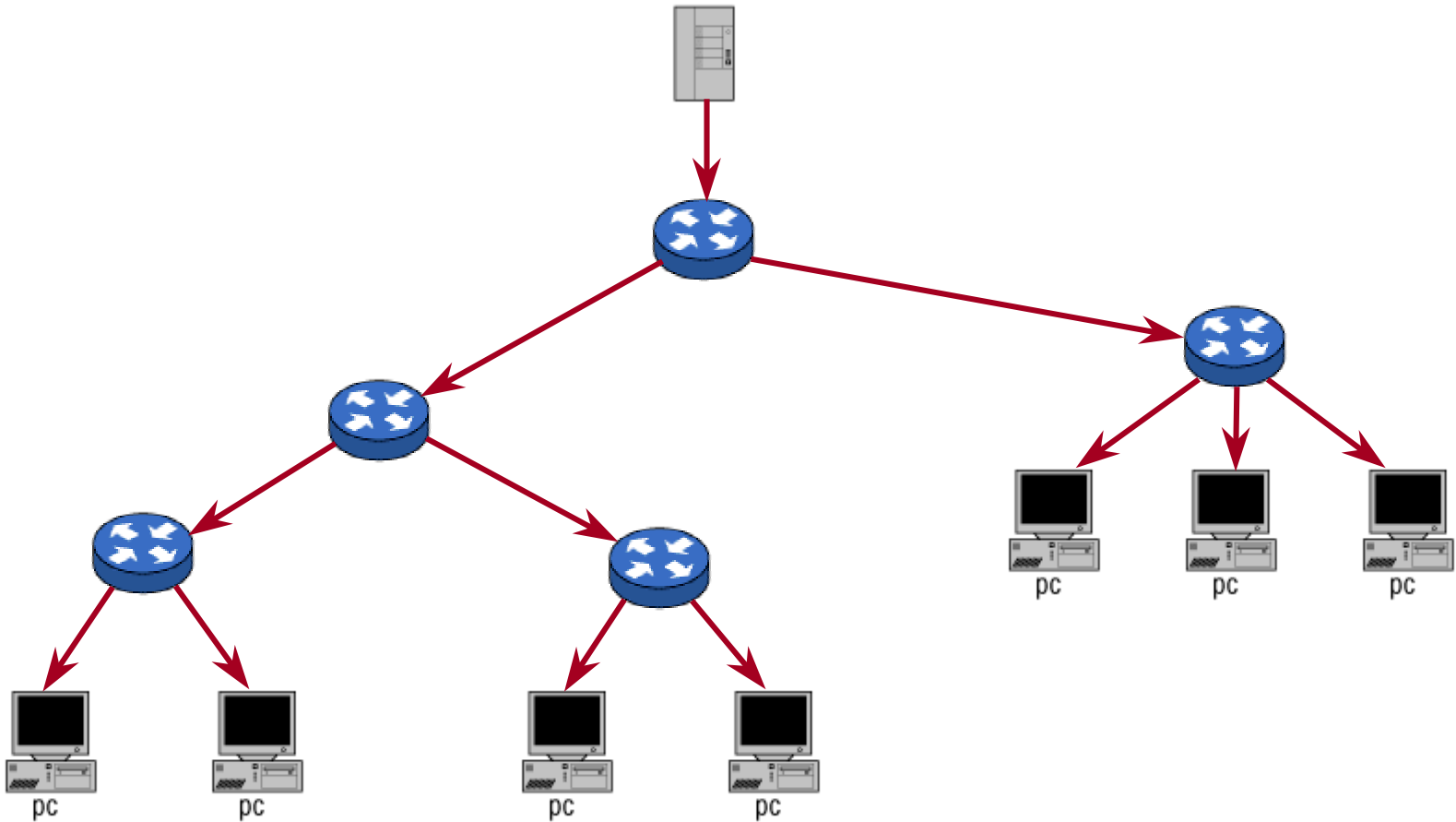


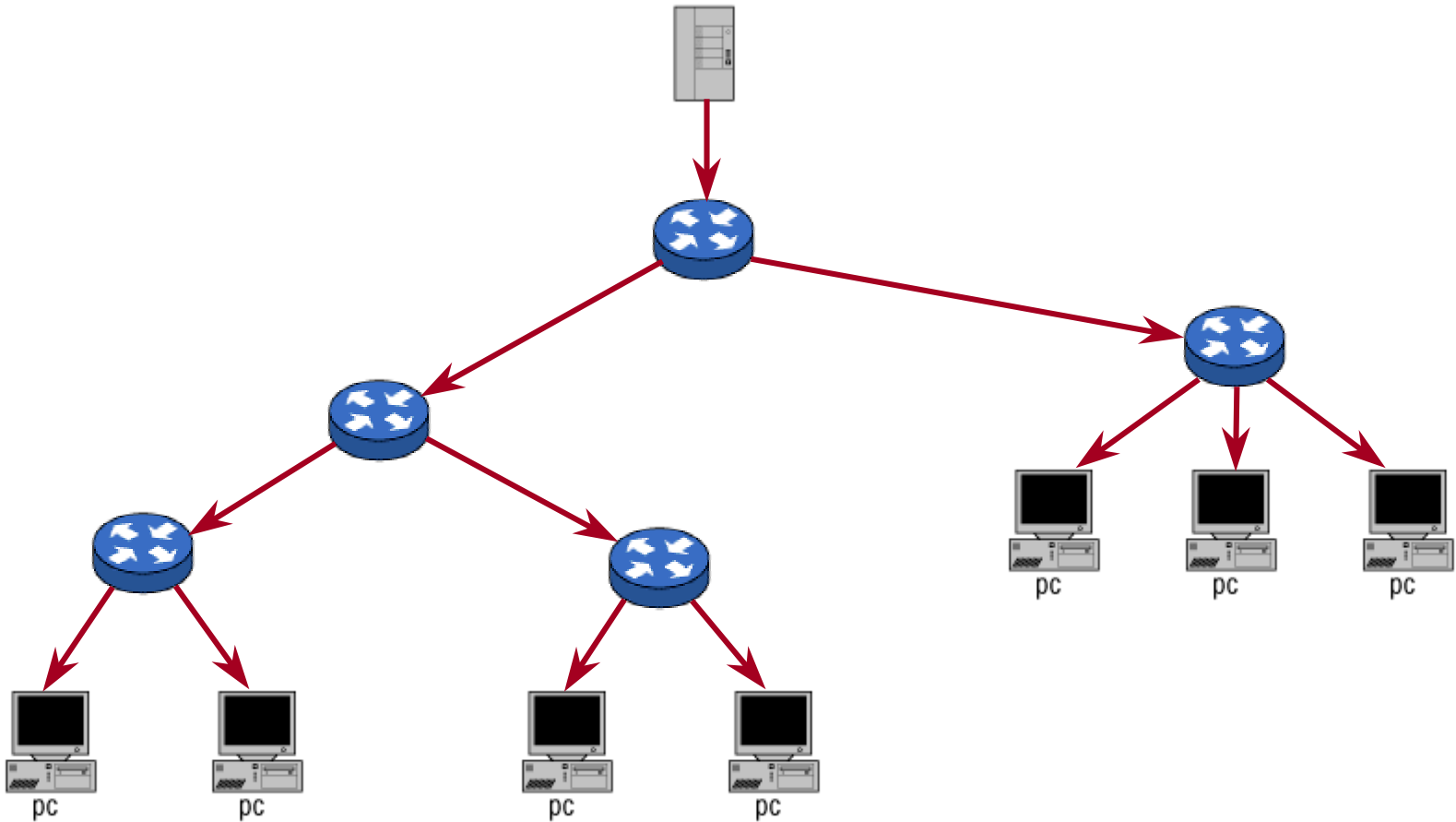
Multicast

- Výzva: *způsob zasílání stejných zpráv skupině koncových stanic*
- Revize všech základních aspektů
 - směrování
 - autonomní systémy
 - adresace
 - reakce na zahlcení
 - kvalita doručení (spolehlivost, uspořádanost, ...)

Multicast



Multicast



Multicast - motivace

- Data pro více „odběratelů“
 - všesměrové vysílání (broadcast)
 - vzdálená spolupráce (telecollaboration)
 - update programového vybavení a dat (antiviry)
- Dotaz „neznámému“ (vyhledávání)
 - peer-to-peer sdílení souborů (gnutella, napster)
 - hledání zdrojů
 - distribuované databáze

Multicast - principy

- Každým spojem data prochází nejvýše jednou
- Vlastnost sítě (nelze zajistit end-to-end)
 - duplikace dat na prvcích sítě („uvnitř“ sítě)
- Doručení
 - nezaručené, (best effort, UDP)
 - skupinová adresa
- TTL kontroluje rozsah šíření (poloměr)

Multicast - komunikující strany

- Vysílající
 - každý může vysílat (znalost skupinové adresy)
 - proměnný počet vysílajících
 - stačí posílat paketu na skupinovou adresu
 - může, ale nemusí být členem skupiny
- Přijímající
 - žádný, jeden, více
 - kdokoliv se může přidat či může opustit skupinu
 - může patřit do více skupin

IP multicast - vlastnosti

- Nelze jej účtovat
- Nelze zjistit přijímající
- Snadný terč útoku Denial of Service (DoS)
- Složitá dynamická alokace adres
- Problematická rozšiřitelnost

IP multicast - jednoduchý model

- Sdílená media (podporují broadcast)
- Aplikace se „přihlásí“ ke skupině
- Uzel začne přijímat všechny pakety vysílané na použitou skupinovou adresu
- Vysílající posílá pakety na skupinovou adresu

Správa skupinové komunikace

- komunikující skupina
 - *statická* || *dynamická*
 - *úzce lokalizovaná* || *široce rozprostřená*
 - *počet členů: jednotky -> desetitisíce*
- protokoly
 - IGMP (Internet Group Management Protocol, RFC 1112)
- adresace
 - adresa třídy D: 224.0.0.0 -> 239.255.255.255

Správa skupinové komunikace

- všichni členové komunikující skupiny komunikují se stejnou adresou
- přijetí člena do skupiny
- opuštění skupiny
- správa skupiny během existence

Protokoly pro multicastové směrování

- stromová struktura multicastové skupiny
 - dynamická skupiny => dynamická struktura
- dva základní přístupy
 - Source Based Tree
 - Shared Tree (Core Based Tree)

Source Based Tree

- Aktivita shora - zakládající uvědomuje zájemce
- Periodický broadcast
- Ořezávání větví, kde nejsou žádní členové
- Omezení šířky - TTL
- Vhodný pro úzce lokalizované skupiny
- Nevýhoda: režie, záplava broadcasty

Shared Tree (Core Based Tree)

- Ustaveno jádro (core) - body setkání (meeting points)
- Zájemce o členství ve skupině kontaktuje nejbližší MP
- Aktivita zdola - od příjemce
- Redukce broadcastu => lepší škálovatelnost
- Nevýhoda: problém závislosti na dostupnosti jádra

Shared Tree (Core Based Tree)

- Ustaveno jádro (core) - body setkání (meeting points)
- Zájemce o členství ve skupině kontaktuje nejbližší MP
- Aktivita zdola - od příjemce
- Redukce broadcastu => lepší škálovatelnost
- Nevýhoda: problém závislosti na dostupnosti jádra

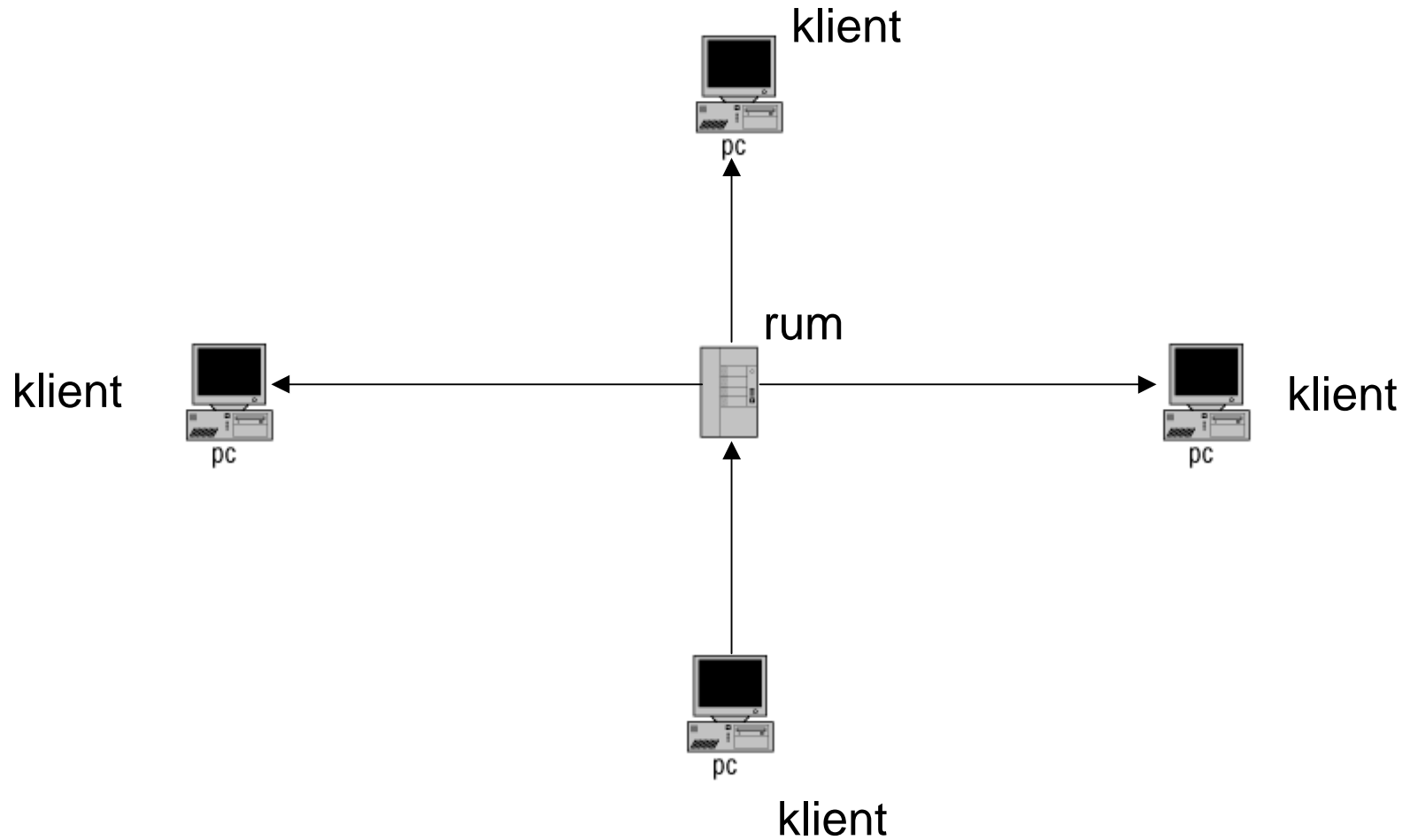
Konkrétní směrovací protokoly

- DVMRP (Distance Vector Multicast Routing Protocol)
 - Source Based Tree
 - obdoba RIP
- MOSPF (Multicast Open Shortest Path First)
 - Source Based Tree
 - obdoba OSPF
 - volba ústředního routeru pro skupinu
- CBT (Core Based Tree)
 - Shared Tree
 - protokolově nezávislý (využívá stávající směrovací informace)
- PIM (Protocol Independent Multicast)
 - optimalizace směrování pro různé typy skupin
 - PIM-SM (Sparse Mode) (Shared Tree)
 - PIM-DM (Dense Mode) (Source Based Tree)

Multicast bez podpory sítě

- Virtuální sítě
 - multicast na úrovni aplikací, tunelování
 - směrování se může přizpůsobit aktuální zátěži
 - omezení kapacity tunelů

UDP Packet Reflector (rum)

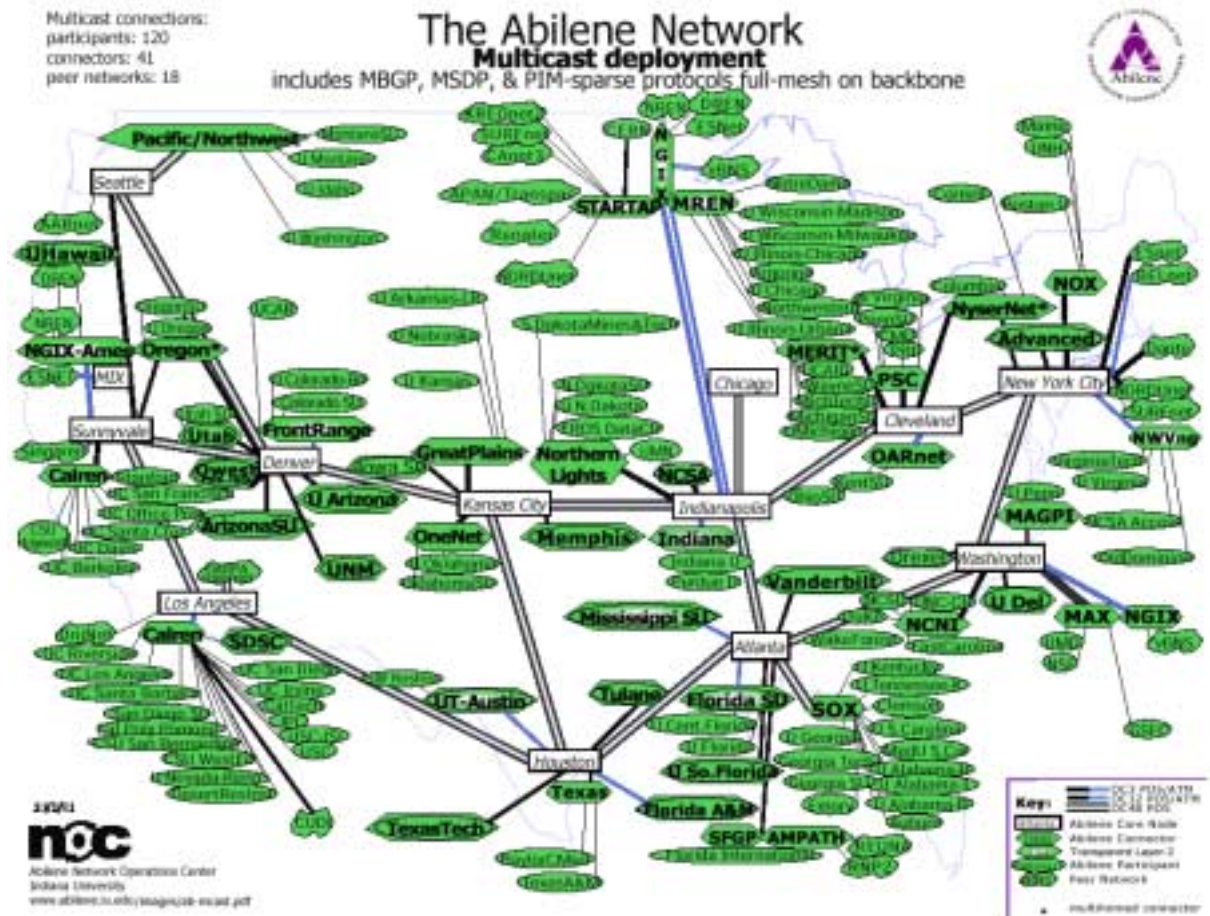


Tunely

- Připojení účastníků za směrovači bez podpory multicastu
- IP multicast paket enkapsulován do unicastového IP paketu, transportován ke své destinaci a dekapulován
- mrouter (mrouted)

MBone

- Multicastová podsít' Internetu



Spolehlivý multicast

- *contradictio in adjecto*
- problém datových služeb
- potvrzování zpráv (ACK, NACK)
 - ACK explosion, baby crying
- zálohování provozu na směrovačích
- problémy s implementací, vysoké nároky na výkon a nároky směrovačů

QoS

- použití pro multimediální přenosy v reálném čase
- kromě spolehlivosti ještě požadavky na další parametry (zpoždění, jitter...)
- pokusy o řešení (aktivní sítě)
- možný přístup
 - dekompozice
 - partikulární řešení
 - suboptimalita (vyšší než nezbytně nutná spotřeba zdrojů)

IPv6 - motivace

- Nedostatek jedinečných IP adres
 - přístroje (včetně domácích)
 - mobilní zařízení
- Příliš velké směrovací tabulky v páteřních směrovačích
- Manuální konfigurace IPv4 (nebo DHCP)
- Původně sekundární motivace:
 - nedostatečná variabilita IP
 - bezpečnost
 - podpora mobility

IPv6 - architektura

- Struktura IPv6 packetů



IPv6 - architektura

- Struktura adres IPv6

The following is an IPv6 address in binary form:

```
001000011101101000000000110100110000000000000000010111100111011  
000000101010101000000000111111111111110001010001001110001011010
```

The 128-bit address is divided along 16-bit boundaries, as follows:

```
0010000111011010    0000000011010011    0000000000000000    0010111100111011  
0000001010101010    0000000011111111    1111111000101000    1001110001011010
```

Each 16-bit block is converted to hexadecimal and delimited with colons. The result is:

```
21DA:00D3:0000:2F3B:02AA:00FF:FE28:9C5A
```

IPv6 representation can be further simplified by removing the leading zeros within each 16-bit block. However, each block must have at least a single digit. With leading zero suppression, the address representation becomes:

```
21DA:D3:0:2F3B:2AA:FF:FE28:9C5A
```

- vzhledem ke složitosti adres se předpokládá použití přes DNS

IPv6 - architektura

- Prefixy

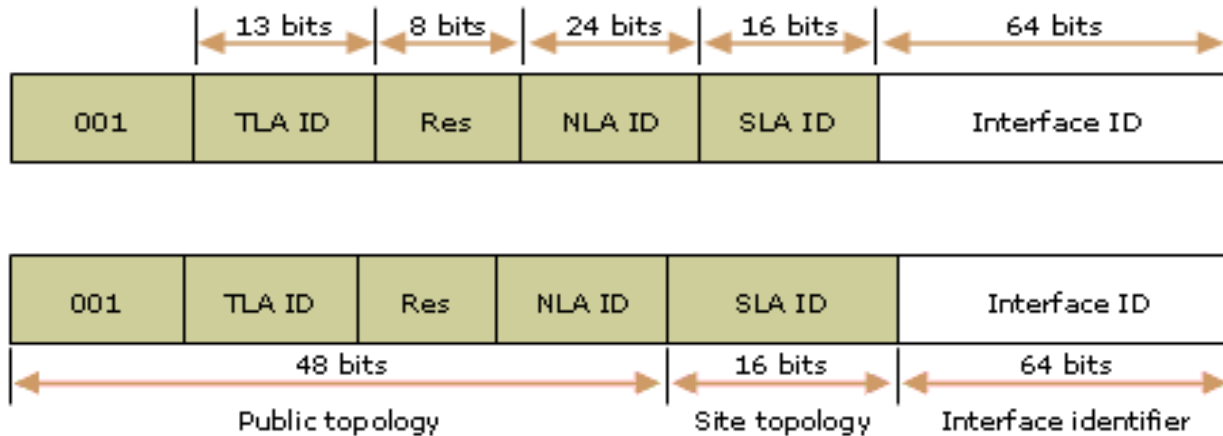
| <i>prefix</i> | <i>význam</i> |
|---------------|--|
| 0000 0000 | rezervováno (např. ::1 je loopback) |
| 0000 001 | rezervováno pro NSAP alokaci |
| 0000 010 | rezervováno pro IPX alokaci |
| 001 | agregovatelné globální individuální adresy - odpovídají současným klasickým IP adresám a identifikují dotyčné rozhraní tak, aby bylo celosvětově jednoznačné |
| 1111 1110 10 | lokální linkové adresy - jsou jednoznačné jen v rámci dané fyzické sítě |
| 1111 1110 11 | místní lokální adresy - jsou jednoznačné jen v rámci dané instituce |
| 1111 1111 | skupinové adresy |

| Allocation | Format Prefix (FP) | Fraction of the address space |
|---------------------------------------|---------------------------|--------------------------------------|
| Reserved | 0000 0000 | 1/256 |
| Reserved for NSAP allocation | 0000 001 | 1/128 |
| Aggregatable global unicast addresses | 001 | 1/8 |
| Link-local unicast addresses | 1111 1110 10 | 1/1024 |
| Site-local unicast addresses | 1111 1110 11 | 1/1024 |
| Multicast addresses | 1111 1111 | 1/256 |

The remainder of the IPv6 address space is unassigned.

IPv6 - architektura

- Struktura unicastových adres



IPv6 - architektura

- Speciální adresy

Special addresses

The following are special IPv6 addresses:

- Unspecified address

The unspecified address (0:0:0:0:0:0:0:0 or ::) is used only to indicate the absence of an address. It is equivalent to the IPv4 unspecified address of 0.0.0.0. The unspecified address is typically used as a source address for packets that are attempting to verify the uniqueness of a tentative address. The unspecified address is never assigned to an interface or used as a destination address.

- Loopback address

The loopback address (0:0:0:0:0:0:0:1 or ::1) is used to identify a loopback interface, enabling a node to send packets to itself. It is equivalent to the IPv4 loopback address of 127.0.0.1. Packets addressed to the loopback address are never sent on a link or forwarded by an IPv6 router.

Compatibility addresses

To aid in the migration from IPv4 to IPv6 and facilitate the coexistence of both types of hosts, the following addresses are defined:

- IPv4-compatible address

The IPv4-compatible address, 0:0:0:0:0:0:w.x.y.z or ::w.x.y.z (where w.x.y.z is the dotted decimal representation of a public IPv4 address), is used by dual-stack nodes that are communicating with IPv6 over an IPv4 infrastructure. Dual-stack nodes are nodes with both IPv4 and IPv6 protocols. When the IPv4-compatible address is used as an IPv6 destination, IPv6 traffic is automatically encapsulated with an IPv4 header and sent to the destination by using the IPv4 infrastructure.

- IPv4-mapped address

The IPv4-mapped address, 0:0:0:0:FFFF:w.x.y.z or ::FFFF:w.x.y.z, is used to represent an IPv4-only node to an IPv6 node. It is used only for internal representation. The IPv4-mapped address is never used as a source or destination address for an IPv6 packet. The IPv6 protocol for Windows does not support the use of IPv4-mapped addresses.

- 6to4 address

The 6to4 address is used for communicating between two nodes running both IPv4 and IPv6 over an IPv4 routing infrastructure. The 6to4 address is formed by combining the prefix 2002::/16 with the 32 bits of the public IPv4 address of the node, forming a 48-bit prefix. For example, for the IPv4 address of 131.107.0.1, the 6to4 address prefix is 2002:836B:1::/48. For more information about 6to4, see [IPv6 traffic between nodes in different sites across the Internet \(6to4\)](#)

IPv6 - architektura

- Struktura multicastových adres



- Flags

The Flags field indicates flags that are set on the multicast address. The size of this field is 4 bits. As of RFC 2373, the only flag defined is the Transient (T) flag. The T flag uses the low-order bit of the Flags field. When set to 0, the T flag indicates that the multicast address is a permanently-assigned (well-known) multicast address allocated by the Internet Assigned Numbers Authority (IANA). When set to 1, the T flag indicates that the multicast address is a transient (not permanently assigned) multicast address.

- Scope

The Scope field indicates the scope of the IPv6 internetwork for which the multicast traffic is intended. The size of this field is 4 bits. In addition to information provided by multicast routing protocols, routers use the multicast scope to determine whether multicast traffic can be forwarded.

The following scopes are defined in RFC 2373:

| Scope field value | Scope |
|-------------------|--------------------|
| 1 | Node-local |
| 2 | Link-local |
| 5 | Site-local |
| 8 | Organization-local |
| E | Global |

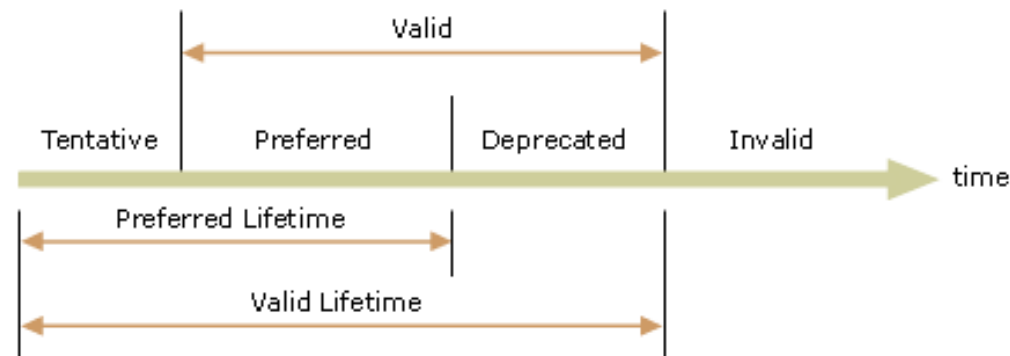
For example, traffic with the multicast address of FF02::2 has a link-local scope. An IPv6 router never forwards this traffic beyond the local link.

- Group ID

The Group ID field identifies the multicast group and is unique within the scope. The size of this field is 112 bits. Permanently assigned group IDs are independent of the scope. Transient group IDs are only relevant to a specific scope. Multicast addresses from FF01:: through FFOF:: are reserved, well-known addresses.

IPv6 - architektura

- Autokonfigurace unicastových adres
 - stavová (obdobná DHCP)
 - bezstavová (neighbor discovery)
 - novinka IPv6 založená na tom, že router opakovaně inzeruje tzv. *ohlášení směrovače*
 - snaha po Plug-and-Play (nebo Plug-and-Pray??)
 - klient se z ohlášení dozví, jaké prefixy používá daná síť a k ní si připojí svoji 64bitovou část vytvořenou ze své ethernetové adresy a také informace potřebné pro routování
 - tento způsob vůbec neřeší DNS, což je v IPv6 nezbytnost
- časové omezení automaticky přidělovaných adres

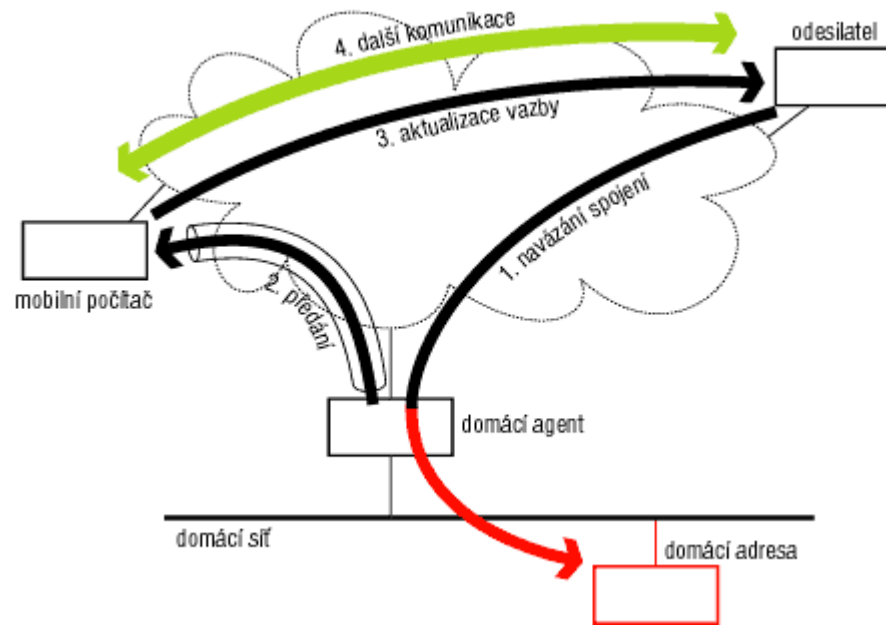


IPv6 - bezpečnost

- Implementace bezpečnosti je v IPv6 povinná (i když mnoha autory dosud odkládána)
- Authentication Header (AH) paketu
 - ověření totožnosti odesílatele
 - možnost ochrany před opakovaným vysláním téhož (aby vetřelec nemohl jednoduše odeslat ještě jednou sekvenci vašich paketů, které se mu podařilo zachytit)
- Encapsulating Security Payload (ESP) paketu
 - širší služby než AH
 - umožňuje buď řešit šifrování paketu nebo ověřování totožnosti odesílatele, avšak ne současně
- Security Policy Database -> Security Association
 - zahodit, akceptovat bez prověření, poslat na prověření

IPv6 - mobilita

- Provoz „domácího agenta“



- v případě změny IP pohybující se stanice pošle informace jak svému domácímu agentovi tak i všem strojům, s nimiž aktuálně komunikuje
- bezpečnostní otázky

IPv6 - implementace

- projekt KAME - NetBSD/FreeBSD/OpenBSD
 - ve velmi dobrém stavu včetně podpory mobility a bezpečnosti
- implementace pro Windows 2000 a XP od MS
- Linux - stabilizováno od řady 2.2.x - *ověřit*
- Cisco má podporu IPv6 pouze jako testovací

- 6bone

IPv6 - shruntí

- 128 bitové adresy
 - 340282366920938463463374607431768211456
($3 \cdot 10^{38}$) jedinečných adres
- jednodušší hlavička se 64bitovým zarovnáním
- podpora real-time provozu (flow label)
- směrovače nesmí fragmentovat
- podpora autokonfigurace
- flexibilní mechanismus rozšiřitelnosti hlaviček
 - bezpečnost
 - výběr cest