Častá překvapení při zavádění IPv6

…aneb „co vám internety neřeknou“

Radek Zajíc, radek@zajic.v.pytli.cz • Den IPv6, 6. 6. 2024

Broken World IPv6 Launch (Vygenerováno pomocí Bing AI)


IPV6

V logách serveru vidím :ffff:192.0.2.1 a IP filtry povolující provoz z 192.0.2.0/24 nefungují!

This incident was the result of an infrastructure change that was made to our load balancers to prepare us for IPv6 enablement of GitHub.com. This change was deployed to a subset of our global edge sites.

The change had the unintended consequence of causing IPv4 addresses to start being passed as an IPv4-mapped IPv6-compatible address to our IP Allow List functionality.

*For example **10.1.2.3** became **::ffff:10.1.2.3**. While our **IP Allow List functionality was developed with IPv6 in mind, it wasn't developed to handle these mapped addresses, and hence started blocking requests as it deemed these to be not in the defined list of allowed addresses**. Request error rates peaked at 0.23% of all requests.*

We have so far identified three remediation items here:

- Update the IP Allow List functionality to handle IPv4-mapped addresses.
- Audit the rest of our stack to confirm there are no further places this IPv4-mapped IPv6 addresses flaw exists.
- Improve our testing and monitoring processes to better catch these issues in the future.

GitHub incident, 01/2024

Když přejdu na IPv6, přinese mi to větší bezpečnost a stabilitu a lepší výkon?

Previously, IPv6 mandated implementation of IPsec and recommended the key management approach of IKE. This document updates that recommendation by making support of the IPsec Architecture [RFC4301] a **SHOULD** for all IPv6 nodes. (**RFC 6434, 12/2011**)

Jakou máte zkušenost s rychlostí a peeringem na ipv6?

Jsem u starnetu (/64) a v ČR ipv6 peering stále nefunguje, latence jsou cca dvoj až trojnásobné oproti ipv4.
Když si udělám speedtest, tak na ipv6 dosahuji cca 2/3 rychlosti ipv4.
Takže člověk si na ipv6 může sáhnout, ale provoz musí primárně přes ipv4.

Na IP4 i IP6 mám stejnou latenci (q.cz). IP6 má poloviční rychlost, Mikrotik neumí pro IP6 hw-offload a visí na CPU. To vyřeší časem nový router.

Dual-Stack je jen dočasným řešením

Dual IP Layer Operation

The most straightforward way for IPv6 nodes to remain compatible with IPv4-only nodes is by providing a complete IPv4 implementation. IPv6 nodes that provide a complete IPv4 and IPv6 implementations are called "IPv6/IPv4 nodes." IPv6/IPv4 nodes have the ability to send and receive both IPv4 and IPv6 packets. They can directly interoperate with IPv4 nodes using IPv4 packets, and also directly interoperate with IPv6 nodes using IPv6 packets. (RFC 2893, **Transition Mechanisms for IPv6 Hosts and Routers**, 08/2000)

Potřebujeme tedy (doma) ještě vůbec IPv4?

Do We Need IPv4 at Home/SOHO Any More?

By **Torbjörn Eklöv**
Senior Network Architect, DNSSEC/IPv6

May 02, 2024 | Views: 6,669 | Add Comment

~~Short answer: No!~~

It depends.

(Mostly we do.)

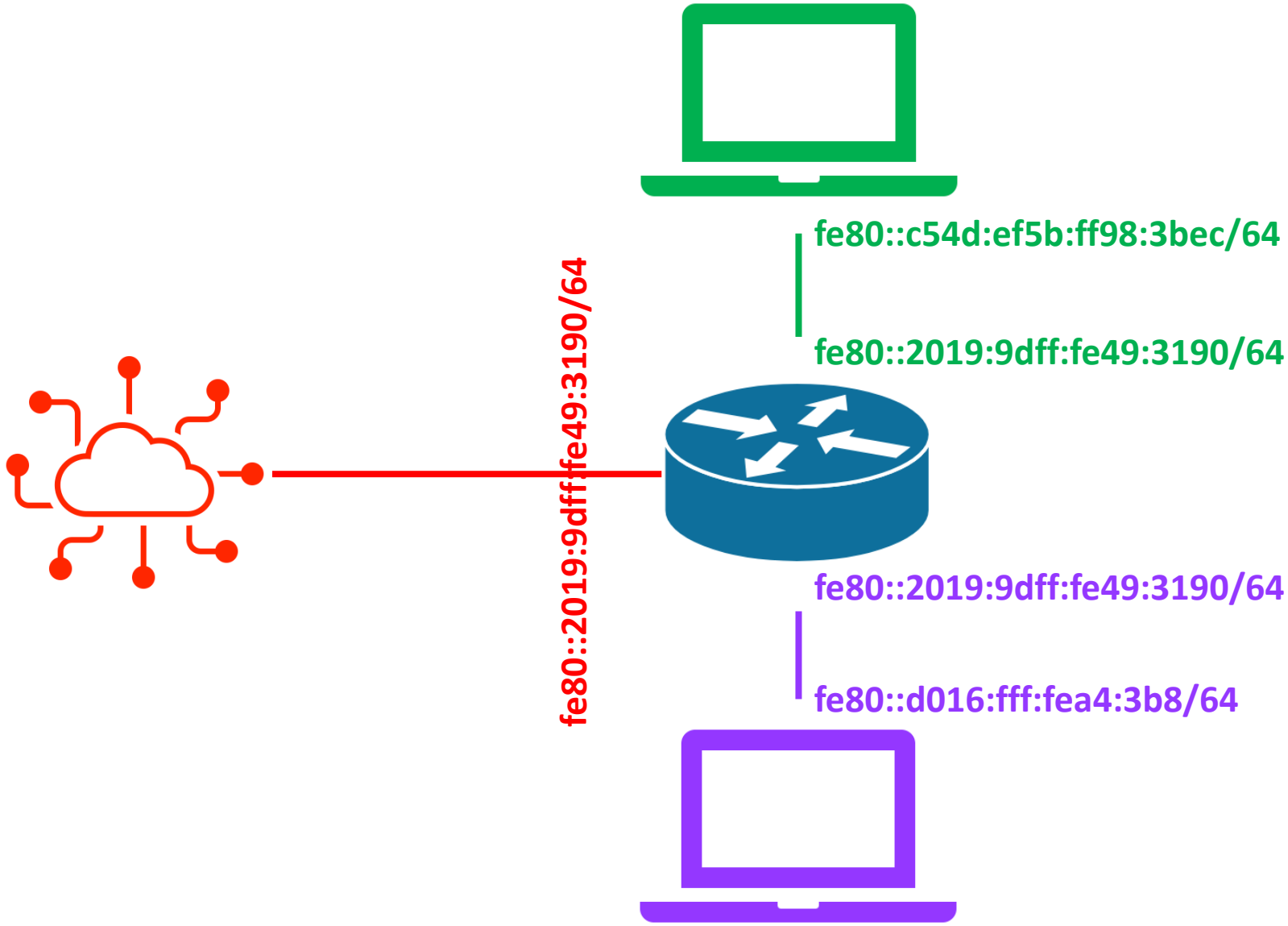
https://circleid.com/posts/20240502-do-we-need-ipv4-at-home-soho-any-more

„Mám IPv6“

I found this on my phone and was hoping someone can explain it to me. This is listed under Ipv6 on my wifi network. Can anyone tell me it it's legit?

Fe80::20:e2ff:fe1a:1996%dummy0. It just doesn't look right.

Provoz z link-local adres neprochází routerem do dalších sítí



„Mám IPv6“ – 6to4 (2002::/16)

U firemního tarifu (ne business) je společně s veřejnou pevnou IPv4 už IPv6 nějakou dobu taky, a to jako tunel 6to4. Což funguje v pohodě.

6to4 nepoužívá jenom Vodafone, ale třeba taky Nej.cz, takže byť k tomu může mít člověk výhrady, tak to zase není až tak ojedinělá věc.

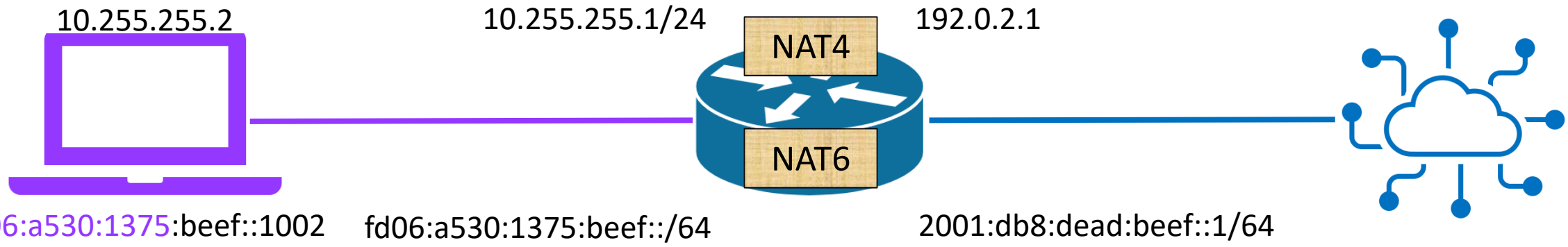
Mám IPv6?

- Máte adresy z globálně routovatelného unicast (GUA) IPv6 rozsahu (adresy z rosahu 2000::/3, tj. začínající dvojkou nebo trojkou)
- Adresy jsou registrované na konkrétního ISP (tj. ne Teredo ani 6to4)
- Máte funkční konektivitu do IPv6 Internetu
- Provoz mezi vaší sítí a Internetem může procházet ručně spravovaným tunelem (např. 6in4, 6rd, OpenVPN, Wireguard od vpsFree)
- Pro kvalitu služby je zpravidla lepší, když je cesta IPv4 a IPv6 paketů od vás stejná (nativní konektivita bývá lepší než tunel)

Mám IPv6?

- Pokud používáte adresy z globálně NEroutovatelného IPv6 rozsahu, tj. typicky ULA (fc00::/7, zpravidla fdXX:XXXX:XXXX::/48), nemáte globálně routovatelnou (plnohodnotnou) IPv6 konektivitu
- ULA jsou adresy pro „vnitřní použití“ v rámci vaší infrastruktury
- 40 bitů označených jako „X“ by mělo být celosvětově unikátních, zaregistrovat si je můžete třeba v neoficiálním registru https://ula.ungleich.ch/, vygenerovat na https://unique-local-ipv6.com/
- Mají v dual-stack sítích nižší prioritu než IPv4 i než globálně routovatelné IPv6
- ULA mohou koexistovat s GUA, hodí se např. pro případy, kdy potřebujete stabilní interní adresu nějaké služby, když GUA může „zmizet“

Tedy když mám LAN 10.255.255.0/24, mám pro IPv6 použít ULA?



`10.255.255.2 <-> 142.251.36.100`

`192.0.2.1 <-> 142.251.36.100`

`fd06:a530:1375:beef::1002 <-> 2a00:1450:4014:80e::2004`

`2001:db8:dead:beef::1 <-> 2a00:1450:4014:80e::2004`

- ULA jsou adresy pro „vnitřní použití“ v rámci vaší infrastruktury
- Mají v dual-stack sítích nižší prioritu než IPv4 i než globálně routovatelné IPv6
- Nepoužívá se NAT z IPv6 do IPv6

Takže v IPv6 není NAT?

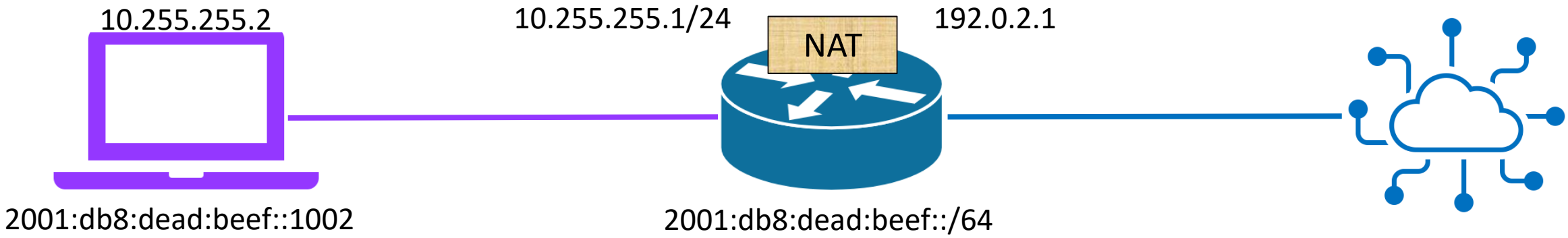
- V IPv6 je spousta druhů NATu!
  - NAT64 pro přístup z IPv6 do IPv4 sítí
  - NPTv6 překládá IPv6 blok A na IPv6 blok B
  - NAT46 zpřístupňující IPv4 strojům vybrané IPv6 prostředky
  - IPv6 DNAT, remapující cílovou adresu
  - IPv6 SNAT 1:1, překládající pakety s jednou IPv6 adresou na jinou IPv6 adresu
  - IPv6 maškaráda 1:M, „schová“ víc různých strojů s IPv6 adresami za jednu (jinou) vybranou IPv6 adresu

NAT64 je přechodový mechanismus, zbavující koncové sítě závislosti na IPv4

NPTv6 pomáhá v konfiguracích „záložního připojení“

NAT46 a DNAT se používají v load balancerech

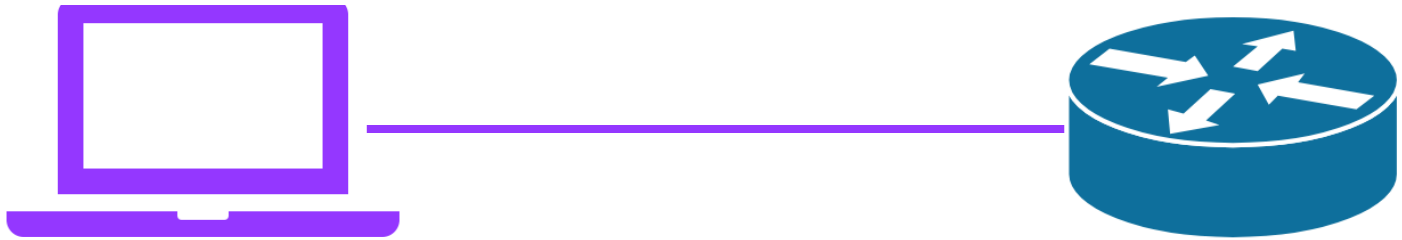
Tedy když mám LAN 10.255.255.0/24, mám pro IPv6 použít GUA?




```
10.255.255.2 <-> 142.251.36.100
  192.0.2.1 <-> 142.251.36.100
2001:db8:dead:beef::1002 <-> 2a00:1450:4014:80e::2004
```

- Provoz z počítače do Internetu jde skrze router, ale na routeru se pakety nemění. Adresa počítače zůstává viditelná i pro server v Internetu.
- Router má zpravidla i svou WAN adresu (ekvivalent 192.0.2.1), ale obvykle ji nemusíte zjišťovat, nepotřebujete ji

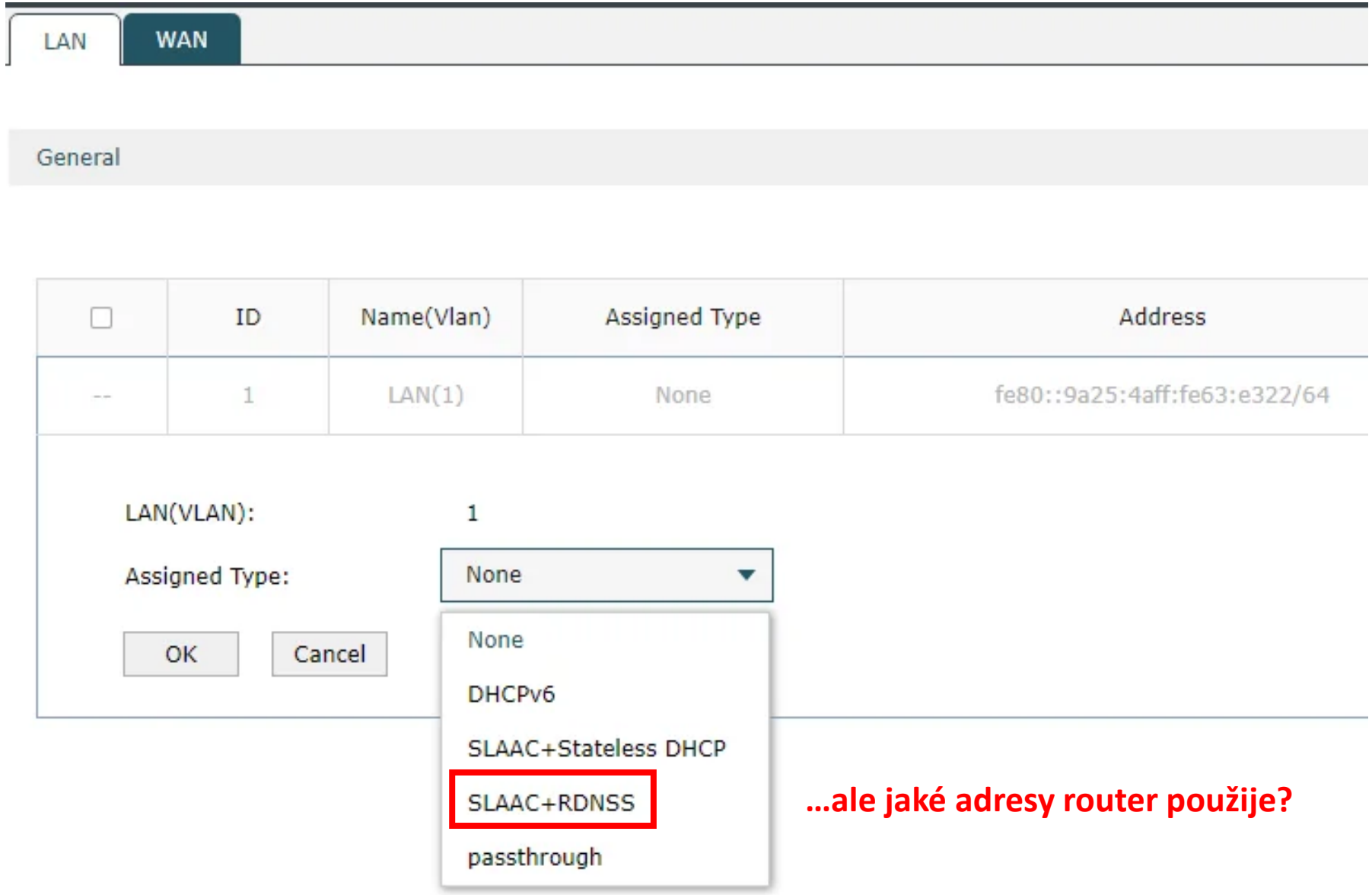
Globální, lokální a link-local adresy na jedné síti společně…?



2001:db8:dead:beef:b0b3:216f:6d48:5aa9
fd06:a530:1375:ceed:b0b3:216f:6d48:5aa9
fe80::b0b3:216f:6d48:5aa9

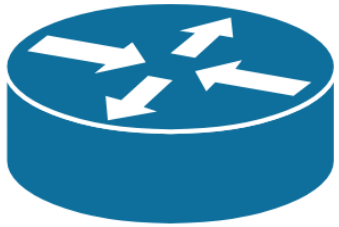
2001:db8:dead:beef::1
fd06:a530:1375:ceed::1
fe80::f89f:2971:302d:859e

Přidělování IPv6 adres v LAN: What a mess!

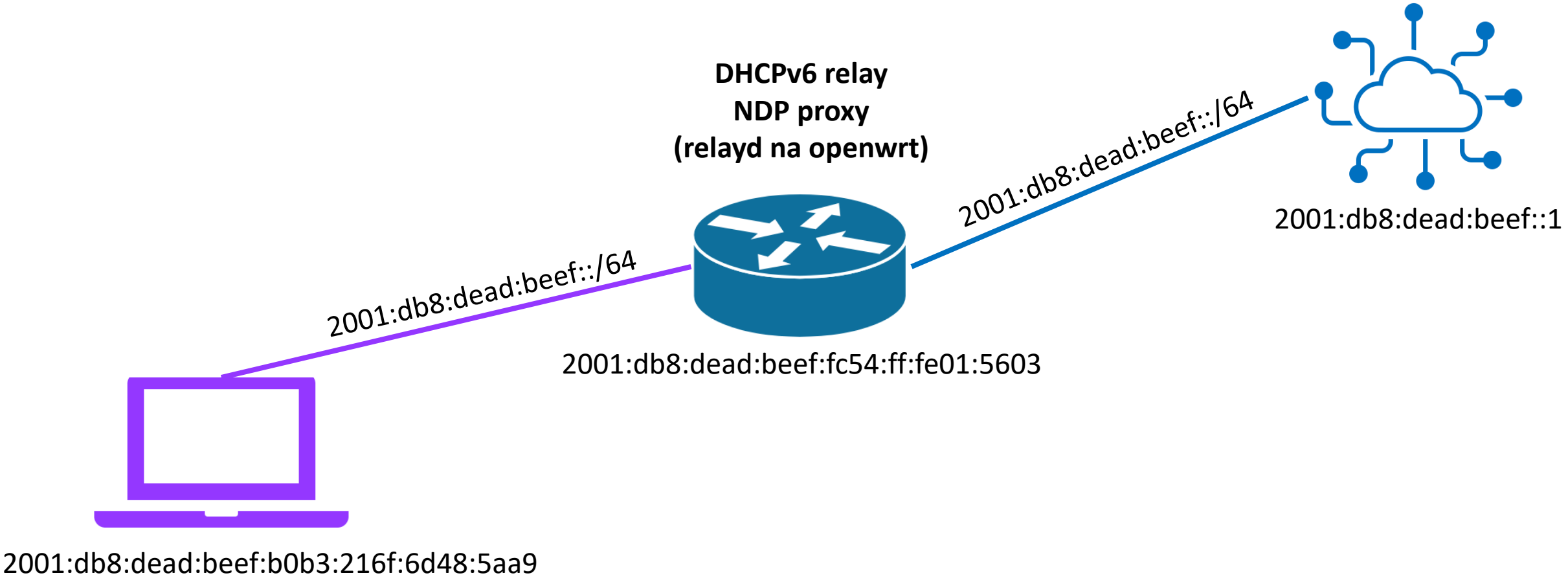


…ale jaké adresy router použije?

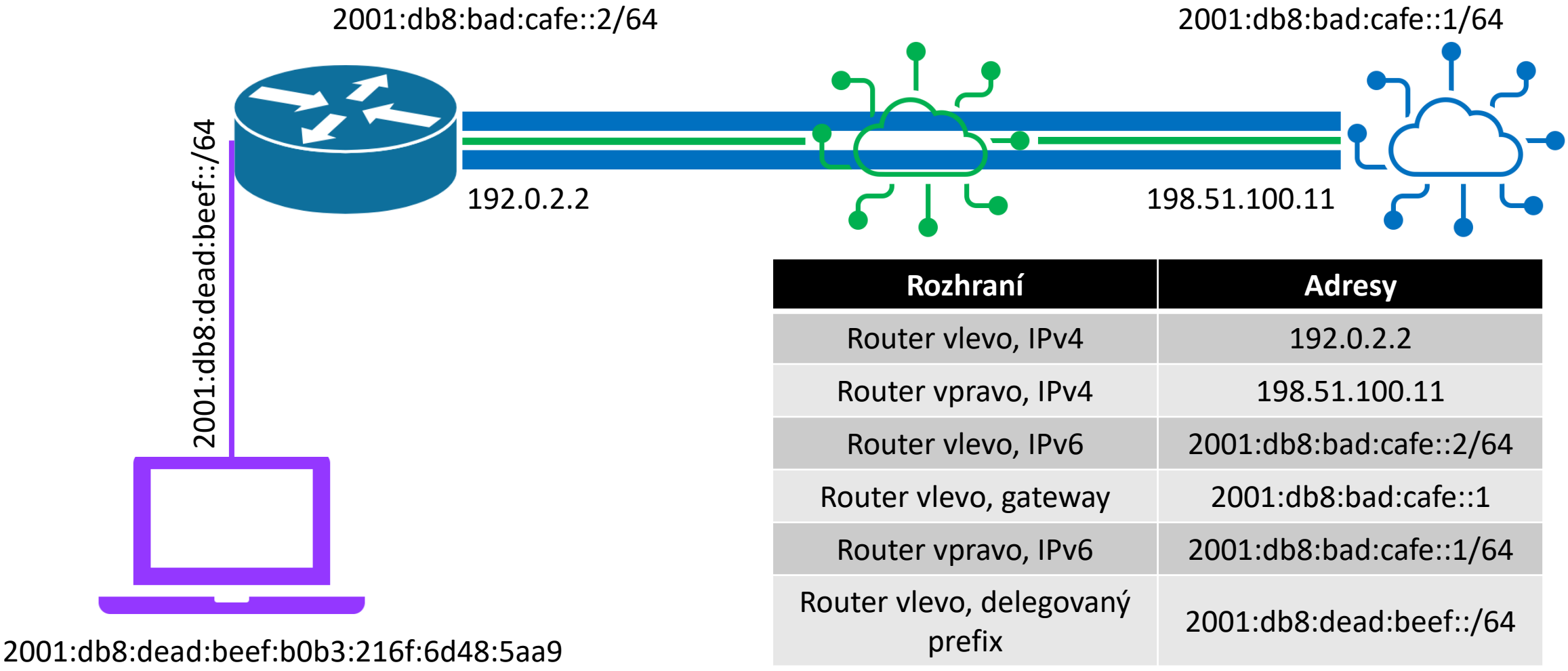
IPv6 WAN: Mezi námi routery



IPv6 WAN: Mezi námi routery: Passthrough



IPv6 WAN: Mezi námi routery: 6in4, 6rd

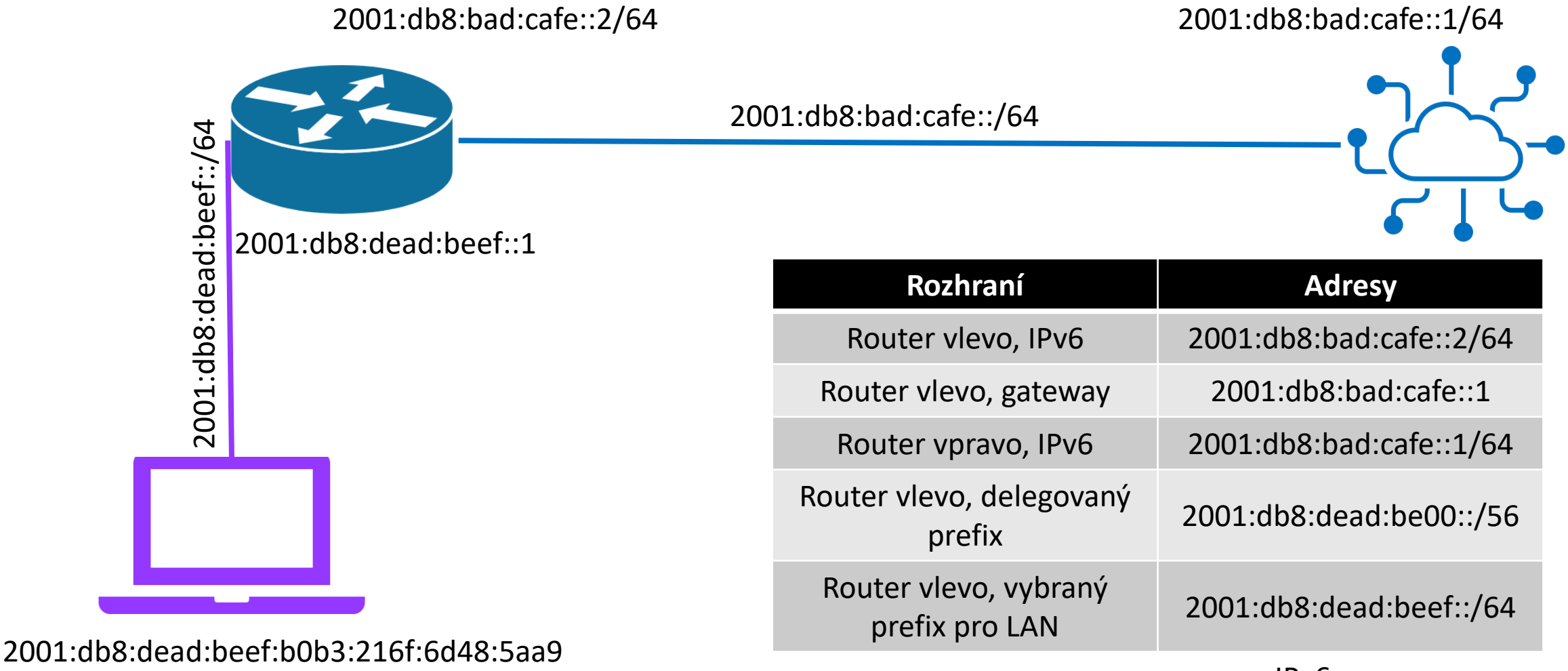


Rozhraní	Adresy
Router vlevo, IPv4	192.0.2.2
Router vpravo, IPv4	198.51.100.11
Router vlevo, IPv6	2001:db8:bad:cafe::2/64
Router vlevo, gateway	2001:db8:bad:cafe::1
Router vpravo, IPv6	2001:db8:bad:cafe::1/64
Router vlevo, delegovaný prefix	2001:db8:dead:beef::/64

IPv6 tunel IPv4 Internetem

IPv4 provoz

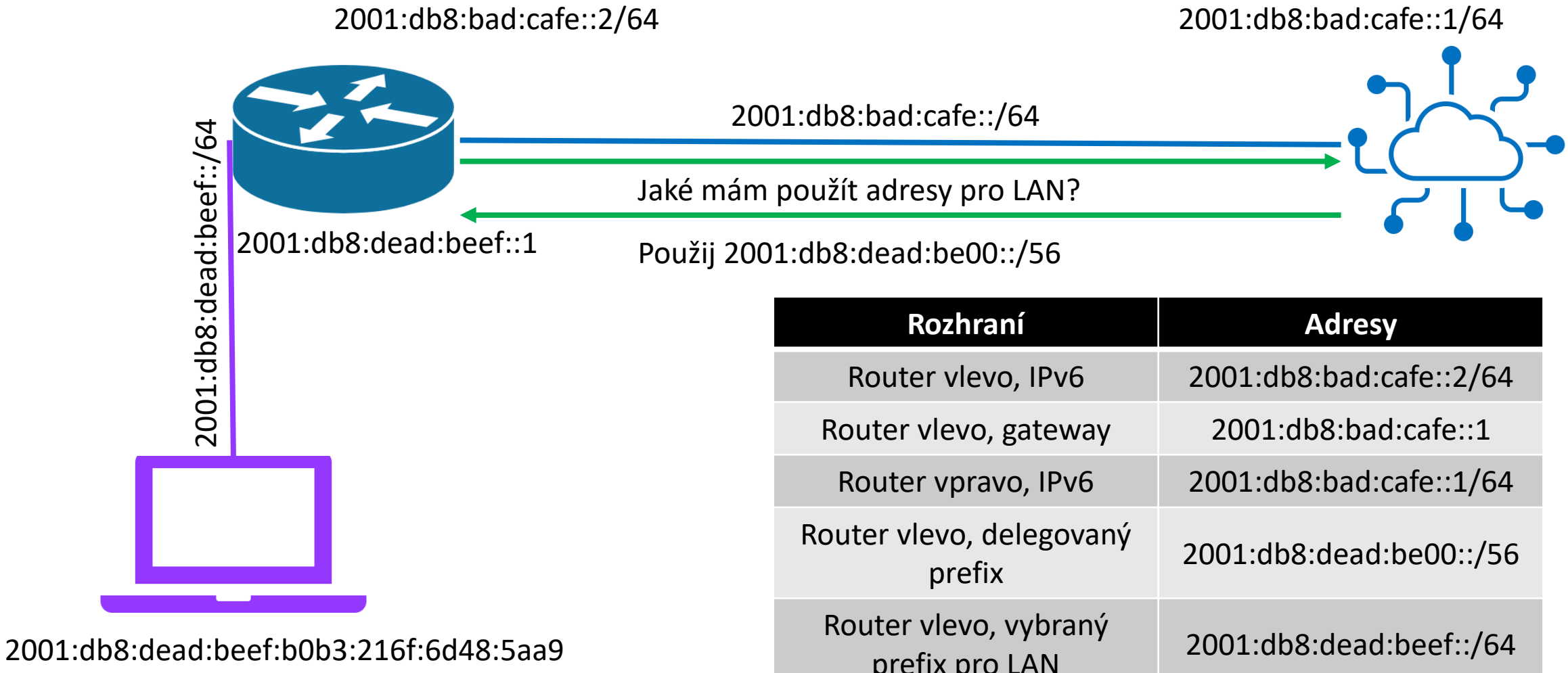
IPv6 WAN: Mezi námi routery: Static



Rozhraní	Adresy
Router vlevo, IPv6	2001:db8:bad:cafe::2/64
Router vlevo, gateway	2001:db8:bad:cafe::1
Router vpravo, IPv6	2001:db8:bad:cafe::1/64
Router vlevo, delegovaný prefix	2001:db8:dead:be00::/56
Router vlevo, vybraný prefix pro LAN	2001:db8:dead:beef::/64

IPv6 provoz

IPv6 WAN: Mezi námi routery: Native (DHCPv6 PD)



Rozhraní	Adresy
Router vlevo, IPv6	2001:db8:bad:cafe::2/64
Router vlevo, gateway	2001:db8:bad:cafe::1
Router vpravo, IPv6	2001:db8:bad:cafe::1/64
Router vlevo, delegovaný prefix	2001:db8:dead:be00::/56
Router vlevo, vybraný prefix pro LAN	2001:db8:dead:beef::/64

IPv6 provoz

DHCPv6 získání prefixu

Jak si router vybere adresy pro LAN?

Pokud je delegovaný prefix od ISP 2001:db8:dead:be00::/56…

…jak si můj router vybere blok adres pro svou LAN?

2001:db8:dead:be00::/64

..

2001:db8:dead:beff::/64

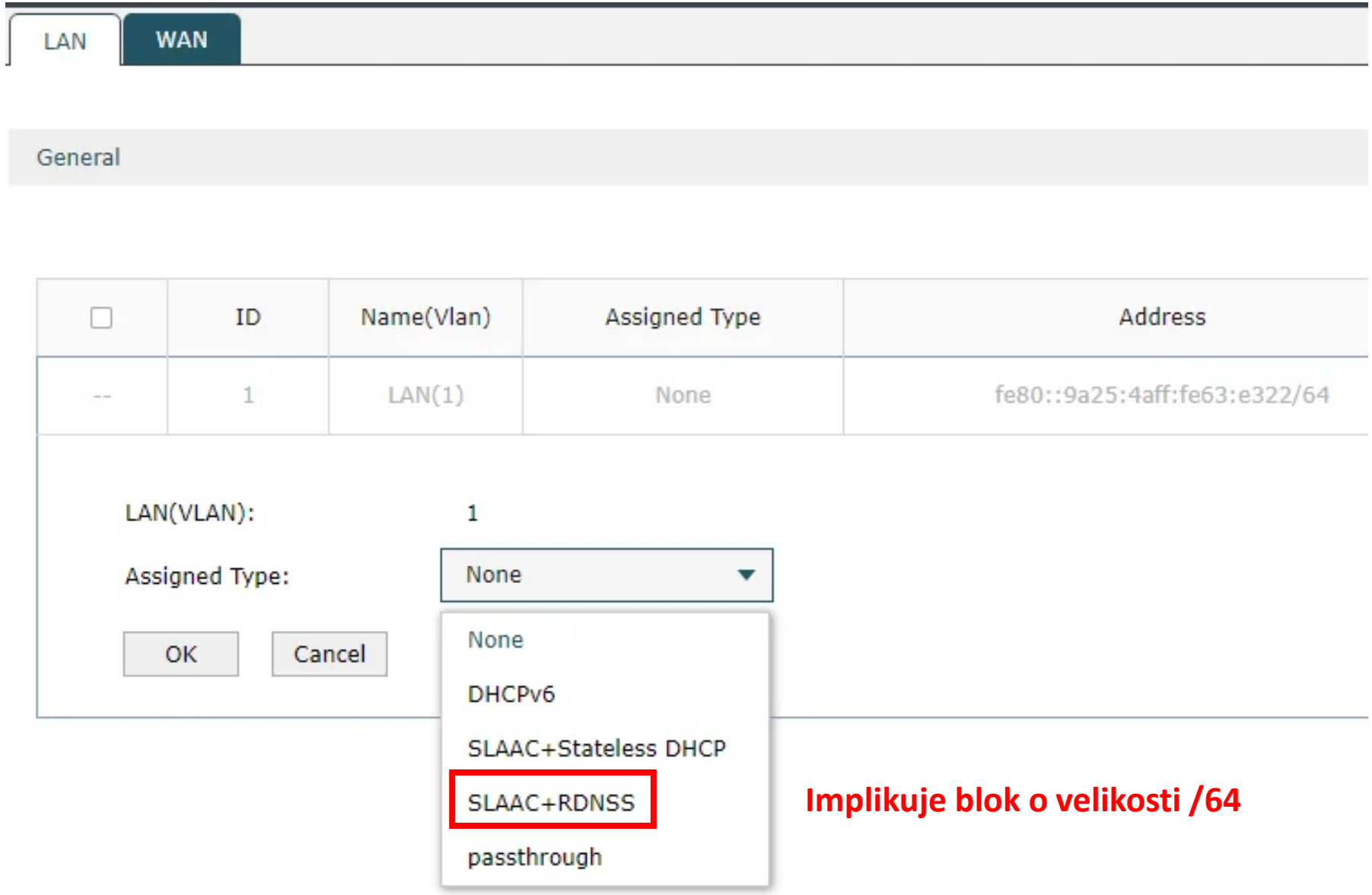
A co pro 2001:db8:dead:0000::/48?

2001:db8:dead:0000::/64

..

2001:db8:dead:ffff::/64

Přidělování IPv6 adres v LAN: What a mess!



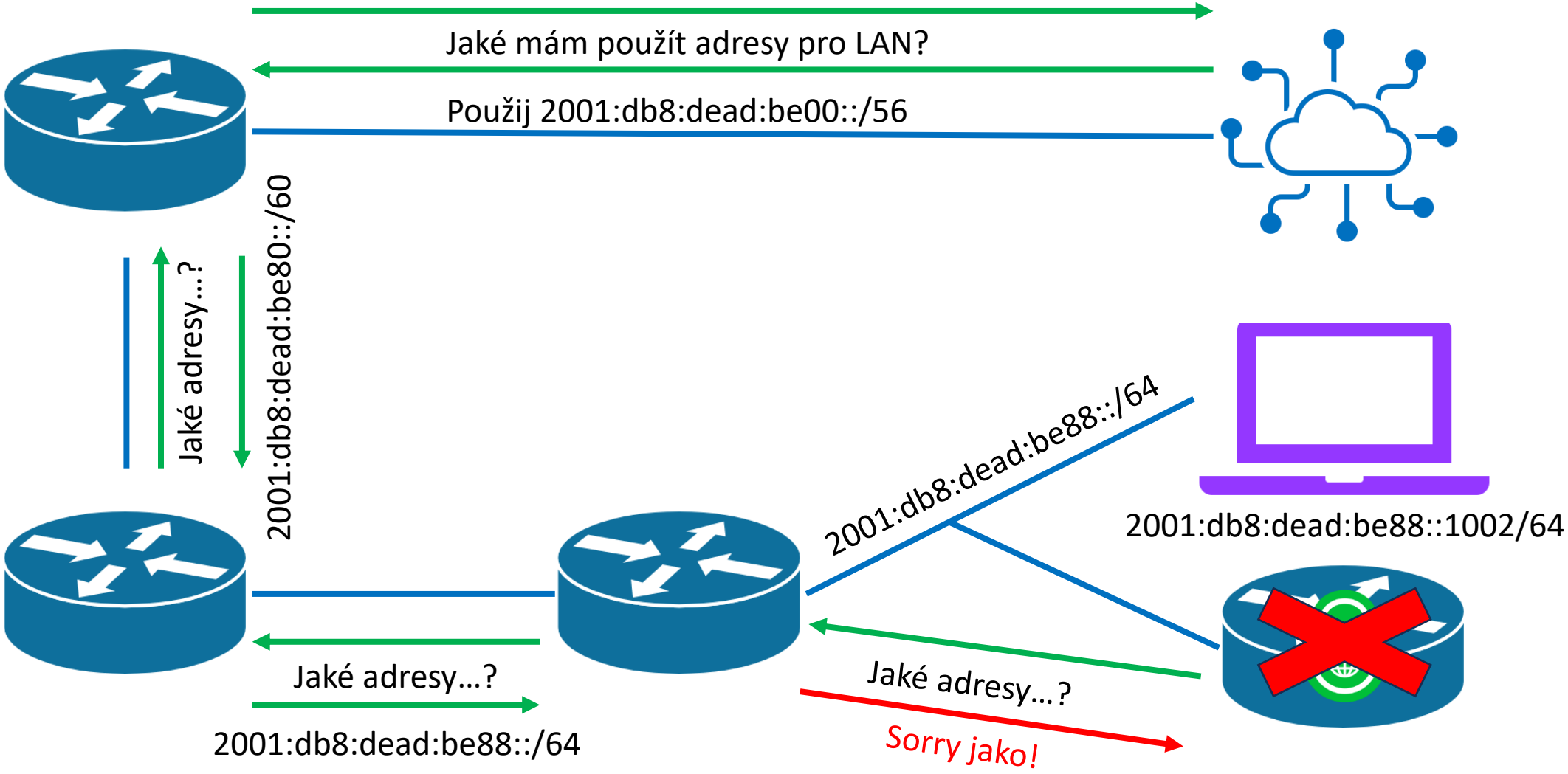
Implikuje blok o velikosti /64

Můžu použít „menší“ (nebo „větší“) blok než /64? Kdy? Jak to funguje?

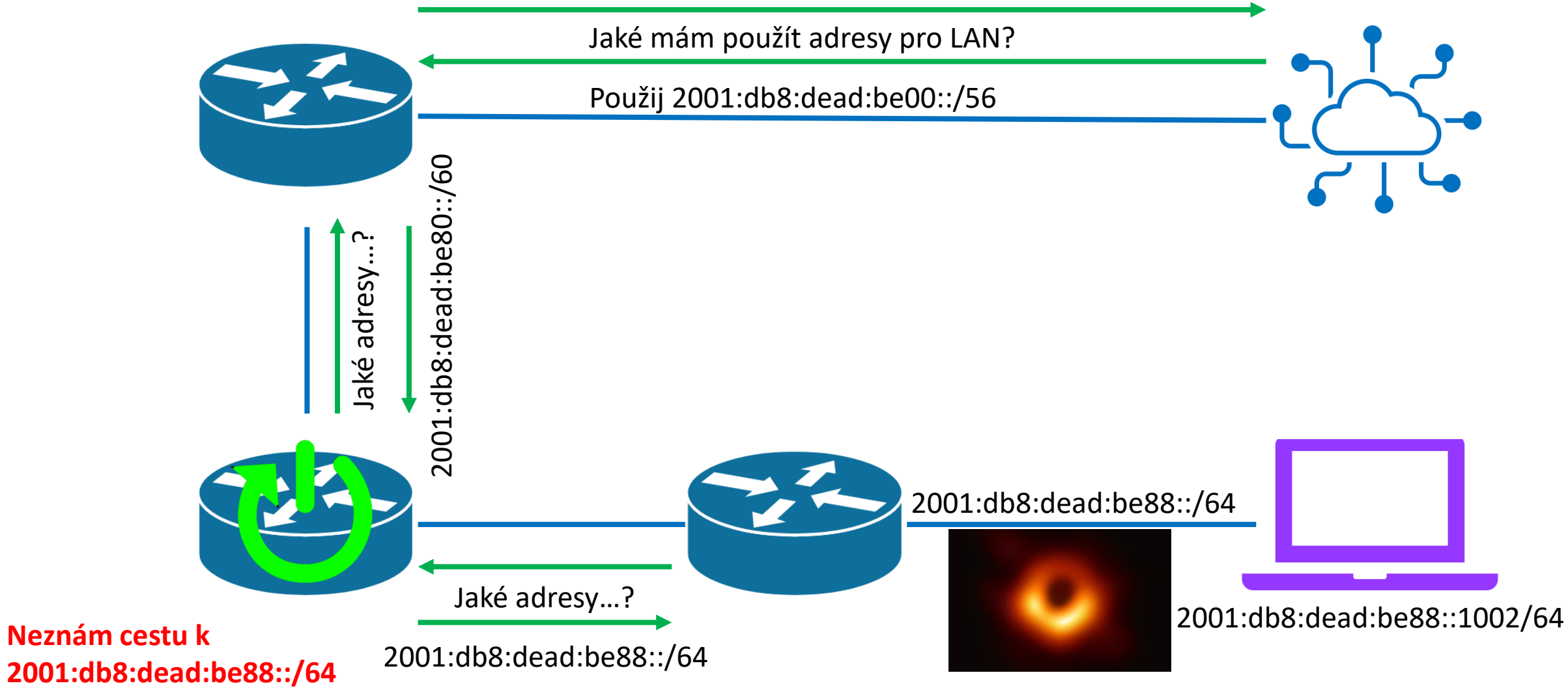
Ano!

(Kdykoli se nepoužívá SLAAC.)

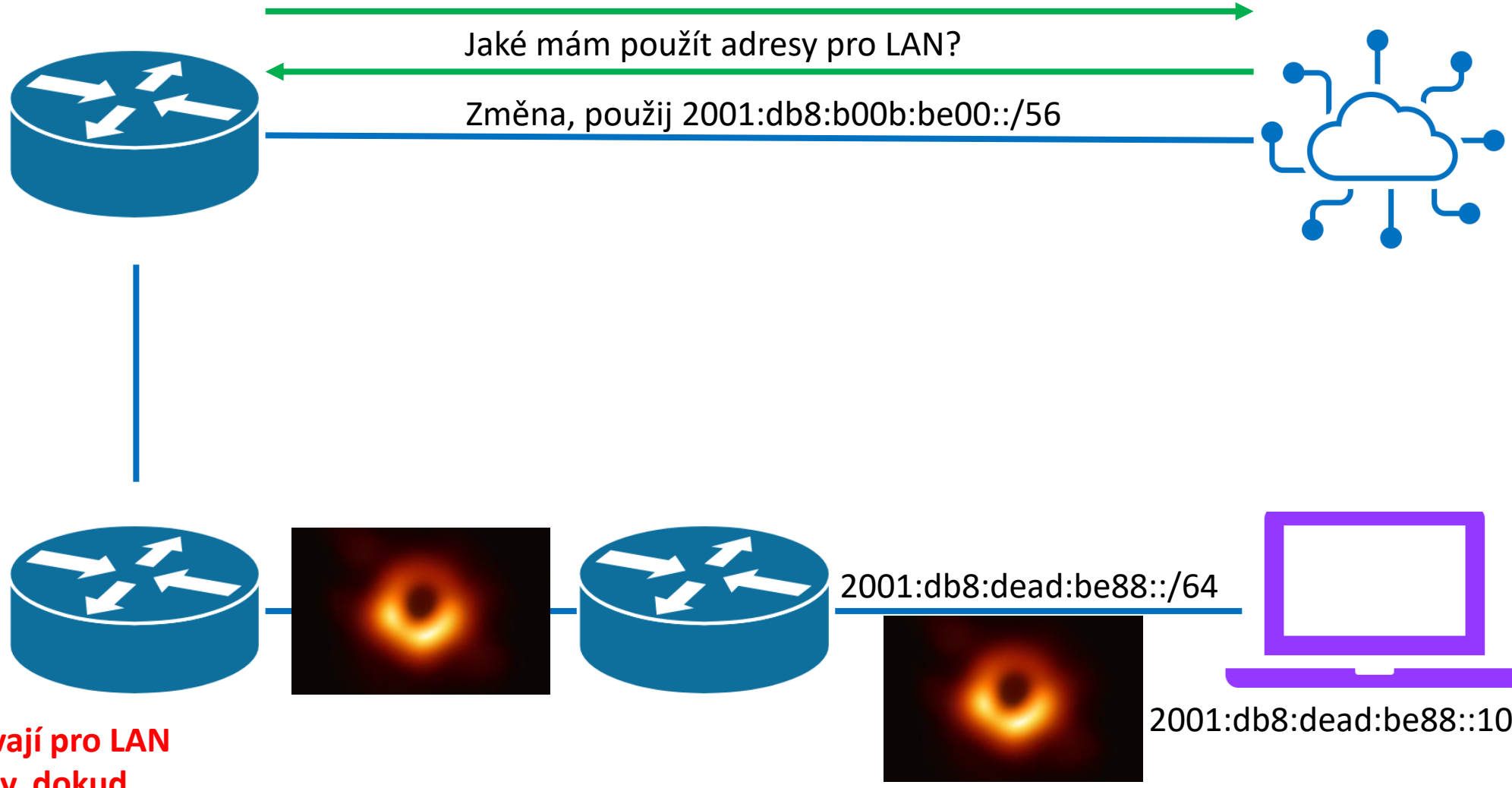
Delegujeme, delegujeme



Delegujeme, delegujeme: reboot routeru



Delegujeme, delegujeme: změna prefixu



R2 a R3 používají pro LAN původní adresy, dokud nevyprší „lease time“

Přišel čas NAT?

Otázky ke změnám prefixů

Když změním ISP, dostanu pro svou LAN tedy nové adresy? Podobně když mě ISP přečísluje? V IPv4 se obvykle mění jen veřejná IPv4 adresa a statické příděly v LAN zůstávají.

Pokud nastavím firewall podle aktuálních prefixů a adresy se mi změní, znamená to, že budu muset celou konfiguraci firewallu předělávat?

A nemůžu si radši nechat LAN na IPv4 a IPv6 použít jen na WAN (od routeru do Internetu)?

Když se v IPv6 nepoužívá NAT, potřebujeme ještě connection tracking? A firewall?

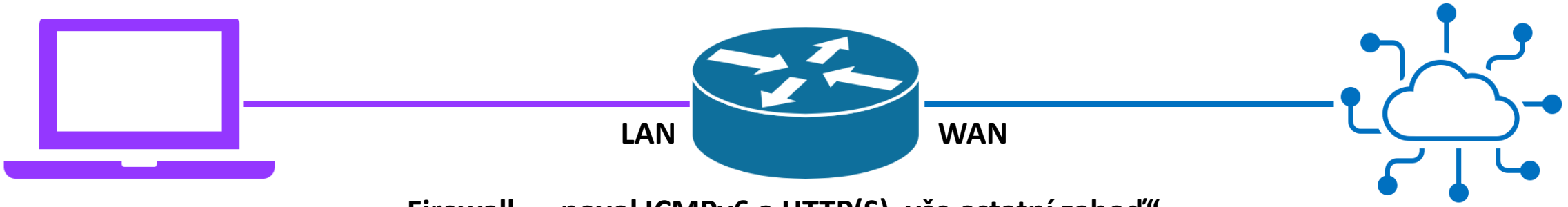
When IPv6 "happens" will most installation be expected not to use NAT ? (and the built-in security block that it represents)

What is being done to mitigate the side effect of retoring the "end-to-end" principle ?

Will there be no NAT, but every router will by default block all inbound connections to simulate how things are on IPv4 plus NAT ?

Will I have to remind my grandmother to remember to set her pre-routing inbound firewall policy to "block" ?

Když se v IPv6 nepoužívá NAT, potřebujeme ještě connection tracking? A firewall?



Firewall – „povol ICMPv6 a HTTP(S), vše ostatní zahoď“

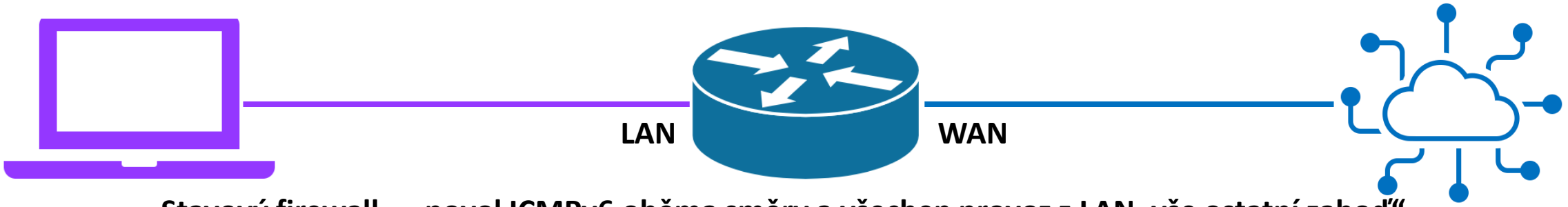
Zdroj	Cíl	Protokol	Zdrojový port	Cílový port	Akce
LAN	WAN	TCP	Libovolný	80 nebo 443	Povolit
WAN	LAN	TCP	80 nebo 443	Libovolný	Povolit
Libovolný	Libovolný	ICMPv6	(n/a)	(n/a)	Povolit
Libovolný	Libovolný	Libovolný	Libovolný	Libovolný	Zakázat

Co se stane, když z Internetu zkusíte navázat spojení z portu 80/tcp na port 22/tcp cíle v LAN?

Problémy tohoto (bezestavového) firewallu:

- Složitá konstrukce pravidel (nutno zadávat oba směry)
- Průstřelný

Když se v IPv6 nepoužívá NAT, potřebujeme ještě connection tracking? A firewall?

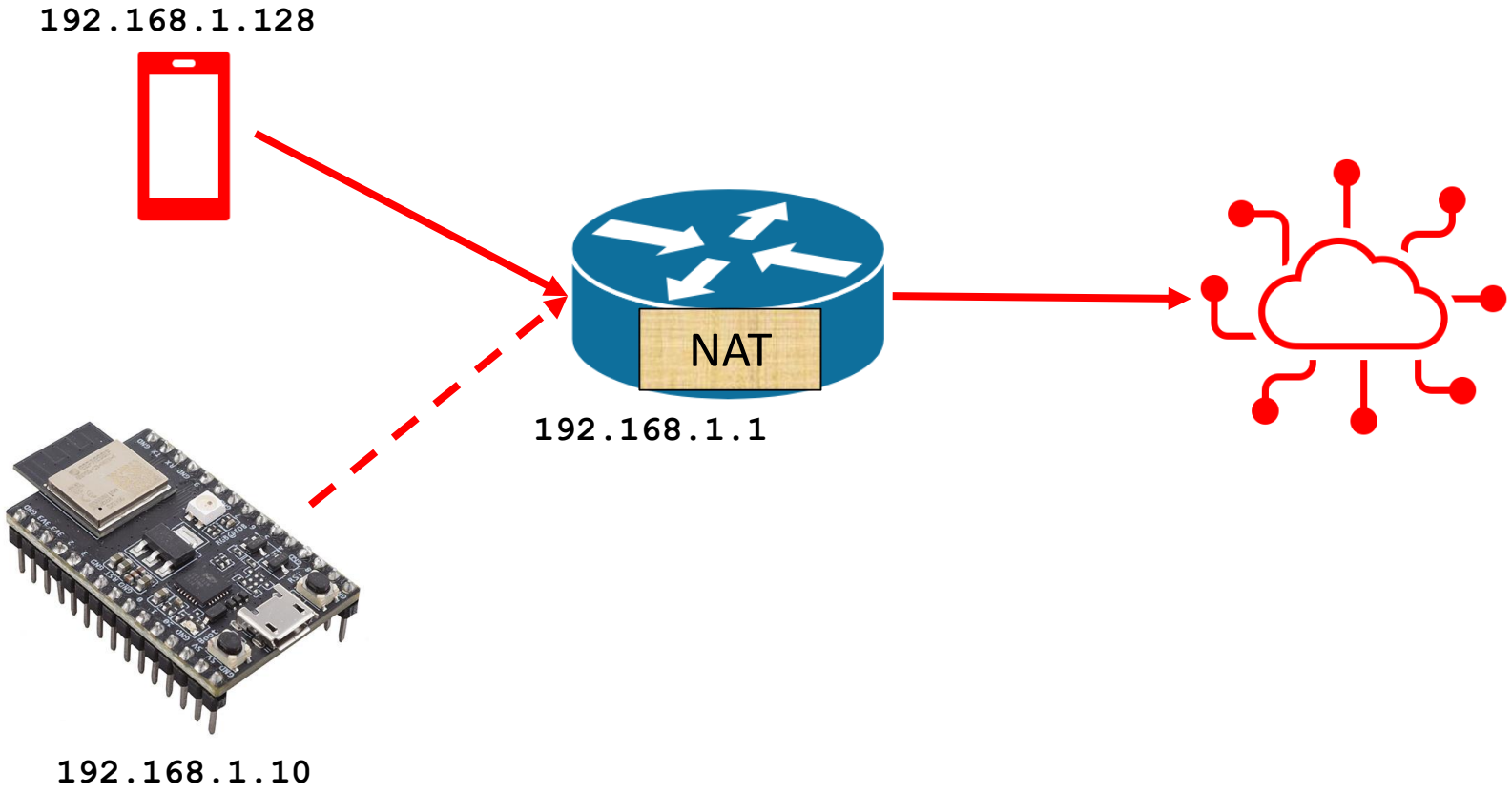


Stavový firewall – „povol ICMPv6 oběma směry a všechen provoz z LAN, vše ostatní zahoď“

Zdroj	Cíl	Protokol	Zdrojový port	Cílový port	Stav	Akce
LAN	WAN	Libovolný	Libovolný	Libovolný	Libovolný	Povolit
WAN	LAN	Libovolný	Libovolný	Libovolný	Neplatný	Zakázat
WAN	LAN	Libovolný	Libovolný	Libovolný	Odpověď na „spojení“ iniciovaná z LAN	Povolit
Libovolný	Libovolný	ICMPv6	(n/a)	(n/a)	Libovolný	Povolit
Libovolný	Libovolný	Libovolný	Libovolný	Libovolný	Libovolný	Zakázat

Co se stane nyní, když z Internetu zkusíte navázat spojení z portu 80/tcp na port 22/tcp cíle v LAN?

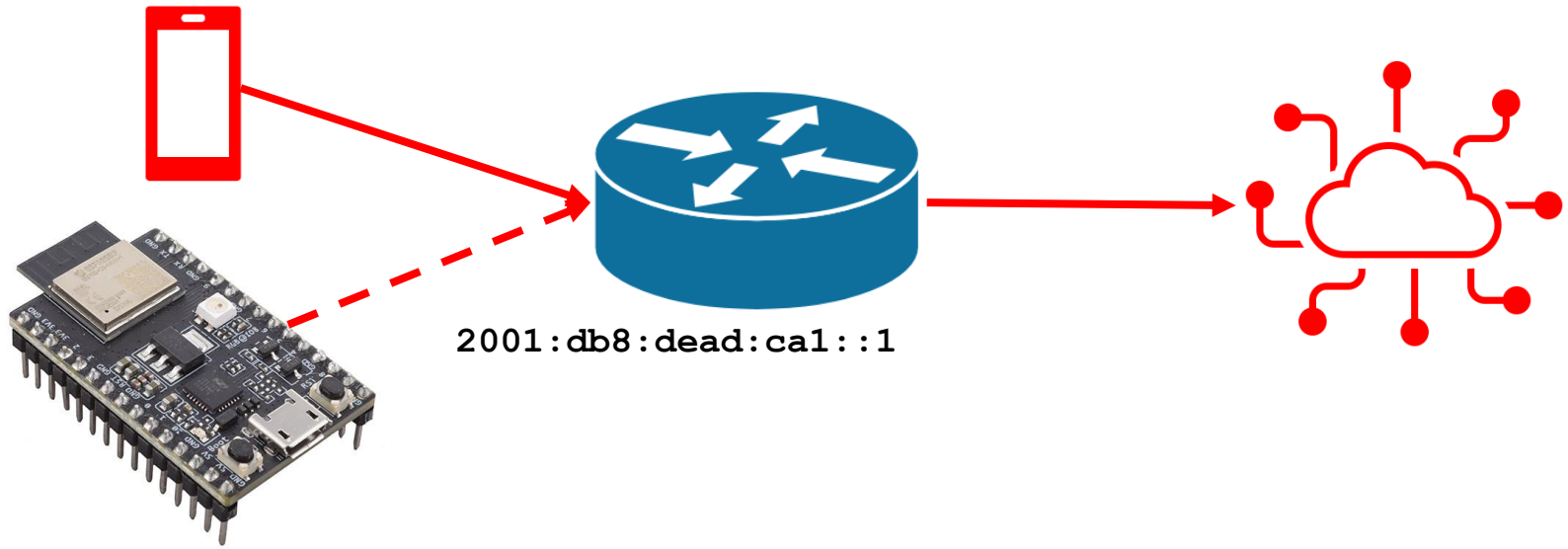
A když chci omezit Internet jen pro některá zařízení v LAN?



IP LAN	IP Internet	Firewall
192.168.1.128/25	Kamkoli	**Povolit**
192.168.1.10	Kamkoli	**Zakázat**

A když chci omezit Internet jen pro některá zařízení v LAN?

2001:db8:dead:ca1:3c4e:984a:ff5d:4245
2001:db8:dead:ca1:f84d:3d87:47de:7715



2001:db8:dead:ca1::1

2001:db8:dead:ca1:3c4e:984a:ff5d:4245
2001:db8:dead:ca1:f84d:3d87:47de:7715

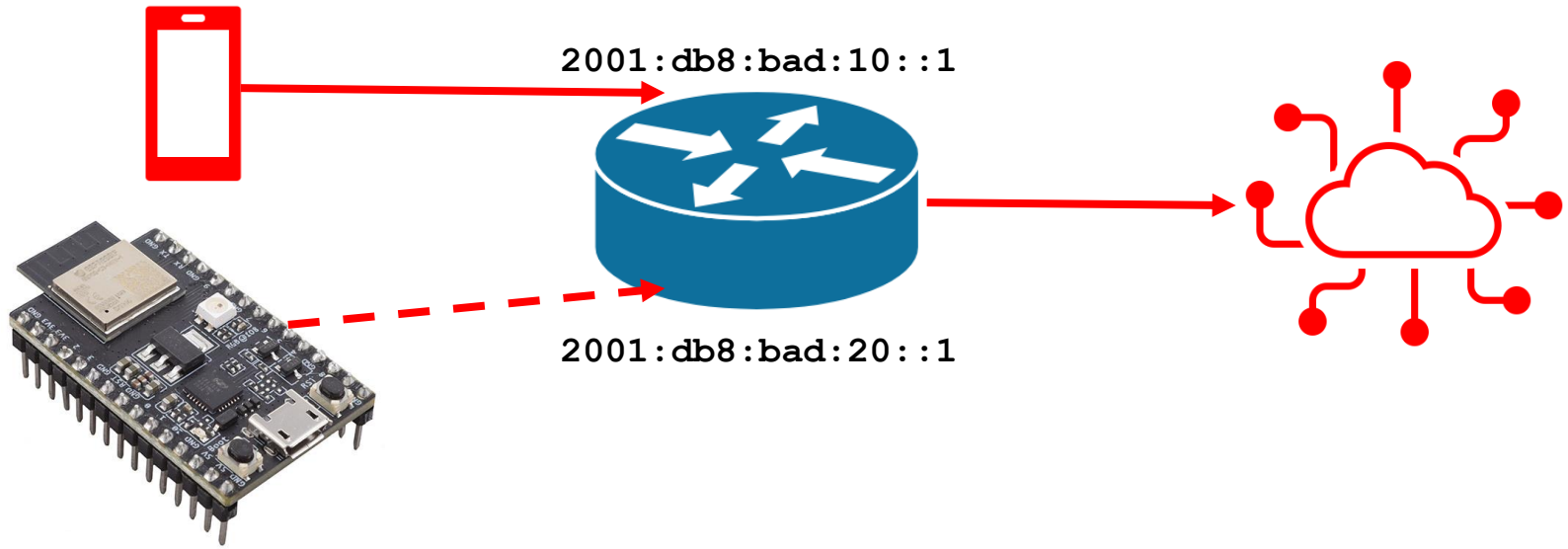
30:AE:A4:07:0D:64

MAC LAN	Cíl	Firewall
30:AE:A4:07:0D:64	Internet	**Zakázat**
Libovolná	Kamkoli	**Povolit**

```
ip6tables -A FORWARD -i lan -m mac --mac-source 30:AE:A4:07:0D:64 -o wan -j REJECT
```

A když chci omezit Internet jen pro některá zařízení v LAN?

2001:db8:bad:10:3c4e:984a:ff5d:4245
2001:db8:bad:10:f84d:3d87:47de:7715

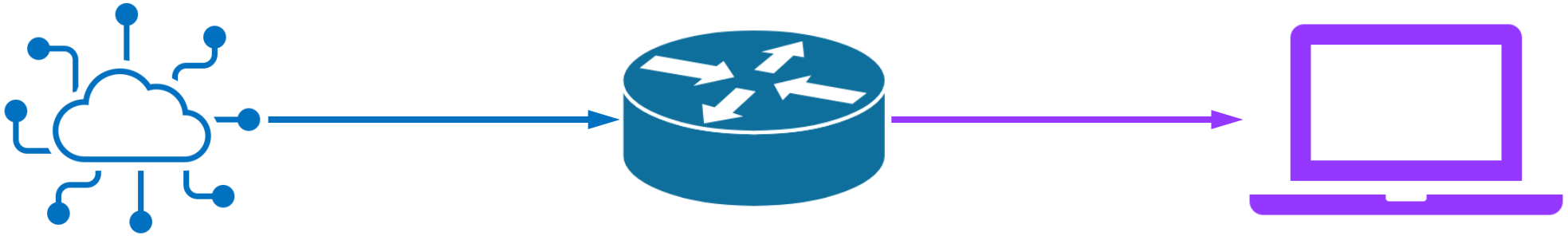


2001:db8:bad:20:3c4e:984a:ff5d:4245
2001:db8:bad:20:f84d:3d87:47de:7715

VLAN		Cíl	Firewall
2001:db8:bad:20::/64	IoT	Internet	Zakázat
2001:db8:bad:10::/64	Users	Kamkoli	Povolit

A jak udělám v IPv6 port forwarding?

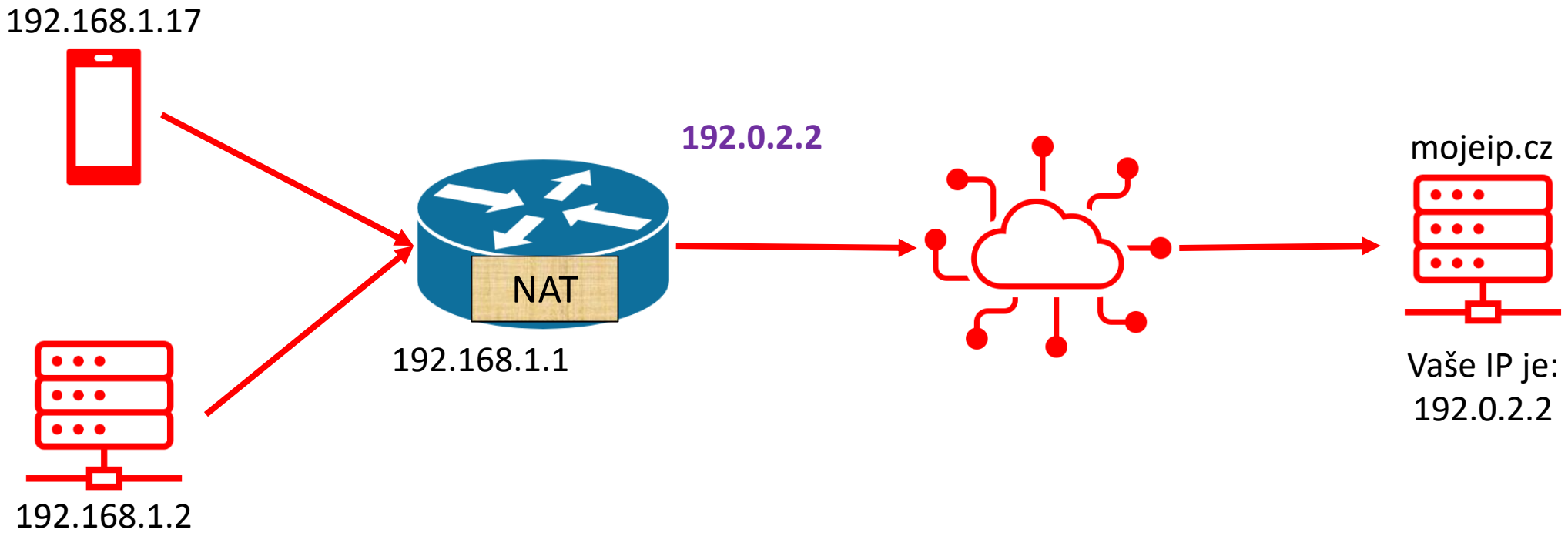
IPv4 port forwarding na routeru:
1. DNAT z vnější IPv4 adresy+portu X routeru na interní adresu+port X počítače
2. Otevření vnějšího portu X na firewallu



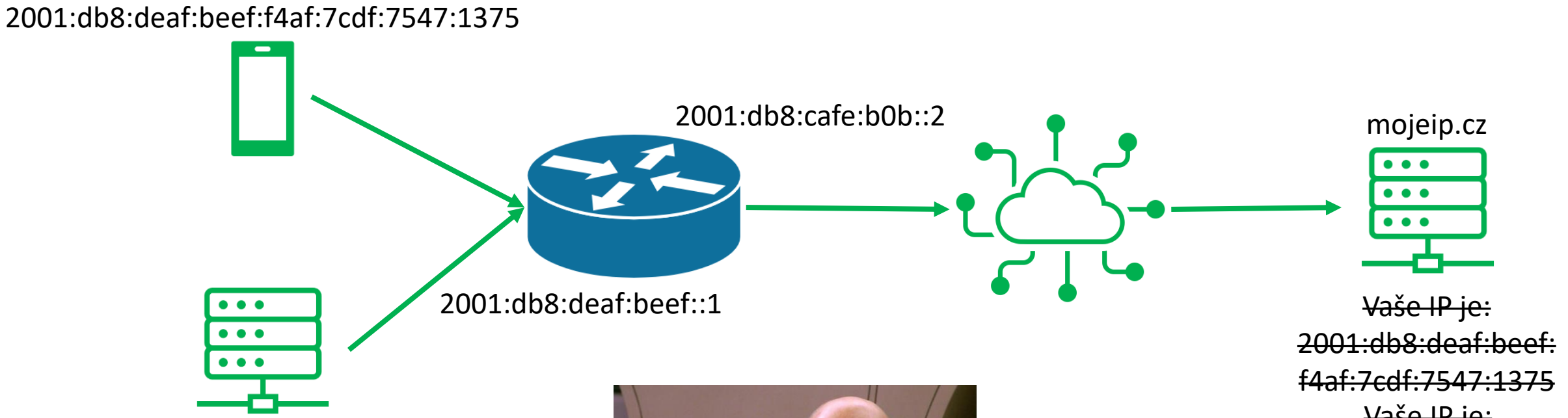
IPv6 „port forwarding“ na routeru (lépe: zpřístupnění služby v LAN):
1. Otevření portu na firewallu („z Internetu na IPv6 adresu počítače a port X v LAN“)

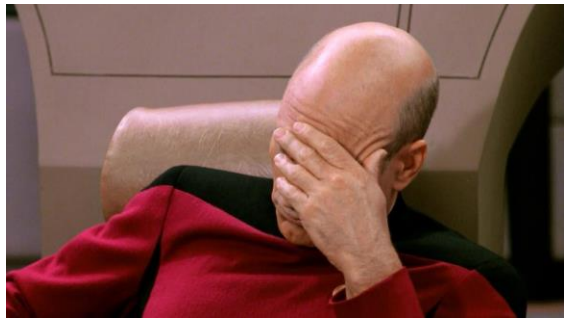
Problém:
Jak na routeru identifikovat počítač v LAN, když obvykle má dynamickou adresu?

Chci zpřístupnit služby na domácím **serveru** z Internetu, ale IPv6 adresa **routeru** je jiná než co mi ukazuje „mojeip.cz“ z **počítače**, co s tím?



Chci zpřístupnit služby na domácím **serveru** z Internetu, ale IPv6 adresa **routeru** je jiná než co mi ukazuje „mojeip.cz“ z **počítače**, co s tím?

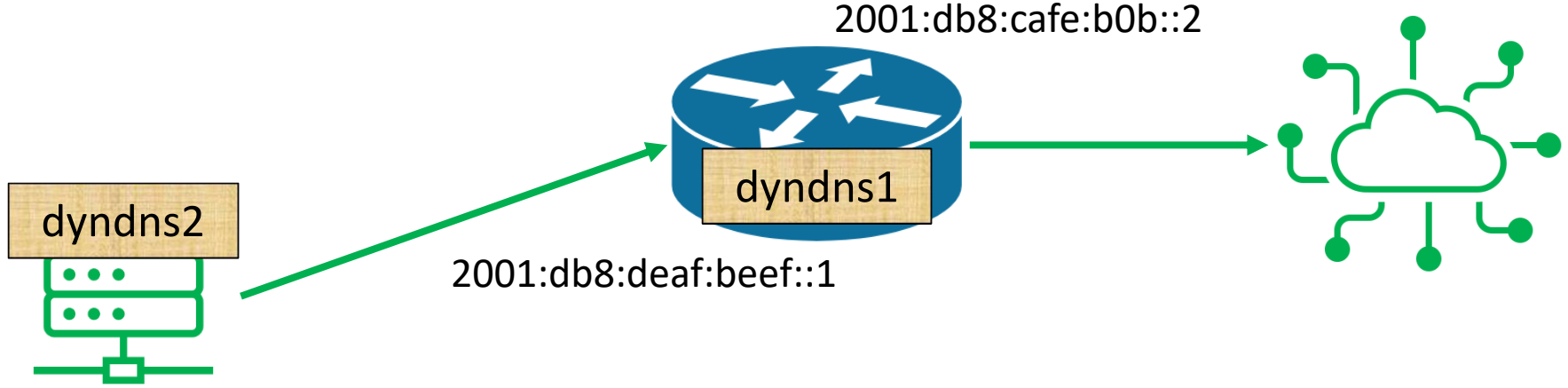




Mám na **routeru** DynDNS, ale na **server** ve vnitřní síti se pomocí jména nedostanu

dyndns1.service.com A **192.0.2.2**
dyndns1.service.com AAAA 2001:db8:cafe:b0b::2
dyndns1.service.com AAAA 2001:db8:deaf:beef::1

192.0.2.2
2001:db8:cafe:b0b::2

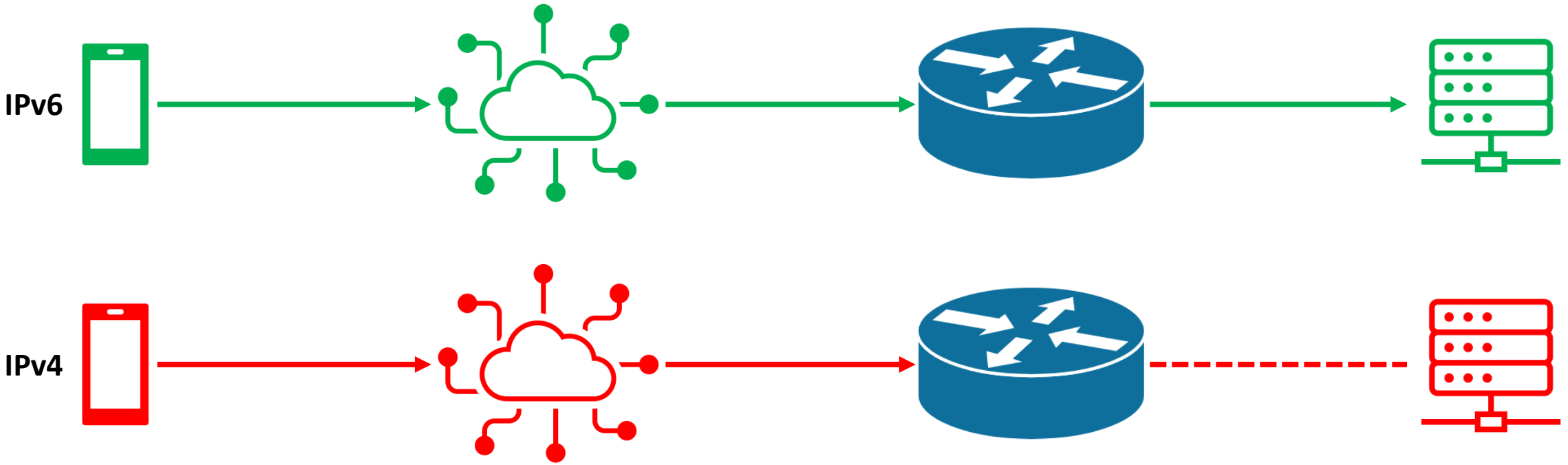


2001:db8:deaf:beef::1

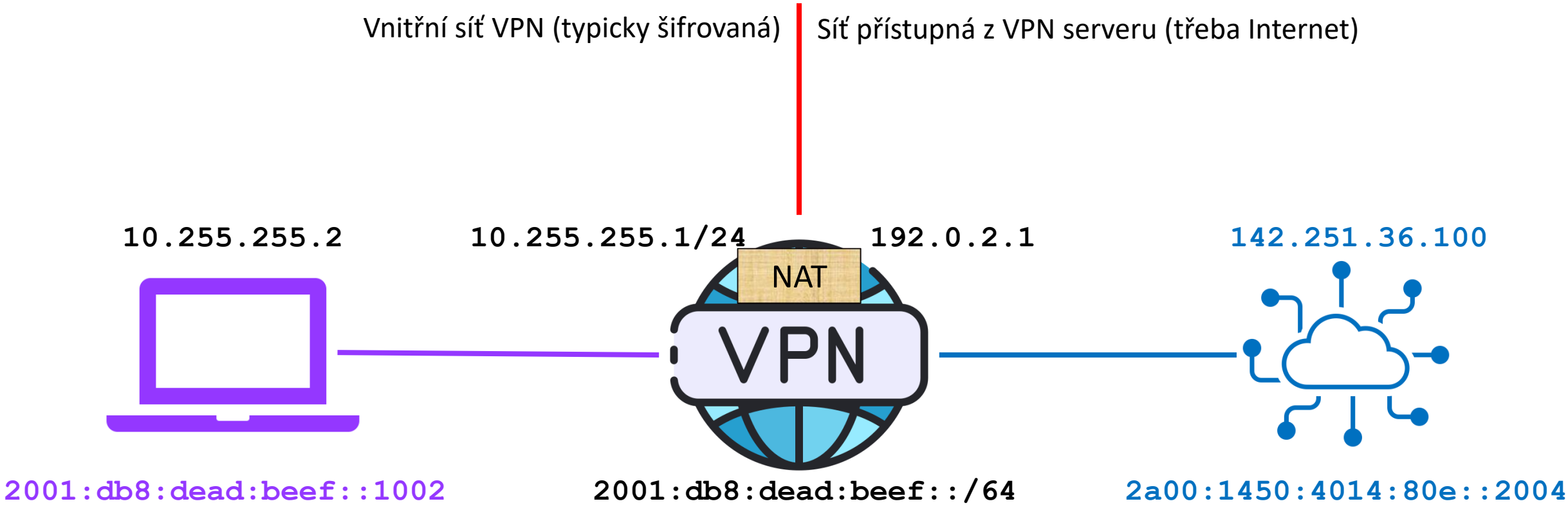
2001:db8:deaf:beef:2019:9d**ff:fe**49:3190
2001:db8:deaf:beef:c438:b8a3:b220:64dd
2001:db8:deaf:beef::**404**

dyndns2.service.com A **192.0.2.2**
dyndns2.service.com AAAA 2001:db8:deaf:beef:2019:9d**ff:fe**49:3190
dyndns2.service.com AAAA 2001:db8:deaf:beef:c438:b8a3:b220:64dd
dyndns2.service.com AAAA 2001:db8:deaf:beef::**404**

Jsem za CGNATem, pomůže mi IPv6 zpřístupnit služby z Internetu?



A jak fungují VPNky, když nemáme privátní adresy?

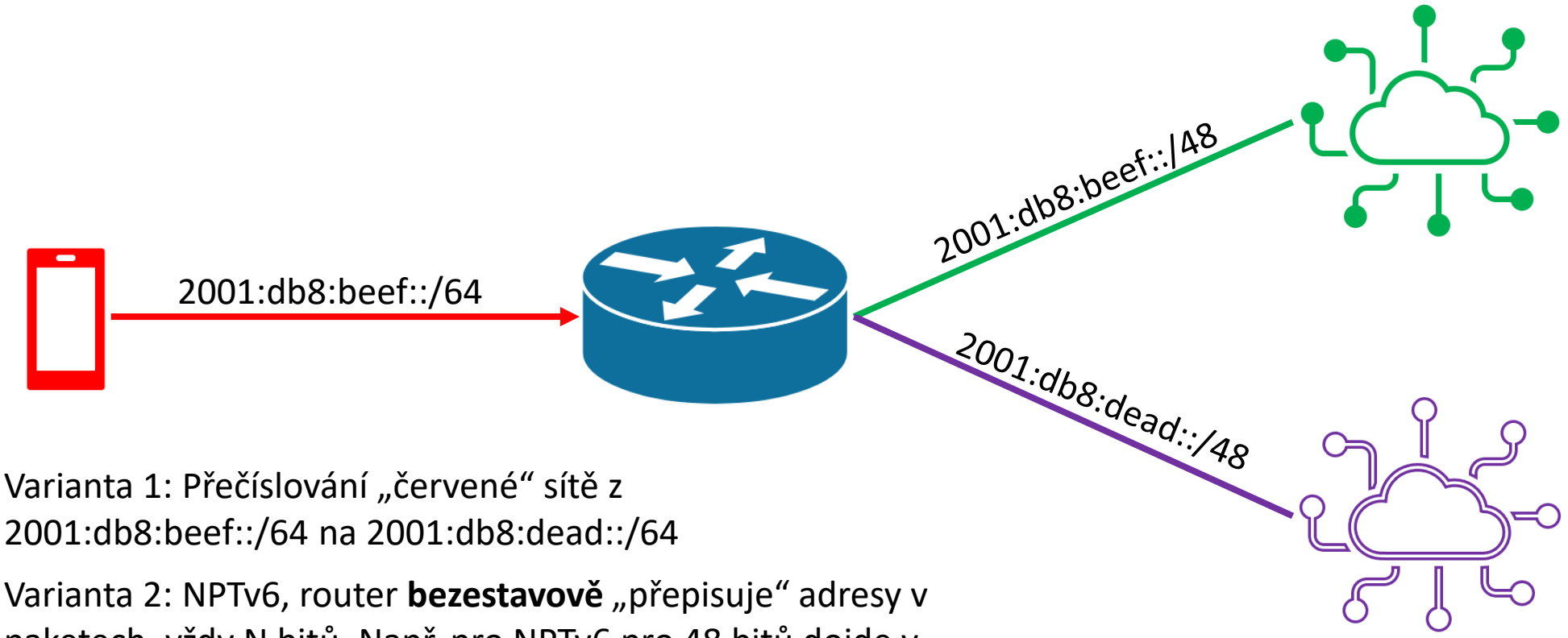


10.255.255.2 <-> 142.251.36.100

192.0.2.1 <-> 142.251.36.100

2001:db8:dead:beef::1002 <-> 2a00:1450:4014:80e::2004

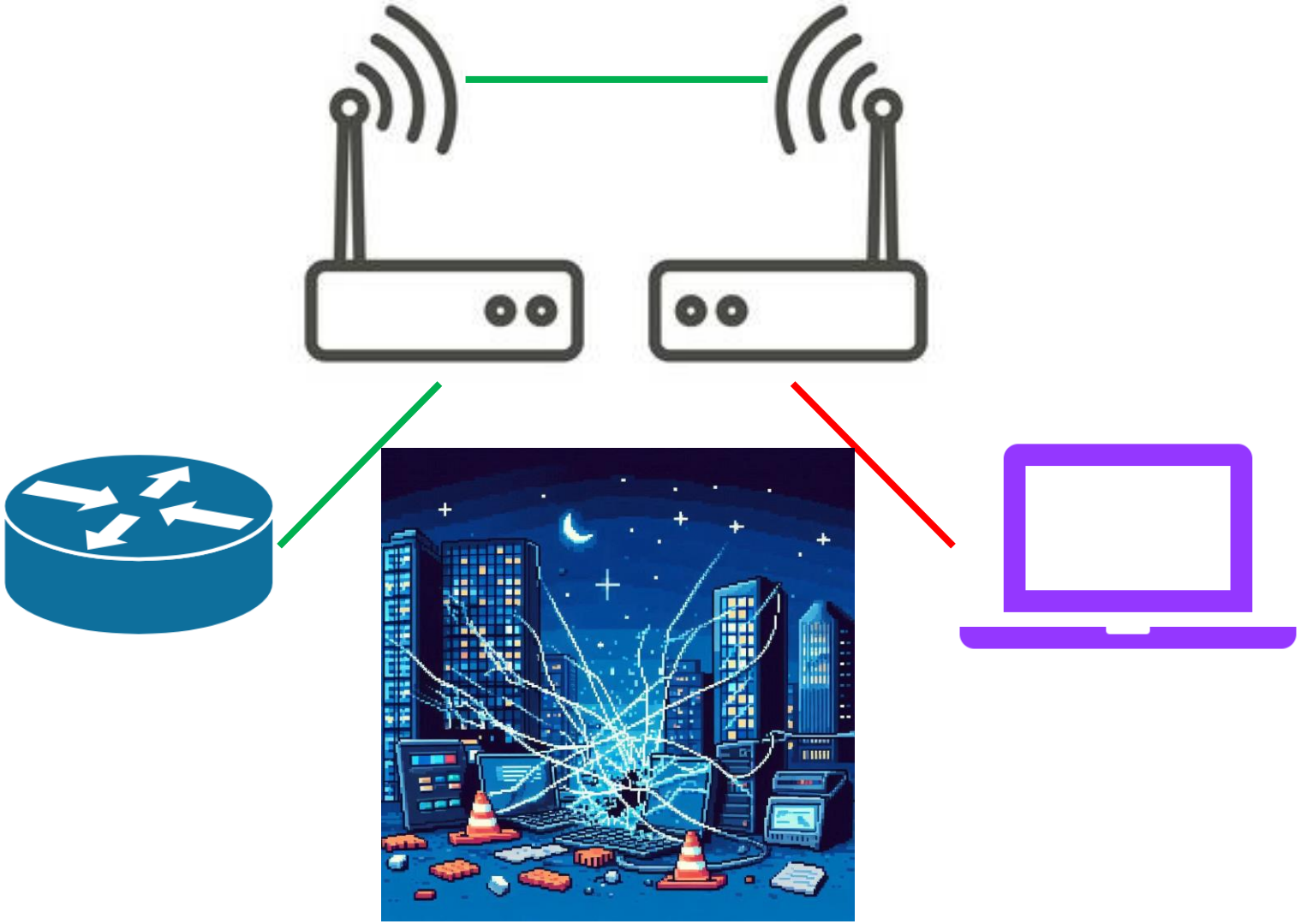
A co takhle „záložní ISP“, jak se to dělá bez NATu?



Varianta 1: Přečíslování „červené“ sítě z 2001:db8:beef::/64 na 2001:db8:dead::/64

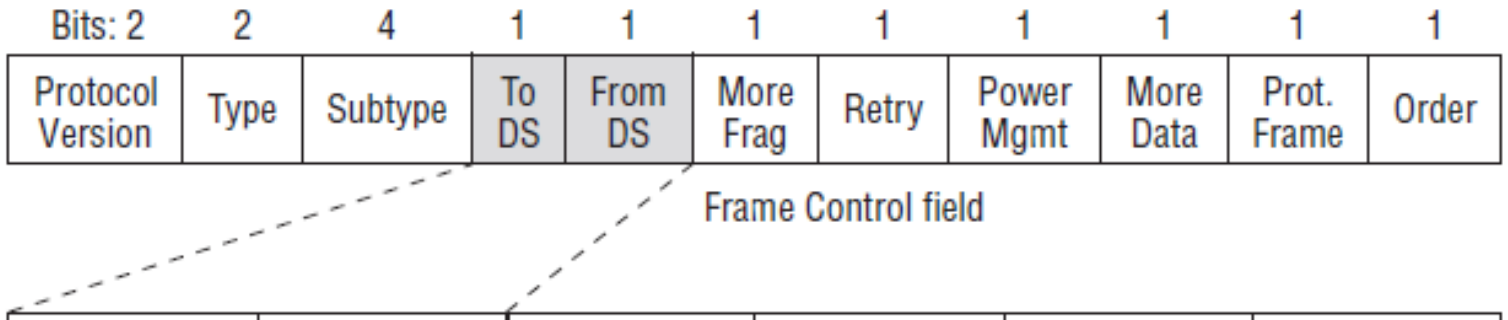
Varianta 2: NPTv6, router **bezestavově** „přepisuje“ adresy v paketech, vždy N bitů. Např. pro NPTv6 pro 48 bitů dojde v paketech k přepsání zdrojové adresy – místo **2001:db8:beef:** v ní bude **2001:db8:dead:** (a naopak při odpovědi z Internetu). Běžný NAT udržuje informace o každém spojení zevnitř ven.

Wi-Fi-Ethernet bridge a IPv6



Wi-Fi-Ethernet bridge a IPv6

FIGURE 3.20 802.11 MAC addressing



To DS	From DS	Address 1	Address 2	Address 3	Address 4	
0	0	RA = DA	TA = SA	BSSID	N/A	
0	1	RA = DA	TA = BSSID	SA	N/A	
1	0	RA = BSSID	TA = SA	DA	N/A	**<- běžný wi-fi klient**
1	1	RA	TA	DA	SA	**<- WDS**

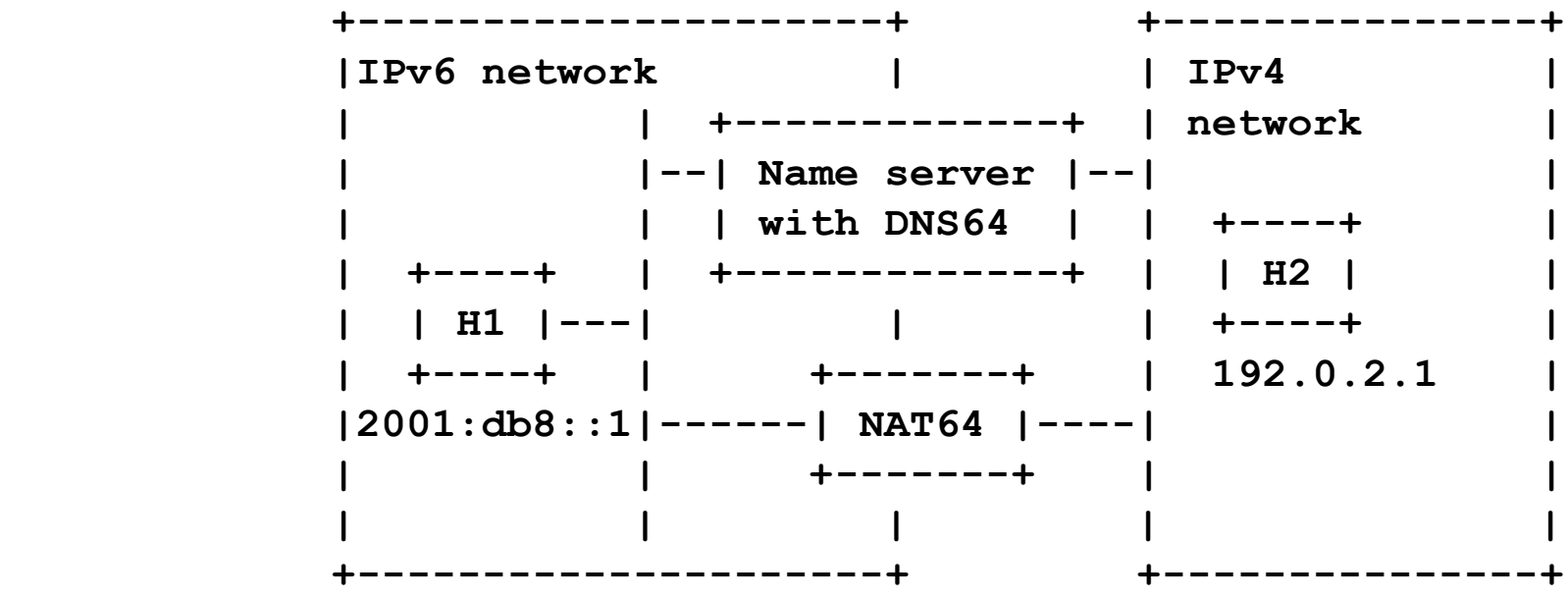
- SA = MAC address of the original sender (wired or wireless)
- DA = MAC address of the final destination (wired or wireless)
- TA = MAC address of the transmitting 802.11 radio
- RA = MAC address of the receiving 802.11 radio
- BSSID = L2 identifier of the basic service set (BSS)

https://mrncciew.com/2014/09/28/cwap-mac-headeraddresses/

IPv4 vs. IPv6 localhost

```
127.0.0.1
127.0.0.1/8
127.0.0.1 až 127.255.255.254
::1
::1/128
```

NAT64, well-known prefix a privátní IPv4 adresy



(rfc6146)

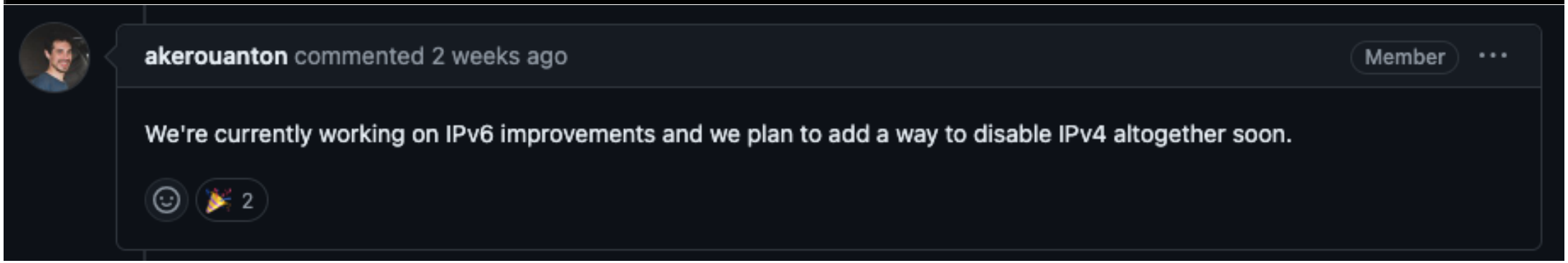
Well-Known Prefix	IPv4 address	IPv4-Embedded IPv6 address
64:ff9b::/96	192.0.2.33	64:ff9b::192.0.2.33

(rfc6052)

The Well-Known Prefix **MUST NOT be used** to represent **non-global IPv4 addresses, such as those defined in RFC1918**

Docker a zařízení bez IPv4 a další potíže

```
/app/bin # ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
26964: eth0@if26965: <BROADCAST,MULTICAST,UP,LOWER_UP,M-DOWN> mtu 1500 qdisc noqueue state UP
    link/ether 02:42:ac:15:00:05 brd ff:ff:ff:ff:ff:ff
    inet 172.21.0.5/16 brd 172.21.255.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 2a           :9900:1000:1:0:5/96 scope global flags 02
       valid_lft forever preferred_lft forever
    inet6 fe80::42:acff:fe15:5/64 scope link
       valid_lft forever preferred_lft forever
/app/bin #
```



Issue 32850 (a dalších 150+ issues obsahujících IPv6)

Mám konektivitu od Cogentu, ale nedostanu se do sítě Hurricane Electric

(NANOG 47, 09/2009, YouTube)

Q & A

Díky

linkedin.com/in/radek-zajic/

@zajDee