Internet Protocol (IP)

[Povinné]

Jeden z nejdůležitějších protokolů z hlediska správy sítí. IP je protokol *internetové* vrstvy a zajišťuje směrování *datagramů* v síti. Existují celkem dvě verze toho protokolu, starší, ale značně rozšířený, IPv4 a novější IPv6. Jelikož operační systémy Windows podporují obě tyto verze protokolu a řada nových služeb či aplikací systému je přímo závislá na IPv6, je potřeba znát obě tyto verze, jenž jsou velice odlišné.

IP adresa

[Povinné]

IP adresa slouží k jednoznačné identifikaci síťového rozhraní (konkrétního zařízení) v rámci dané (pod)sítě. Každý *datagram* obsahuje adresy zdrojového a cílového koncového uzlu a internetová vrstva se snaží doručit *datagram* od zdroje k cíli.

Internet Protocol verze 4 (IPv4)

[Povinné]

Starší, ale nesmírně rozšířená, verze IP protokolu. Většina stávajících interních sítí a podstatná část sítě internet stále používá **IPv4** jako komunikační protokol *internetové* vrstvy. Je proto důležité umět pracovat s touto verzí IP protokolu.

Formát IPv4 adres

[Povinné]

IPv4 adresy jsou 32bitová čísla, jenž se zapisují v dekadickém formátu s tečkovou notací po osmi bitech. Tedy každá adresa je ve formátu X.X.X.X, kde X je číslo od 0 do 255. Z hlediska struktury se dělí **IPv4 adresa** na tři základní části, jak je zobrazeno na obrázku 2.

Obrázek 1. Struktura IPv4 adresy

Dříve byla **IPv4 adresa** tvořena pouze adresami sítě a rozhraní, toto členění ovšem bylo příliš hrubé a docházelo tak k zbytečnému plýtvání adres, jelikož adresa sítě byla tvořena vždy pouze prvními osmi bity a zbylé adresy rozhraní, kterých bylo 16 miliónů pro každou síť, byly využity jen minimálně. Proto se později **IPv4 adresy** rozdělily do tříd, které se odlišovaly velikostí části, jenž byla vyhrazena pro adresu sítě, tak se vytvořilo podstatně více sítí pro méně rozhraní. Nakonec se i toto rozdělení ukázalo jako nevhodné a adresa rozhraní se rozdělila na část adresy podsítě a rozhraní, což umožnilo ještě jemnější rozdělování rozhraní do sítí. Adresu sítě pro danou koncovou síť přiděluje vždy poskytovatel připojení (přesněji lokální registrátor). Jak bude rozdělena lokální část adresy, tedy jaká část bude vyhrazena pro adresy podsítí a jaká část pro adresy rozhraní, určuje již správce dotyčné koncové sítě.

Třída	Prefix sítě	1. bajt	Maska	Bitů sítě	Bitů počítače	Počet sítí	Počet stanic v síti
A	0	0 - 127	255.0.0.0	7	24	126	16 777 214
B	10	128 - 191	255.255.0.0	14	16	16 384	65 534
C	110	192 - 223	255.255.255.0	21	8	2 097 152	254
D	1110	224 - 239	Skupinové vysílání (*multicast*)				
E	1111	240 - 255	Rezervováno pro pozdější využití				

Tabulka 1. Třídy IPv4 adres

Pro určení hranice mezi adresami podsítě a rozhraní se využívá tzv. **masky podsítě** (*subnet mask*). Stejně jako v případě **IPv4 adresy**, i **maska podsítě** je 32bitové číslo zapsané ve stejném formátu jako **IPv4 adresa**. V binárním tvaru obsahuje jedničky tam, kde se v **IPv4 adrese** nachází adresa sítě a podsítě a nuly tam, kde je adresa rozhraní. Jelikož část obsahující adresu podsítě může být různě velká, musí být součástí konfigurace síťového rozhraní vždy i **maska podsítě**.

Tabulka 1 výše zachycuje rozdělení **IPv4 adres** do jednotlivých tříd s informacemi o tom, jak velká část **IPv4 adresy** je vyhrazena pro identifikaci sítě a jak velká část pro identifikaci rozhraní. Z části vyhrazené pro adresu rozhraní lze ještě, v případě potřeby, ubrat pár bitů pro identifikaci podsítě, jak bylo zmíněno dříve. Dnes se již rozdělení do tříd nevyužívá, jelikož bylo nahrazeno rozdělením podle CIDR, které je flexibilnější a bude zmíněno v dalším textu.

Směrování IPv4 adres

[Povinné]

Směrování slouží k dopravě *datagramů* ze zdrojového koncového uzlu do cílového koncového uzlu (tedy nejčastěji k přenosu dat mezi dvěma počítači). Směrování se provádí na základě směrovacích tabulek, jenž mohou být nastaveny staticky uživatelem nebo dynamicky pomocí směrovacích protokolů jako RIP (*Routing Information Protocol*) nebo OSPF (*Open Shortest Path First*).

Směrovací tabulky obsahují informace o tom, kterými porty směrovače nebo skrz které síťové rozhraní počítače se dá dostat do sítě, ve které leží koncový uzel s cílovou adresou. V dnešní době se pro směrování používá hlavně tzv. **beztřídní mezidoménové směrování** (CIDR, *Classless Inter-Domain Routing*), jenž umožňuje explicitně specifikovat předěl mezi částí s adresou sítě a částí s adresou počítače. Adresy se v tomto případě zapisují ve formátu X.X.X.X/Y, kde první část je **IPv4 adresa** a Y je počet bitů adresy sítě.

Pokud směrovači[1] přijde *datagram*, podívá se do směrovací tabulky a zjistí, skrz které porty se dá dostat do sítě, do které náleží cílová **IPv4 adresa** v *datagramu*. Pokud je jich více, některý vybere na základě dalších informací (např. podle nastavené metriky, podle zahlcení dané cesty apod.). V případě, že *datagram* přišel na port, jenž vede do sítě, kam tento *datagram* směřuje, dojde k jeho zahození. Druhá situace, kdy může dojít k cílenému zahození *datagramu*, je v případě, že směrovač odděluje interní síť od sítě internet a cílová adresa v *datagramu* náleží do privátní sítě. Takovéto *datagramy* jsou **nesměrovatelné** v síti internet. Seznam privátních sítí lze nalézt v tabulce 2 níže. Posledním případem je situace, kdy cílová adresa je adresa pro všesměrové vysílání (*broadcast*) a ostatní porty směřují do jiných podsítí, takového *datagramy* nikdy **nesmí** překročit hranice podsítě.

CIDR adresový blok	Popis
0.0.0.0/8	Aktuální síť (pouze pro zdrojové adresy)
10.0.0.0/8	Privátní síť
127.0.0.0/8	Loopback
169.254.0.0/16	Privátní síť (**APIPA**)
172.16.0.0/12	Privátní síť
192.88.99.0/24	IPv6 to IPv4 překlad
192.168.0.0/16	Privátní síť
224.0.0.0/4	Multicast (skupinové vysílání, předchozí třída D)
240.0.0.0/4	Rezervováno (předchozí třída E)
255.255.255.255	Broadcast (všesměrové vysílání)

Tabulka 2. Seznam speciálních rozsahů IPv4 adres

[1] Směrovačem je myšleno jakékoliv zařízení, jenž je schopné směrovat příchozí *datagramy*

Vyhrazené adresy

[Povinné]

Nejnižší adresa v síti (s nulovou adresou stanice) slouží jako označení celé sítě (např. „síť 192.168.24.0“). Adresa sítě se z dané IP adresy určí jako logický součin (AND) IP adresy a masky. Nejvyšší adresa v síti (adresa stanice obsahuje samé binární jedničky) slouží jako adresa pro všesměrové vysílání (*broadcast*), takové adresy tedy nelze použít pro normální účely.

Adresy **127.x.x.x** (tzv. **localhost**, nejčastěji se používá adresa **127.0.0.1**) jsou rezervovány pro tzv. *loopback*, logickou smyčku umožňující posílat pakety sám sobě.

Dále jsou vyčleněny rozsahy tzv. privátních (neveřejných) IP adres, které se používají pouze pro adresování vnitřních sítí (např. lokálních), na Internetu se nikdy nemohou objevit. Jako neveřejné jsou určeny adresy:

- Ve třídě A: **10.0.0.0** až **10.255.255.255** (celkem 16 777 214 adres)
- Ve třídě B: **172.16.0.0** až **172.31.255.255** (celkem 16 krát 65 534 adres (tj. celkem 1 048 544))
- Ve třídě C: **192.168.x.0** až **192.168.x.255** (celkem 256 krát 254 adres)

Subnetting a Supernetting

[Povinné]

Nedostatečná granularita přidělování třídních bloků adres vedla k preferování přidělování většího počtu menších bloků adres. To s sebou přineslo jeden nepříjemný problém a to výrazný nárůst velikostí směrovacích tabulek. Tento problém se navíc akceleroval se zavedením beztřídního mezidoménového směrování (CIDR), kdy se projevily ho další výhody v oblasti lepší delegace správy a zodpovědnosti za jednotlivé bloky adres. Proto byly zavedeny metody jak rozdělit, resp. sloučit jednotlivé bloky a tím zefektivnit obsah směrovacích tabulek.

Subnetting je starší metoda, jejíž obvyklé použití nevyžaduje žádnou změnu ve způsobu práce s IP adresami v globálním měřítku. Základní myšlenkou je lépe hospodařit s přiděleným blokem IP adres, který si můžeme rozdělit použitím jednoho nebo více bitů určených na adresu rozhraní na více podsítí vyhovujících našim potřebám (jedna podsíť může odpovídat např. pobočce, budově nebo patru v budově). Tímto zásahem můžeme definovat omezení jednotlivých podsítí jak z hlediska správy, tak i dosáhnout zvýšení propustnosti v jednotlivých podsítích (např. dojde k omezení dosahu broadcastu). Nevýhodu subnettingu představuje snížení celkového počtu adresovatelných síťových rozhraní – každá (pod)síť totiž potřebuje svou adresu a adresu pro broadcast.

Supernetting je přesným opakem subnettingu v tom, že posouvá pomyslnou dělicí čáru mezi adresou sítě a rozhraní směrem k vyšším bitům. Tím dochází ke spojení (tzv. agregaci) několika původně samostatných po sobě jdoucích bloků adres do jednoho většího. Základním předpokladem je tedy nutnost shody vyšších bitů adresy v délce nově použité masky.

APIPA

[Povinné]

Adresy IP můžete zadat do počítačů v síti nakonfigurováním jednoho nebo více serverů DHCP, které adresy IP dynamicky poskytují dalším počítačům. Jestliže síť neobsahuje server DHCP, použije se omezená možnost přidělení adresy IP označovanou jako automatické přidělování soukromých adres IP (APIPA). Po dobu, po kterou počítač používá funkci APIPA, může komunikovat pouze s počítači, které tuto funkci používají ve stejném síťovém segmentu. Počítač využívající funkci APIPA nemůže navázat připojení k síti Internet. APIPA (*Automatic Private IP Addressing*) k vytvoření automatické konfigurace využívá rozsahu adres IP od **169.254.0.1** do **169.254.255.254** a masky podsítě **255.255.0.0**.

Sdílení připojení k internetu

[Povinné]

Sdílení připojení k internetu (*Internet Connection Sharing*, zkráceně *ICS*) je služba systému Windows dostupná již od Windows 98 Second Edition a Windows 2000. Tato služba umožňuje na počítači s jakoukoliv internetovou konektivitou (včetně dial-up, ISDN, xDSL, PPPoE, …) vybaveným dalším síťovým adaptérem (i bezdrátovým) tuto konektivitu nasdílet tím, že na tomto tzv. "privátním" adaptéru začne poskytovat službu směrovače s NAT, DHCP a DNS. Standardně je použita síť **192.168.137.0/24**, kdy 192.168.137.1 je přiřazeno privátnímu adaptéru a zároveň je tato IP použita jako výchozí brána pro DHCP klienty. Použitou adresu sítě lze změnit v registrech.

Mobilní hotspot

[Povinné]

Windows 10 umožňuje sdílet internetové připojení přes ethernet, Wi-Fi nebo mobilní data, vytvořením bezdrátového hotspotu. Aby to fungovalo, musí být váš počítač vybaven alespoň jedním Wi-Fi nebo Bluetooth adaptérem. V případě sdílení připojení Wi-Fi na Wi-Fi dojde po aktivaci funkce Mobilní hotspot k vytvoření bezdrátového adaptéru.

Ve starších verzích systému Windows 10 bylo tuto funkcionalitu nutné konfigurovat z příkazové řádky. V novějších je dostupná v Nastavení (Settings) – Síť a internet (Network & Internet) – Mobilní hotspot (Mobile hotspot).

K mobilnímu hotspotu lze připojit maximálně 8 zařízení v případě Wi-Fi nebo 7 zařízení v případě Bluetooth.

Nástroje pro diagnostiku síťového připojení

[Povinné]

Všechny níže uvedené nástroje pracují jak s protokolem IPv4, tak protokolem IPv6. U starších verzí systému Windows mohou existovat nástroje pro každý protokol zvlášť (např. **ping** a **ping6**).

Ipconfig

[Povinné]

Zobrazí všechny aktuální hodnoty konfigurace sítě TCP/IP a aktualizuje nastavení protokolu DHCP (*Dynamic Host Configuration Protocol*) a služby DNS (*Domain Name System*). Při použití bez parametrů zobrazí příkaz **ipconfig** adresy IPv6 nebo adresu IPv4, masku podsítě a výchozí bránu pro všechny adaptéry.

Syntaxe

ipconfig [**/all**] [**/renew** [*Adaptér*]] [**/release** [*Adaptér*]] [**/flushdns**] [**/displaydns**] [**/registerdns**] [**/showclassid** *Adaptér*] [**/setclassid** *Adaptér* [*ID_třídy*]]

Parametry

/all

Zobrazí úplnou konfiguraci protokolu TCP/IP u všech adaptérů. Bez tohoto parametru zobrazí příkaz **ipconfig** pro každý adaptér pouze adresy IPv6 nebo adresu IPv4, masku podsítě a výchozí bránu. Adaptéry mohou reprezentovat fyzická rozhraní, například instalované síťové karty, nebo logická rozhraní, například telefonická připojení.

/renew [*Adaptér*]

Obnoví konfiguraci DHCP u všech adaptérů (není-li určen adaptér) nebo u konkrétního adaptéru, je-li uveden parametr *Adaptér*. Tento parametr je k dispozici pouze v počítačích s adaptéry

nakonfigurovanými pro automatické přidělování adres IP. Chcete-li určit název adaptéru, zadejte název adaptéru, který se zobrazí při použití příkazu **ipconfig** bez parametrů.

/release [*Adaptér*]

Odešle serveru DHCP zprávu **DHCPRELEASE**, která uvolní aktuální konfiguraci DHCP a vymaže konfiguraci adresy IP u všech adaptérů (není-li určen adaptér) nebo u konkrétního adaptéru, je-li uveden parametr *Adaptér*. Tento parametr zakáže protokol TCP/IP u adaptérů konfigurovaných pro automatické získání adresy IP. Chcete-li určit název adaptéru, zadejte název adaptéru, který se zobrazí při použití příkazu **ipconfig** bez parametrů.

/flushdns

Vyprázdní a vynuluje obsah vyrovnávací paměti přeložených adres klienta DNS. Během řešení potíží se službou DNS můžete v případě nutnosti použít tento postup k odstranění negativních položek vyrovnávací paměti stejně jako kterýchkoli jiných položek, které byly přidány dynamicky.

/displaydns

Zobrazí obsah vyrovnávací paměti přeložených adres klienta DNS. Do zobrazení budou zahrnuty jak položky načtené předem z místního souboru **hosts**, tak i záznamy získané později řešením dotazů na názvy. Tyto informace využívá klientská služba DNS k rychlému překladu často zjišťovaných názvů před odesláním dotazu na konfigurované servery DNS.

/registerdns

Spouští ruční dynamickou registraci názvů DNS a adres IP konfigurovaných v počítači. Tento parametr lze použít při řešení potíží s nezdařenou registrací názvu DNS nebo při řešení problému dynamické aktualizace mezi klientem a serverem DNS bez nutnosti restartování počítače klienta. Názvy registrované službou jsou určeny nastavením služby DNS v rozšířených vlastnostech protokolu TCP/IP.

/showclassid *Adaptér*

Zobrazí identifikátor třídy DHCP pro určený adaptér. Chcete-li zobrazit ID třídy DHCP pro všechny adaptéry, použijte místo parametru *Adaptér* zástupný znak ***** (hvězdička). Tento parametr je k dispozici pouze v počítačích s adaptéry, které jsou konfigurovány pro automatické přidělování adres IP.

/setclassid *Adaptér* [*ID_třídy*]

Nastaví identifikátor třídy DHCP pro určený adaptér. Chcete-li nastavit ID třídy DHCP pro všechny adaptéry, použijte místo parametru *Adaptér* zástupný znak ***** (hvězdička). Tento parametr je k dispozici pouze v počítačích s adaptéry, které jsou konfigurovány pro automatické přidělování adres IP. Není-li určeno ID třídy DHCP, dojde k odebrání aktuálního ID třídy.

Příklady

ipconfig	Zobrazení informací
ipconfig /all	Zobrazení podrobných informací
ipconfig /renew	Obnovení všech adaptérů
ipconfig /renew EL*	Obnovení všech připojení s názvem začínajícím na EL
ipconfig /release *Přip*	Uvolnění všech odpovídajících připojení, např. Připojení k místní síti 1 nebo Připojení k místní síti 2
ipconfig /allcompartments	Zobrazí informace o všech oddílech
ipconfig /allcompartments /all	Zobrazí podrobné informace o všech oddílech

Ping

[Povinné]

Ověřuje dostupnost připojení na úrovni protokolu IP k jinému počítači s protokolem TCP/IP odesíláním zpráv požadavku odezvy ICMP (*Internet Control Message Protocol*). Zobrazí odpovídající přijaté zprávy Odpověď echa spolu s údaji o době přenosu. Příkaz **ping** je základním příkazem protokolu TCP/IP využívaným k odstraňování potíží se spojením, dosažitelností a rozlišením názvů. Při použití bez parametrů příkaz **ping** zobrazí nápovědu.

Syntaxe

ping [**-t**] [**-a**] [**-n** *Počet*] [**-l** *Velikost*] [**-f**] [**-i** *Doba_života*] [**-v** *Typ_služby*] [**-r** *Počet*] [**-s** *Počet*] [{**-j** *Seznam_hostitelů* | **-k** *Seznam_hostitelů*}] [**-w** *Časový_limit*] [**-R**] [**-S** *Zdrojová_adresa*] [**-4**] [**-6**] *Název_cíle*

Parametry

-t

Určuje, že příkaz **ping** má pokračovat v odesílání zpráv požadavku odezvy, dokud nebude přerušen. Chcete-li odesílání zpráv přerušit a zobrazit statistické údaje, stiskněte kombinaci kláves **CTRL+BREAK**. Chcete-li přerušit odesílání zpráv a ukončit práci příkazu **ping**, stiskněte kombinaci kláves **CTRL+C**.

-a

Určuje, že pro cílovou adresu IP má být prováděn zpětný překlad názvů. V případě úspěšného provedení příkaz ping zobrazí odpovídající název hostitele.

-n *Počet*

Určuje počet odeslaných zpráv požadavku odezvy. Výchozí hodnota je 4.

-l *Velikost*

Určuje počet bajtů datového pole v odeslaných zprávách požadavku odezvy. Výchozí hodnota je 32. Maximální hodnota parametru *Velikost* je 65527.

-f

Určuje, že zprávy s požadavkem na odezvu jsou odesílány s příznakem **nefragmentovat** v hlavičce nastaveným na hodnotu 1 (k dispozici pouze v protokolu IPv4). Zprávu s požadavkem na odezvu nemohou směrovače na cestě k cíli fragmentovat. Tento parametr vám může pomoci při odstraňování potíží s jednotkami PMTU (*Path Maximum Transmission Unit*).

-i *Doba_života*

Určuje hodnotu pole TTL v záhlaví IP odeslaných zpráv požadavku odezvy. Výchozí hodnotu pole TTL určuje hostitel. Maximální hodnota parametru *Doba_života* je 255.

-v *Typ_služby*

Určuje hodnotu pole TOS (*Type of Service*) v hlavičce protokolu IP odeslaných zpráv s požadavkem na odezvu (k dispozici pouze v protokolu IPv4). Výchozí hodnota je 0. Parametr *Typ služby* může nabývat desítkových hodnot od 0 do 255.

-r *Počet*

Určuje, že má být použita možnost Záznam trasy v záhlaví IP, která zaznamená trasu zprávy požadavku odezvy a odpovídající zprávy Odpověď echa (k dispozici pouze v protokolu IPv4). Každému směrování na trase odpovídá jedna položka možnosti Záznam trasy. Pokud je to možné, použijte hodnotu parametru *Počet* větší nebo rovnou počtu směrování na trase mezi zdrojem a cílem. Minimální hodnota parametru *Počet* je 1, maximální 9.

-s *Počet*

Určuje, že má být použita možnost Časové razítko Internetu v záhlaví IP, která zaznamená okamžik přijetí požadavku odezvy a odpovídající zprávy Odpověď echa jednotlivými směrovači. Minimální hodnota parametru *Počet* je 1, maximální 4. Tento parametr je povinný pro cílové místní adresy v rámci propojení.

-j *Seznam_hostitelů*

Určuje, že zprávy požadavku odezvy použijí možnost Volného režimu v hlavičce protokolu IP s množinou mezilehlých cílových umístění uvedených v *Seznamu_hostitelů* (k dispozici pouze v protokolu IPv4). U směrování ve volném režimu lze následné prostřední cíle oddělit jedním nebo více směrovači. Maximální počet adres nebo názvů v seznamu hostitelů je 9. Seznam hostitelů je sada adres IP (pomocí čísel v desítkové soustavě oddělených tečkami) oddělených mezerami.

-k *Seznam_hostitelů*

Určuje, že zprávy požadavku odezvy použijí možnost Striktního režimu v hlavičce protokolu IP s množinou mezilehlých cílových umístění uvedených v *Seznamu_hostitelů* (k dispozici pouze v protokolu IPv4). V případě pevného režimu směrování musí být následující postupný cíl vždy přímo dosažitelný (musí se jednat o sousední směrovač rozhraní aktuálního směrovače). Maximální počet adres nebo názvů v seznamu hostitelů je 9. Seznam hostitelů je sada adres IP (pomocí čísel v desítkové soustavě oddělených tečkami) oddělených mezerami.

-w *Časový_limit*

Určuje dobu čekání v milisekundách na zprávu Echo Response, odpovídající dané zprávě požadavku odezvy. Není-li tato zpráva přijata v daném časovém intervalu, zobrazí se chybová zpráva „Vypršel časový limit žádosti“. Výchozí interval je 4 000 (4 sekundy).

-R

Určuje, že je sledována cesta přenosu paketů (k dispozici pouze v protokolu IPv6).

-S *Zdrojová_adresa*

Určuje, zdrojovou adresu, která má být použita (k dispozici pouze v protokolu IPv6).

-4

Určuje, že pro příkaz **ping** je použit protokol IPv4. Tento parametr není nutný k označení cílového hostitele s adresou protokolu IPv4. Nutný je pouze k identifikaci cílového hostitele podle názvu.

-6

Určuje, že pro příkaz **ping** je použit protokol IPv6. Tento parametr není nutný k označení cílového hostitele s adresou protokolu IPv6. Nutný je pouze k identifikaci cílového hostitele podle názvu.

Název_cíle

Určuje název hostitele nebo adresu IP cíle.

Tracert

[Povinné]

Určuje trasu k cíli tím, že do cíle odesílá zprávy protokolu ICMP (*Internet Control Message Protocol*) nebo protokolu ICMPv6 s požadavkem na odezvu se zvyšujícími se hodnotami polí TTL (*Time-To-Live*). Zobrazenou cestu představuje seznam bližších rozhraní směrovačů na trase mezi zdrojovým hostitelem a cílem. Bližší rozhraní je rozhraní směrovače, které je k odesílajícímu hostiteli z hlediska cesty nejblíže. Samotný příkaz **tracert** bez parametrů zobrazí nápovědu.

Syntaxe

tracert [**-d**] [**-h** *Maximální_počet_směrování*] [**-j** *Seznam_hostitelů*] [**-w** *Časový_limit*] [**-R**] [**-S** *Zdrojová_adresa*] [**-4**] [**-6**] *Cílový_název*

Parametry

-d

Způsobí, že příkaz **tracert** nebude překládat adresy IP zprostředkujících směrovačů na jejich názvy. Tímto lze zobrazení výstupu příkazu **tracert** urychlit.

-h *Maximální_počet_směrování*

Určuje maximální počet směrování v cestě pro vyhledání cíle. Výchozí počet je 30 směrování.

-j *Seznam_hostitelů*

Určuje, zda má být ve zprávách s požadavkem na odezvu použita možnost volného režimu v hlavičce IP se sadou zprostředkujících cílů určených parametrem *Seznam_hostitelů*. U směrování ve volném režimu lze následné prostřední cíle oddělit jedním nebo více směrovači. Maximální počet adres nebo názvů v seznamu hostitelů je 9. Parametr *Seznam_hostitelů* je sada adres IP (v desítkovém zápisu s tečkami) oddělených mezerami. Tento parametr použijte pouze v případě trasování adres protokolu IPv4.

-w *Časový_limit*

Určuje dobu v milisekundách, po kterou bude očekáváno přijetí zprávy protokolu ICMP o překročení času nebo zprávy s odpovědí echa odpovídající odeslané zprávě s požadavkem na odezvu. Není-li v daném časovém limitu žádná zpráva přijata, zobrazí se hvězdička (*). Výchozí časový limit je 4 000 (4 sekundy).

-R

Určuje, že má být při odeslání zprávy s požadavkem na odezvu do místního počítače použita rozšířená hlavička směrování IPv6 a že jako cíl má být použit zprostředkující cíl spolu s testováním zpáteční trasy.

-S

Určuje zdrojovou adresu ve zprávách s požadavkem na odezvu. Tento parametr použijte pouze v případě trasování adres protokolu IPv6.

-4

Určuje, že program **tracert** použije k trasování pouze protokol IPv4.

-6

Určuje, že program **tracert** použije k trasování pouze protokol IPv6.

Název_cíle

Určuje cíl určený adresou IP nebo názvem hostitele.

Pathping

[Povinné]

Poskytuje informace o zpoždění a ztrátách v síti u jednotlivých směrovačů na trase mezi zdrojem a cílem. Příkaz **pathping** po určitou dobu opakovaně zasílá všem směrovačům mezi zdrojem a cílem zprávy s požadavkem na odezvu a na základě paketů vrácených od jednotlivých směrovačů pak vypočte výsledky. Protože příkaz **pathping** zobrazuje úroveň ztráty paketů na všech zadaných směrovačích nebo propojeních, můžete určit, u kterých směrovačů nebo podsítí pravděpodobně vznikají problémy. Příkaz **pathping** provede ekvivalent příkazu **tracert** pomocí identifikace jednotlivých směrovačů v cestě. Všem směrovačům pak po stanovenou dobu zasílá testovací pakety a na základě počtu navrácených paketů vypočte statistiku. Při použití bez parametrů zobrazí příkaz **pathping** nápovědu.

Syntaxe

pathping [**-n**] [**-h** *Maximální_počet_směrování*] [**-g** *Seznam_hostitelů*] [**-p** *Perioda*] [**-q** *Počet_dotazů*] [**-w** *Časový_limit*] [**-i** *Adresa_IP*] [**-4**] [**-6**] [*Název_cíle*]

Parametry

-n

Zabrání příkazu **pathping** v pokusu o převedení adres IP směrovačů na trase na názvy. Tímto způsobem lze někdy urychlit zobrazení výsledků příkazu **pathping**.

-h *Maximální_počet_směrování*

Určuje maximální počet směrování v cestě pro vyhledání cíle. Výchozí počet je 30 směrování.

-g *Seznam_hostitelů*

Určuje, zda má být ve zprávách s požadavky na odezvu použita možnost volné trasy zdroje v hlavičce protokolu IP se sadou dočasných cílů určených parametrem *Seznam_hostitelů*. U směrování ve volném režimu lze následné prostřední cíle oddělit jedním nebo více směrovači. Maximální počet adres nebo názvů v seznamu hostitelů je 9. Parametr *Seznam_hostitelů* je sada adres IP (v desítkovém zápisu s tečkami) oddělených mezerami.

-p *Perioda*

Určuje počet milisekund mezi jednotlivými po sobě jdoucími testovacími pakety. Výchozí doba je 250 milisekund (1/4 sekundy).

-q *Počet_dotazů*

Určuje počet zpráv požadavku odezvy odeslaných jednotlivým směrovačům na trase. Výchozí hodnota je 100 dotazů.

-w *Časový_limit*

Určuje počet milisekund doby čekání na odpověď. Výchozí doba je 3 000 milisekund (3 s).

-i *Adresa_IP*

Určuje zdrojovou adresu.

-4

Určuje, že příkaz **pathping** použije pouze protokol IPv4.

-6

Určuje, že příkaz **pathping** použije pouze protokol IPv6.

Název_cíle

Určuje cíl zadaný jako adresa IP nebo jako název hostitele.

Příklady

pathping -n corp1	Vypíše informace o zpožděních a ztrátách u jednotlivých směrovačů na cestě k počítači **corp1**

Společné úkoly

- Pro přístup na server **file** (a jiné) přes síťové rozhraní *Default switch* je nutné použít jeho plně kvalifikované doménové jméno **file.nepal.local**
- Přístupové údaje na server file: **nepal\hstudent** heslo: **aaa**

Lab LS00 – konfigurace virtuálních stanic

[Provést]

Připojte sítové adaptéry stanic k následujícím virtuálním přepínačům:

Adaptér (MAC suffix)	LAN1 (-01)	LAN2 (-02)	LAN3 (-03)	LAN4 (-04)
w10-base	Default switch	Private1	Nepřipojeno	Nepřipojeno
w10-wadk	Nepřipojeno	Private1	Private2	Nepřipojeno
w2016-base	Nepřipojeno	Nepřipojeno	Private2	Nepřipojeno

Lab LS01 – Deaktivace firewallu

[Povinné]

Cíl cvičení

Pro zjednodušení následujících úkolů vypneme na všech použitých stanicích firewall. (Pozn.: Technologii Windows Firewall bude věnováno samostatné cvičení)

Potřebné virtuální stroje

w10-base (w10-base)
w10-wadk (w10-wadk)
w2016-base (w2016-base)

1. Přihlaste se na **w10-base** pod účtem student (heslo **aaa**)
2. Spusťte příkazový řádek nebo powershell jako administrátor
3. Zadejte příkaz **netsh advfirewall set allprofiles state off**
4. Opakujte kroky 1-3 na **w10-wadk**
5. Přihlaste se na **w2016-base** pod účtem administrator (heslo **aaa**)
6. Zopakujte kroky 2 a 3 na **w2016-base**

Lab LS02 – Deaktivace nepoužitých síťových adaptérů

[Povinné]

Cíl cvičení

Pro zjednodušení následujících úkolů vypneme na všech použitých stanicích nevyužité síťové adaptéry.

Potřebné virtuální stroje

w10-base (w10-base)
w10-wadk (w10-wadk)
w2016-base (w2016-base)

Další prerekvizity

Dokončený úkol LS01.

1. Přihlaste se na **w10-base** pod účtem student (heslo **aaa**)
2. Otevřete okno síťových připojení pomocí příkazu **ncpa.cpl**

- Alternativně lze vyvolat proklikem na **Change adapter settings** (Změnit nastavení adaptéru) v **Network and Sharing Center** (Centrum síťových připojení a sdílení) nebo proklikem z centra **Settings** (Nastavení) – sekce **Network & Internet** (Síť a internet) – **Ethernet** – odkaz **Change adapter options** (Změnit možnosti adaptéru)

3. Vyberte adaptér **LAN3** a z kontextové nabídky zvolte **Disable** (Zakázat)
4. Vyberte adaptér **LAN4** a z kontextové nabídky zvolte **Disable** (Zakázat)
5. Přihlaste se na **w10-wadk** pod účtem student (heslo **aaa**)
6. Spusťte příkazový řádek nebo powershell jako administrátor
7. Zadejte příkaz **netsh interface set interface name="LAN1" admin=DISABLED**
8. Zadejte příkaz **netsh interface set interface name="LAN4" admin=DISABLED**
9. Přihlaste se na **w2016-base** pod účtem administrator (heslo **aaa**)
10. Spusťte powershell jako administrátor
11. Zadejte příkaz **Get-NetAdapter** pro zobrazení dostupných síťových adaptérů
12. Zadejte **Disable-NetAdapter -Name LAN1 -Confirm:$false**
13. Opět zobrazte síťové adaptéry pomocí **Get-NetAdapter**
14. Zakažte všechny odpojené adaptéry (disconnected) pomocí příkazu **Get-NetAdapter | where Status -eq "Disconnected" | Disable-NetAdapter -confirm:$false**

Studentské úkoly

Lab S01 – APIPA a Link-local IPv6

[Povinné]

Cíl cvičení

Naše síťové adaptéry jsou nastavené na získání IP adresy z DHCP serveru. Žádný DHCP server však v naší topologii nemáme (s výjimkou sítě *Default switch* připojené k adaptéru LAN1 stanice w10-base). Ověřme si tedy, že si naše stanice vygenerovaly automatickou IP adresu z rozsahu **169.254.0.0/16**. Zároveň si povšimněte přítomnosti Link-local IPv6 adresy z rozsahu fe80::/10.

Potřebné virtuální stroje

w10-base (w10-base)
w10-wadk (w10-wadk)
w2016-base (w2016-base)

Další prerekvizity

Dokončený úkol LS02.

1. Přihlaste se na **w10-base** pod účtem student (heslo **aaa**)
2. Otevřete okno síťových připojení pomocí příkazu **ncpa.cpl**
3. Vyberte adaptér **LAN2** a z kontextové nabídky zvolte **Status** (Stav) a následně **Details…** (Podrobnosti…)
4. Přihlaste se na **w10-wadk** pod účtem student (heslo **aaa**).
5. Spusťte příkazový řádek nebo powershell jako administrátor
6. Zadejte příkaz **ipconfig**
   - U rozhraní LAN2 i LAN3 naleznete položku **Autoconfiguration IPv4 Address** (APIPA) a Link-local IPv6 Address
   - Pozn.: další informace o rozhraních můžete získat pomocí **ipconfig /all**
7. Přihlaste se na **w2016-base** pod účtem administrator (heslo **aaa**)
8. Spusťte powershell jako administrátor
9. Zadejte příkaz **Get-NetIPAddress | where InterfaceAlias -eq LAN3**
   - Všimněte si zápisu masky sítě u APIPA v CIDR formátu jako položku PrefixLength
   - Alternativně můžete údaje zobrazit přehledněji v tabulce – toho docílíte přidáním další roury a příkazu format-table, tj.:
     Get-NetIPAddress | where InterfaceAlias -eq LAN3 | Format-Table
10. Ověřte konektivitu z **w2016-base** na **w10-wadk** pomocí příkazu **ping -4 <APIPA_w10-wadk_na_LAN3>**
    - Jelikož má w10-wadk APIPA na obou rozhraních, proto nemusí být **ping -4 w10-wadk** úspěšný)
11. Ověřte nedostupnost **w10-base** z **w2016-base**
    - Stanice nejsou na stejné síti, proto nelze použít překlad jména
      i. Zjistěte APIPA adresu stanice w10-base
      ii. Na w2016-base zadejte příkaz **ping <APIPA_w10-base>**
12. Ověřte nedostupnost přístupu k internetu pomocí **ping 1.1.1.1** (veřejný DNS server CloudFlare) nebo **ping 8.8.8.8** (veřejný DNS server Google), případně jinou veřejnou IP, u níž je jistota dostupnosti při fungujícím připojení k internetu.

Lab S02 – Internet Connection Sharing [Povinné]

Cíl cvičení

V předchozím úkolu jsme si ukázali, jak nám APIPA může umožnit omezenou základní síťovou komunikaci mezi dvěma stanicemi. APIPA nám však neumožní přístup do dalších sítí nebo k internetu. V tomto nám může pomoci služba sdílení připojení k internetu (Internet Connection Sharing), kdy můžeme na pár kliknutí rozchodit veškeré potřební síťové služby. Tuto službu můžeme v případě potřeby i použít opakovaně. Jedinou podmínkou je modifikace adresy použité sítě.

Potřebné virtuální stroje

w10-base (w10-base)
w10-wadk (w10-wadk)
w2016-base (w2016-base)

Další prerekvizity

Dokončený úkol S01.

1. Přihlaste se na **w10-base** pod účtem student (heslo **aaa**)
2. Otevřete okno síťových připojení pomocí příkazu **ncpa.cpl**
3. Vyberte adaptér **LAN1** a z kontextové nabídky zvolte **Properties** (Vlastnosti) a následně přejděte na kartu **Sharing** (Sdílení)
4. Zaškrtněte políčko **Allow other network users to connect through this computer's Internet connection** (Umožnit ostatním uživatelům v síti využívat připojení k internetu tohoto počítače)
5. V případě kdy je aktivních více dalších síťových rozhraní, je ještě nutné z nabídky **Home networking connection** (Připojení k domácí síti) zvolit rozhraní na kterém bude konektivita dostupná (LAN2).
6. Pod tlačítkem **Settings…** (Nastavení…) lze zpřístupnit služby z privátní sítě uživatelům internetu (jsou připraveny základní síťové služby, např. služba označená 1706 je http na TCP portu 80, apod., samozřejmě lze definovat vlastní)
7. Potvrďte **OK**
8. Potvrzením dojde k nastavení statické IP adresy na rozhraní LAN2 a spuštění služby Internet Connection Sharing
   - Ověřte přítomnost statické adresy 192.168.137.1
   - Spuštění služby ověřte v MMC konzoli služeb **services.msc**
9. Přihlaste se na **w10-wadk** pod účtem student (heslo **aaa**).
10. Spusťte příkazový řádek nebo powershell jako administrátor
11. Zadejte příkaz **ipconfig /release LAN2**
    - Dojde k uvolnění/odebrání IP adresy z daného rozhraní
12. Zadejte příkaz **ipconfig /renew LAN2**
    - Dojde k získání IP adresy z rozsahu 192.168.137.0/24 pomocí DHCP ze stanice w10-base
13. Zadejte příkaz **ipconfig /all** a ověřte přidělenou konfiguraci – Default Gateway (výchozí bránu), DHCP server, DNS server (všechny budou odkazovat na 192.168.137.1 a specifický DNS sufix domény mshome.net)
14. Nyní budeme chtít nasdílet konektivitu z **w10-wadk** stanici **w2016-base**. Aby nedošlo ke kolizi, musíme nejdříve upravit v registrech adresu sítě používanou službou ICS. Spusťte příkaz **regedit**.

15. V levém panelu přejděte do **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\SharedAccess\Parameters**
16. Upravte hodnoty **ScopeAddress** a **ScopeAddressBackup** na **192.168.138.1**
    - Pomocí položky **Modify** z kontextové nabídky na jménu vlastnosti (nebo jen dvojklikem na jméno vlastnosti) se zobrazí dialog, kde lze hodnotu upravit
17. Zavřete okno editoru registrů
18. Nasdílejte síťovou konektivitu z rozhraní **LAN2** pro rozhraní **LAN3** zopakováním kroků 2 – 7
19. Přihlaste se na **w2016-base** pod účtem administrator (heslo **aaa**)
20. Spusťte příkazový řádek nebo powershell jako administrátor
21. Zadejte příkaz **ipconfig /release LAN3**
    - Dojde k uvolnění/odebrání IP adresy z daného rozhraní
22. Zadejte příkaz **ipconfig /renew LAN3**
    - Dojde k získání IP adresy z rozsahu 192.168.138.0/24 pomocí DHCP ze stanice w10-wadk
23. Ověřte dostupnost přístupu k internetu pomocí **ping 1.1.1.1** (veřejný DNS server CloudFlare) nebo **ping 8.8.8.8** (veřejný DNS server Google), případně jinou veřejnou IP, u níž je jistota dostupnosti při fungujícím připojení k internetu.
24. Ověřte funkčnost DNS pomocí **ping one.one.one.one** (veřejný DNS server CloudFlare s IP 1.1.1.1) a **ping www.google.com**

Lab S03 – Vypnutí Internet Connection Sharing

[Povinné]

Cíl cvičení

Vypnout službu sdílení připojení k internetu na stanicích w10-base a w10-wadk.

Potřebné virtuální stroje

w10-base (w10-base)
w10-wadk (w10-wadk)

Další prerekvizity

Dokončený úkol S02.

1. Přihlaste se na **w10-base** pod účtem student (heslo **aaa**)
2. Otevřete okno síťových připojení pomocí příkazu **ncpa.cpl**
3. Vyberte adaptér **LAN1** a z kontextové nabídky zvolte **Properties** (Vlastnosti) a následně přejděte na kartu **Sharing** (Sdílení)
4. Odškrtněte políčko **Allow other network users to connect through this computer's Internet connection** (Umožnit ostatním uživatelům v síti využívat připojení k internetu tohoto počítače)
5. Potvrďte **OK**
6. Přihlaste se na **w10-wadk** pod účtem student (heslo **aaa**)
7. Vypněte službu ICS na rozhraní LAN2 zopakováním kroků 2 – 5

Lab S04 – Nastavení statických IP adres

[Povinné]

Cíl cvičení

Vyzkoušet si různé možnosti jak nakonfigurovat statickou adresu.

Potřebné virtuální stroje

w10-base (w10-base)
w10-wadk (w10-wadk)
w2016-base (w2016-base)

Další prerekvizity

Dokončený úkol S03.

1. Přihlaste se na **w10-base** pod účtem student (heslo **aaa**)
2. Otevřete okno síťových připojení pomocí příkazu **ncpa.cpl**
3. Vyberte adaptér **LAN2** a z kontextové nabídky zvolte **Properties** (Vlastnosti).
4. Vyberte **Protokol IP verze 4 (TCP/IPv4)** a zvolte **Properties** (Vlastnosti).
5. Nastavte:
   - IP adresa: 192.168.1.1
   - Maska: 255.255.255.0
   - Výchozí bránu a DNS ponechte prázdné
6. Potvrďte **OK**
7. Zavřete ok s Vlastnostmi adaptéru pomocí **Close**
8. Přihlaste se na **w10-wadk** pod účtem student (heslo **aaa**)
9. Spusťte příkazový řádek nebo powershell jako administrátor
10. Zadejte příkaz **netsh interface ipv4 set address "LAN2" static 192.168.1.20 255.255.255.0 192.168.1.1**
11. Zadejte příkaz **netsh interface ipv4 set address "LAN3" static 10.10.10.1 255.255.255.0**
12. Přihlaste se na **w2016-base** pod účtem administrator (heslo **aaa**)
13. Spusťte powershell jako administrátor
14. Zadejte příkaz **New-NetIPAddress -IPAddress 10.10.10.20 -DefaultGateway 10.10.10.1 -PrefixLength 24 -InterfaceIndex (Get-NetAdapter | where Name -eq "LAN3").InterfaceIndex**

Lab S05 – Zobrazení směrovací tabulky

[Povinné]

Cíl cvičení

Zobrazit si směrovací tabulku.

Pozor: Desktopové Windows, jakožto klientský systém, nemají na rozdíl od serverové verze k dispozici jednoduše uživatelsky konfigurovatelnou podporu směrování a NAT (mimo dříve zmíněné ICS). U serverových Windows má toto na starosti role Remote Access, resp. její funkcionalita označovaná Routing and Remote Access. V případě desktopového systému lze vhodným zásahem do registrů zneužít funkcionalitu navazující na Hyper-v a Default switch. Konfigurace však přesahuje potřeby kurzu IW1.

Potřebné virtuální stroje

w10-base (w10-base)

Další prerekvizity

Dokončený úkol S04.

1. Přihlaste se na **w10-base** pod účtem student (heslo **aaa**)

2. Spusťte příkazový řádek nebo powershell jako administrátor
3. Zadejte příkaz **route print**
4. Prostudujte obsah směrovací tabulky
5. Zadejte příkaz **netsh interface ipv4 show route**
6. Prostudujte obsah směrovací tabulky

Lab S06 – Nástroje ping, tracert a pathping

[Povinné]

Cíl cvičení

Vyzkoušet si ICMP diagnostické nástroje

Potřebné virtuální stroje

w10-base (w10-base)

Další prerekvizity

Dokončený úkol S05.

1. Přihlaste se na **w10-base** pod účtem student (heslo **aaa**)
2. Spusťte příkazový řádek nebo powershell jako administrátor
3. Vyzkoušejte si příkaz ping
   - **ping /?**
     i. Zobrazení dostupných přepínačů
   - **ping one.one.one.one**
   - **ping 1.1.1.1**
4. Vyzkoušejte příkaz tracert
   - **tracert /?**
   - **tracert one.one.one.one**
5. Vyzkoušejte příkaz pathping
   - **pathping /?**
   - **pathping one.one.one.one**
     i. zobrazení výsledků může dle délky trasy trvat až 5 minut

Lab S07 – základy IPv4 adresace

[Povinné]

Cíl cvičení

Vyzkoušet si práci s IP adresami

Potřebné virtuální stroje

N/A

Mějme IP adresu 147.229.136.13 s maskou délky 19 bitů. Vypočítejte:

1. binární zápis IP adresy
2. adresu sítě (tj. adresa rozhraní obsahuje pouze samé nulové bity)
3. broadcastovou adresu (tj. adresa rozhraní obsahuje pouze samé jedničkové bity)
4. binární zápis masky
5. masku v tečkové notaci
6. počet adresovatelných zařízení v síti

Lab S08 – Subnetting

[Povinné]

Cíl cvičení

Vyzkoušet si práci s IP adresami

Potřebné virtuální stroje

N/A

Mějme rozsah IP adres 10.0.0.0 s maskou délky 21 bitů. Rozdělte síť na několik menších rozsahů, tak abyste splnili následující požadavky:

- síť A, alespoň 800 stanic
- síť B, alespoň 340 stanic
- síť C, alespoň 150 stanic

Postup:

1. seřadíme si požadované sítě podle velikosti od největší (doporučeno)
2. ke každé síti najdeme, kolik bitů bude potřeba na adresu sítě nalezením nejbližšího *n*, takového aby *2n – 2 > počet stanic*
   - obvykle je vhodné počítat i s rezervou na úrovni alespoň 5-10%, tj. při požadavku na 250 stanic je sice dostačující 8 bitů, které umožní adresovat 254 stanic, ale v blízké budoucnosti může dojít k potřebě přidat další stanice, což povede k nutnosti síť znovu přerozdělit
   - síť A => 1024-2 stanic => 10 bitů
   - síť B => 512-2 stanic => 9 bitů
   - síť C => 256-2 stanic => 8 bitů
3. dostupný rozsah = 21 bitů maska = 11 bitů rozhraní = 2048-2 stanic = 10.0.0.1-10.0.7.254
4. rozdělíme rozsah
   - síť A => 10.0.0.0/22 = 10.0.0.1-10.0.3.254
   - síť B => 10.0.4.0/23 = 10.0.4.1-10.0.5.254
   - síť C => 10.0.6.0/24 = 10.0.6.1-10.0.6.254
   - nevyužito = 10.0.7.0/24 = 10.0.7.1-10.0.7.254