

# Serverové systémy Microsoft Windows

IW2/XMW2 2012/2013

**Jan Fiedor**

ifiedor@fit.vutbr.cz

Fakulta Informačních Technologií

Vysoké Učení Technické v Brně

Božetěchova 2, 612 66 Brno

Revize 17. 3. 2013

# Active Directory

## Replikace

# Replikace

- Přesun dat mezi řadiči domény (v doméně i lese)
  - Zajišťuje dostupnost dat potřebných pro fungování Active Directory (autentizaci, vyhledávání, ...)
- Probíhá tzv. *pull* metodou
  - Stahování dat z okolních řadičů domény
- Řeší dva základní problémy
  - Výběr dat, jenž mají být přesunuta
    - Výběr na úrovni oddílů databáze Active Directory
  - Zjištění (nejvhodnější) cesty pro přesun dat
    - Zjištění na základě topologie sítě Active Directory

# Místa (*Sites*)

- Oblasti vyznačující se dobrou konektivitou
  - Většinou odpovídají fyzickým umístěním (budova, ...)
- Definovány rozsahy jedné nebo více (pod)sítí
  - Rozsahy reprezentovány objekty podsítí (*subnets*)
- Reprezentovány objekty míst (*site objects*)
  - Uloženy v kontejneru **Sites** v oddílu konfigurace
- Určují průběh replikace
  - Tvoří hranici mezi místní a mezimístní replikací
- Slouží k lokalizaci služeb

# Vytvoření (objektu) podsítě

The image shows the 'Lokality a služby Active Directory' (Active Directory Sites and Services) console. A context menu is open over the 'Subnets' folder, with 'Nová podsít...' (New Subnet...) selected. A blue arrow points from this menu item to the 'Nový objekt – Podsít' (New Object - Subnet) dialog box.

**Nový objekt – Podsít**

Umístění: testing.local/Configuration/Sites/Subnets

Zadejte pomocí zápisu síťových předpon (adresa/délka předpony) předponu adresy, kde délka předpony označuje počet pevných bitů. Můžete zadat předponu podsítě IPv4 nebo IPv6.  
[Další informace o zadávání předpon adres](#)

Příklad formátu IPv4: 157.54.208.0/20  
 Příklad formátu IPv6: 3FFE:FFFF:0:C000::/64

Předpona:

Název předpony ve službě Active Directory Domain Services:

Vyberte pro tuto předponu objekt lokality.

Název lokality  
 Default-First-Site-Name

OK Storno nápověda

# Vytvoření (objektu) místa

The screenshot shows the 'Lokality a služby Active Directory' console. The left pane shows the 'Sites' folder selected, with a context menu open. The 'Nová lokalita...' option is highlighted. A blue arrow points from this option to the 'Nový objekt - Síť' dialog box.

The dialog box 'Nový objekt - Síť' has the following fields and content:

- Umístění: testing.local/Configuration/Sites
- Název: (empty text box)
- Text: **Vyberte objekt propojení lokalit pro tuto lokalitu. Objekty propojení lokalit jsou umístěny v kontejneru Lokality nebo přenos mezi lokalitami.**
- Table of site connections:
 

Název propojení	Přenos
DEFAULTIPSITELINK	IP
- Buttons: OK, Storno

# Správa replikačního provozu

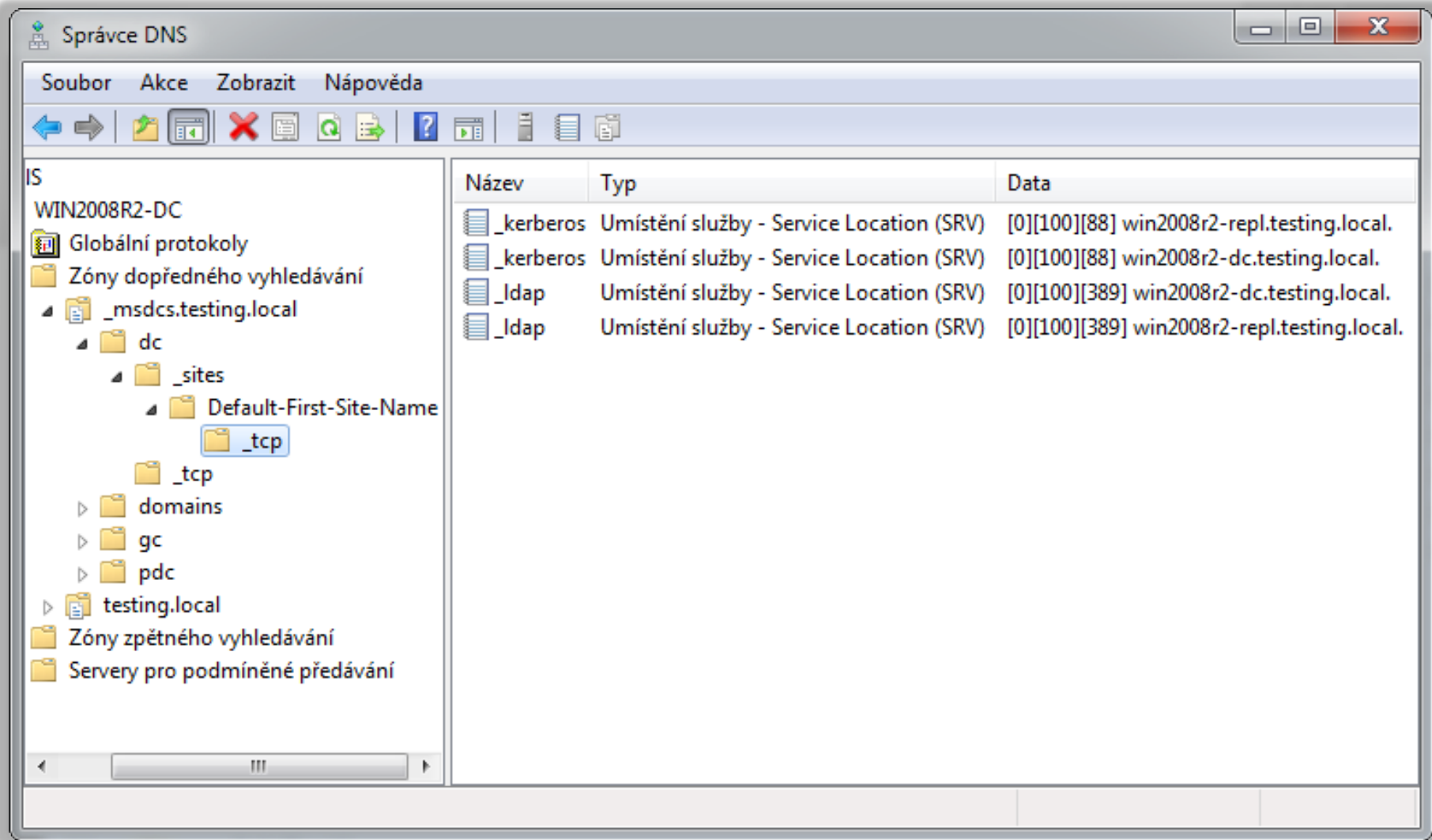
- *Highly connected* sítě (sítě uvnitř míst)
  - Rychlá konektivita
  - Vysoká propustnost
  - Replikace prováděna okamžitě (ihned po změně)
  - Dokončení replikace v rámci sekund
- *Less highly connected* sítě (sítě mezi místy)
  - Pomalá nebo nespolehlivá spojení
  - Replikace prováděna v definovaných intervalech
  - Plánování replikace na konkrétní dobu

# Lokalizace služeb

- Výběr nejbližšího serveru, jenž může poskytnout klientovi (počítači) požadovanou službu
  - Výběr serveru, jenž patří to stejného místa jako klient
- Probíhá na základě SRV záznamů systému DNS
  - Překládají názvy služeb na doménová jména serverů, jenž tyto služby poskytují
  - Každý SRV záznam obsahuje
    - Název služby a port, na kterém služba naslouchá
    - Transportní protokol, který služba využívá (TCP nebo UDP)
    - Doménový název poskytovatele služby (serveru)



# Uložení informací o službách v DNS



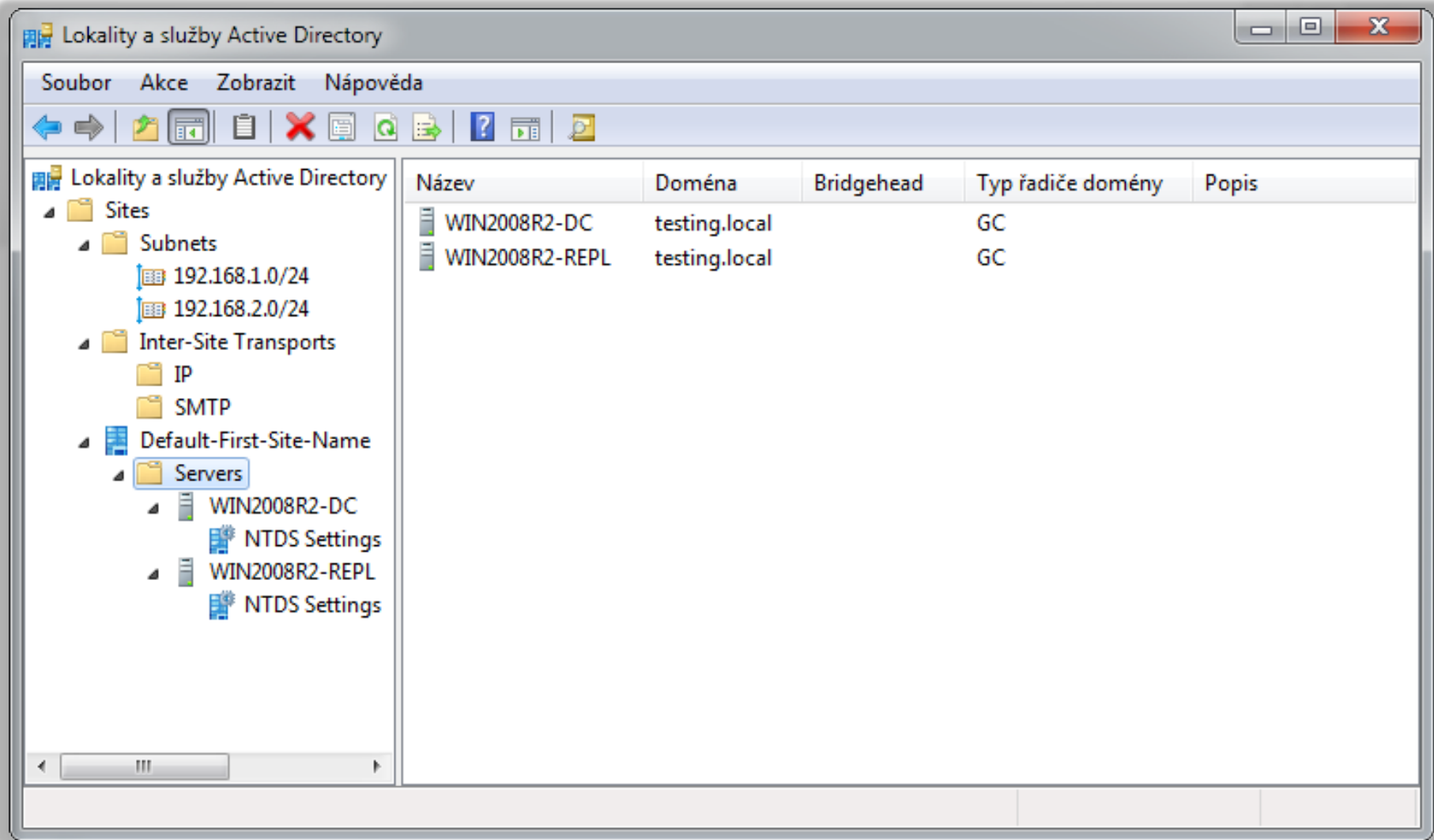
The screenshot shows the DNS Manager console for a server named WIN2008R2-DC. The left pane displays the tree structure of the DNS zones, with the following path selected: IS > WIN2008R2-DC > Globální protokoly > Zóny dopředného vyhledávání > \_msdcs.testing.local > dc > \_sites > Default-First-Site-Name > \_tcp. The right pane displays a table of SRV records for the selected zone.

Název	Typ	Data
_kerberos	Umístění služby - Service Location (SRV)	[0][100][88] win2008r2-repl.testing.local.
_kerberos	Umístění služby - Service Location (SRV)	[0][100][88] win2008r2-dc.testing.local.
_ldap	Umístění služby - Service Location (SRV)	[0][100][389] win2008r2-dc.testing.local.
_ldap	Umístění služby - Service Location (SRV)	[0][100][389] win2008r2-repl.testing.local.

# Lokalizace řadičů domény

- Řadiče domény přiřazovány do míst explicitně
  - Přiřazení je nezávislé na IP adresách řadiče domény
    - Řeší problém nejednoznačnosti přiřazení, pokud má řadič domény přiřazeno více IP adres
  - Výchozí místo řadiče domény (místo, kde je umístěn po vytvoření) je vybráno na základě jeho IP adresy
    - První řadič domény v novém lese je automaticky umístěn do místa **Default-First-Site-Name**
- Lokalizace na základě SRV záznamů systému DNS
  - **\_kerberos** (autentizace) a **\_ldap** (adresářové služby)

# Umístění řadičů domény do míst



The screenshot shows the 'Lokality a služby Active Directory' (Active Directory Sites and Services) console. The left pane shows a tree view with 'Servers' expanded under 'Default-First-Site-Name'. The right pane displays a table of domain controllers.

Název	Doména	Bridgehead	Typ řadiče domény	Popis
WIN2008R2-DC	testing.local		GC	
WIN2008R2-REPL	testing.local		GC	

# Klíčové vlastnosti replikace AD (1)

- Rozdělení úložiště dat (na oddíly)
  - Replikují se pouze data z vybraných oddílů
    - Minimalizace množství přenášených dat
  - Lze vytvářet vlastní oddíly, tzv. oddíly aplikací
    - Obsahují objekty využívané aplikacemi nebo službami, jenž nepatří mezi základní (*core*) služby Active Directory
    - Nemohou obsahovat identity (*security principals*)
    - Správa pomocí nástroje **ntdsutil** (**create / delete nc**)
- Adaptace na podmínky okolní sítě
  - Odlišný průběh replikace v rámci místa a mezi místy

# Klíčové vlastnosti replikace AD (2)

- Automatické vytváření replikační topologie
  - Dynamické (znovu)vytváření cest pro přenos dat
- Replikace na úrovni atributů
  - Přenáší se jen atributy objektů změněné od poslední replikace (inkrementální přenos dat)
- Detekce a řešení kolizí
  - Algoritmy pro řešení různých konfliktů při paralelních změnách atributů stejných objektů
  - Pokud nelze kolizi nijak vyřešit, pak je konfliktní verze objektu přesunuta do kontejneru **LostAndFound**

# Spojení, replikační partneři a cesty

- Spojení (*Connection*)
  - Reprezentují konektivitu mezi dvěma řadiči domény
  - Vždy jednosměrná a to v příchozím (*inbound*) směru
- Replikační partner (*Replication Partner*)
  - Existuje-li spojení z řadiče domény **A** do **B**, pak řadič domény **A** je replikačním partnerem **B**
- Replikační cesta (*Replication Path*)
  - Posloupnost navazujících (sousedících) spojení mezi dvěma řadiči domény

# Vytvoření (objektu) spojení

The screenshot shows the 'Lokality a služby Active Directory' console. The left pane shows the tree structure: Sites > Subnets > Inter-Site Transports > Default-First-Site-Name > Servers > WIN2008R2-DC > NTDS Settings. A context menu is open over 'NTDS Settings', with 'Nové připojení služby Active Directory' selected. A blue arrow points from this menu item to the 'Najít' button in the dialog box.

The dialog box 'Najít - Řadiče domény služby Active Directory' contains the following text:

Řadiče domény služby Active Directory

V následujícím seznamu vyberte podle názvu nebo lokality řadič domény služby Active Directory.

(Seznam aktualizujte kliknutím na tlačítko Najít nebo zvolením příkazu Aktualizovat v nabídce Zobrazit.)

Buttons: Najít, Zastavit, Vymazat vše, OK

Výsledky hledání:

Název serveru	Síť	Doména
WIN2008R2-REPL	Default-First-Site-Name	testing.local
WIN2008R2-DC	Default-First-Site-Name	testing.local

Počet nalezených položek: 2

# Nastavení (objektů) spojení

The image shows two overlapping windows from a Windows Server administration tool. The background window is titled '<Vygenerováno automaticky> - vlastnosti' and has tabs for 'Obecné', 'Objekt', 'Zabezpečení', and 'Editor atributů'. The 'Obecné' tab is active, showing a description field, a 'Změnit plán...' button, and replication source information: 'Server: WIN2008R2-REPL', 'Server: Default-First-Site-Name', 'Replikované názvové kontexty: ForestDnsZones.testing.lo', and 'Částečně replikované názvové kontexty: Všechny další domény'. A blue arrow points from the 'Změnit plán...' button to the foreground window.

The foreground window is titled 'Plán uživatele <Vygenerováno automaticky>'. It features a 24-hour timeline at the top (0, 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 0) and a grid for scheduling. The grid has columns for each hour and rows for days of the week: 'Vše', 'pondělí', 'úterý', 'středa', 'čtvrtek', 'pátek', 'sobota', and 'neděle'. All cells in the grid are filled with blue, indicating a schedule every hour every day. To the right of the grid are radio button options: 'Nikdy', 'Jednou za hodinu' (selected), 'Dvakrát za hodinu', and 'Čtyřikrát za hodinu'. 'OK' and 'Storno' buttons are at the top right. Below the grid, it says 'pondělí až neděle od 0:00 do 0:00'.

- Plán určuje interval pro dotazování replikačních partnerů při vyzývání



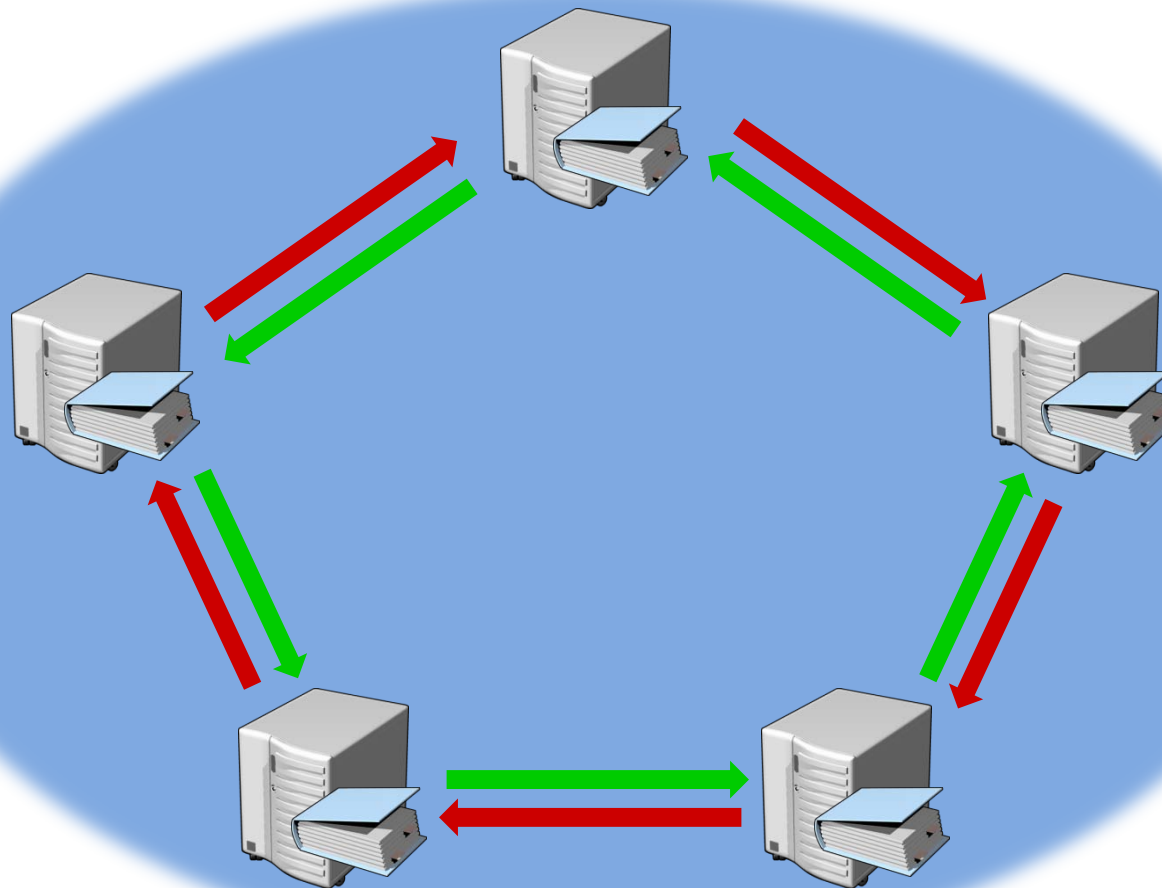
# Replikační topologie

- Množina všech možných replikačních cest
  - Definuje jak přenést data mezi dvěma řadiči domény (přes které řadiče domény musí přenos probíhat)
- Určuje replikační partnery *pull* metody replikace
  - Stahování dat od replikačních partnerů
- Vytváření zajišťuje komponenta Active Directory KCC (*Knowledge Consistency Checker*)
  - Automaticky vytváří potřebné (objekty) spojení
  - Spojení lze vytvářet i manuálně (jsou perzistentní)

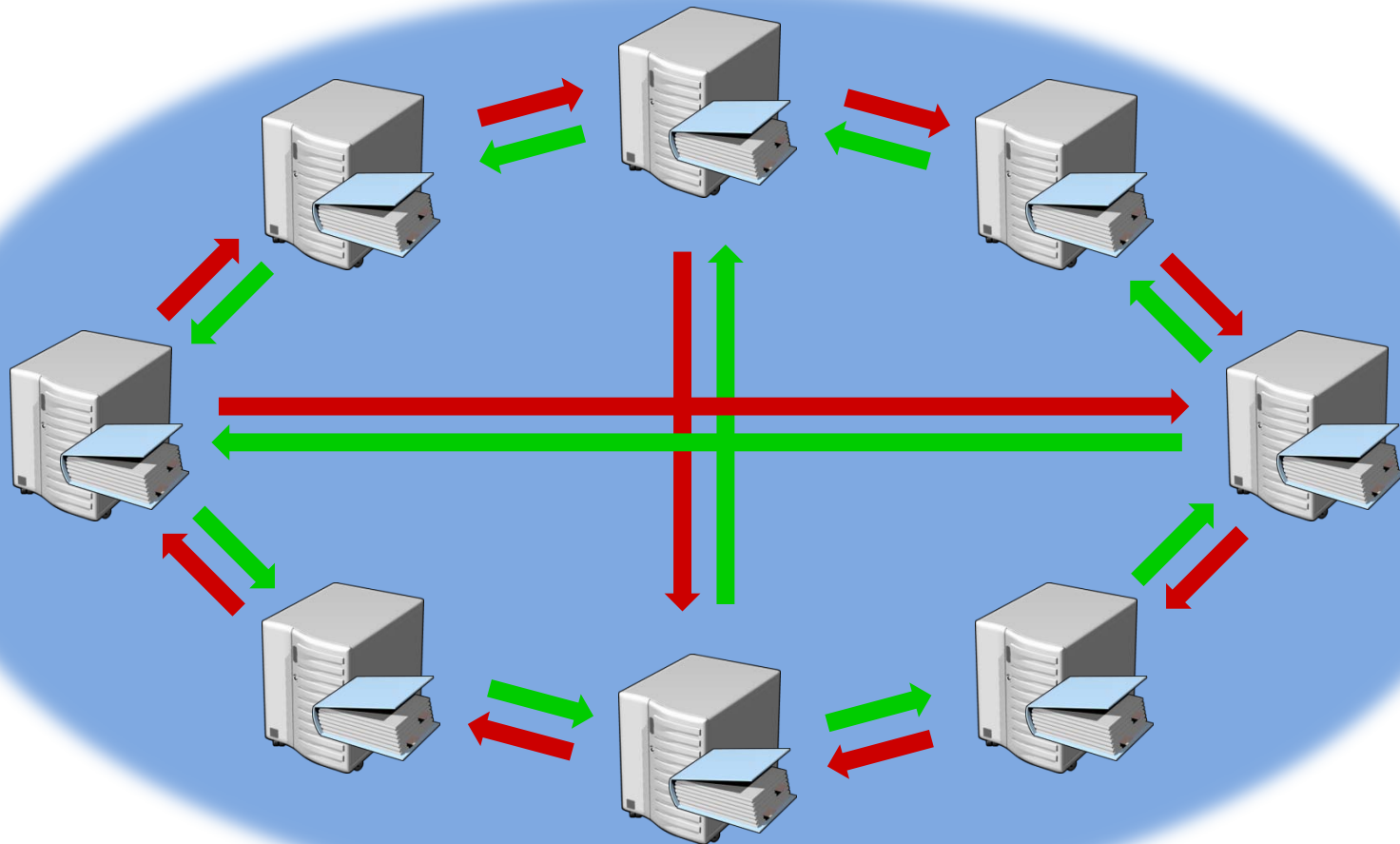
# Generovaná replikační topologie

- Dvoucestná topologie
  - Vždy existují alespoň 2 rozdílné replikační cesty mezi dvěma řadiči domény
- Maximální počet tří skoků
  - Mezi dvěma řadiči domény musí existovat replikační cesta o maximální délce 3
- 2 typy vytvářených topologií
  - Kruh (*ring*) v případě malého počtu řadičů domény
  - Mřížka (*mesh*) pro větší počet řadičů domény

# Topologie typu kruh (*ring*)



# Topologie typu mřížka (*mesh*)



# Místní (*intrasite*) replikace

- Replikace změn v rámci jediného místa
  - Rychlý přenos změn v databázi Active Directory
- Každé dva řadiče domény jsou síťově dostupné
  - Každý řadič domény může komunikovat s kterýmkoliv jiným řadičem domény v daném místě
  - Ignoruje se (fyzická) topologie sítě
- 2 možnosti iniciace replikace
  - Oznámení (*notification*)
  - Vyzývání (*polling*)

# Oznámení (*notification*)

- Zasílá zdrojový řadič domény (replikační partner) po provedení změny v některém svém oddílu AD
  - Po uplynutí 15 sekund prvnímu řadiči domény, který má zdrojový řadič jako svého replikačního partnera
  - Každé 3 sekundy dalšímu (cílovému) řadiči domény
- Po přijetí oznámení řadič domény spustí replikaci
  - Realizuje agent replikace adresáře (DRA)
  - Po dokončení replikace se řadič sám stává zdrojovým řidičem domény a celý proces oznámení se opakuje
    - Replikace změn na všechny řadiče domény v rámci minut

# Vyzývání (*polling*)

- Dotazování se replikačních partnerů na změny
  - Provádí cílový řadič domény co 1 hodinu
  - Pokud došlo ke změnám, je provedena replikace
- Při selhání (replikační partner neodpovídá) dojde k ověření replikační topologie pomocí KCC
  - Ověření dostupnosti všech replikačních partnerů
  - Umožňuje dynamicky měnit replikační topologii když je nedostupný (selže) některý z řadičů domény

# Mezimístní (*intersite*) replikace

- Replikační topologii vytváří generátor mezimístní topologie (ISTG, *Intersite Topology Generator*)
  - Generuje (objekty) spojení na základě propojení míst
- Propojení míst (*site link*)
  - Reprezentuje síťovou konektivitu mezi místy
  - Může zahrnovat dva nebo více míst (*sites*)
  - Vytvářeny vždy manuálně



# Vytvoření (objektu) propojení míst

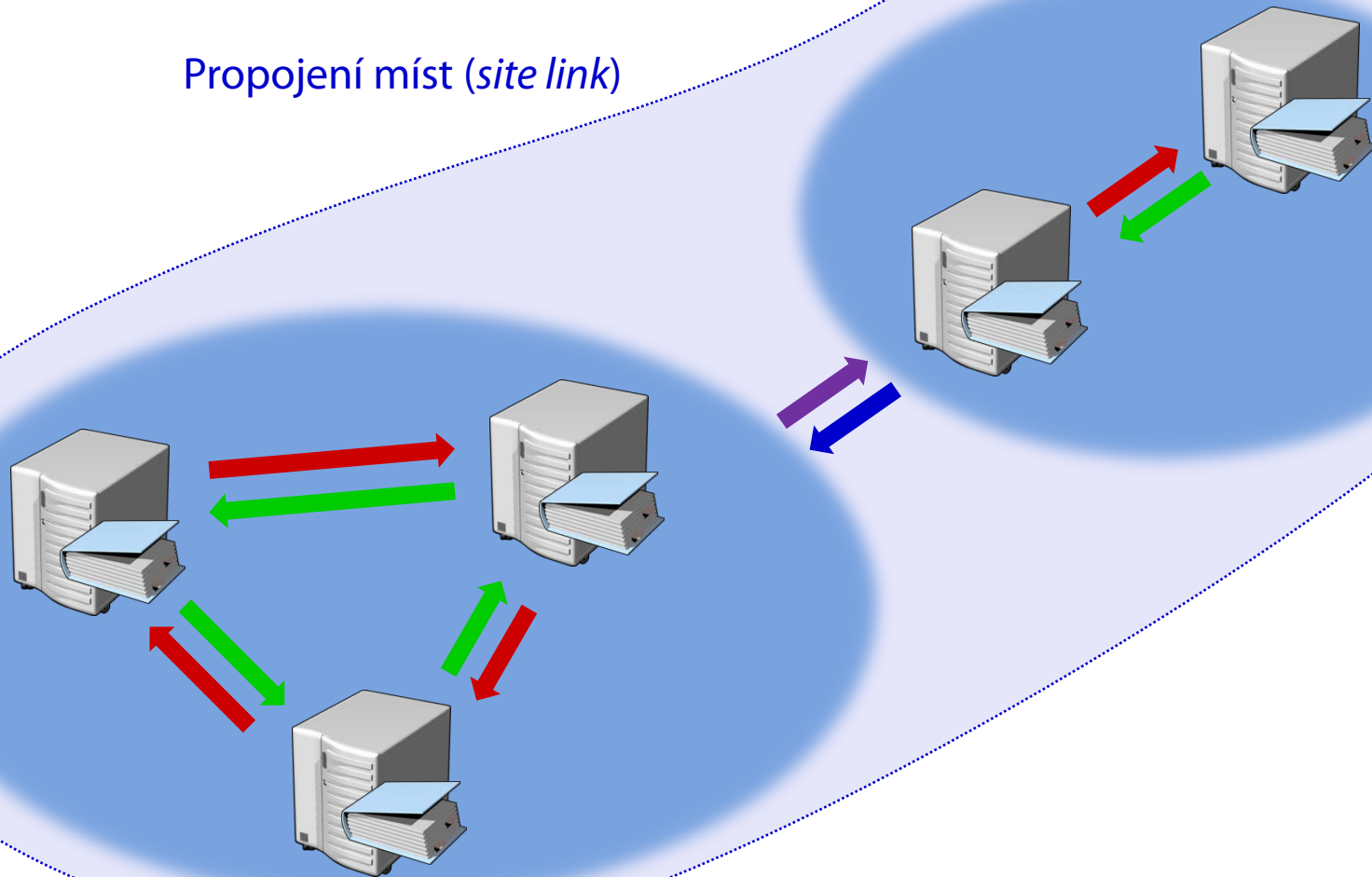
The screenshot shows the Active Directory Sites and Services console. The left pane displays a tree view with 'Sites' expanded to show 'Subnets' (192.168.1.0/24, 192.168.2.0/24) and 'Inter-Site Transports' (IP). A context menu is open over the 'IP' folder, with 'Nové propojení lokalit...' selected. A blue arrow points from this menu item to the 'Nový objekt - Spojení sítí' dialog box.

The dialog box 'Nový objekt - Spojení sítí' has the following fields and options:

- Umístění: testing.local/Configuration/Sites/Inter-Site Tr
- Název: [Empty text box]
- Lokality neobsažené v tomto propojení lokalit: [Empty list box]
- Lokality obsažené v tomto propojení lokalit: Default-First-Site-Name, Second-Site-Name
- Buttons: Přdat >>, << Odebrat
- Footer: Propojení lokalit musí obsahovat alespoň dvě lokality.
- Buttons: OK, Storno

# Ilustrace (objektu) propojení míst

Propojení míst (*site link*)



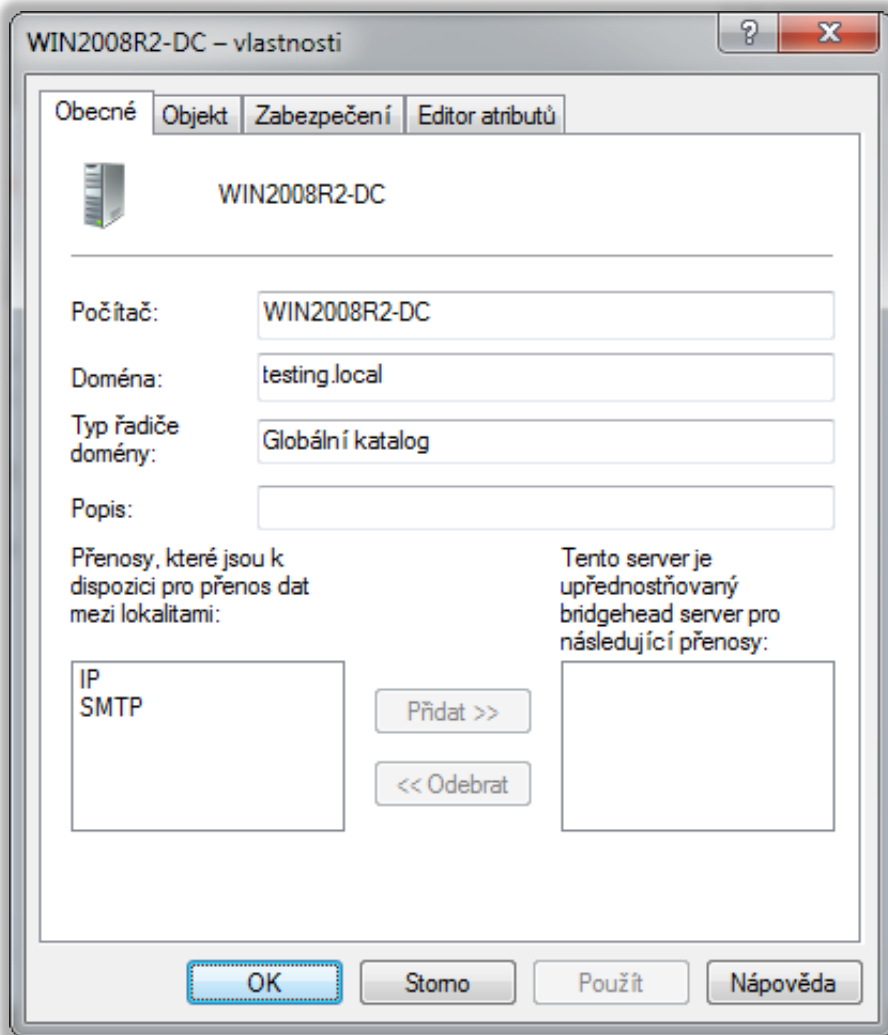
# Protokoly pro přenos (replikaci) dat

- DS-RPC (*Directory Service RPC*)
  - Jediný protokol pro místní replikaci
  - Upřednostňovaný protokol pro mezimístní replikaci
  - Může replikovat oddíl domény (*domain partition*)
- ISM-SMTP (*Inter-Site Messaging SMTP*)
  - Nemůže replikovat oddíl domény
  - Vyžaduje přítomnost certifikační autority (CA)
  - Robustnější (využíván při nespolehlivém spojení mezi místy, pokud tato místa nenáleží do stejné domény)

# Bridgehead servery

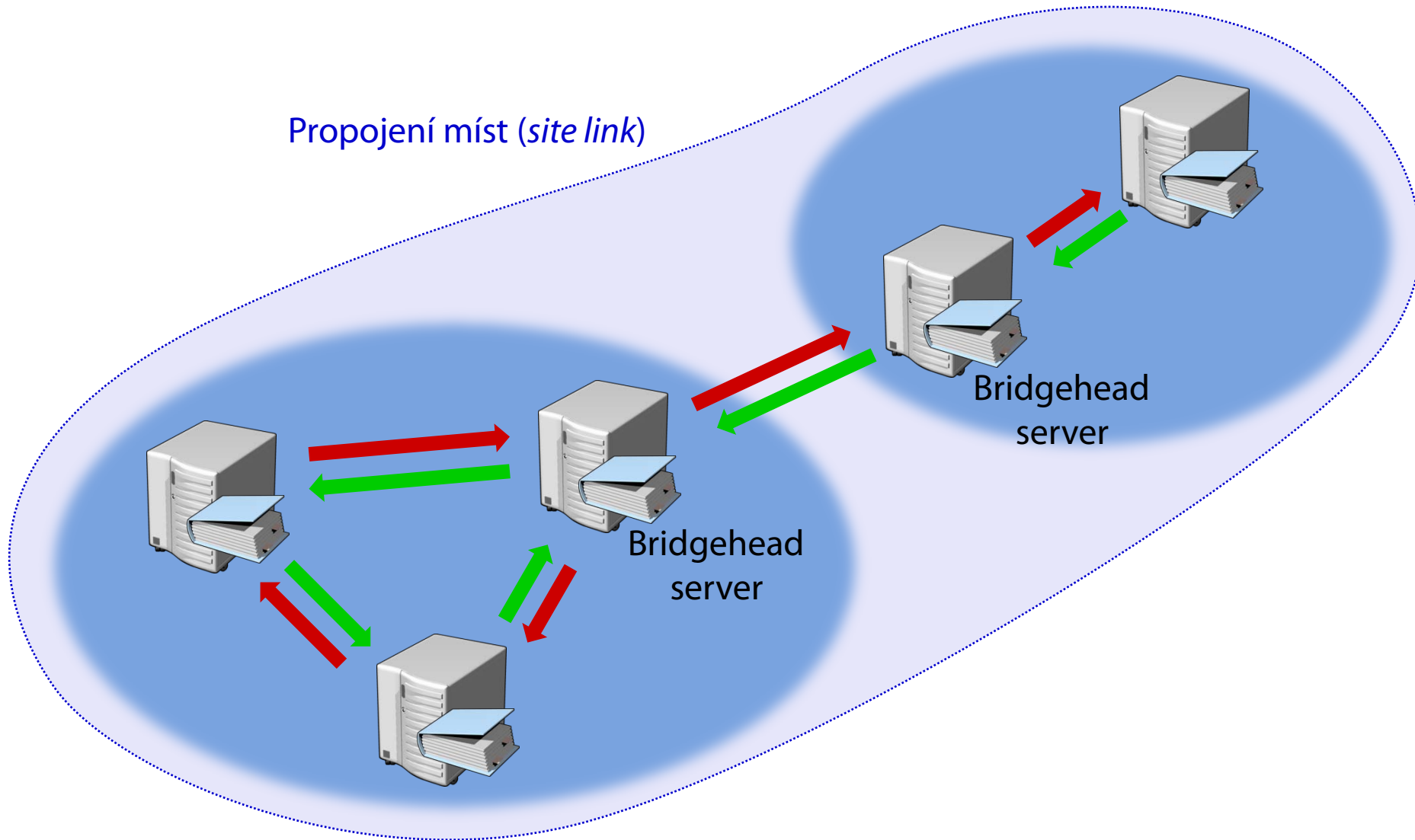
- Řadiče domény, jenž zajišťují mezimístní replikaci vybraných oddílů databáze Active Directory
  - V každém místě existuje jeden bridgehead server pro každý oddíl databáze Active Directory
- Lze explicitně vybrat preferované řadiče domény, jenž by měly plnit úlohu bridgehead serverů
  - Při výpadku přesun na jiný preferovaný řadič domény
- Minimalizují přenos dat mezi jednotlivými místy
  - Data se přenášejí pouze jednou mezi každou dvojicí míst v daném (objektu) propojení míst

# Preferované bridgehead servery



- Vždy pouze pro určitý typ transportního protokolu
- Pokud není žádný z řadičů domény preferován, jsou automaticky preferovány všechny přítomné řadiče
- V případě nedostupnosti všech preferovaných řadičů domény selže mezimístní replikace

# Ilustrace bridgehead serverů

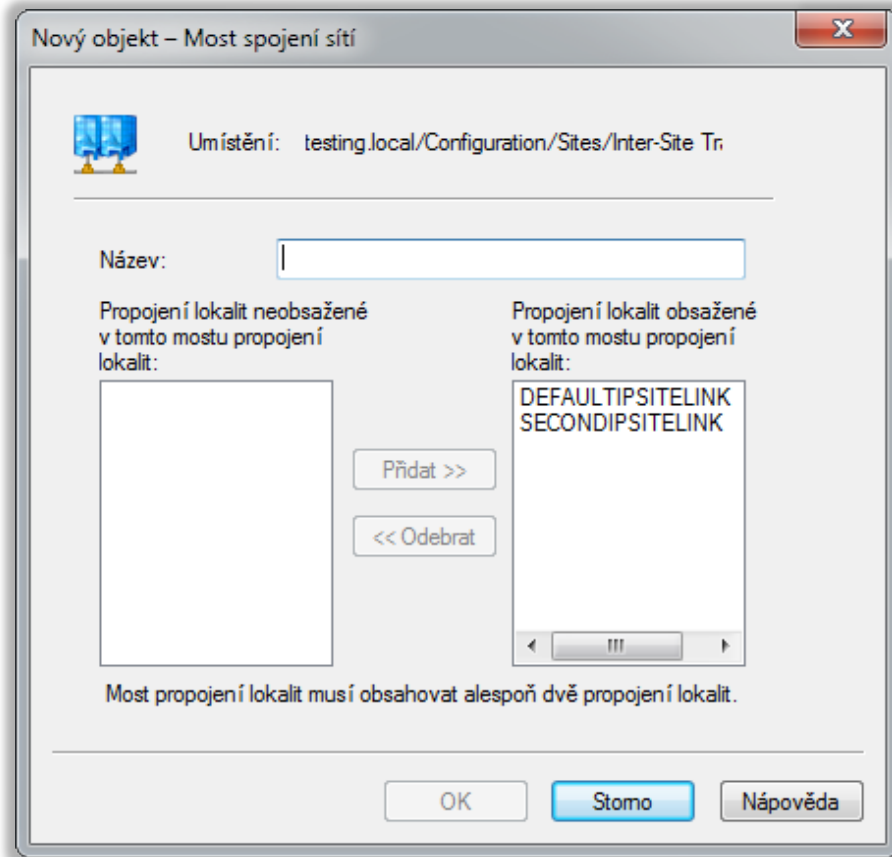


# Nastavení mezimístní replikace

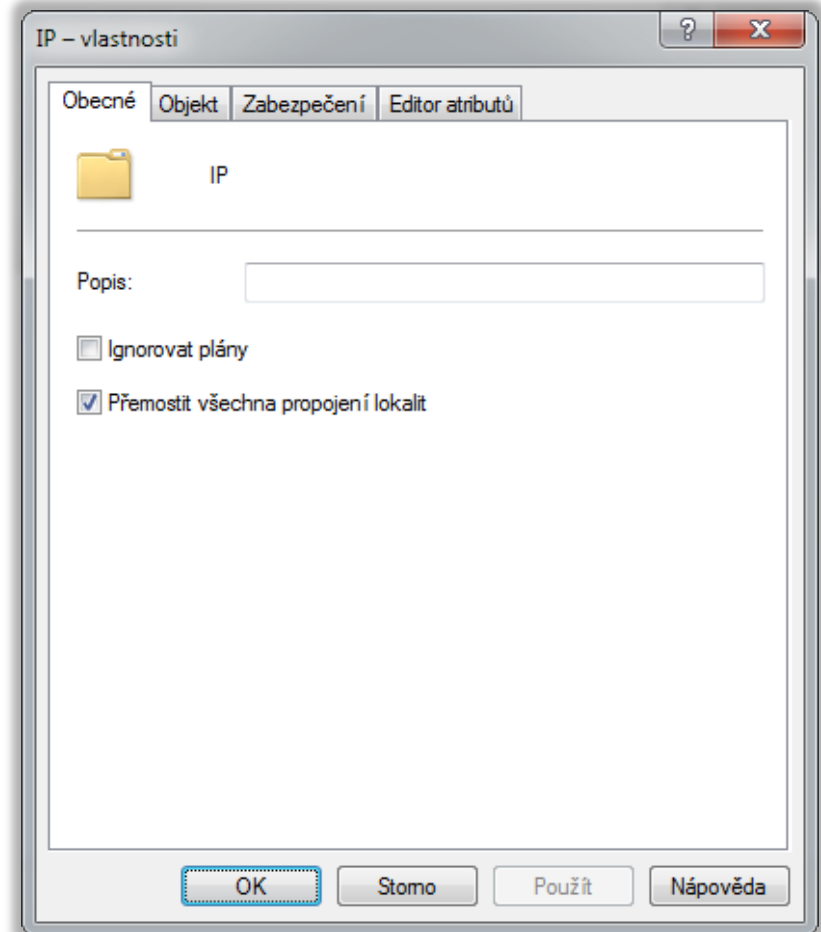
- Tranzitivita (objektů) propojení míst
  - Pokud lze provést replikaci mezi dvojicemi míst A a B a B a C, pak lze provést replikaci také mezi A a C
  - Ve výchozím nastavení povolena
- Mosty (objektů) propojení míst (*site link bridges*)
  - Spojení dvou a více (objektů) propojení míst, které vytváří jedno tranzitivní propojení míst
  - Pokud je povolena tranzitivita propojení míst, jsou ignorovány

# Vytváření mostů propojení míst

## Manuálně

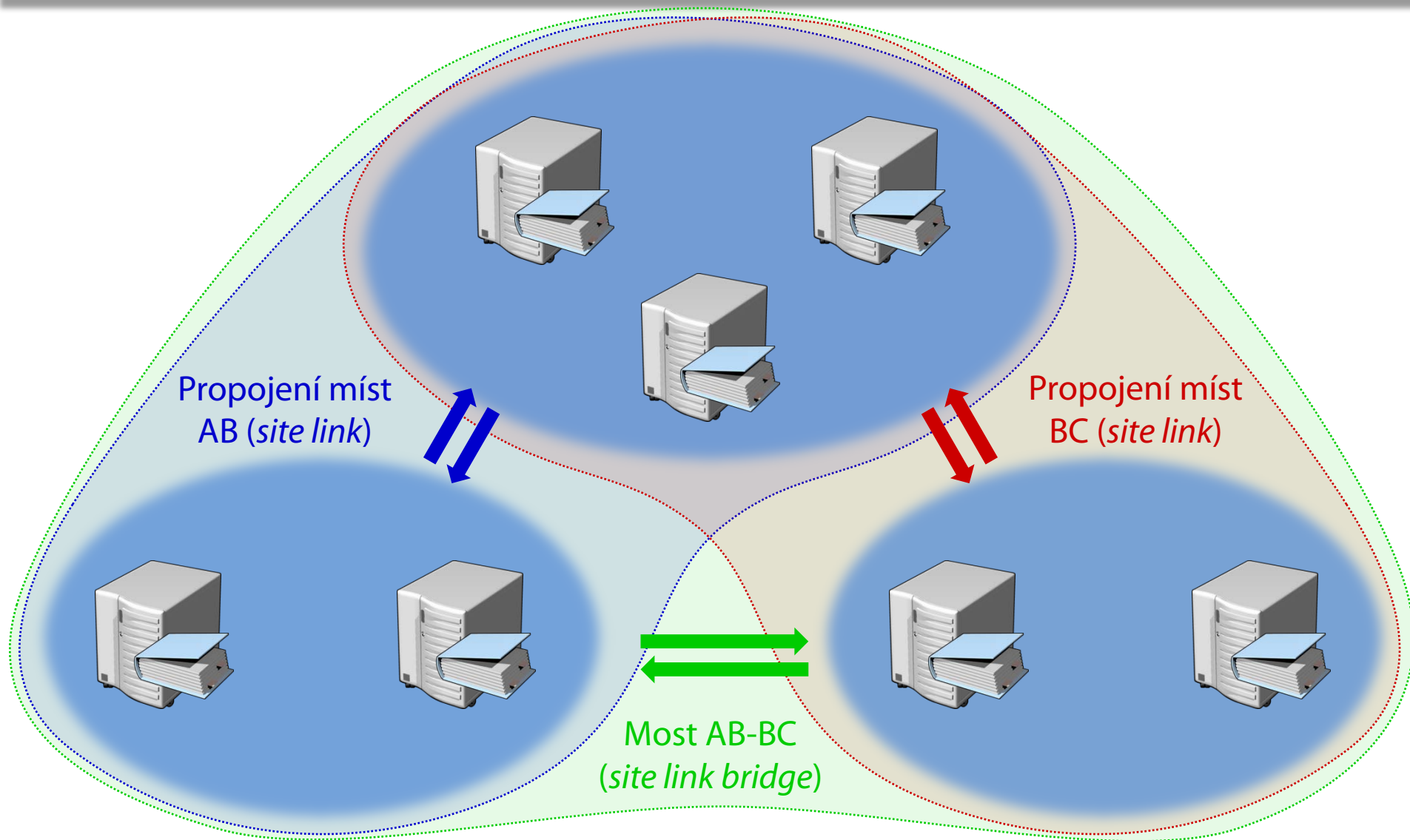


## Automaticky (tranzitivita)





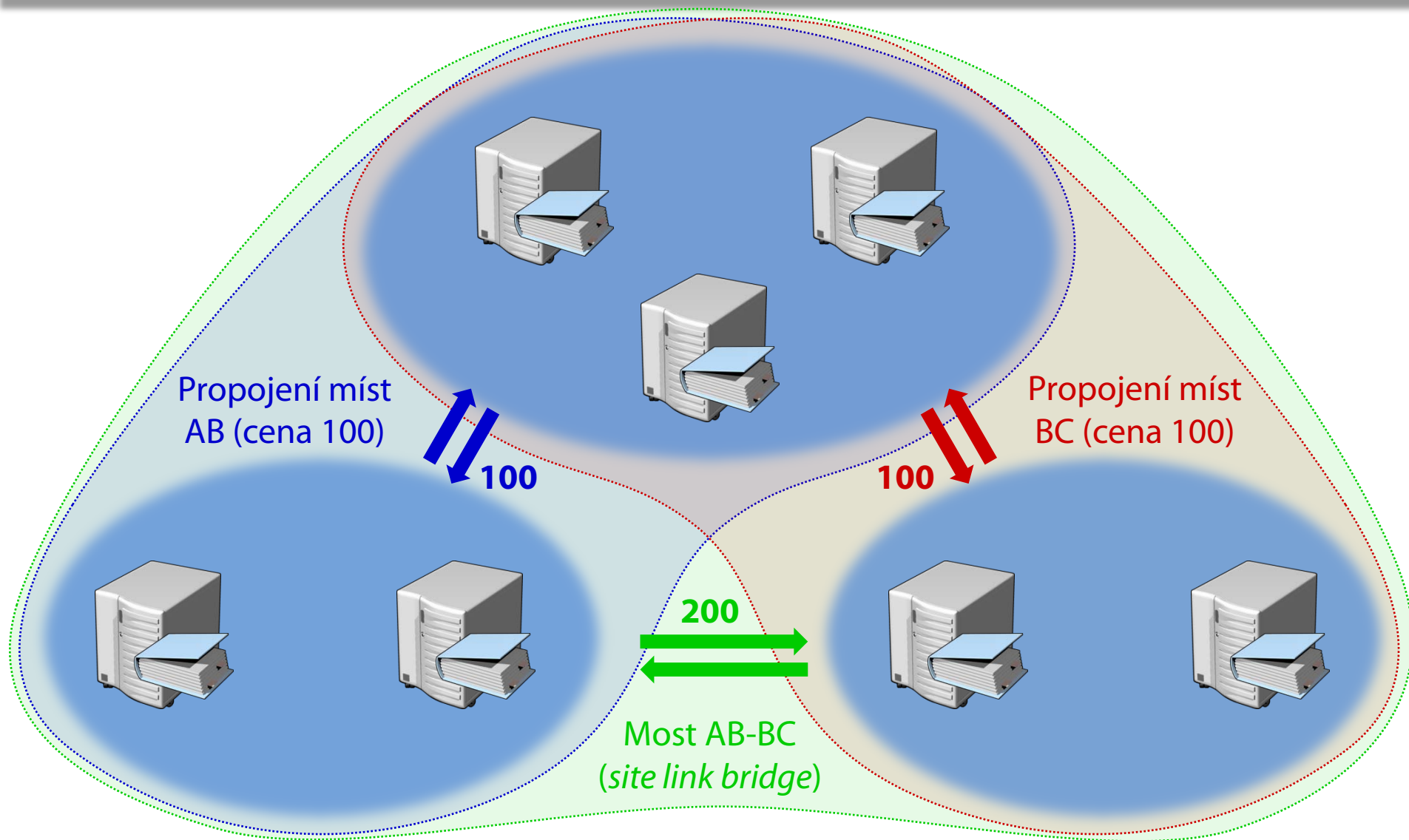
# Ilustrace mostů propojení míst



# Vlastnosti (objektů) propojení míst (1)

- Cena (objektů) propojení míst (*site link cost*)
  - Určuje pořadí výběru replikační cesty, pokud existuje více možných cest mezi dvěma řadiči domény
  - Ve výchozím nastavení mají všechna propojení míst cenu 100
- Cena replikační cesty
  - Součet cen propojení míst, přes které replikační cesta prochází
  - Čím nižší cena, tím více bude cesta preferována před ostatními cestami

# Ilustrace cen replikačních cest



# Vlastnosti (objektů) propojení míst (2)

- Frekvence replikace (*frequency*)
  - Mezimístní replikace založena výhradně na vyzývání
  - Interval dotazování se bridgehead serverů, zda u nich nedošlo k nějakým změnám
- Plánování replikace (*schedule*)
  - Možnost omezení replikace na určité hodiny
  - Ve výchozím nastavení může být replikace provedena vždy (povolena 24 hodin denně)

# Nastavení vlastností propojení míst

DEFAULTIPSITELINK – vlastnosti

Obecné | Objekt | Zabezpečení | Editor atributů

DEFAULTIPSITELINK

Popis:

Lokality neobsažené v tomto propojení lokalit:

Lokality obsažené v tomto propojení lokalit:

Default-First-Site-Name  
Second-Site-Name

Přidat >>

<< Odebrat

Náklady: 100

Replikovat vždy po 180 minutách

Změnit plán...

OK Stomo Použít nápověda

Plán uživatele DEFAULTIPSITELINK

0 · 2 · 4 · 6 · 8 · 10 · 12 · 14 · 16 · 18 · 20 · 22 · 0

Vše

pondělí

úterý

středa

čtvrtek

pátek

sobota

neděle

Replikace není k dispozici

Replikace je k dispozici

pondělí až neděle od 0:00 do 0:00

- Plán určuje, kdy je možné mezimístní replikaci přes propojení míst provádět

# Nástroj repadmin.exe

- Výpis replikačních partnerů / (objektů) spojení
  - **repadmin /showrepl <dc-list>**
  - **repadmin /showconn <dc-list>**
- Spuštění KCC
  - **repadmin /kcc**
- Spuštění replikace mezi dvěma řadiči domény
  - **repadmin /replicate <dest-dc-list> <src-dc> <nc>**
- Synchronizace se všemi replikačními partnery
  - **repadmin /syncall <dc> /A /e**

# Výpis seznamu replikačních partnerů

```
cmd Správce: Příkazový řádek repadmin /showrepl win2008r2-dc
DC=testing,DC=local
  Second-Site-Name\WIN2008R2-REPL přes RPC
  Identifikátor GUID objektu agenta DSA: 664a2856-e213-4cf2-8aef-e27acaee6a21
  Poslední pokus z 2011-03-20 22:52:08 byl úspěšný.
CN=Configuration,DC=testing,DC=local
  Second-Site-Name\WIN2008R2-REPL přes RPC
  Identifikátor GUID objektu agenta DSA: 664a2856-e213-4cf2-8aef-e27acaee6a21
  Poslední pokus z 2011-03-20 22:52:08 byl úspěšný.
CN=Schema,CN=Configuration,DC=testing,DC=local
  Second-Site-Name\WIN2008R2-REPL přes RPC
  Identifikátor GUID objektu agenta DSA: 664a2856-e213-4cf2-8aef-e27acaee6a21
  Poslední pokus z 2011-03-20 22:52:08 byl úspěšný.
DC=DomainDnsZones,DC=testing,DC=local
  Second-Site-Name\WIN2008R2-REPL přes RPC
  Identifikátor GUID objektu agenta DSA: 664a2856-e213-4cf2-8aef-e27acaee6a21
  Poslední pokus z 2011-03-20 22:52:08 byl úspěšný.
DC=ForestDnsZones,DC=testing,DC=local
  Second-Site-Name\WIN2008R2-REPL přes RPC
  Identifikátor GUID objektu agenta DSA: 664a2856-e213-4cf2-8aef-e27acaee6a21
  Poslední pokus z 2011-03-20 22:52:08 byl úspěšný.
```

# Nástroj dcdiag.exe

- Provádí testování funkčnosti doménových služeb Active Directory (AD DS)
  - Spuštění testu příkazem **dcdiag /test:<název-testu>**

Název testu	Popis testu
<b>FrsEvent</b>	Zjišťuje chyby služby replikace souborů (FRS)
<b>DFSREvent</b>	Zjišťuje chyby replikace distribuovaného souborového systému (DFS-R)
<b>Intersite</b>	Zjišťuje problémy ovlivňující provádění mezimístní replikace
<b>KccEvent</b>	Zjišťuje chyby komponenty KCC
<b>Replications</b>	Kontroluje včasnou replikaci mezi řadiči domény
<b>Topology</b>	Kontroluje, zda replikační topologie zahrnuje všechny řadiče domény
<b>VerifyReplicas</b>	Ověří replikaci oddílů aplikací na řadiče domény, jenž je mají obsahovat