)



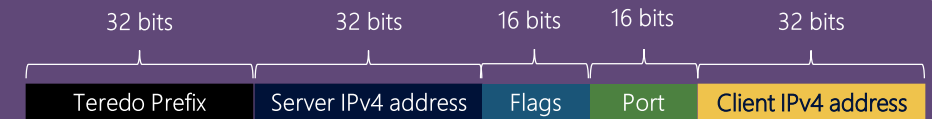
Permettono la comunicazione tra due nodi IPv6 su un'infrastruttura di routing IPv4 utilizzando un indirizzo IPv4 pubblico

Indirizzo ISATAP (RFC 5214)



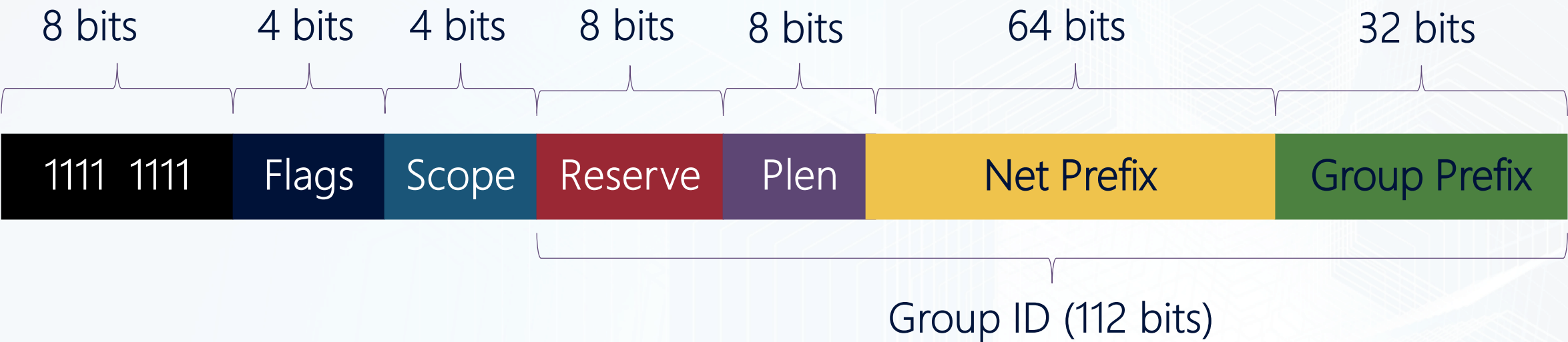
Utilizzato per la comunicazione tra due nodi che eseguono IPv4 e IPv6 su un'infrastruttura di routing IPv4

Indirizzo Teredo (RFC 4380)



Incapsula i pacchetti IPv6 in pacchetti UDP IPv4, permettere l'utilizzo di tunnel anche in presenza di NAT IPv4

Indirizzi multicast (RFC 3513)



Identificano un gruppo d'interfacce generalmente di nodi diversi

- **Prefisso ff00::/8**
- Sono una sorta di broadcast con ambito, i membri di un gruppo multicast hanno lo stesso Group ID
- Ogni nodo deve supportare l'indirizzo multicast di nodo sollecitato per il rilevamento di indirizzi duplicati e la risoluzione degli indirizzi Link Local degli host col protocollo NDP (Neighbor Discovery Protocol)

Flag	Prefisso	Interpretazione
0000	ff00::12	Group ID a 112 bits assegnato permanentemente, indirizzo coincidente con Group ID
0001	ff10::/12	Group ID a 112 bits assegnato temporaneamente, indirizzo coincidente con Group ID
0011	ff30::/12	Indirizzo multicast con prefisso unicast temporaneo
0111	ff70::12	Indirizzo multicast con ID d'interfaccia Rendezvous Point e prefisso unicast temporaneo

L'RFC 3513 consiglia di assegnare Group ID usando solo i 32 bit meno significativi

Concetti e terminologia IPv4 vs IPv6

IPv4

Un **Host** è identificato da un **indirizzo IP**

Gli host appartengono a **Segmenti di rete** Ethernet identificati tramite una **Subnet mask**

Per comunicare in una rete IPv4 sono richiesti

- **Indirizzo IP**
- **Subnet mask**
- **Indirizzo IP Gateway**

La **comunicazione tra segmenti Ethernet** differenti richiede un **Router**

Le **configurazioni** sono impostate **manualmente** o tramite **DHCP**

IPv6

Un **Nodo** è un **Device di rete** (host, router) identificato da un **indirizzo Multicast**

Un **Interfaccia** è una **Connessione** Fisica (NIC) o Logica (tunnel) di un Nodo ad un Link identificata da un **indirizzo Unicast**

Un **Link** (Collegamento) è **una o più LANs** (Ethernet) o **WANs** (PPP) **connesse da Routers**, indicato anche come Network Segment può essere Logico o Fisico ed identificato da un **Subnet Prefix**

I **Neighbors** (Vicini) sono i **Nodi connessi allo stesso Link** Fisico o Logico

Un **Host** è un **Device di rete che non inoltra pacchetti**, ovvero un endpoint sorgente o destinazione

Un **Router** è un **Device di rete che inoltra pacchetti** ed esegue l'advertise della sua presenza verso gli host connessi ai suoi links

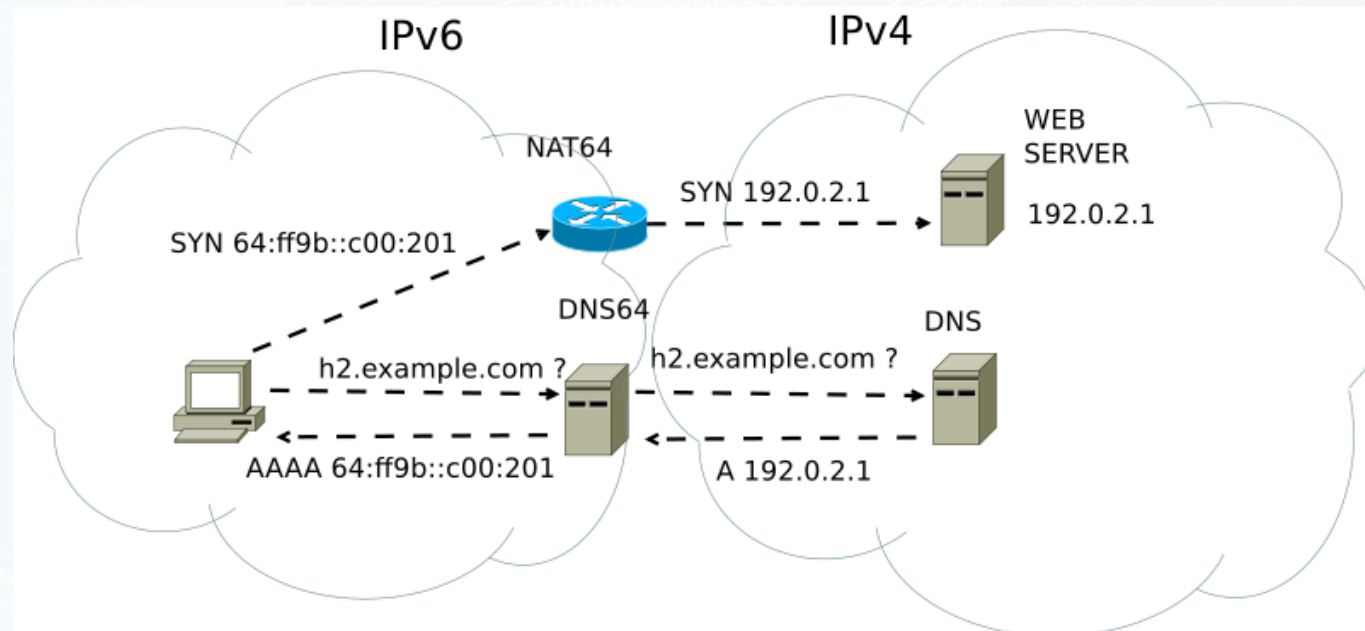
Indirizzamento IPv4 vs IPv6

IPv4	IPv6
Unicast	Unicast
Multicast (224.0.0.0/4)	Multicast (FF00::/8)
Public	Global Unicast
RFC 1918 Private (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16)	RFC 4193 Unique Local Address (FD00::/8)
APIPA (169.254.0.0/16)	Link-local (FE80::/64)
Loopback (127.0.0.1)	Loopback (::1)
Unspecified (0.0.0.0)	Unspecified (::)

Tecnologie di Traslation

NAT64 (RFC 6164)

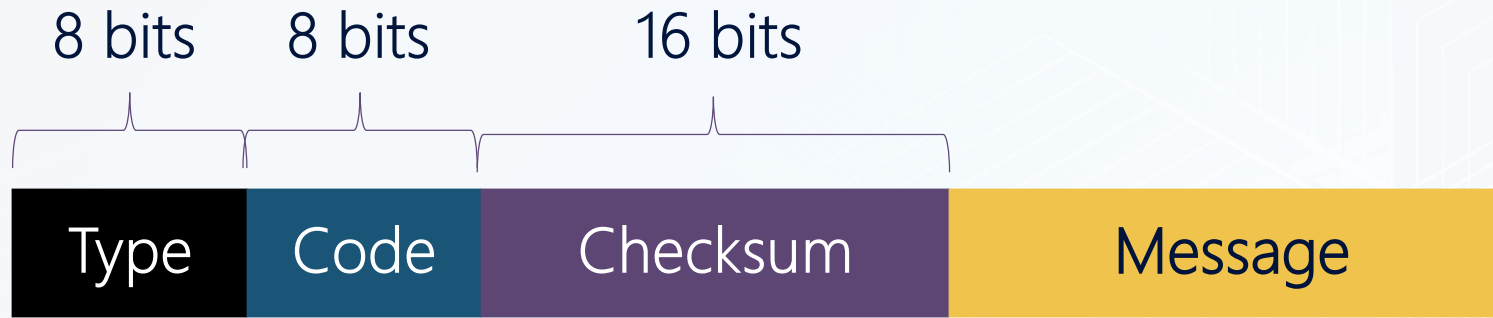
- Consente a host IPv6 di avviare connessioni IPv4, ma non il contrario
- Utilizza tecnologie NAPT (Network Address and Port Translation) per mappare un indirizzo IPv4 a più indirizzi IPv6 differenziando la porta TCP/UDP di origine



DNS64 (RFC 6147)

- Server DNS ricorsivo che elabora query di record AAAA e fornisce risposte per indirizzi IPv6
- Nel caso non sia possibile fornire indirizzi IPv6 esegue query per record A e fornisce l'indirizzo IPv4 convertito in IPv6 tramite NAT64

ICMPv6 (RFC 2463)



Monitoraggio stato rete e invio pacchetti di gestione ed errore

- **Unico protocollo di controllo** che Integra funzionalità che in IPv4 erano demandate ad ARP e IGMP
- **MLD (Multicast Listener Discovery)** è una serie di tre messaggi ICMPv6 che sostituisce la versione 2 del protocollo IGMP (Internet Group Management Protocol) per IPv4, per la gestione dell'appartenenza multicast alla subnet.
- **ND (Neighbor Discovery)** è una serie di cinque messaggi ICMPv6 per la gestione delle comunicazioni tra nodi in un collegamento che sostituisce il protocollo ARP (Address Resolution Protocol), il rilevamento router ICMPv4 e il messaggio di reindirizzamento ICMPv4, fornendo inoltre funzionalità aggiuntive

```
ping -6 HostName  
ping IPv6Address%ZoneID
```

```
tracert -d -6 HostName  
tracert IPv6Address%ZoneID
```

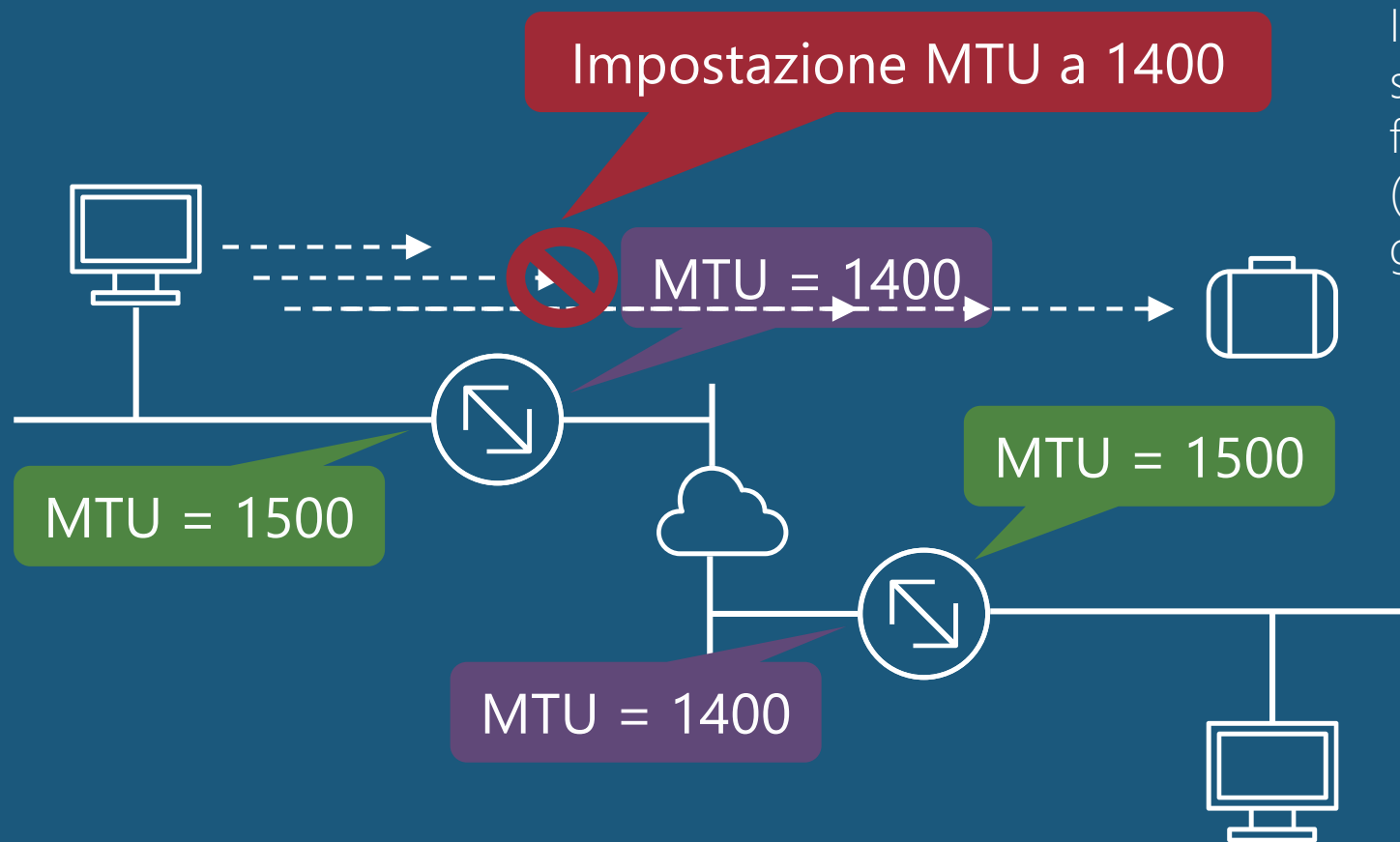
**0-127
Errori**

**128-255
Info**

Type	Significato
1	Destination Unreachable
2	Packet Too Big
3	Time Exceeded
4	Parameter Problem
128	Echo Request
129	Echo Replay
130	Multicast Listener Query
131	Multicast Listener Report
132	Multicast Listener Done
133	Router Solicitation
134	Router Advertisement
135	Neighbor Solicitation
136	Neighbor Advertisement
137	Redirect Message
138	Router Renumbering

Importanza dell'MTU nell'IPv6

Occorre
permettere
il traffico
ICMPv6
nella rete

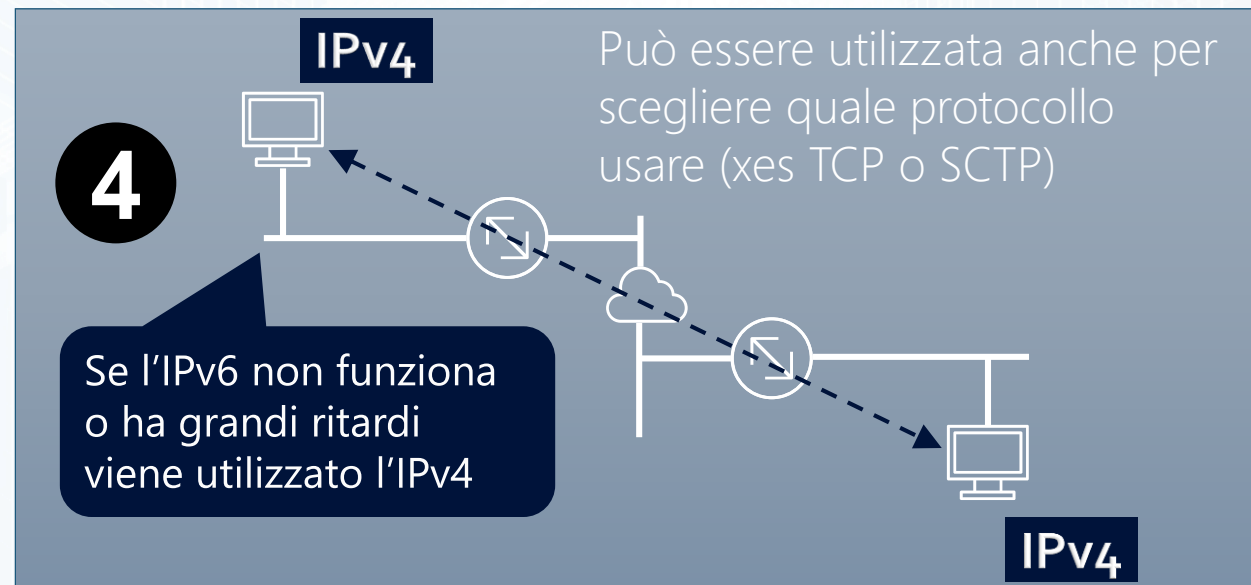
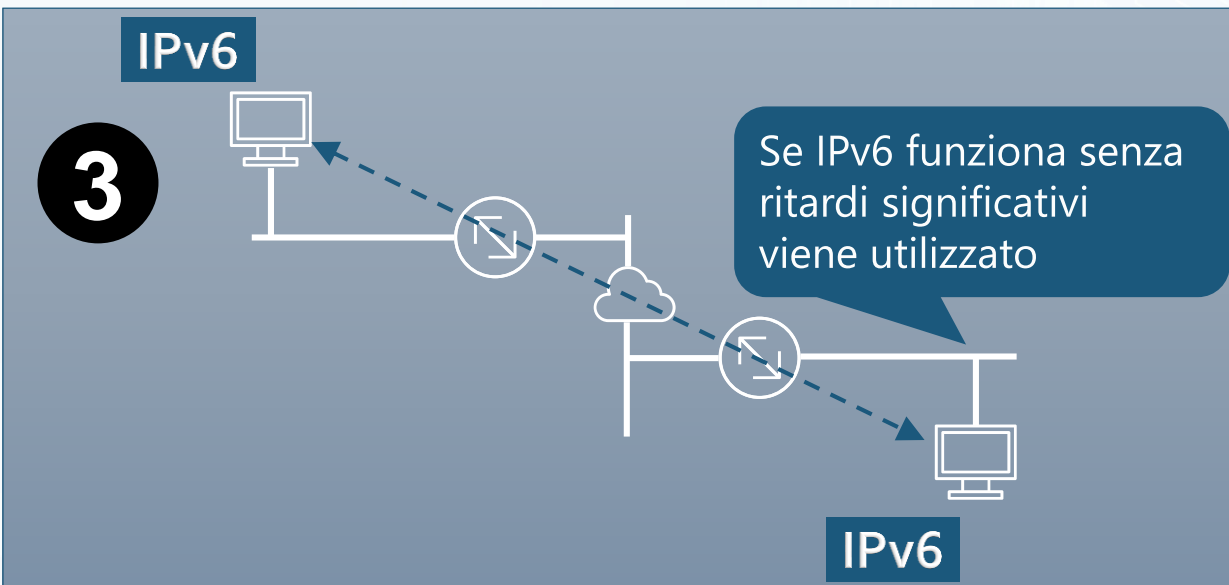
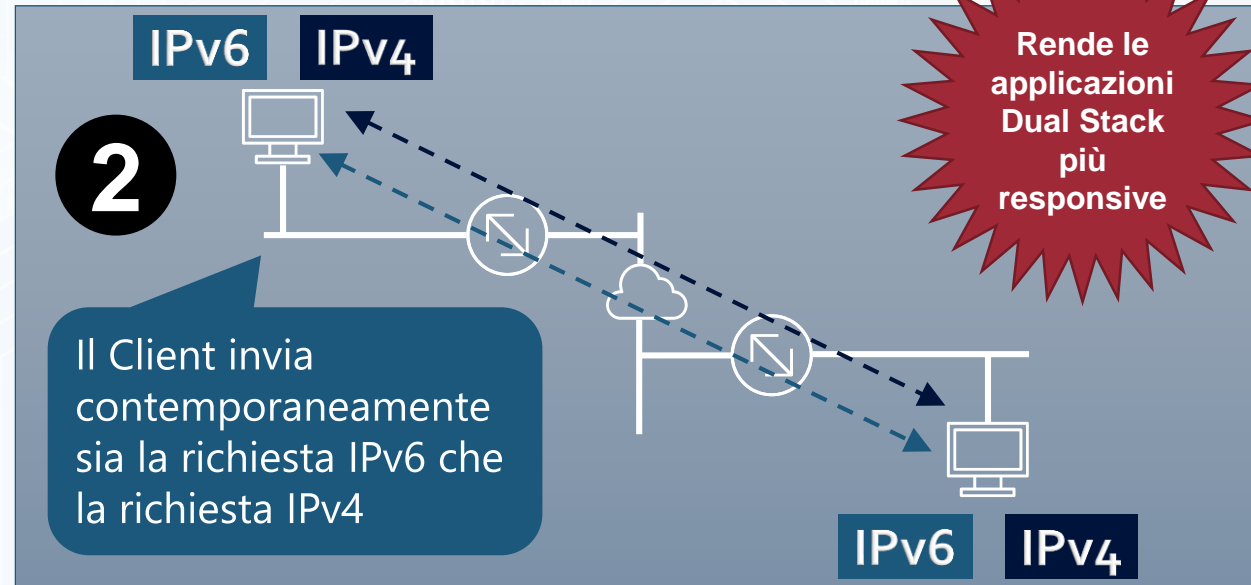
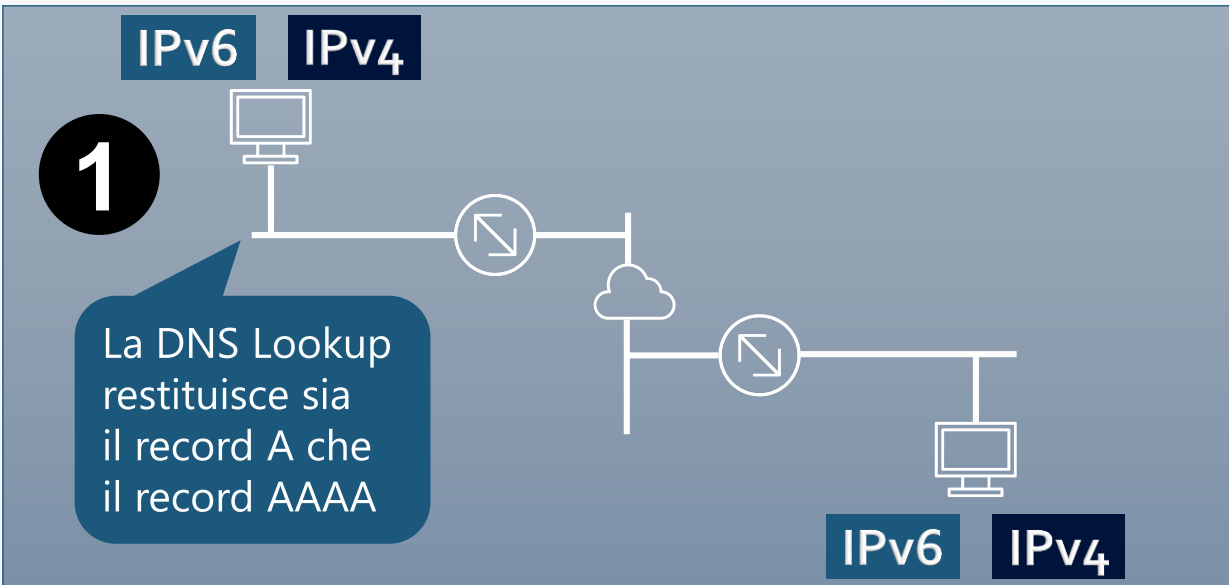


In IPv6 la frammentazione può essere eseguita solo alla sorgente, ovvero i router IPv6 non frammentano i pacchetti che ritrasmettono (anche se possono frammentare i pacchetti che generano loro stessi), mentre i router IPv4 si

Viene utilizzato il path MTU discovery che permette di determinare il path MTU fra due stazioni (RFC 1981)

Quando il pacchetto è maggiore dell'MTU viene eseguito il drop del pacchetto e inoltrato un ICMPv6 Packet Too Big (Type 2)

Funzionamento Happy Eyeballs (RFC 6556)



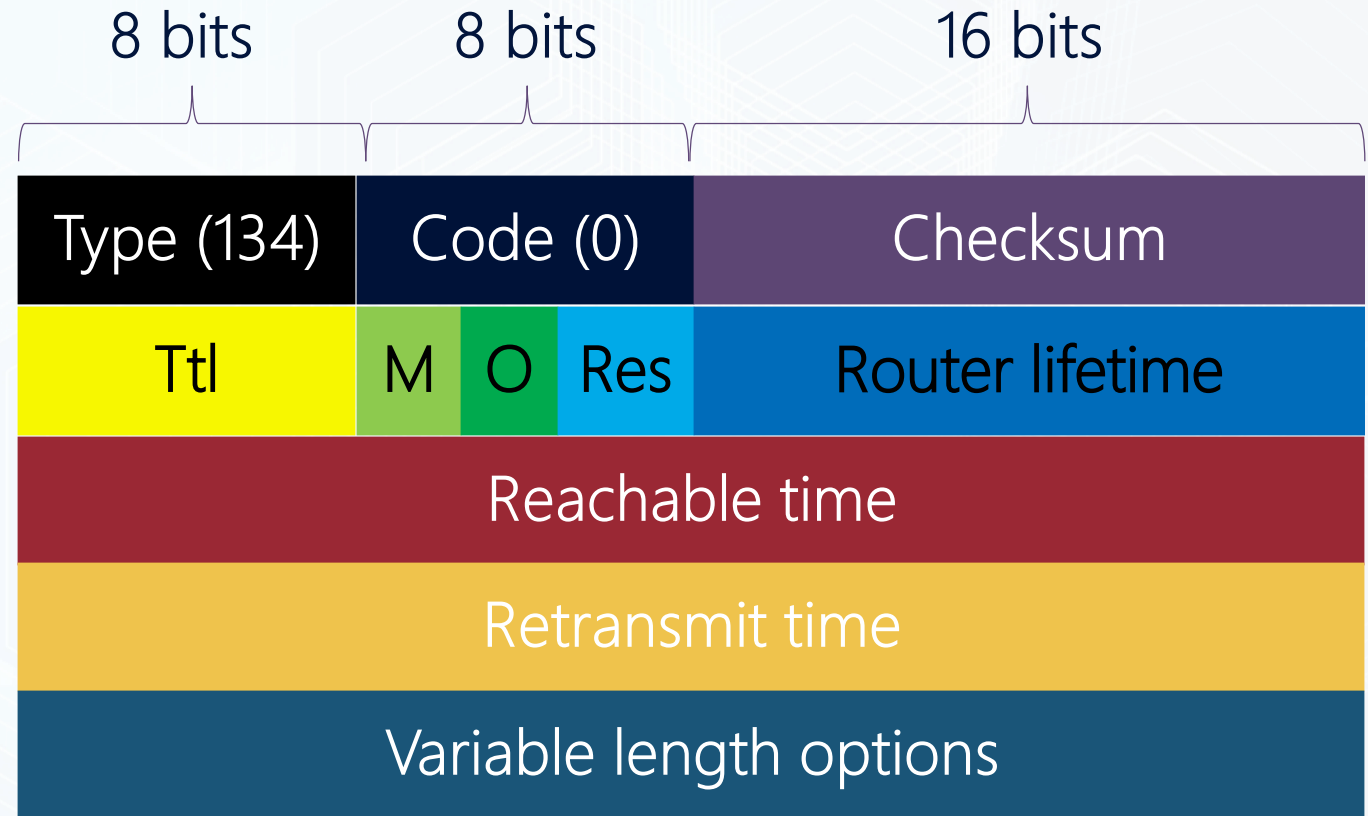
Ricerca dei router

Tutti i **Router** devono appartenere al **gruppo multicast All Router** (FF02::2)

I **Client** inviano una **query Router Solicitation (RS)**

I **Router** inviano un **Router Advertisement (RA) message**

- Periodicamente
- In risposta ad una RS query



Router advertisements message (RA)

M=Address via DHCPv6
O=Options via DHCPv6

- Prefix information
 - Prefix ID e Prefix Length
 - Prefix Lifetime
- Maximum Transmission Unit (MTU)
- Source Link-layer address

Demo



Torino
Technologies
Group

ICT  POWER.IT

Router Advertising



Torino
Technologies
Group

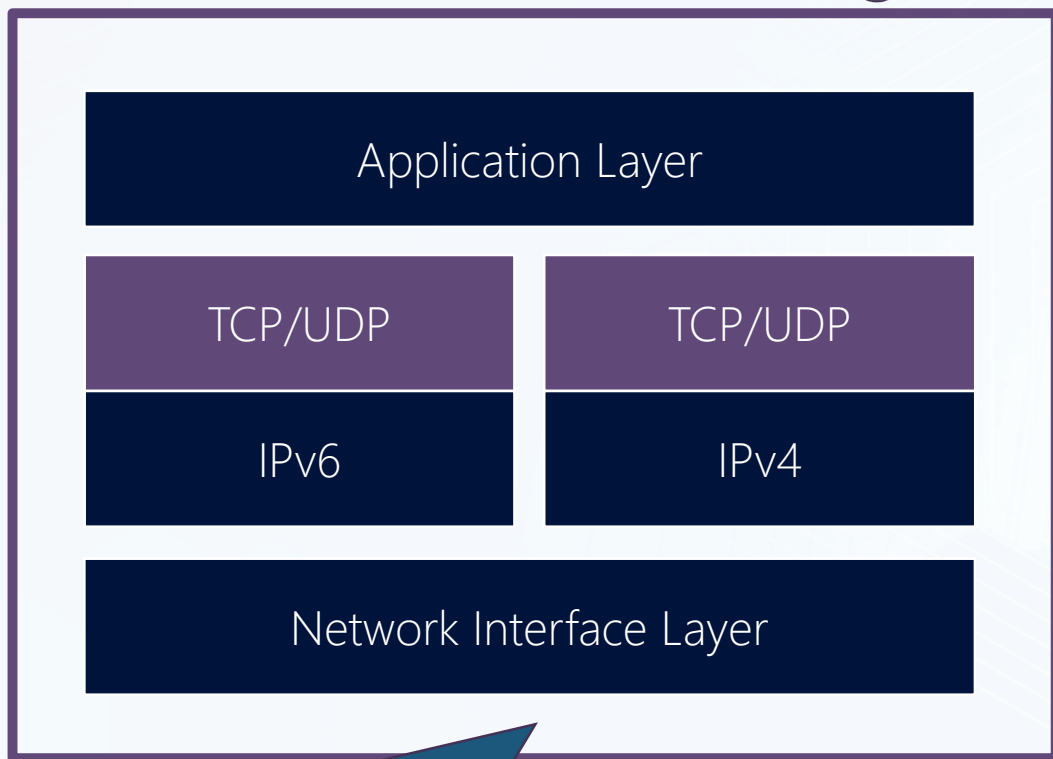
ICT  POWER.IT

Supporto all'IPv6 in Windows

Fondamenti e utilizzo del protocollo IPv6 in ambiente Windows

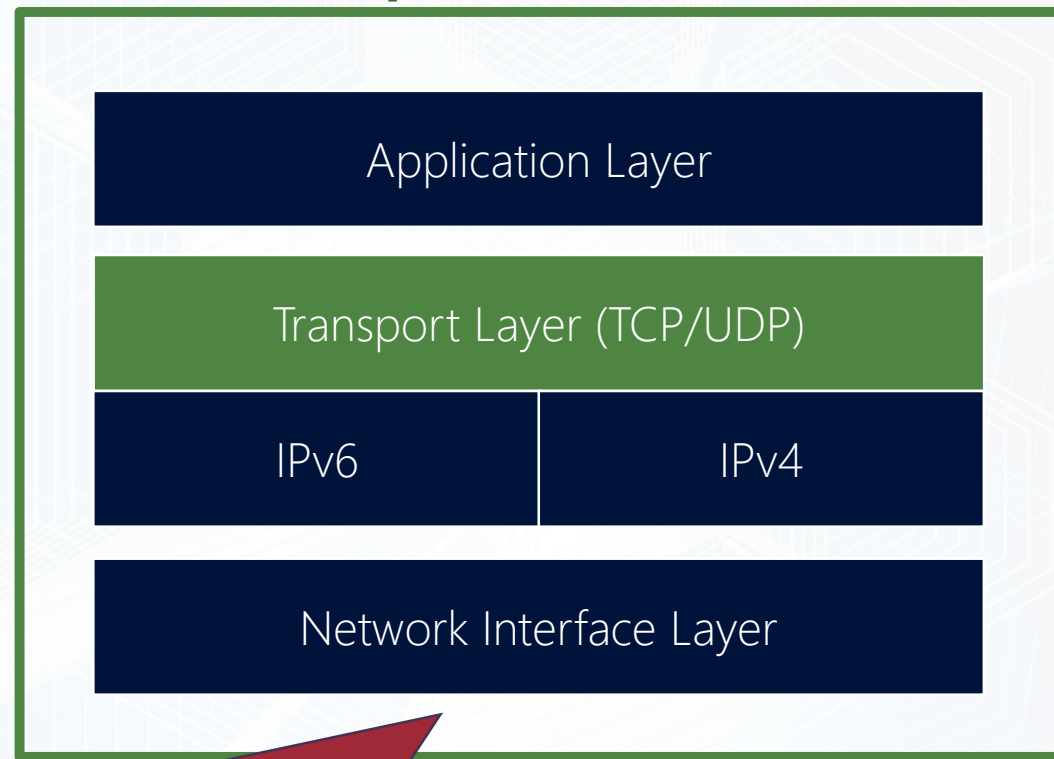
Evoluzione dello stack IPv6 negli OS Microsoft

Dual Stack (XP/WS 2003)



- 1998 1° Stack per NT 4.0, W98/95 non supportato in produzione
- 2000 Technical Preview per WS2000 non supportato in produzione
- 2003 Add-on per XP SP1 (KB817778), WS2003 integra IPv6
- 2004 XP SP2 integra IPv6

Dual IP Layer (Vista/WS 2008)



- Non è possibile rimuovere l'IPv6 dallo stack di rete (tcpip.sys)
- La KB929852 indica come limitare alcune funzionalità, ma per disabilitare completamente l'IPv6 occorre rimuovere il TCP/IP
- E' sempre possibile eseguire il ping verso il localhost (::1) in quanto l'OS deve poter eseguire chiamate a determinate funzionalità indipendentemente che l'host sia connesso o meno ad una rete

Versioni OS e supporto a IPv6

Windows 2000 or Windows 98

IPv6 non supportato

Windows XP e Windows Server 2003

Supporto limitato all'IPv6, non raccomandati per il deploy

Windows Vista e Windows Server 2008

- Dual IP layer architecture
- Installato e abilitato by default (IPv6 prioritario rispetto IPv4)
- Configurazione tramite Graphical user interface (GUI)
- Full support per IPsec
- Supporto a Multicast Listener Discovery version 2 (MLDv2)
- Supporto a Link-local Multicast Name Resolution (LLMNR)
- Literal IPv6 addresses in Uniform Resource Locators (URLs)
- Supporto a ipv6-literal.net names
- IPv6 over the Point-to-Point Protocol (PPP)
- Supporto a Dynamic Host Configuration per IPv6 (DHCPv6)
- Random interface IDs

Windows 7 e Windows Server 2008 R2

- HomeGroup
- DirectAccess
- IP-HTTPS
- Group Policy settings per transition technologies

Windows 8 e Windows Server 2012

- Miglioramenti alla connettività Internet
- NAT64/DNS64
- Windows PowerShell
- Supporto a Happy Eyeballs (RFC 6556)

Windows 8.1 e Windows Server 2012 R2

- Group Policy settings per encompasses printers, item-level targeting e VPN networks

Windows 10 e Windows Server 2019

- Supporto a RDNSS (RFC 8106, RFC 6106)
- ISATAP e 6to4 disabilitati per default

Funzionalità non supportate

Mobile IPv6

Mantenimento della connessione di un nodo IPv6 con altri nodi anche se cambia la sua posizione in Internet e/o il suo indirizzo

Al momento è poco diffuso

RFC 6106

L'IPv6 Router Advertisement Options for DNS Configuration fornisce l'IP del server DNS tramite il router locale attraverso un Router Advertisement (RA) message

Se è necessario avere informazioni DNS è probabile che si utilizzi un DHCP

Supportato
in W10
1703

DS-Lite

Transition technology che permette di utilizzare reti IPv6 per pubblicare servizi IPv4 incapsulando il traffico IPv4 in un tunnel IPv6

Tecnologia per i service providers, non avrebbe senso implementarla nell'OS

6in4

Transition technology precedente a 6to4 con le stesse funzionalità, ma con configurazione manuale e statica

Poco diffusa e sostituita da 6to4, non ha senso implementarla se si supporta 6to4

6rd

Transition technology che permette di utilizzare reti IPv4 per pubblicare servizi IPv6 incapsulando il traffico IPv6 in un tunnel IPv4

Tecnologia per i service providers, non avrebbe senso implementarla nell'OS

SEND

Secure Neighbor Discovery (RFC 3971) permette la validazione del processo di neighbor discovery

Al momento non supportato perché è una soluzione IPv6 only, mentre nel prossimo futuro si utilizzerà Dual-Stack

Gestione connessioni in Vista/WS2008 e successivi

1

Se viene restituito un record DNS AAAA viene utilizzato l'IPv6



2

Se disponibile verrà utilizzata una tecnologia di transizione

In Windows 10 1703 6to4 e ISATAP sono disabilitate per default



3

Se la connessione non è riuscita viene utilizzato IPv4



IPv6 Best Practices

Non disabilitare l'IPv6

In Vista / WS2008 e succ. alcune componenti potrebbero non funzionare (Remote Assistance, HomeGroup, DirectAccess, Windows Mail, Clustering, AD Replica, autenticazione). Il PSS può richiedere la riabilitazione, l'IPv6 disabilitato non è una configurazione supportata. Avvio OS ritardato di 5 sec (KB929852).



Aggiornare device di rete e firewall se non supportano IPv6 e non duplicare le firewall rule IPv4 su IPv6

IPv6 fa un largo utilizzo dell'ICMPv6 (ad esempio per stabilire la MTU) e non ha un equivalente di NAT e PAT. TMG non supporta IPv6 nativo.



Se non utilizzate disabilitare 6to4, ISATAP e Teredo su server e client

Le tecnologie di tunneling transition possono essere causa di comportamenti inaspettati o rallentamenti (in particolare con Lync, SMTP, Exchange, IIS, SharePoint, SQL Server). DirectAccess utilizza una tecnologia di tunneling transition.



Utilizzare l'integrazione di AD nel DNS e gestire tramite GPO le configurazioni IPv6

Per garantire l'alta disponibilità il DNS deve essere dual-stacked e avere una appropriate policy ICMPv6 per non avere problemi con MTU di grandi dimensioni o path MTU discovery (PMTUD). Creare una correlazione tra Subnet IPv4 e Prefix IPv6 per gestire correttamente Replica e Autenticazione



Comandi Windows con supporto a IPv6

Ping

ping -6 host

Pathping

pathping -6 host

Tracert

tracert -6 host

Route print

route print -6

Ipconfig

Nslookup

Netsh


Telnet

Disabilitazione tunneling transition technologies




Netsh (Windows Vista / Windows Server 2008 e successivi)

Netsh interface 6to4 set state disabled
Netsh interface isatap set state disabled
Netsh interface teredo set state type = disabled



Teredo sui
client AD è
disabilitato
per default



6to4 e
ISATAP in
W10 1703 e
succ. sono
disabilitati
per default

Registry

HKLM\SYSTEM\CurrentControlSet\Services\tcpip6\Parameters\DisabledComponents
Impostare la registry key a 0x2 (DWORD) per disabilitare 6to4
Impostare la registry key a 0x4 (DWORD) per disabilitare ISATAP
Impostare la registry key a 0x8 (DWORD) per disabilitare Teredo
Riavviare il computer

Group Policy (Windows 7 / Windows Server 2008 R2 e successivi)

Computer Configuration Policies | Administrative Templates | Network | TCP/IP Settings |
IPv6 Transition Technologies to Disabled |
6to4 State / ISATAP State / Teredo State

Assegnazione automatica indirizzi IPv6 (RFC 2462)

Scheda Ethernet Ethernet 6:

Suffisso DNS specifico per connessione:

Descrizione : Intel(R) 82579LM Gigabit Network Connection

Indirizzo fisico. : 3C-A9-F4-28-4F-E0

DHCP abilitato. : Sì

Configurazione automatica abilitata : Sì

Indirizzo IPv6 : 2002:4f14:d576:e472:1d6a:122:d129:b6a8(Preferenziale)

Indirizzo IPv6 temporaneo. : 2002:4f14:d576:e472:3959:c71c:cfb9:eeee(Preferenziale)

Indirizzo IPv6 locale rispetto al collegamento : fe80::1d6a:122:d129:b6a8%17(Preferenziale)

Indirizzo IPv4. : 10.0.0.100(Preferenziale)

Subnet mask : 255.255.255.0

Lease ottenuto. : sabato 4 aprile 2015 23.54.07

Scadenza lease : domenica 5 aprile 2015 23.54.06

Gateway predefinito : fe80::9ed3:6dff:fea1:5673%17
10.0.0.1

Server DHCP : 10.0.0.1

IAID DHCPv6 : 775727604

DUID Client DHCPv6. : 00-01-00-01-19-2D-5C-A3-3C-A9-F4-28-4F-E0

Server DNS : 10.0.0.1

NetBIOS su TCP/IP : Attivato

In IPv4 esiste l'APIPA (169.254.0.0/16) descritto nella RFC 3927, ma gli IP appartengono ad un range privato non instradabili in Internet

Gli indirizzi Link-local hanno una Zone ID (o Scope ID) rappresentato da %<ID> dopo l'indirizzo IPv6

StateLess Address AutoConfiguration (SLAAC): indirizzo Globale e Link-Local generati automaticamente con **Interface ID** randomica (Vista/2008 e succ.) o basato sul MAC (EUI-64 in XP/2003)

W7/2008 R2 riutilizzano il random ID nell'indirizzo Global e nell'ULA

Indirizzi IPv6 temporanei (RFC 4941 sec. 3.3)

Scheda Ethernet Ethernet 6:

Suffisso DNS specifico per connessione:

Descrizione : Intel(R) 82579LM Gigabit Network Connection

Indirizzo fisico. : 3C-A9-F4-28-4F-E0

DHCP abilitato. : Sì

Configurazione automatica abilitata : Sì

Indirizzo IPv6 : 2002:4f14:d576:e472:1d6a:122:d129:b6a8(Preferenziale)

Indirizzo IPv6 temporaneo. : 2002:4f14:d576:e472:3959:c71c:cfb9:eeee(Preferenziale)

Indirizzo IPv6 locale rispetto al collegamento . : fe80::1d6a:122:d129:b6a8%17(Preferenziale)

Indirizzo IPv4. : 10.0.0.100(Preferenziale)

Subnet mask : 255.255.255.0

Lease ottenuto. : sabato 4 aprile 2015 23.54.07

Scadenza lease : domenica 5 aprile 2015 23.54.06

Gateway predefinito : fe80::9ed3:6dff:fea1:5673%17
10.0.0.1

Server DHCP : 10.0.0.1

IAID DHCPv6 : 775727604

DUID Client DHCPv6. : 00-01-00-01-19-2D-5C-A3-3C-A9-F4-28-4F-E0

Server DNS : 10.0.0.1

NetBIOS su TCP/IP : Attivato

Generati negli OS Client
Windows Vista e succ.

L'ID random
garantisce
la privacy rispetto
all'EUI-64 che è
basato sul MAC

Indirizzo Global non viene registrato dinamicamente nel DNS dal Windows Client con una durata temporanea (7 giorni per default)

Utilizzati da applicazioni client per inizializzare le comunicazioni (xes. Web browser)

DHCPv6 (RFC 3315)

Statefull

- Router advertisements message (RA) con flag M=1 e O=1
- Indirizzo IPv6 non-link-local assegnato tramite server DHCPv6
- Opzioni assegnate tramite scope DHCPv6 (tranne Gateway)

- Network prefix
- DNS server(s)
- NTP server (s)
- TFTP server(s)
- Option code(s)

L'impostazione del **default Gateway** viene gestita tramite i router col processo di Router Advertisement

Stateless

- Router advertisements message (RA) con flag M=0 e O=1
- Il server DHCPv6 assegna solo le opzioni (tranne Gateway)
- Assegnazione indirizzi IPv6 link-local e non-link-local assegnati tramite interscambio di RA Solicitation e RA con routers vicini

Lo scopo di questa modalità operativa è quello di permettere la gestione di opzioni alla SLAAC

Il DHCPv6 non utilizza il MAC address come il DHCPv4, ma il **DHCP Unique Identifier (DUID)** unico per host e l'**Interface Association Identifier (IAID)** unico per interfaccia

Le **IPv6 address reservation** in DHCPv6 si configurano specificando il DUID e l'IAID

In ogni caso un indirizzo IPv6 link-local viene configurato automaticamente

Stateless Address Autoconfiguration (SLAAC)

- Router advertisements message (RA) con flag M=0 e O=0
- Assegnazione indirizzi IPv6 link-local e non-link-local assegnati tramite interscambio di RA Solicitation e RA con routers vicini

Get-Command -Module DHCPServer



DNSv6 (RFC 3596)

Supportato
in WS2008
e succ.

Mapping di un FQDN ad un indirizzo IPv6

Nuovo record Type (28) AAAA di 128 bit
Il record AAAA per il dominio office.com diventa:
office.com. 300 IN AAAA 2a01:111:f406:2402::20

Equivale al
record A in IPv4

Mapping di un indirizzo IPv6 ad un FQDN

Nuovo reverse record domain name ip6.arpa
Il record PTR per l'indirizzo 2001:db8::20:219f:bd8c:17af diventa:
f.a.7.1.c.8.d.b.f.9.2.1.0.2.0.0.0.0.0.0.0.0.0.0.8.b.d.0.1.0.0.2.ipv6.arpa.

Equivale al domain
in-addr.arpa in IPv4

Gestione operativa dell'DNS IPv6

- Per default si esegue il fall back su IPv4 se l'IPv6 non è disponibile
- E' possibile configurare il DNS per restare in ascolto solo sull'IPv6

Get-Command -Module DNSServer

Add-DnsServerPrimaryZone	Get-DnsServerGlobalQueryBlockList
Add-DnsServerResourceRecordAAAA	Get-DnsServerRootHint
Remove-DnsServerResourceRecord	Import-DnsServerRootHint
Get-DnsServerSetting	Add-DnsServerRootHint
Get-DnsClientServerAddress	Remove-DnsServerRootHint
Resolve-DnsName	



Dynamic DNS (DDNS) in Windows

- Il metodo utilizzato per la registrazione automatica varia a seconda che vengano utilizzate le tecnologie di transazione.
- In generale vengono registrati solo indirizzi Unicast Global o Unique Local Address (ULA)
- Se si utilizza ISATAP con un prefisso Global Unicast o Unique Local, questi verranno registrati nel DNS
- Gli indirizzi temporanei, 6to4, Teredo, Loopback e Link-Local per default non sono registrati (è possibile modificare tale comportamento per esempio in scenari DirectAccess)

Altri tipi di Name Resolution

Link-Local Multicast Name Resolution

RFC4795

LLMRN esegue la risoluzione dei nomi single label per host IPv4 e IPv6 sullo stesso link locale sfruttando lo stesso formato dei pacchetti DNS

LLMRN invia messaggi Name Query Request sulla porta UDP 5355 e riceve messaggi Name Query Response sulla porta UDP 5355

I messaggi hanno uno specifico indirizzo multicast di 224.0.0.252 per IPv4 e ff02::1:3 per IPv6

LLMRN è implementato in Windows Vista e successivi

Name Resolution Policy Table

NRPT permette la gestione di speciali richieste di name resolution tramite una tabella di associazioni tra determinati DNS namespaces e specifici DNS server e configurazioni

NRPT è configurabile tramite GPO o registry key

NRPT è implementato in Windows 7 e successivi

Ordine di utilizzo

- 1 NRPT se FQDN
- 2 DNS se FQDN
- 3 LLMRN se Single Label Name
- 4 NetBT se IPv4 e Single Label Name

IPv6 Literals

Semplice modo per specificare un hostname che permettere ad un host Windows Vista o successivo la risoluzione automatica in un indirizzo IPv6

L'hostname si costruisce partendo dall'indirizzo IPv6 sostituendo i : con il - e aggiungendo il suffisso .ipv6-literal.net

Ad esempio l'hostname dell'indirizzo 2001:470:0:11a::403e:a5c5 diventa 2001-470-0-11a--403e-a5c5.ipv6-literal.net

Configurazione Domain Controller in IPv6 only

Configurazione server Domain Controller



1. Disabilitare l'IPv4
2. Impostare un indirizzo IPv6 statico per evitare il warning relativo alla mancanza dell'IP statico impostare un unicast Global (2000::/64), ma è possibile utilizzare anche un indirizzo unicast Unique Local Address (fc00::/64) anche se non viene riconosciuto come indirizzo fisso
3. Promuovere il server a Domain Controller e configurare il DHCP
4. Configurare l'interfaccia IPv6

```
# Configurare il domain controller come un advertising e forwarding IPv6 router
Set-NetIPInterface -InterfaceAlias "Ethernet" -AddressFamily IPv6 -Advertising
Enabled -Forwarding Enabled -OtherStatefulConfiguration Enabled -
AdvertiseDefaultRoute Enabled
```

```
# Consentire l'utilizzo dei protocolli stateful
Set-NetIPInterface -InterfaceAlias "Ethernet" -AddressFamily IPv6 -
ManagedAddressConfiguration Enabled -OtherStatefulConfiguration Enabled
```

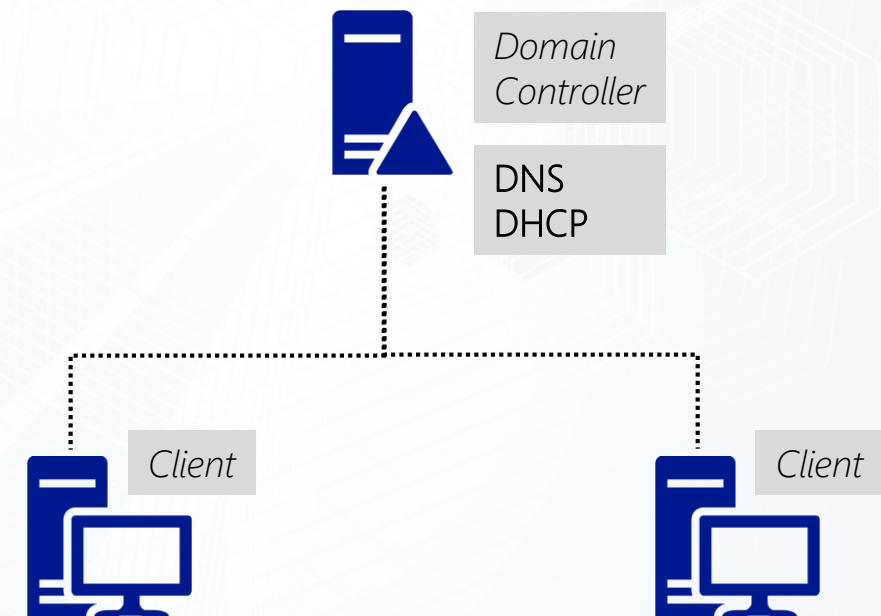
```
# Disabilitazione DHCP
Set-NetIPInterface -InterfaceAlias "Ethernet" -DHCP Disabled
```



Configurazione client



1. Disabilitare l'IPv4
2. Eseguire join a dominio



Demo



Torino
Technologies
Group

ICT  POWER.IT

DNSv6 e DHCPv6



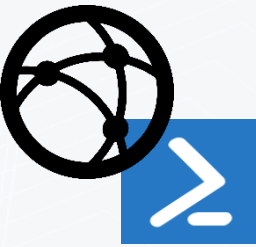
Torino
Technologies
Group

ICT  POWER.IT

Gestione IPv6 tramite PowerShell

Fondamenti e utilizzo del protocollo IPv6 in ambiente Windows

Gestione semplificata dell'IPv6 e IPv4



W8/Ws2012 (PowerShell v3)
introduce i cmdlet per il networking

Get-Command -Module Net*

Non è più necessario utilizzare
esclusivamente **Netsh** o il **registry**
per gestire IPv6

Due cmdlet specifici per IPV6 e
due per IPv4

- **Get-NetIPv6Protocol / Set-NetIPv6Protocol**
- **Get-NetIPv4Protocol / Set-NetIPv4Protocol**

30 cmdlet relativi al TCP/IP
condivisi tra IPv4 e IPv6
(-AddressFamily IPv4 o IPv6)

Get-Command -Module NetTCPIP

Panoramica cmdlets per il networking

Interfacce di rete (64 cmdlets)

Get-NetAdapter
Set-NetAdapter
Disable-NetAdapter
Enable-NetAdapter
Rename-NetAdapter
Restart-NetAdapter

Indirizzamento

Get-NetIPInterface
Set-NetIPInterface
Get-NetIPAddress
New-NetIPAddress
Set-NetIPAddress
Remove-NetIPAddress
Get-NetIPConfiguration

Gestione DNS IPv4 e IPv6

Get-DnsClientServerAddress
Set-DnsClientServerAddress

Tunneling transition technology

Get-Net6to4Configuration
Set-Net6to4Configuration
Reset-Net6to4Configuration
Get-NetIsatapConfiguration
Set-NetIsatapConfiguration
Reset-NetIsatapConfiguration
Get-NetTeredoConfiguration
Get-NetTeredoState
Set-NetTeredoConfiguration
Reset-NetTeredoConfiguration

Routing IPv4 e IPv6

Find-NetRoute
Get-NetRoute
New-NetRoute
Remove-NetRoute
Set-NetRoute

IPsec IPv6 (55 cmdlets)

Show-NetIPsecRule
Get-NetIPsecRule
Enable-NetIPsecRule
Disable-NetIPsecRule
New-NetIPsecRule
Remove-NetIPsecRule
Set-NetIPsecRule

VPN IPv6

Get-VpnConnection
Add-VpnConnection
Remove-VpnConnection
Set-VpnConnection
Set-VpnConnectionProxy

Demo



Torino
Technologies
Group

ICT  POWER.IT

Gestione IPv6 tramite PowerShell



Torino
Technologies
Group

ICT  POWER.IT

Considerazioni sull'adozione dell'IPv6

Fondamenti e utilizzo del protocollo IPv6 in ambiente Windows

Miglioramenti dell'IPv6

Prestazioni



Elaborazione pacchetti più rapida grazie all'Header semplificato (7 campi contro i 13 dell'IPv4)

Scalabilità



Indirizzamento ampliato con 128 bit assegnati in modo gerarchico

Estensibilità



Le extension header consentono di integrare un meccanismo estensibile per nuovi tipi di header e un routing più efficiente

QoS



Supporto integrato del Quality of Service grazie a campo Flow Label dell'header

Sicurezza



IPSec nativo grazie all'integrazione della cifratura (ESP Encapsulating Security Payload) e dell'autenticazione (AH Authentication Header)

Autoconfigurazione



Configurazione automatica dei nodi IPv6 grazie alla Stateless Address Autoconfiguration

Supporto a IPv6 nei prodotti e servizi Microsoft

Prodotto	Completo	Limitato
Exchange	2013	2010/2007
Lync Server	2013	2010
Office	2007 e succ.	
SharePoint Server	2007 e succ.	
SharePoint Foundation	2010 e succ.	
Windows SharePoint Services	3.0	
SQL Server	2005 e succ.	
System Center		2012 R2
Visual Studio	2010 e succ.	
Dynamics AX	2012	
Dynamics CRM	2011	
Dynamics NAV		2009 R2
Dynamics SL	2011	
Dynamics GP	2010	
Internet Explorer	XP SP1 e succ.	
Forefront IM	●	

Servizi	Completo	Limitato
DNS	2008 e succ.	2003
DHCP	2008/Vista e succ.	
IIS	6	
DirectAccess	W7 e succ.	
WSUS	●	
Office 365	2013	
Windows Update	●	
Azure		●

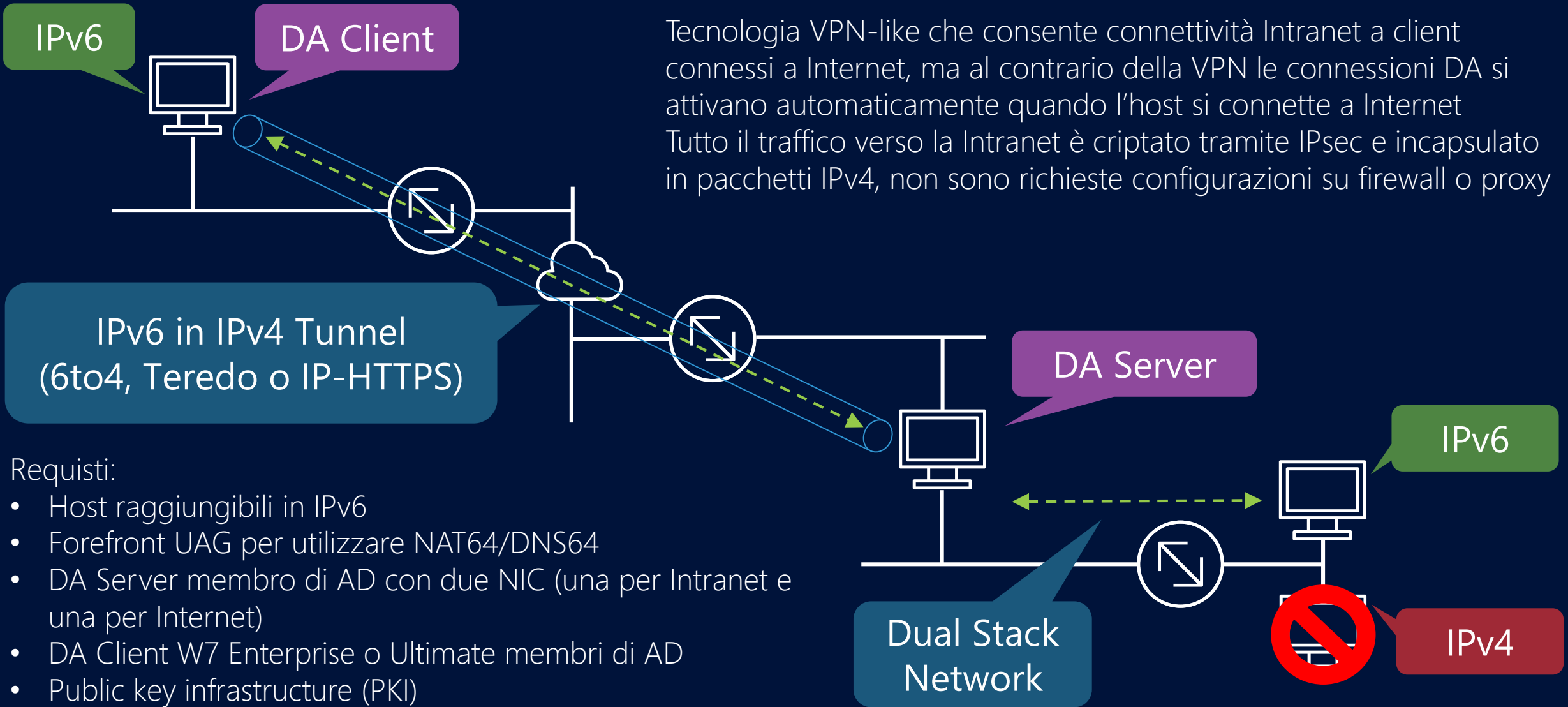
Prodotti senza supporto a IPv6

Forefront TMG
Forefront UAG
Forefront OPE
Microsoft Identity Integration Server
Office Communications Server

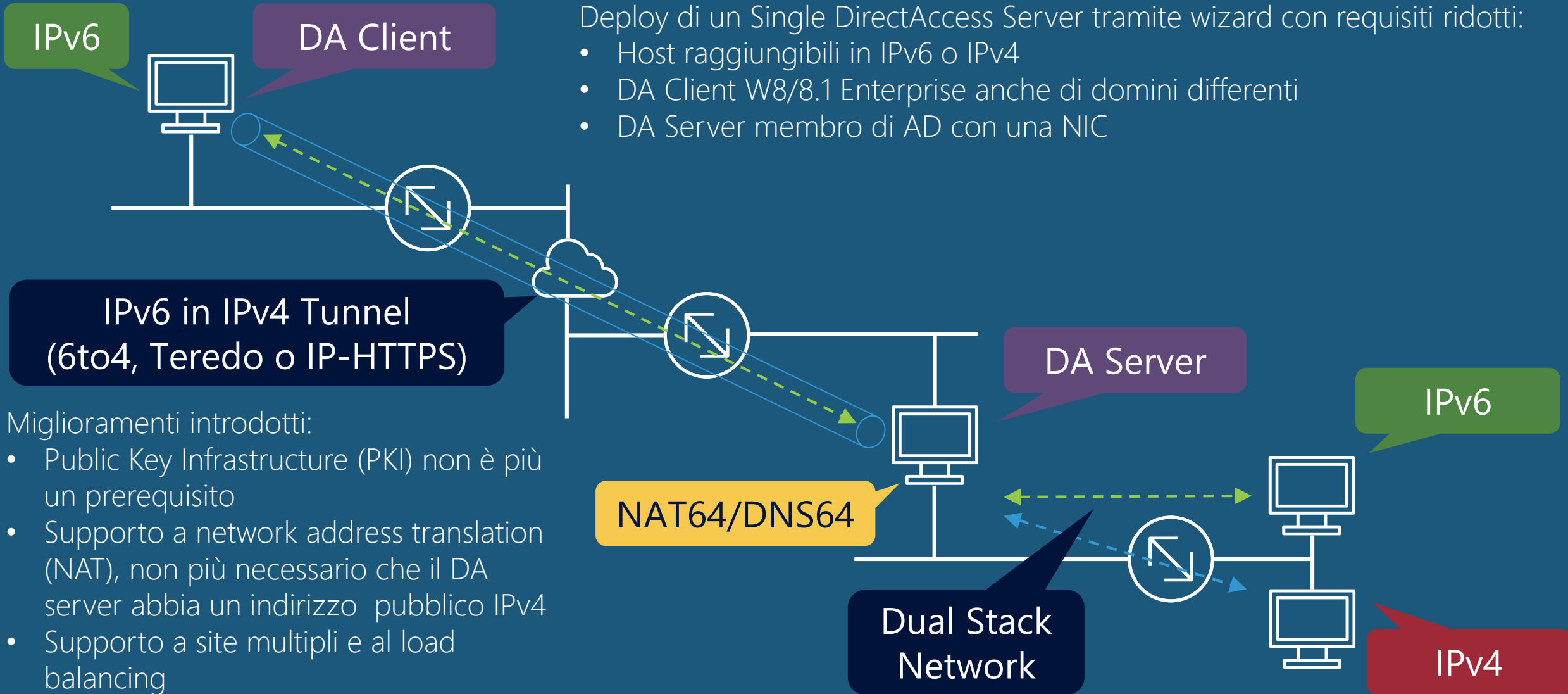
Servizi senza supporto a IPv6

Skype for Business
Azure Active Directory Connect

DirectAccess in Windows 2008 R2 e Windows 7



DirectAccess in Windows 2012 e Windows 8



Sicurezza

Spazio di indirizzamento



Lo spazio di indirizzamento di IPv6 rende il Port-Scanning di una subnet IPv6 quasi impossibile

IPSec



L'Authentication Header rende gli attacchi Man in the middle non praticabili

NAT



L'assenza di NAT e l'addressing gerarchico rende l'anonimato più difficile

SEND



L'utilizzo di SEND permette di evitare risposte falsificate a messaggi di Router Advertisements (RA)

Firewall



Aggiornare o sostituire i device non in grado di gestire IPv6 ed eseguire la DPI (Deep Packet Inspection)

I tunnel Teredo, 6to4 e Isatap possono essere sfruttati per attacchi di tipo cloak perché i pacchetti IPv6 appaiono come traffico IPv4

La funzionalità di cifratura dell'IPv6 può essere sfruttata per sferrare attacchi in tunnel criptati

Rivedere le rule di ingresso e uscita

Parte del traffico ICMPv6 è necessario, ma non tutto

Dual Stack



L'utilizzo contemporaneo di IPv4 e IPv6 nella rete implica un aumento dell'overhead amministrativo relativo alla sicurezza e maggiore vulnerabilità agli attacchi

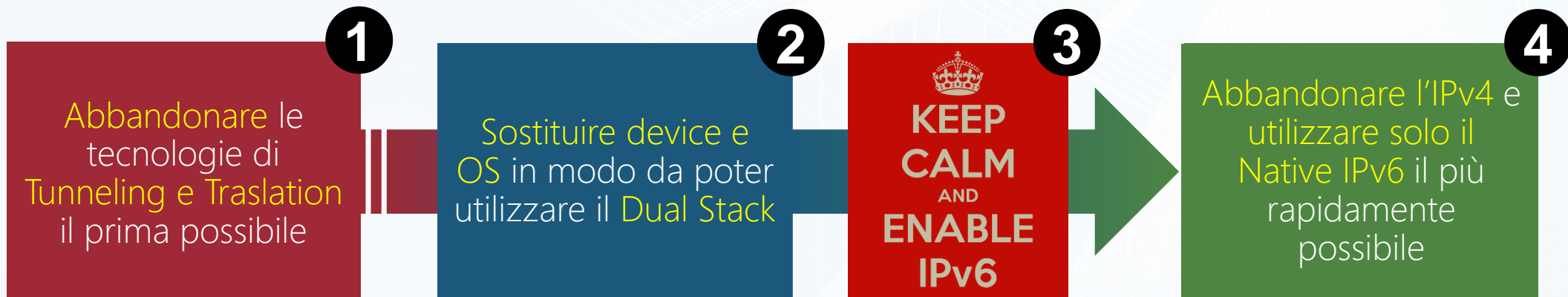
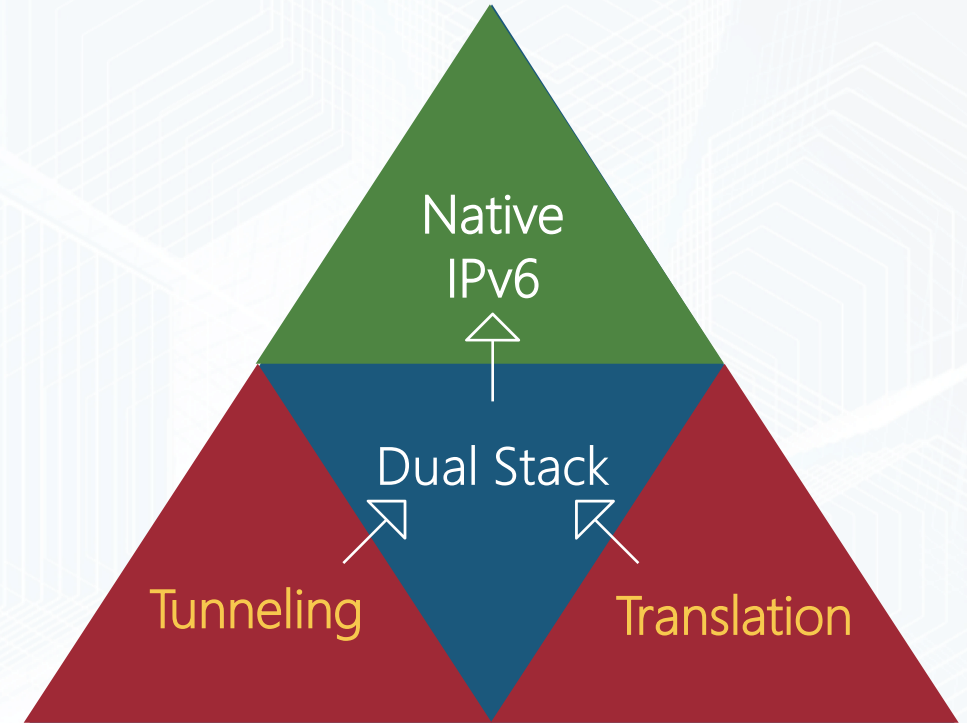
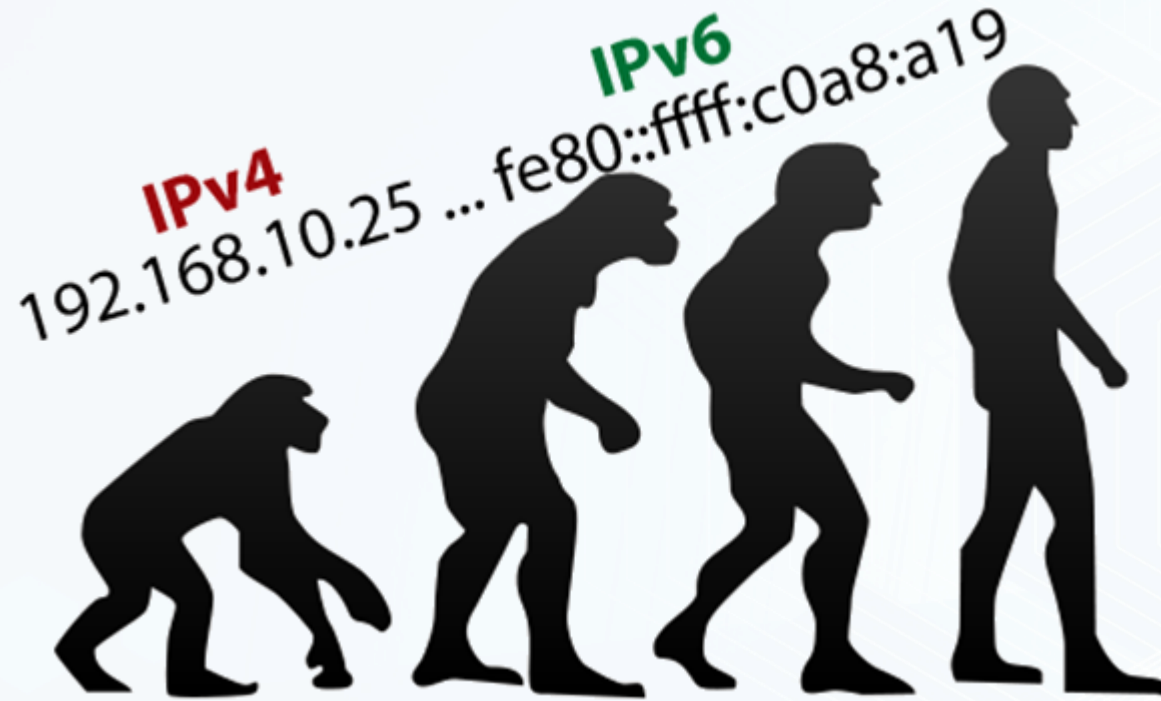
Autoconfigurazione



L'autoconfigurazione degli indirizzi IP può essere sfruttata per definire Rogue Gateway che assegnano IP e realizzano Router IPv6 in grado di analizzare il traffico di rete

Occorre filtrare gli indirizzi interni alla LAN (site-local e multicast specifici) sugli edge routers

Passaggi per la migrazione a IPv6





Torino
Technologies
Group



Question & Answer