Serverové systémy Microsoft Windows

IW2/XMW2 2014/2015

Jan Fiedor

ifiedor@fit.vutbr.cz

Fakulta Informačních Technologií

Vysoké Učení Technické v Brně

Božetěchova 2, 612 66 Brno

Revize 24. 3. 2015

Active Directory

Replikace

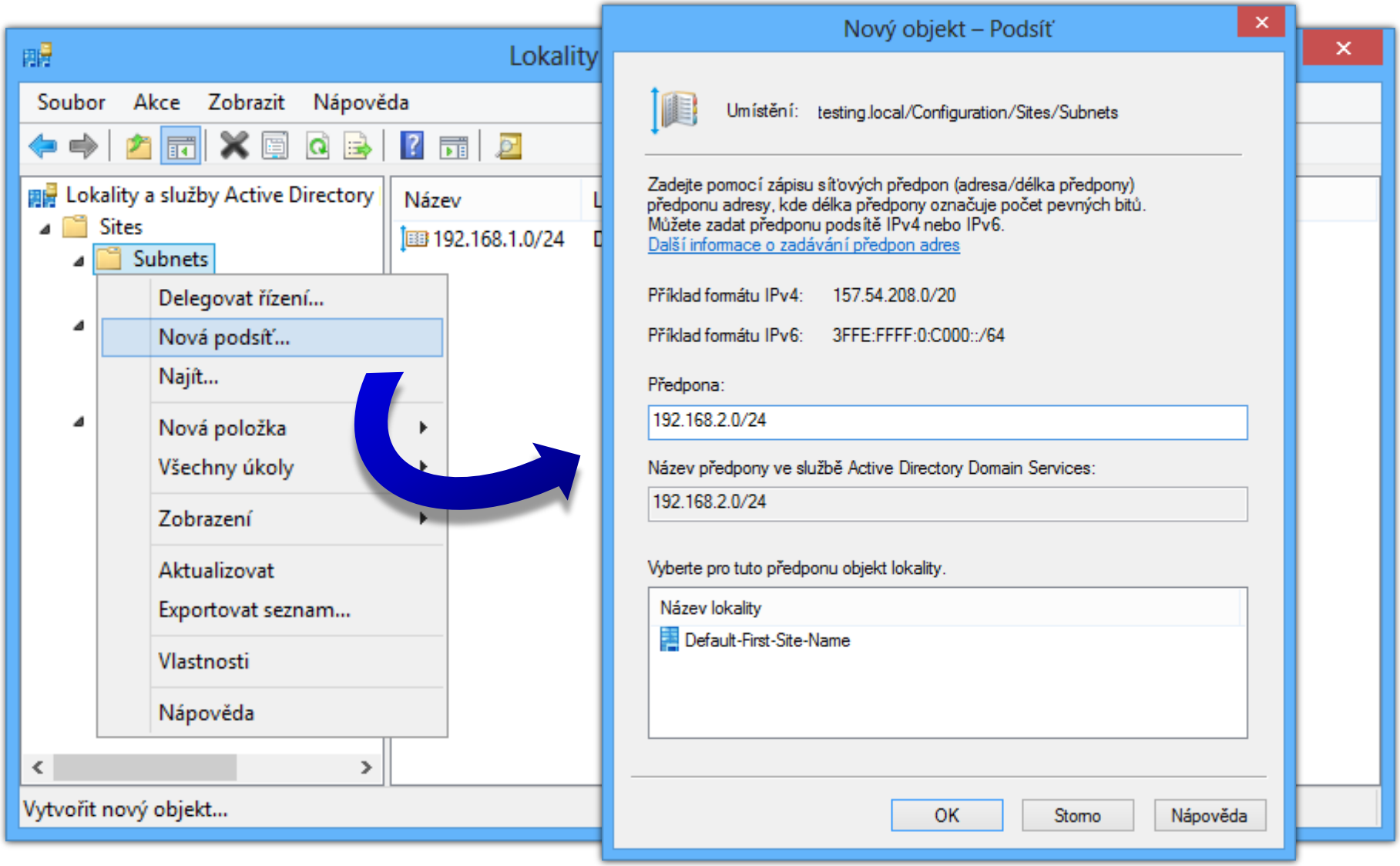
Replikace

- 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

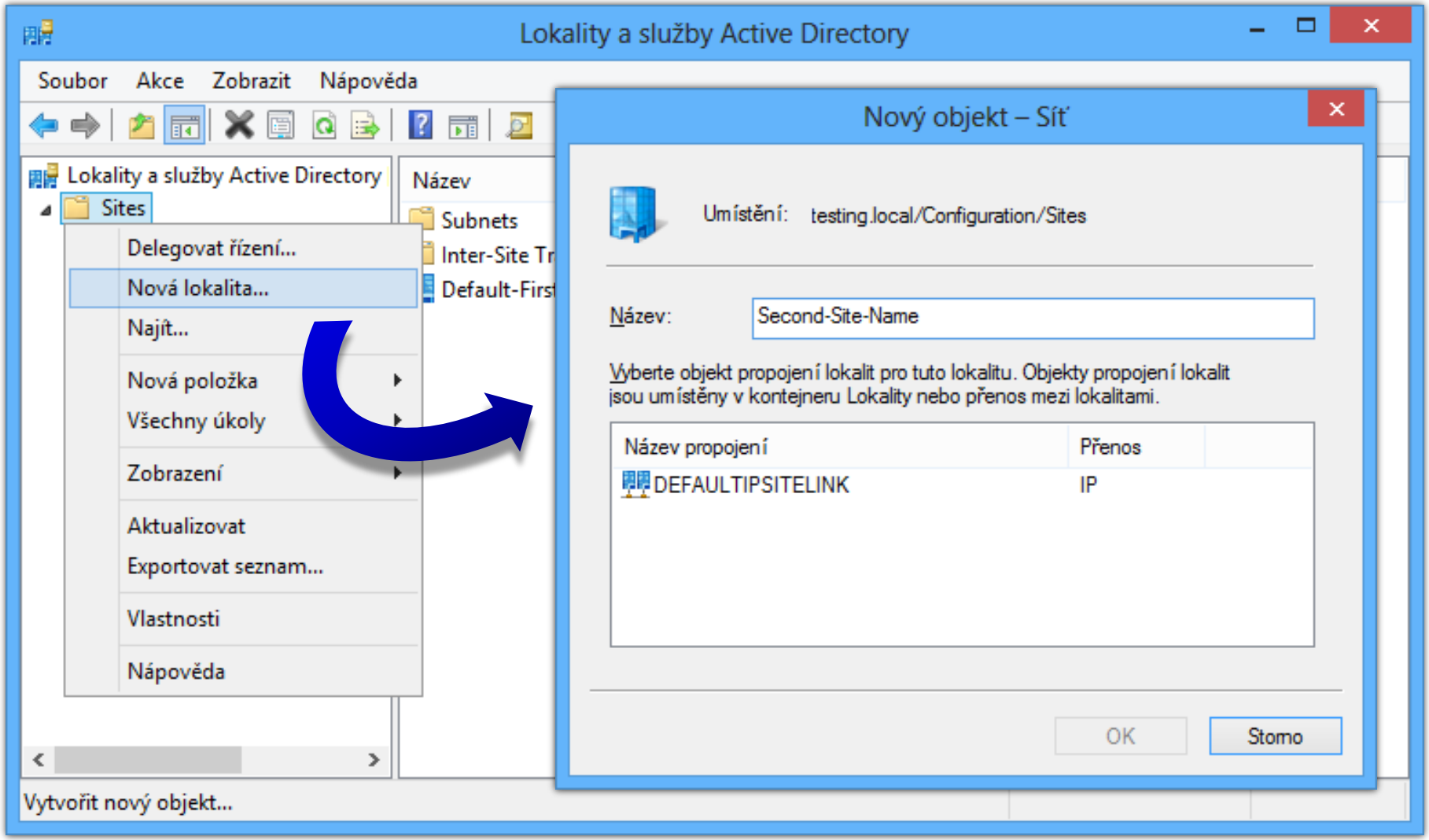
Místa (*Sites*)

- 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



Vytvoření (objektu) místa



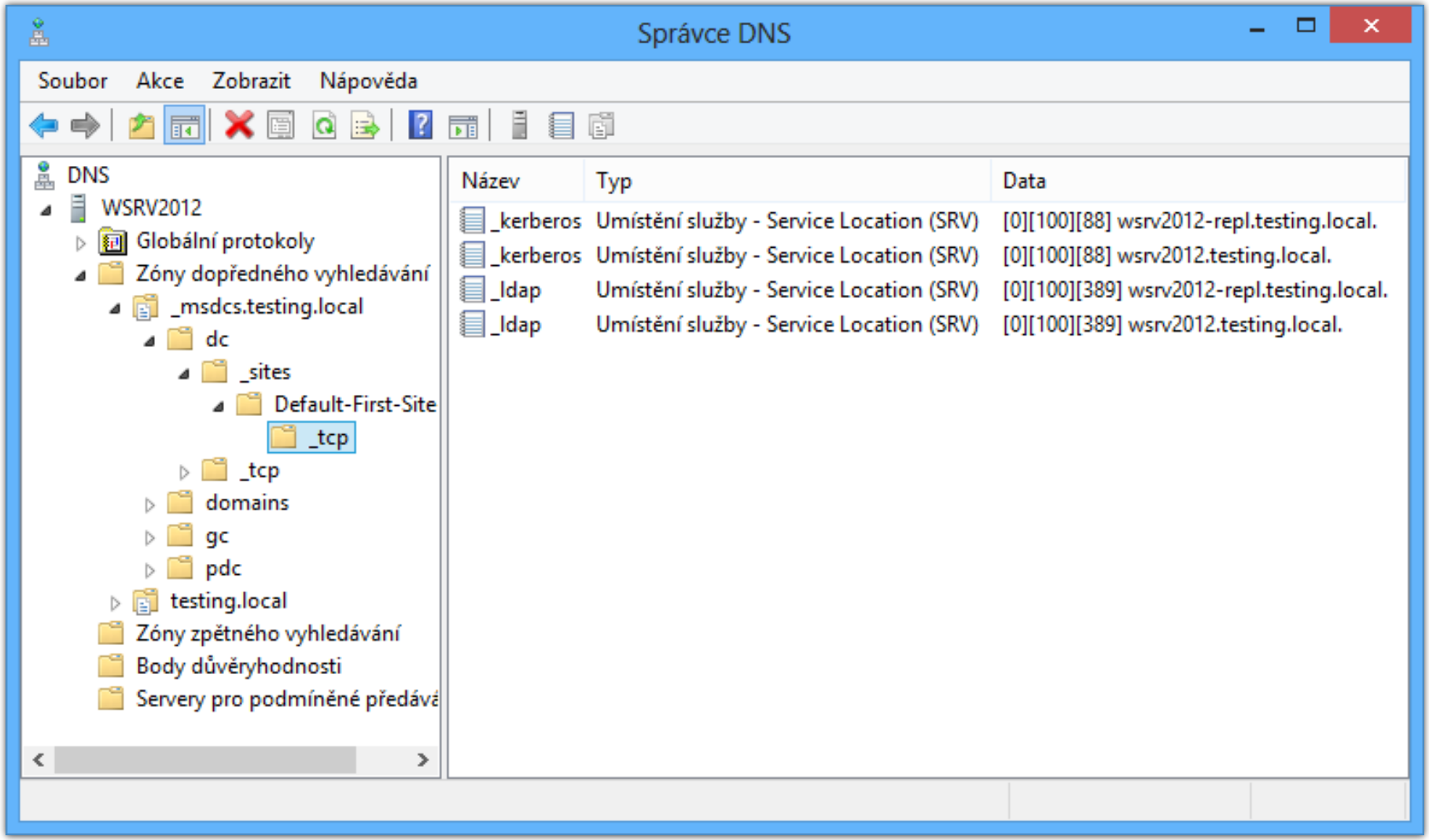
Správa replikačního provozu

- *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)

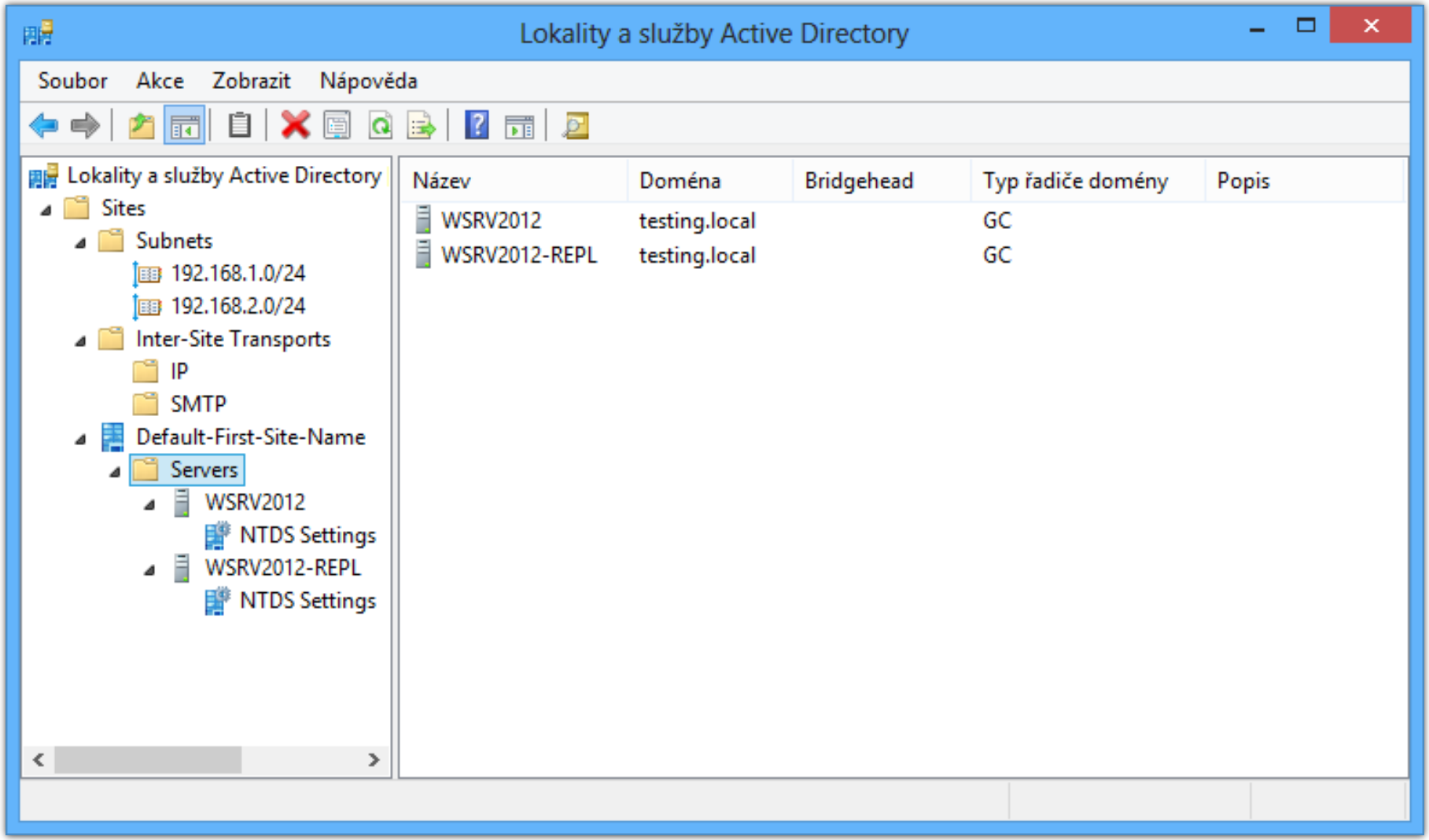
Uložení informací o službách v DNS



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



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

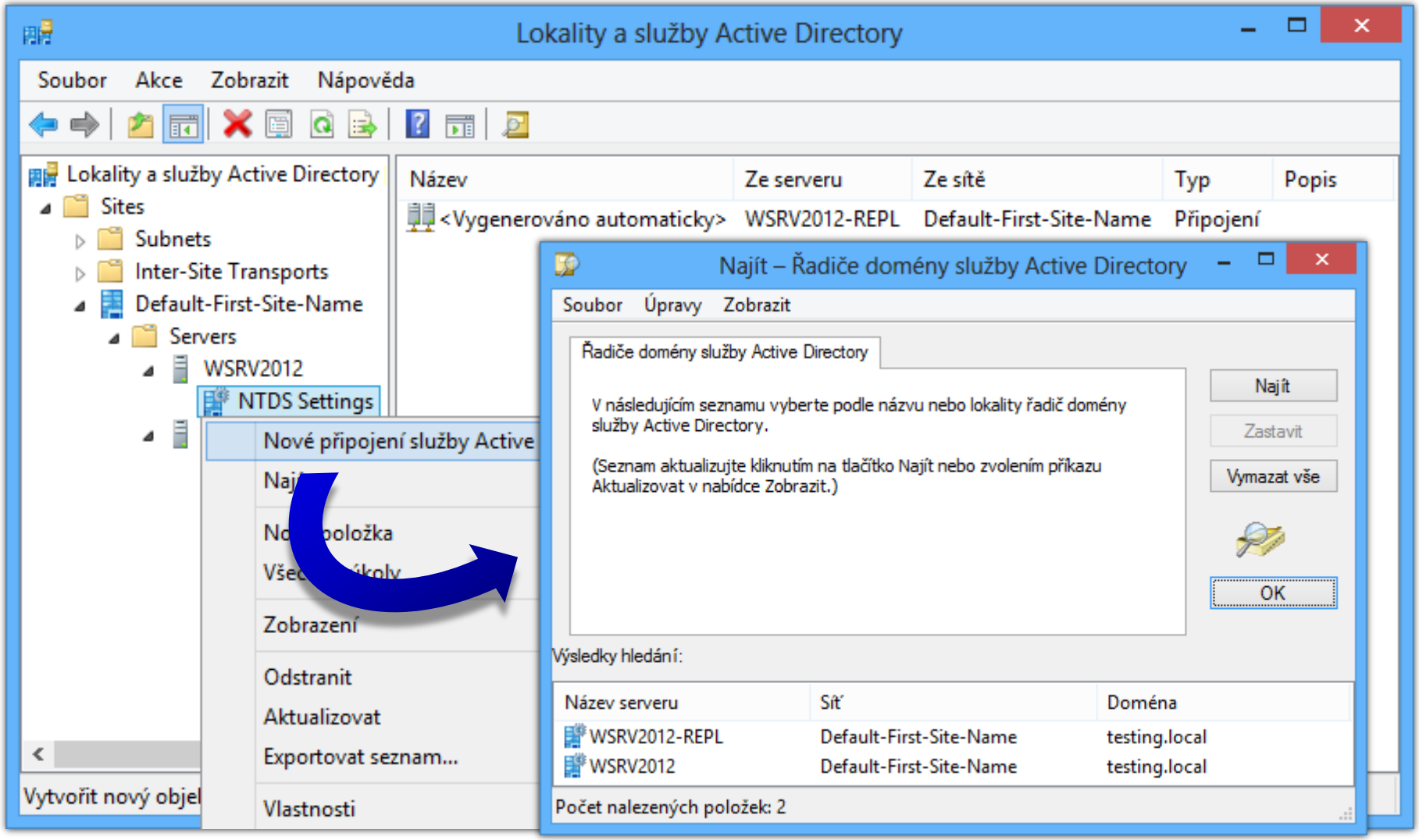
Klíčové vlastnosti replikace AD (2)

- 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



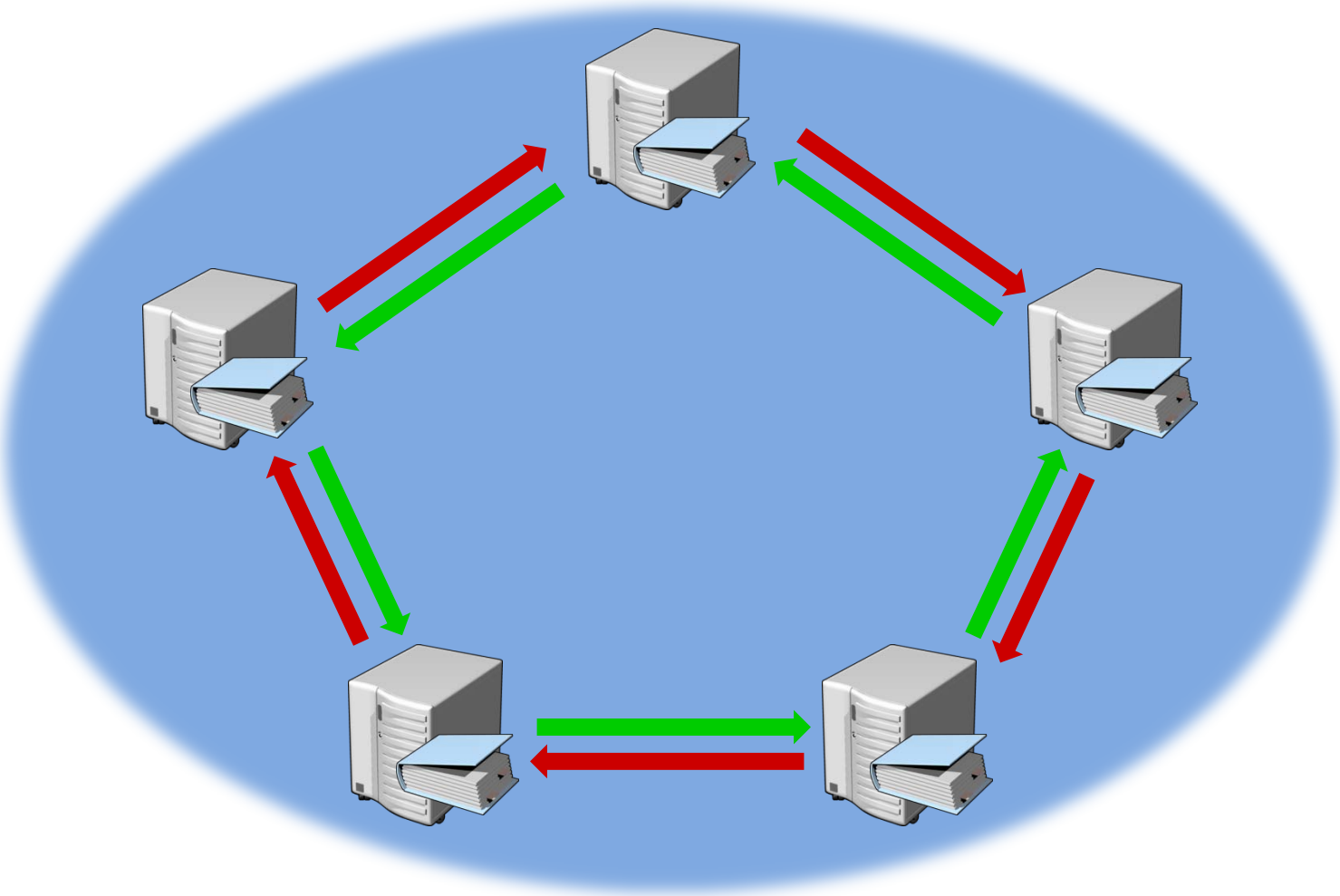
Replikační topologie

- 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)

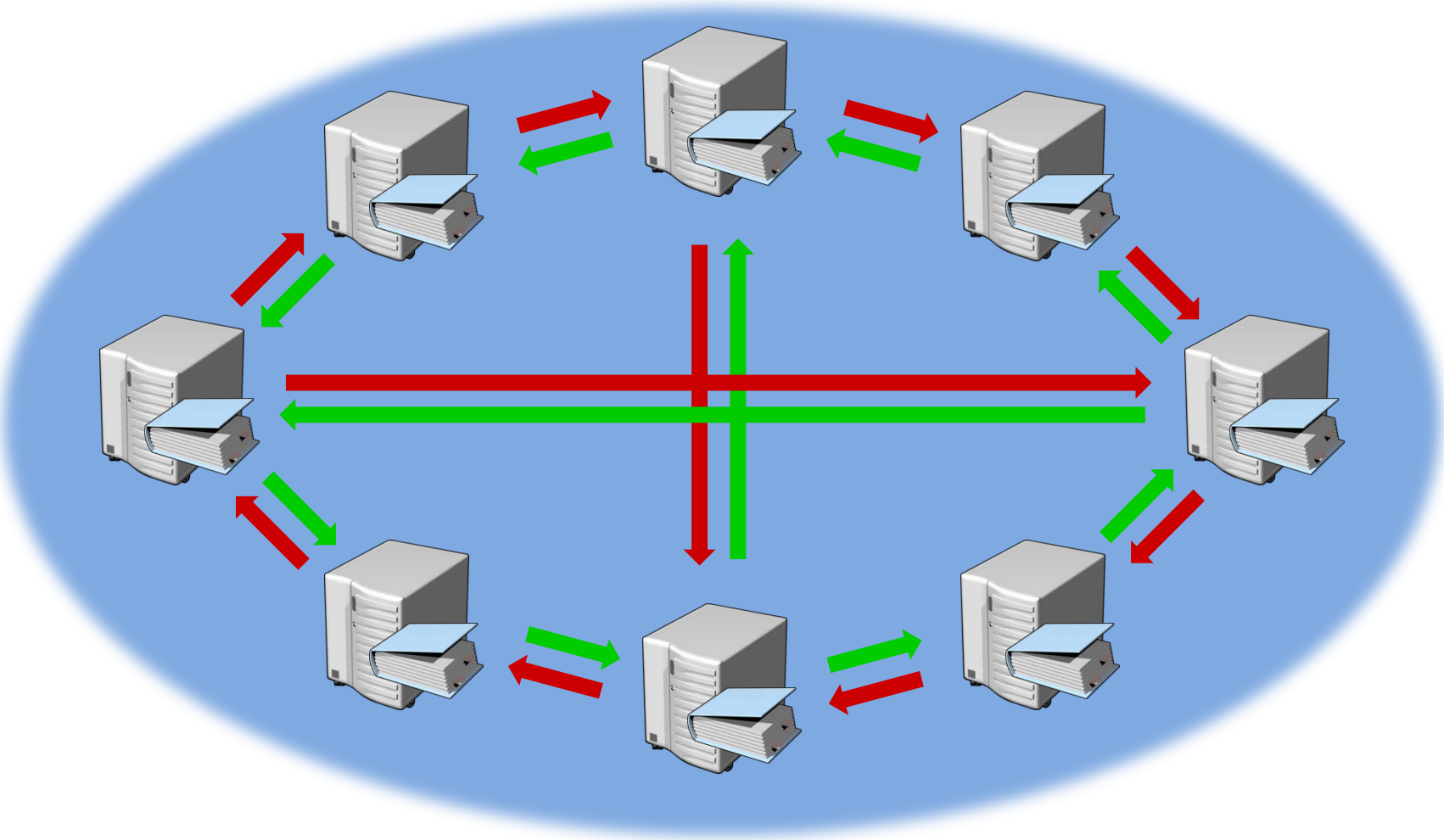
Generovaná replikační topologie

- 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*)

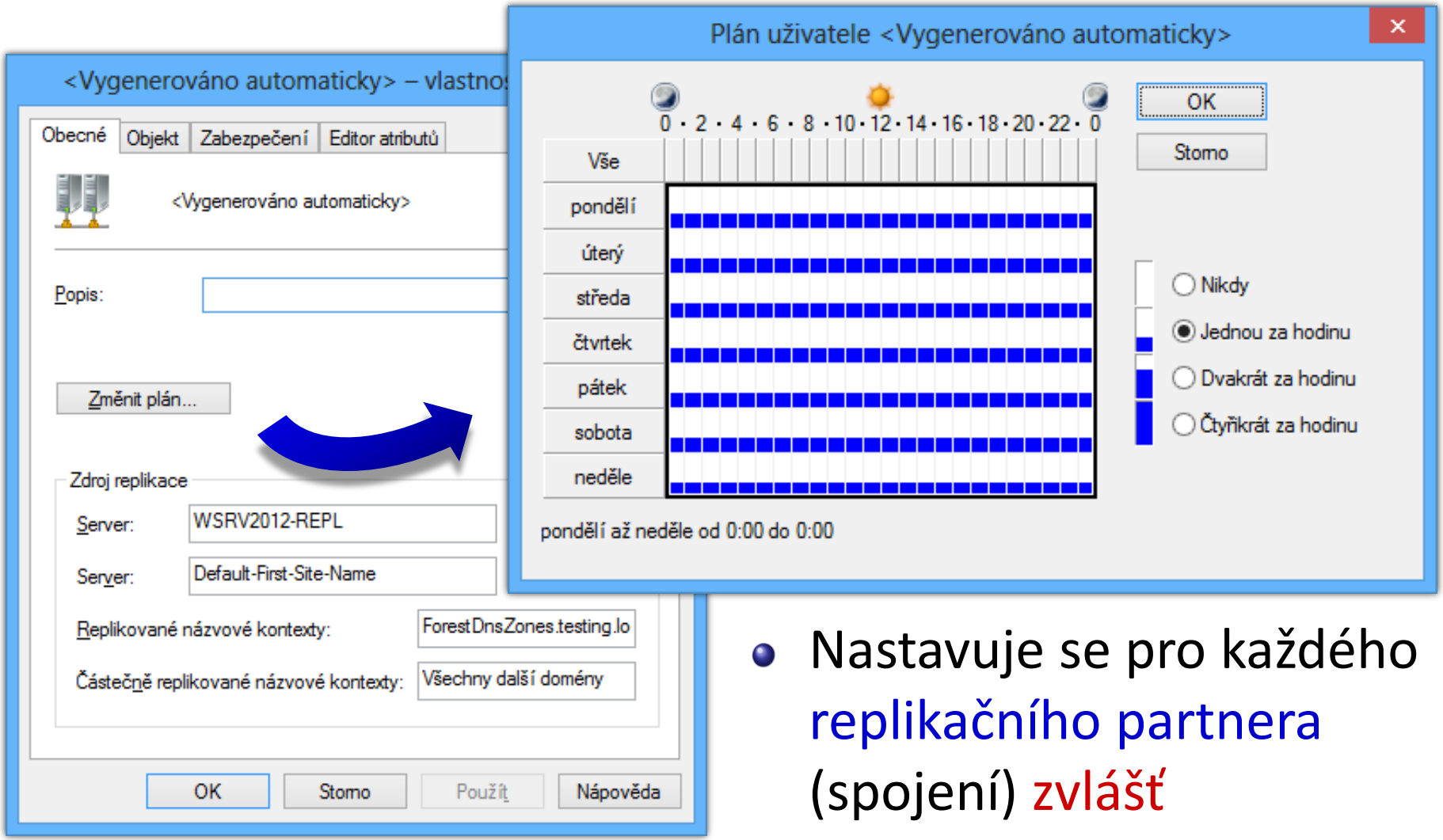
Oznámení (*notification*)

- 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 (lze změnit)
  - 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

Nastavení intervalu vyzývání

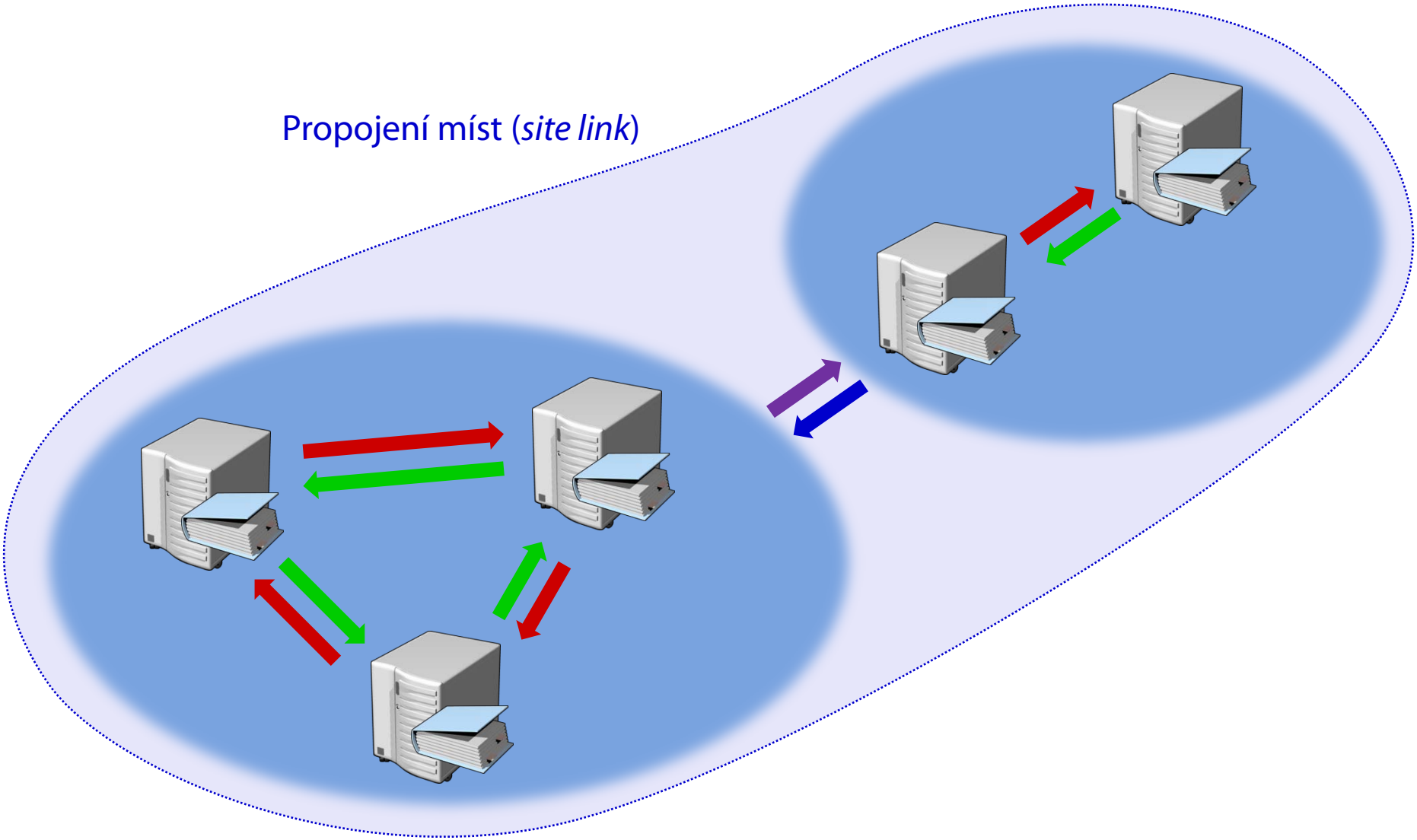


- Nastavuje se pro každého replikačního partnera (spojení) zvlášť

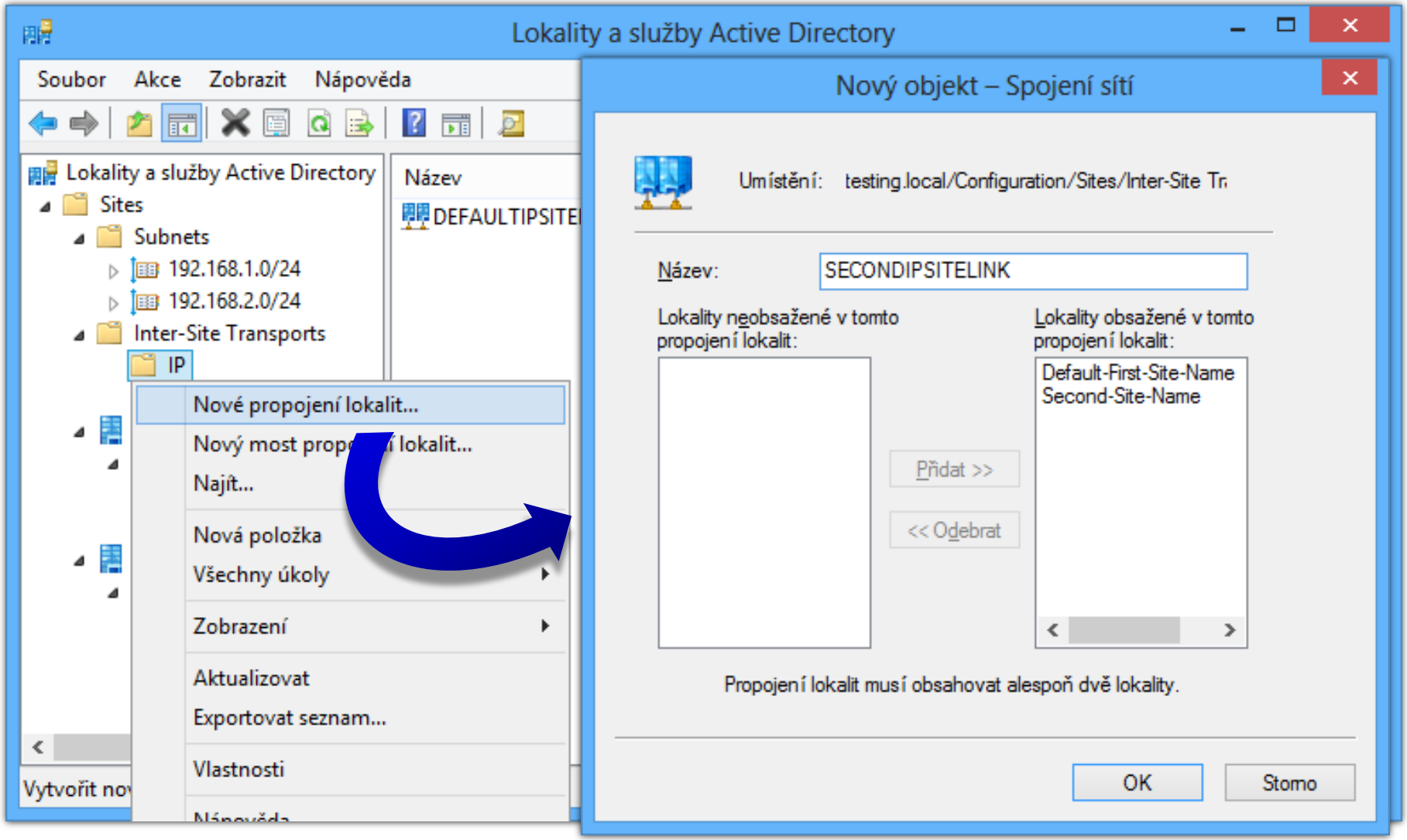
Mezimístní (*intersite*) replikace

- 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

Ilustrace propojení míst



Vytvoření (objektu) propojení míst



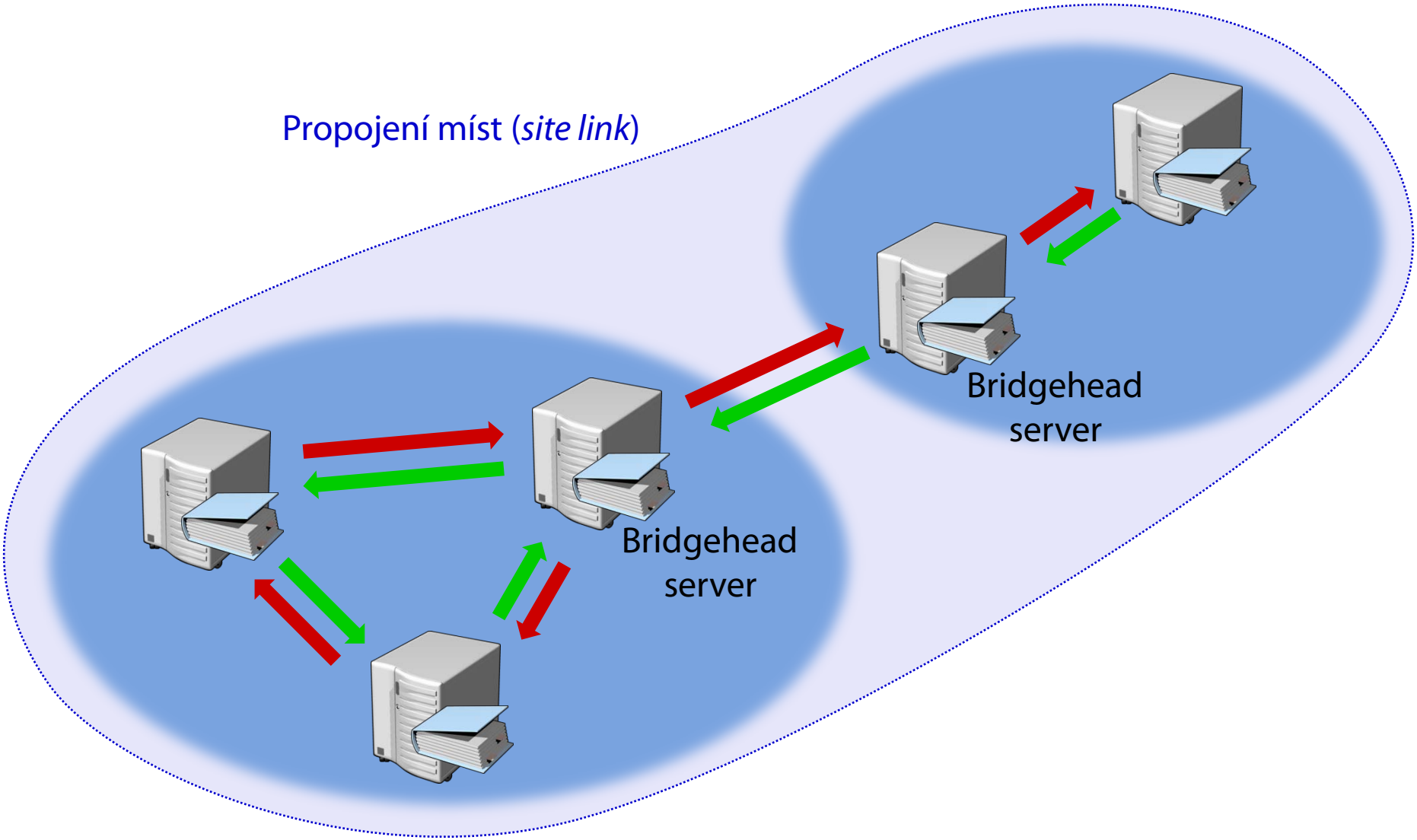
Protokoly pro přenos (replikaci) dat

- 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)

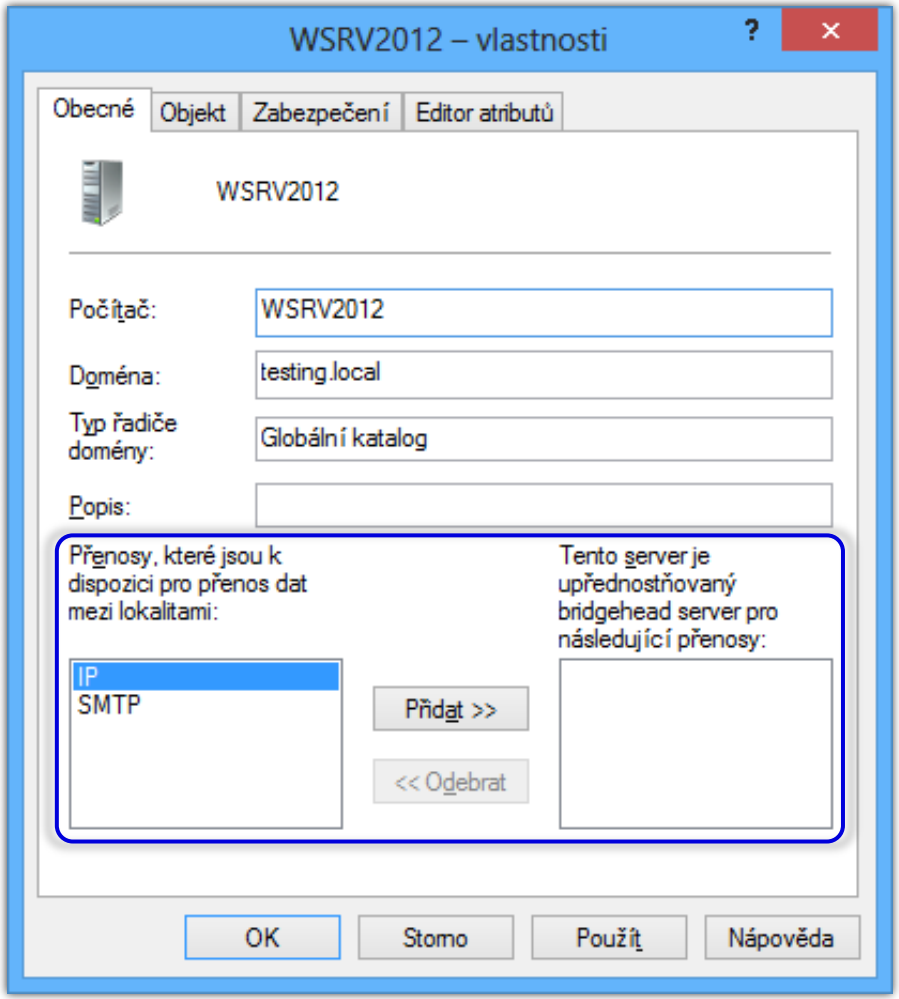
Bridgehead servery

- 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

Ilustrace bridgehead serverů



Preferované bridgehead servery

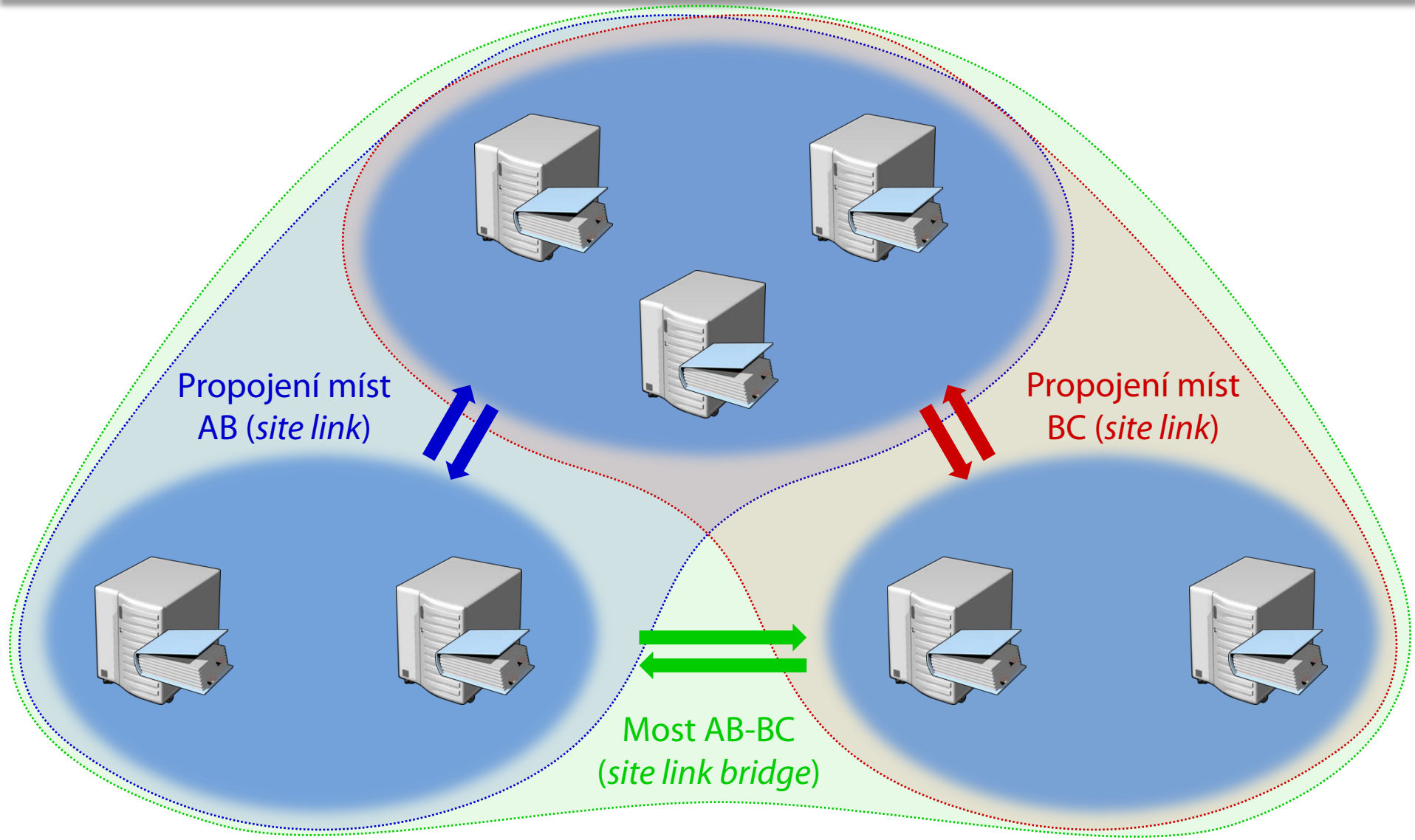


- Vždy pouze pro určitý typ transportního protokolu
- Pokud není žádný z řadičů domény preferován, jsou automaticky preferovány všechny přítomné řadiče
- V případě nedostupnosti všech preferovaných řadičů domény selže mezimístní replikace

Nastavení mezimístní replikace

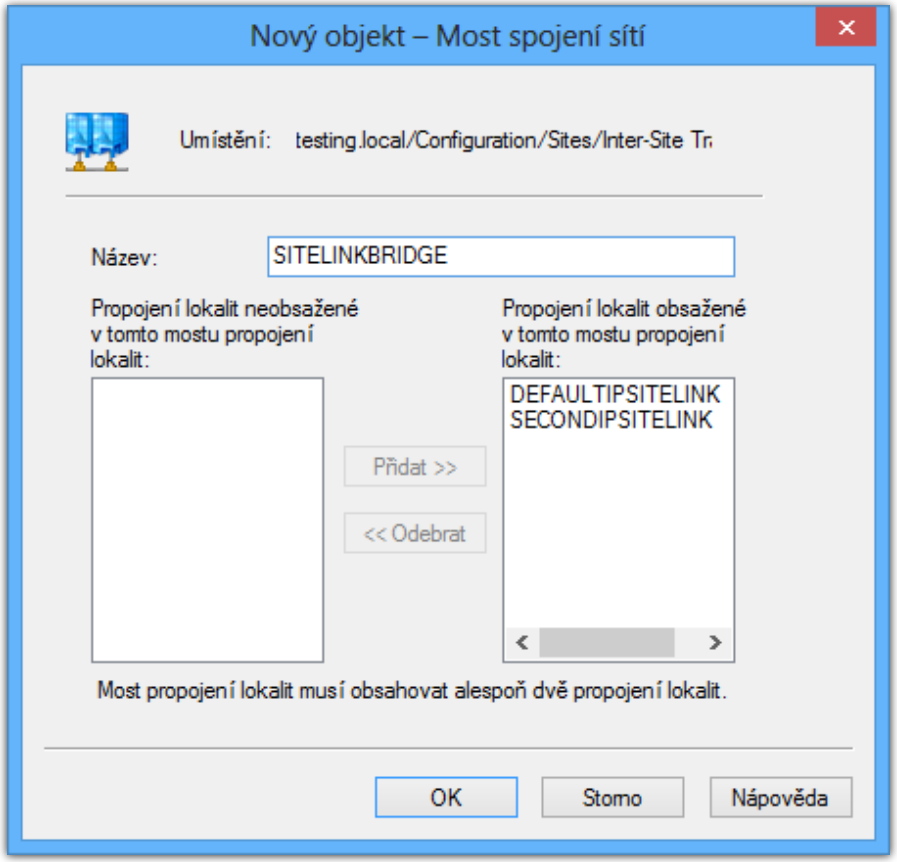
- Tranzitivita (objektů) propojení míst
  - Pokud lze provést replikaci mezi dvojicemi míst **A** a **B** a **B** a **C**, pak lze provést replikaci také mezi **A** a **C**
  - Ve výchozím nastavení povolena
- Mosty (objektů) propojení míst (*site link bridges*)
  - Spojení dvou a více (objektů) propojení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

Ilustrace mostů propojení míst

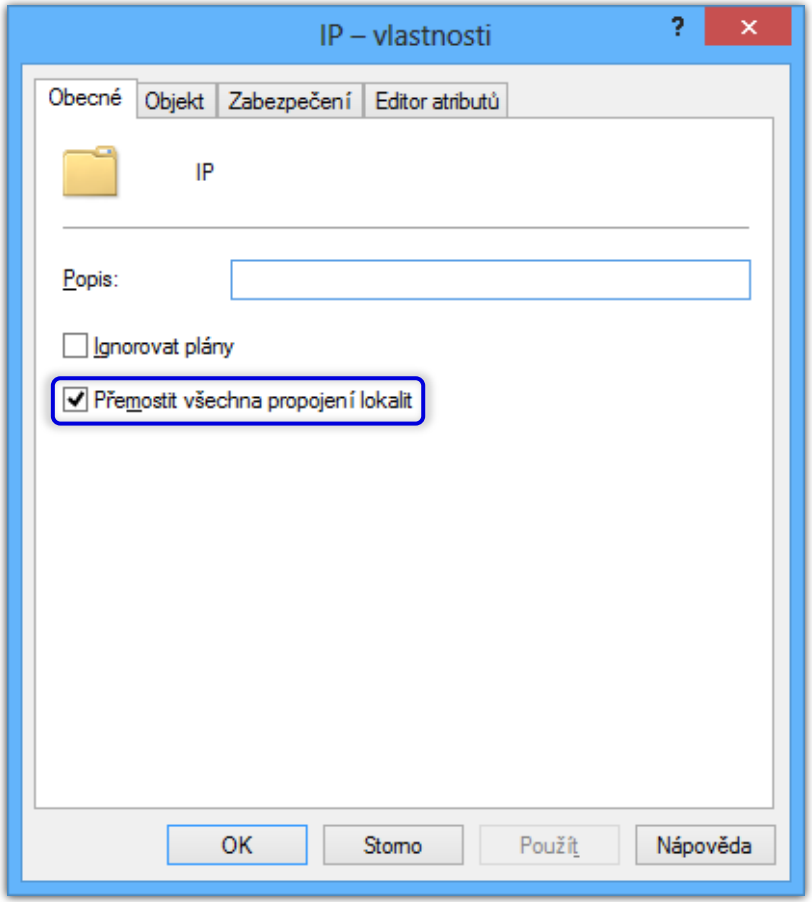


Vytváření mostů propojení míst

Manuálně



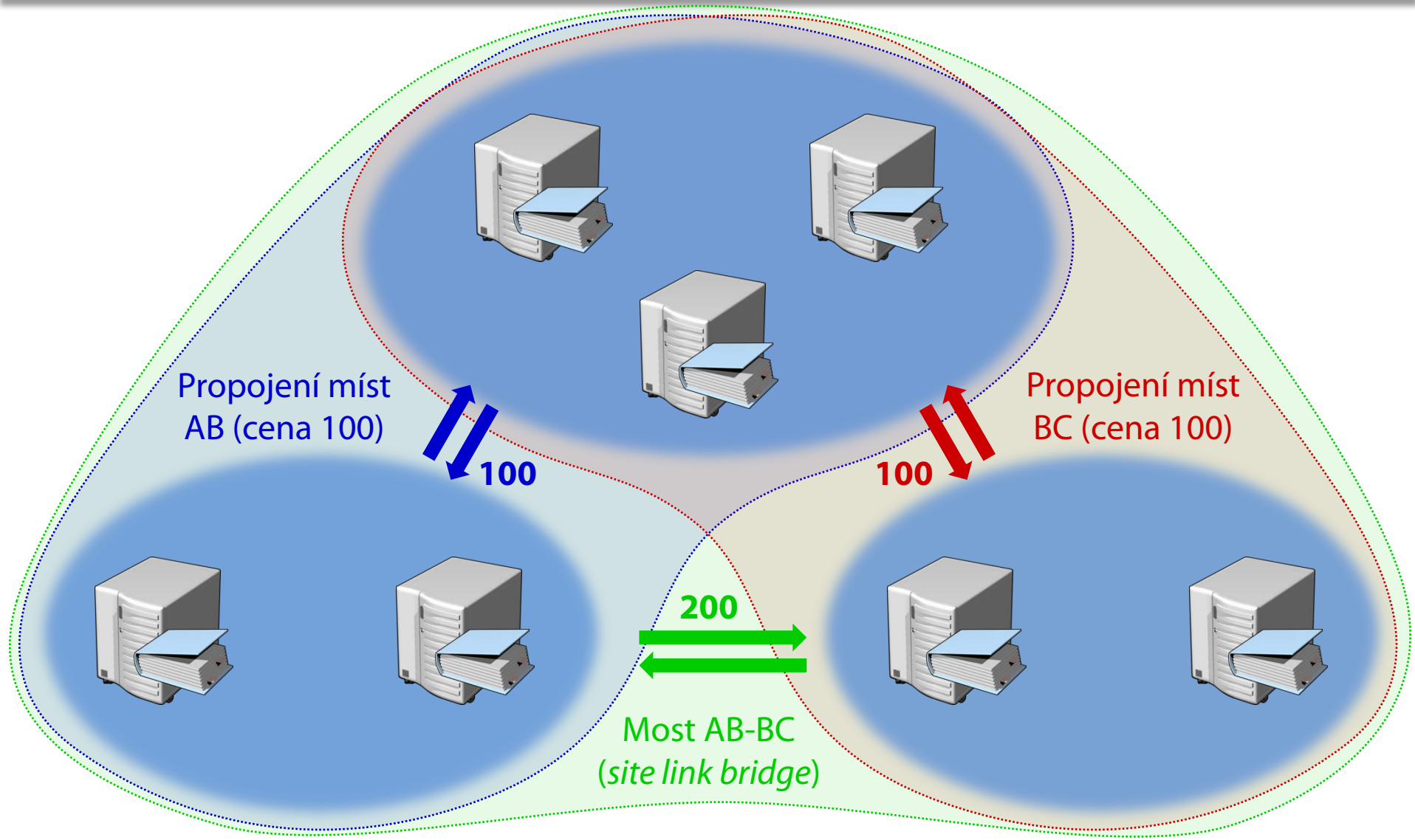
Automaticky (tranzitivita)



Cena replikačních cest

- 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

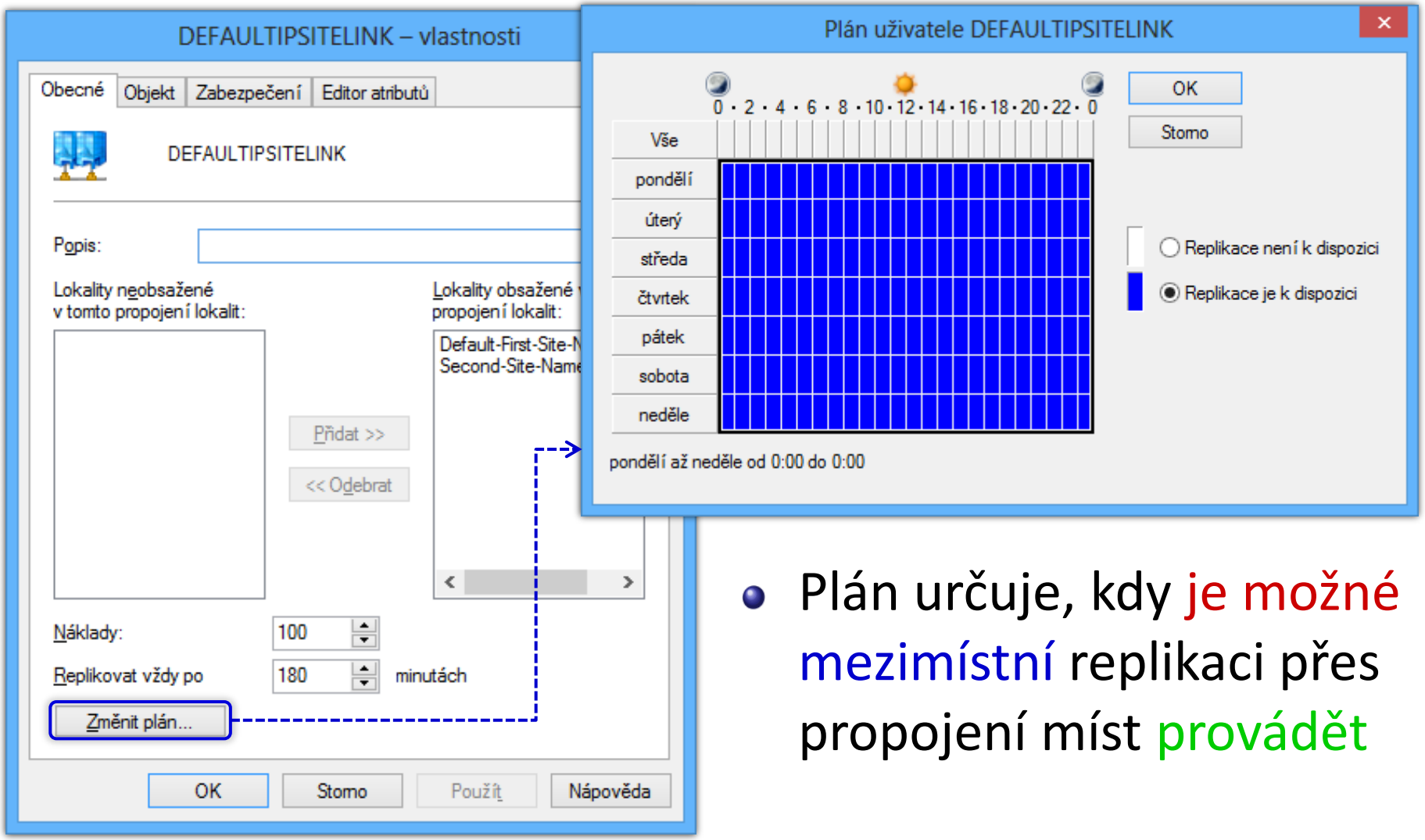
Ilustrace cen replikačních cest



Plánování mezimístní replikace

- 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 ceny, frekvence a plánu

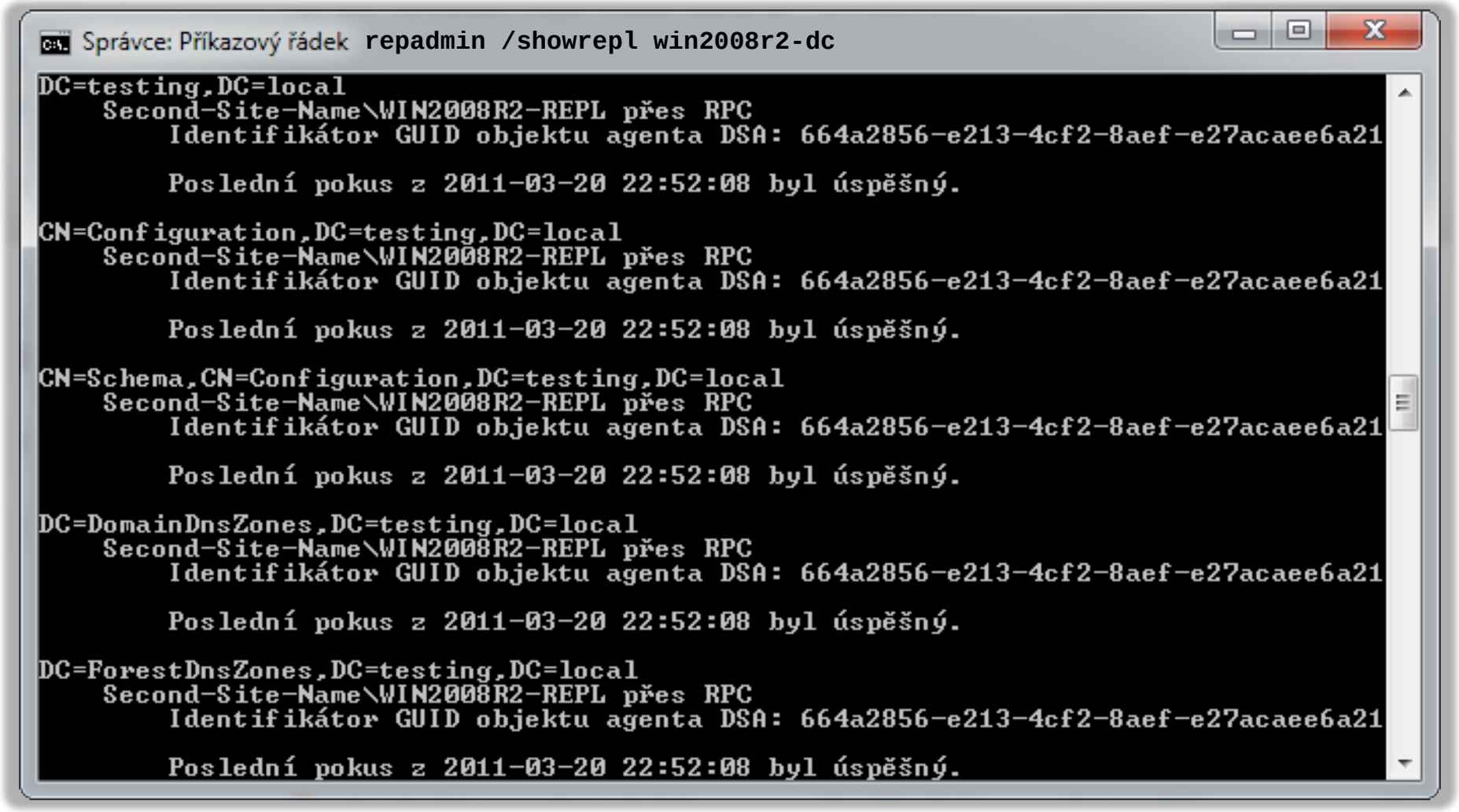


- Plán určuje, kdy je možné mezimístní replikaci přes propojení míst provádět

Nástroj repadmin.exe

- Výpis replikačních partnerů / (objektů) spojení
  - **repadmin /showrepl *<dc-list>***
  - **repadmin /showconn *<dc-list>***
- Spuštění KCC (aktualizace replikační topologie)
  - **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



Nástroj dcdiag.exe

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

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