Designing an Effective Authentication Topology

Gil Kirkpatrick
CTO, NetPro

Introduction

- NetPro
  - *"The Directory Experts"*
- Gil Kirkpatrick
  - CTO
  - Architect of *DirectoryAnalyzer* and *DirectoryTroubleshooter* for Active Directory
  - Author of *Active Directory Programming* from MacMillan

Question

Why do we worry so much about optimizing replication traffic when 90% of directory traffic is authentication and lookup?

Agenda

- DC location
  - How does a workstation determine which DCs to communicate with?
- Active Directory configuration
  - How do you configure AD for optimal client authentication?
- Some scenarios
  - Hub-and-spoke
  - Network Operations Center (NOC)

DC Location

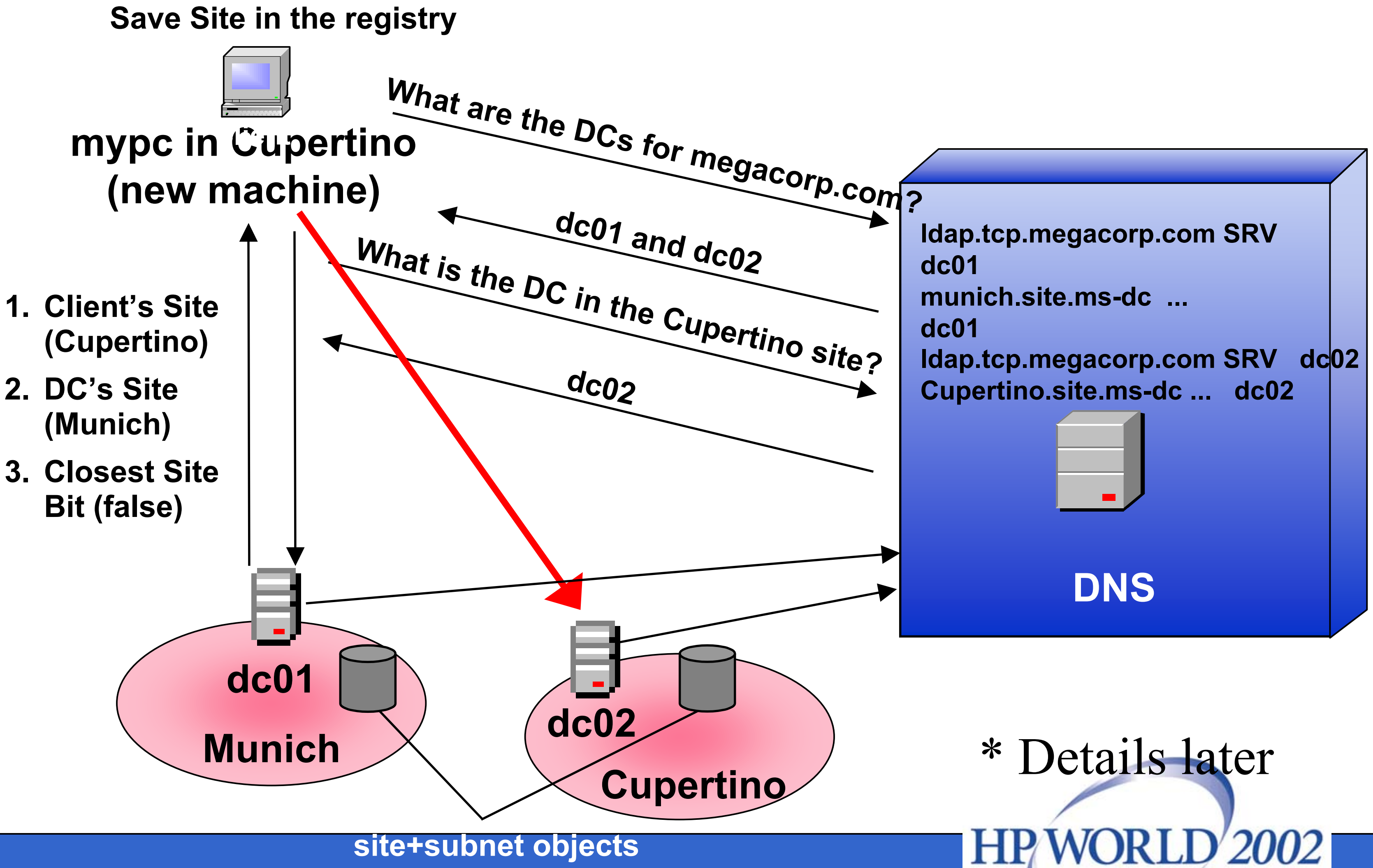
Discovery Process

- Workstations use DNS to locate DCs
- Clients need to locate AD servers that offer directory services
  - For authentication purpose: DC – GC – Kerberos KDC
  - For directory lookup: GC
- Discovery process
  - Performed when user logs in – Called by the NetLogon Service
  - Called by applications that use DsGetDCName API
- DC Locator provides the mechanism to locate AD server

DC Locator

- Two sub-components:
  - IP/DNS compatible locator
  - NETBIOS compatible locator
- IP/DNS compatible locator:
  - Used by DNS-enabled clients
  - Always tried first
  - Locate servers by querying Service Records (SRV) in DNS
- NETBIOS compatible locator
  - Used by legacy clients: WFW – WNT 3.5 – Win9x; Use WINS as name resolution service

Locator and Sites



Save Site in the registry

mypc in Cupertino (new machine)

What are the DCs for megacorp.com?

dc01 and dc02

What is the DC in the Cupertino site?

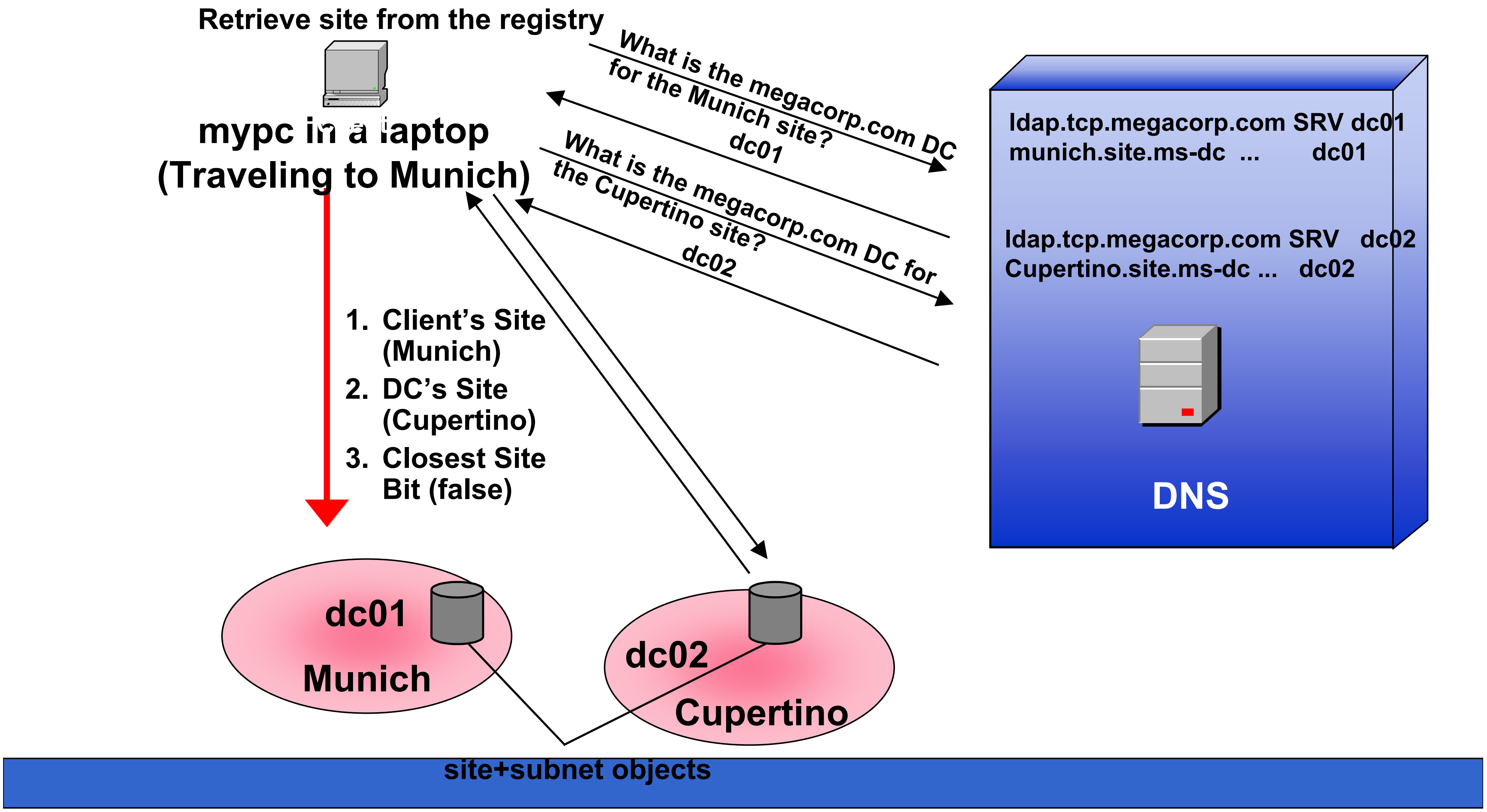
dc02

1. Client's Site (Cupertino)
2. DC's Site (Munich)
3. Closest Site Bit (false)

ldap.tcp.megacorp.com SRV dc01
munich.site.ms-dc ... dc01
ldap.tcp.megacorp.com SRV dc02
Cupertino.site.ms-dc ... dc02

* Details later

Locator and Sites



Retrieve site from the registry

mypc in a laptop
(Traveling to Munich)

What is the megacorp.com DC for the Munich site?

dc01

What is the megacorp.com DC for the Cupertino site?

dc02

ldap.tcp.megacorp.com SRV dc01
munich.site.ms-dc ... dc01

ldap.tcp.megacorp.com SRV dc02
Cupertino.site.ms-dc ... dc02

DNS

1. Client's Site (Munich)
2. DC's Site (Cupertino)
3. Closest Site Bit (false)

dc01

Munich

dc02

Cupertino

site+subnet objects

Query for Directory Services

DC Locator: Process Flow (1)

- DC Locator queries DNS for specific host names
  - Using Site Name information
  - Hosts offering specific services
- DNS returns a list of SRV records sorted by priority and weight
  - Always select SRV recs with lowest priority
  - Prefer higher weighting amongst records with same priority
- DC Locator pings each DC in the list until it gets a first reply

DC Locator: Process Flow (2)

- Once a DC is found, the Site name is registered in

  ```
  HKLM\CCS\Services\NetLogon\Para
  meters\DynamicSiteName
  ```

- To override this value, create an entry

  ```
  HKLM\CCS\Services\NetLogon\Para
  meters\SiteName
  ```

Cache Time-out and Closest Site

- DC Locator can return a DC in a different site
- Client stores the location of this DC in memory
- Cache lifetime is controlled by the registry entry

```
HKLM\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters\CloseSiteTimeout
```

Cache Time-out and Closest Site cont.

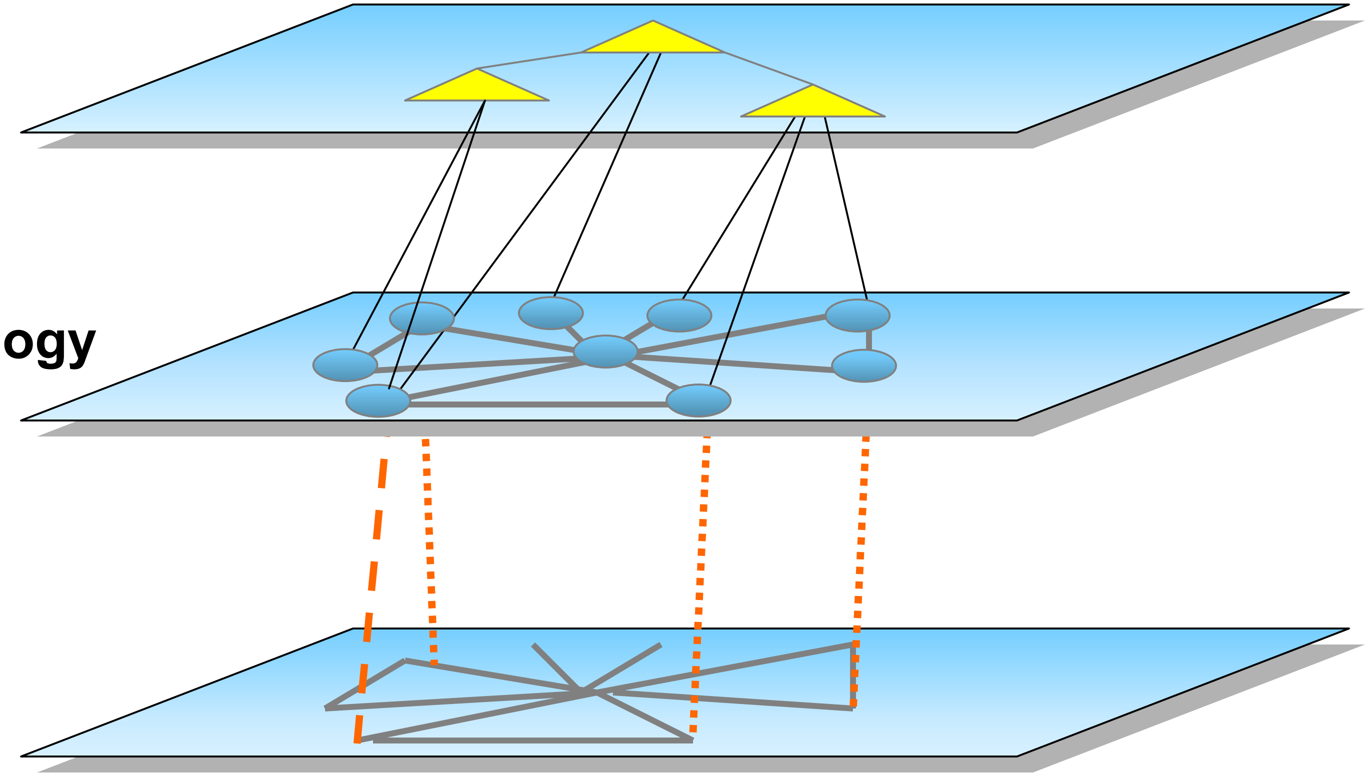
- DC Locator will search for a DC in client’s site when the timeout expires
- Example: Exchange 2000 SP2 DSACCESS component

DC Locator characteristics

- DC Locator uses SRV records in DNS to find a DC/GC
  - Site specific SRV to locate services in the same site as clients
  - Priority and weight of SRV allows prioritization of DC/GC
- Issues:
  - DNS configuration on workstation
  - DNS may contain useless or incorrect SRV records
  - DNS updates may augment the network traffic

Registering Service Records on Servers

Overview of Site Topology Design



Logical Design

Site Topology Design

Physical Network

Site Topology design’s Objectives

- Build an efficient replication topology
  - Sites - Subnets
  - Site Links: Cost, Schedule
  - Bridgehead Servers – Global Catalogs (GC)
- Lay out an optimized authentication infrastructure
  - Placement of Domain Controllers (DC) in sites
  - Number of servers required: DC – GC
  - Sizing the server profile for DC

What are the challenges?

- Find a good trade-off between replication traffic and fast authentication against local DCs
- Optimize the number of servers deployed
  - Reduce the burden of administration
  - Reduce the overall Total cost of Ownership
  - Minimize security threats in exposing DCs in “un-trusted” sites
- Design the right profile for server
  - Number of concurrent clients supported
  - CPU – RAM

Directory Services Publication

- Domain Controllers announce their services when assigned to a Windows 2000 site:
  - SRV records registered in DNS with site information
  - Operation performed by the NETLOGON service
- AD clients look up in DNS for these SRV records to search for Directory Services

Service Records registered in DNS

- Service Record (SRV) maps the name of a service to a DNS computer name
- Allows DC/GC to publish directory services
- Each DC/GC registers:
  - Non-site specific SRV
    - _ldap._tcp.*DnsDomainName*
    - _gc._tcp.*DnsForestName*
  - Site-specific SRV
    - _ldap._tcp.*SiteName.*_sites.*DnsDomainName*
    - _gc._tcp.*SiteName*._sites.*DnsForestName*

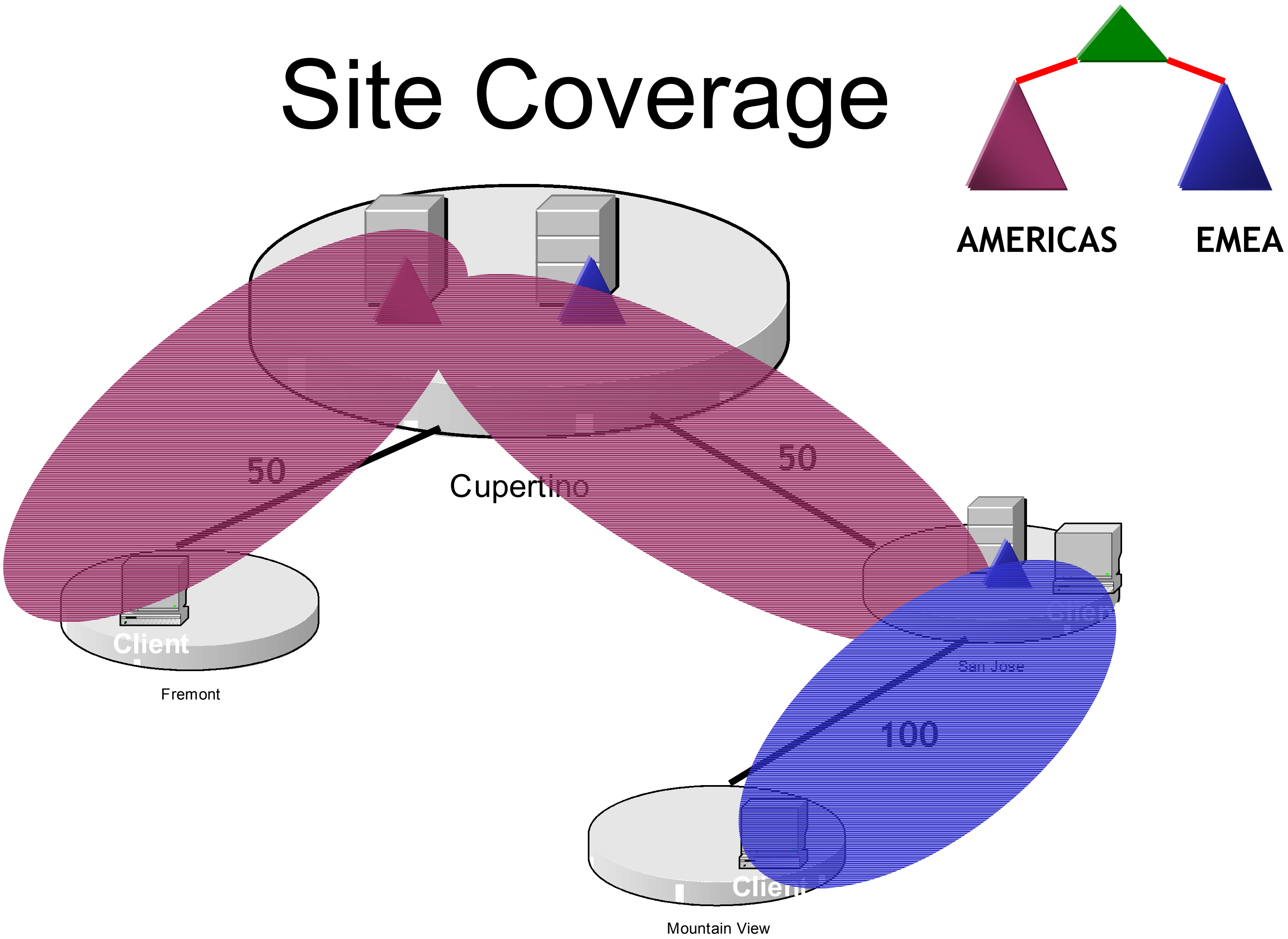
Site Coverage

- Each DC/GC advertises Directory Services for:
  - Its home site
  - DC-less sites that are “adjacent” to its site
- DC creates 4 SRV per site for authentication service
- GC creates 2 SRV per site for directory services

Site Coverage cont.

- DC-less sites:
  - Locations with few users that do not justify presence of DC/GC
  - Locations that do not necessarily contain DC/GC of every domain
- Adjacent sites are evaluated using site link cost

Site Coverage



Site Coverage: Issues

- May augment network traffic:
  - Significant number of SRV records registered in DNS
  - Updated every hour by the NetLogon Service

- Number of SRV records:
  - DC: 4* N * M
  - GC: 2 *N *M

  Where N = number of AD servers (DC/GC)
  M = number of DC-less sites to be covered

- 3 DCs - 2 GCs – 10 Client sites ➔
  4*(3+2)*10 + 2*2*10 = 240 SRV records in DNS!

- 2 DC/GC – 50 Client sites ➔
  4* 2 *50 + 2*2* 50 = 600 SRV records in DNS!

Site Coverage: Optimization

- Site Coverage is enabled by default
- To reduce SRV registration:
  - Turn off Site Coverage
  - Manually specify site names that a DC can cover

- Action performed on each DC/GC
- Different customizations for GC and DC
- Windows 2000: registry keys
  Windows .NET: GPO

Site Coverage: Optimization

- Windows 2000: HKLM\CCS\Services\NetLogon\Parameters\AutoSiteCoverage 0 | 1 (D)

- Windows .NET

  Computer Configuration -> Administrative Templates -> System-> NetLogon

  AutoSiteCoverage Disabled | Enabled (D)

Site Coverage: Optimization

- Windows 2000:

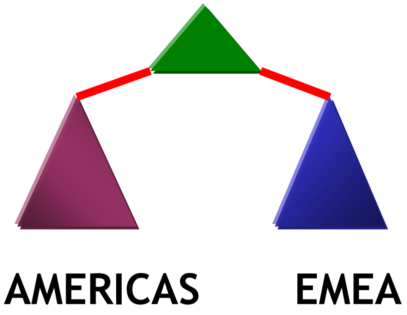
  `HKLM\CCS\Services\NetLogon\Parameters\`<u>`SiteCoverage`</u> = *List of site names to be covered*

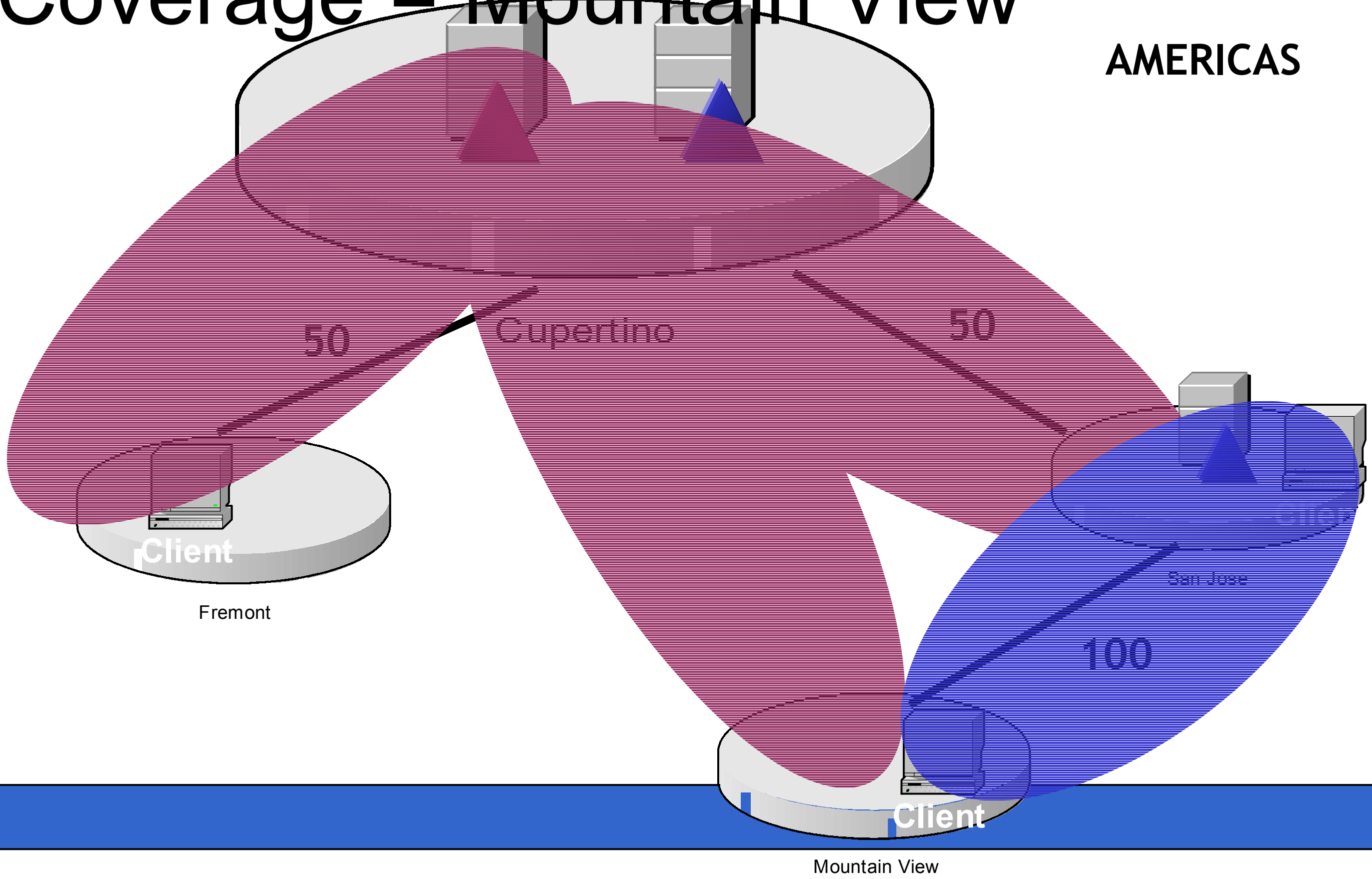
- Windows .NET:

  Computer Configuration -> Administrative Templates -> System-> NetLogon-> <u>SiteCoverage</u> = *List of site names to be covered*

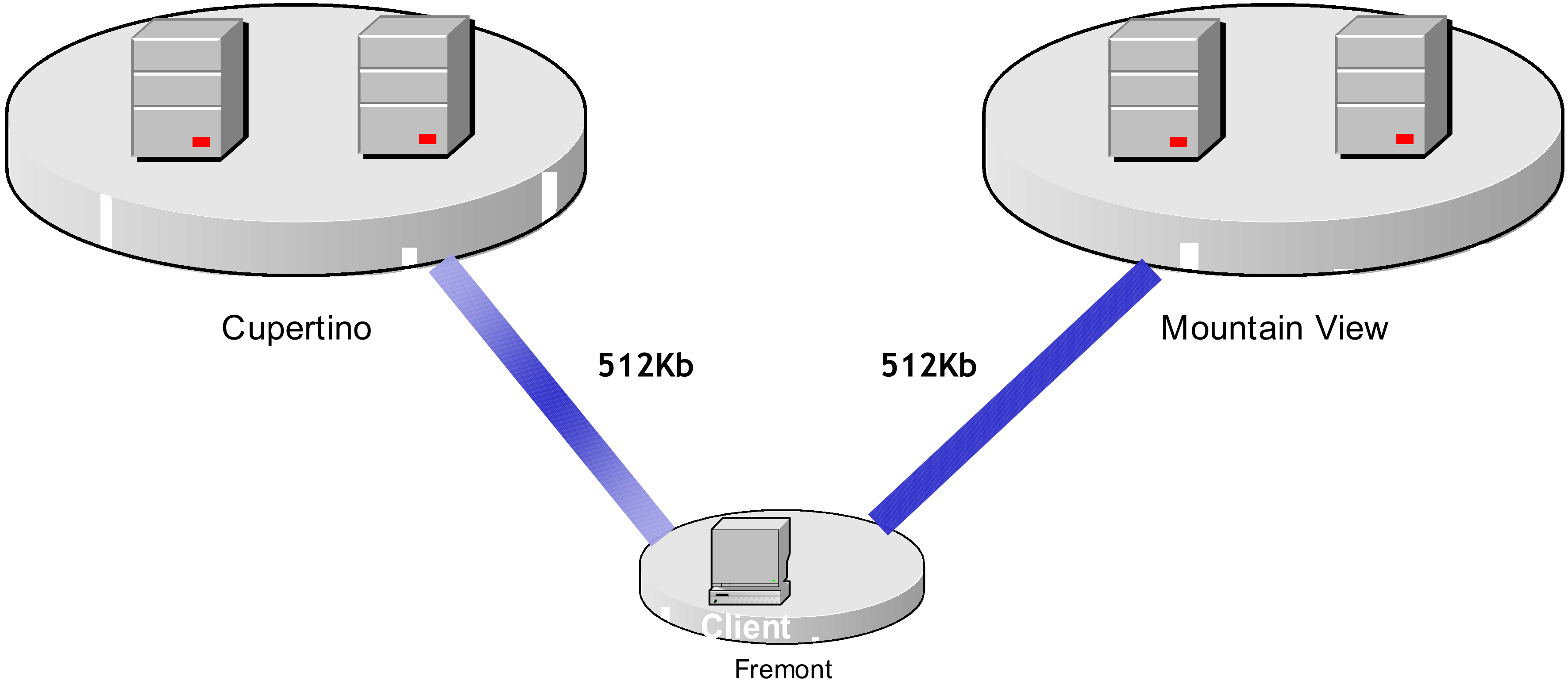
Site Coverage: Example

- AutoSiteCoverage = Enabled
- SiteCoverage = Mountain View

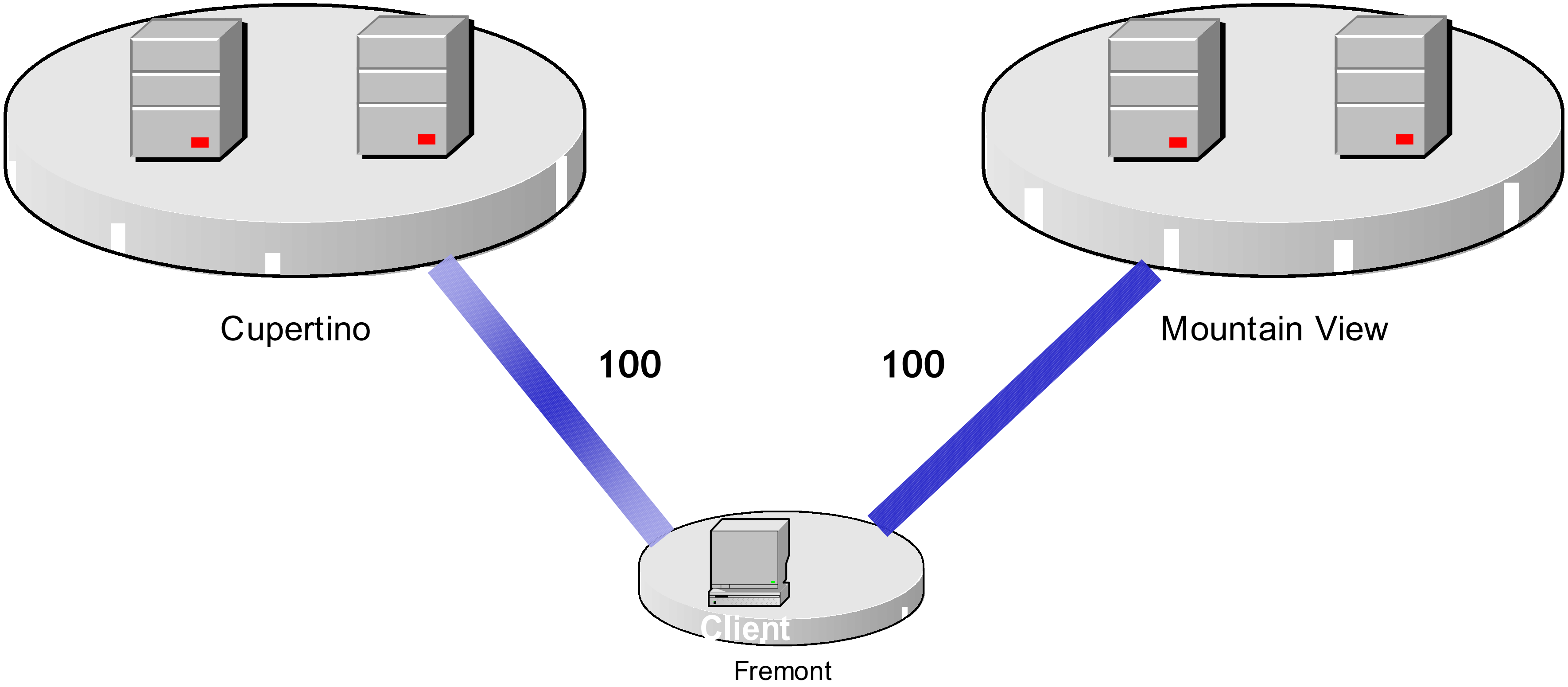




Site Coverage: Example

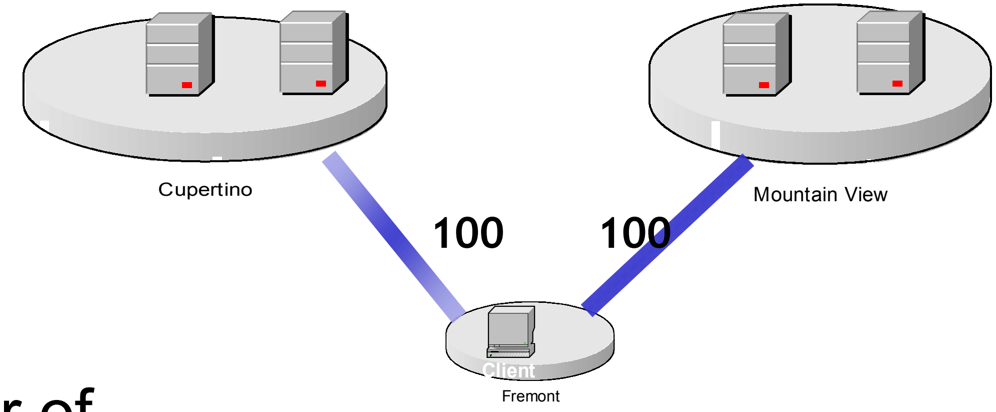


Site Coverage: Example



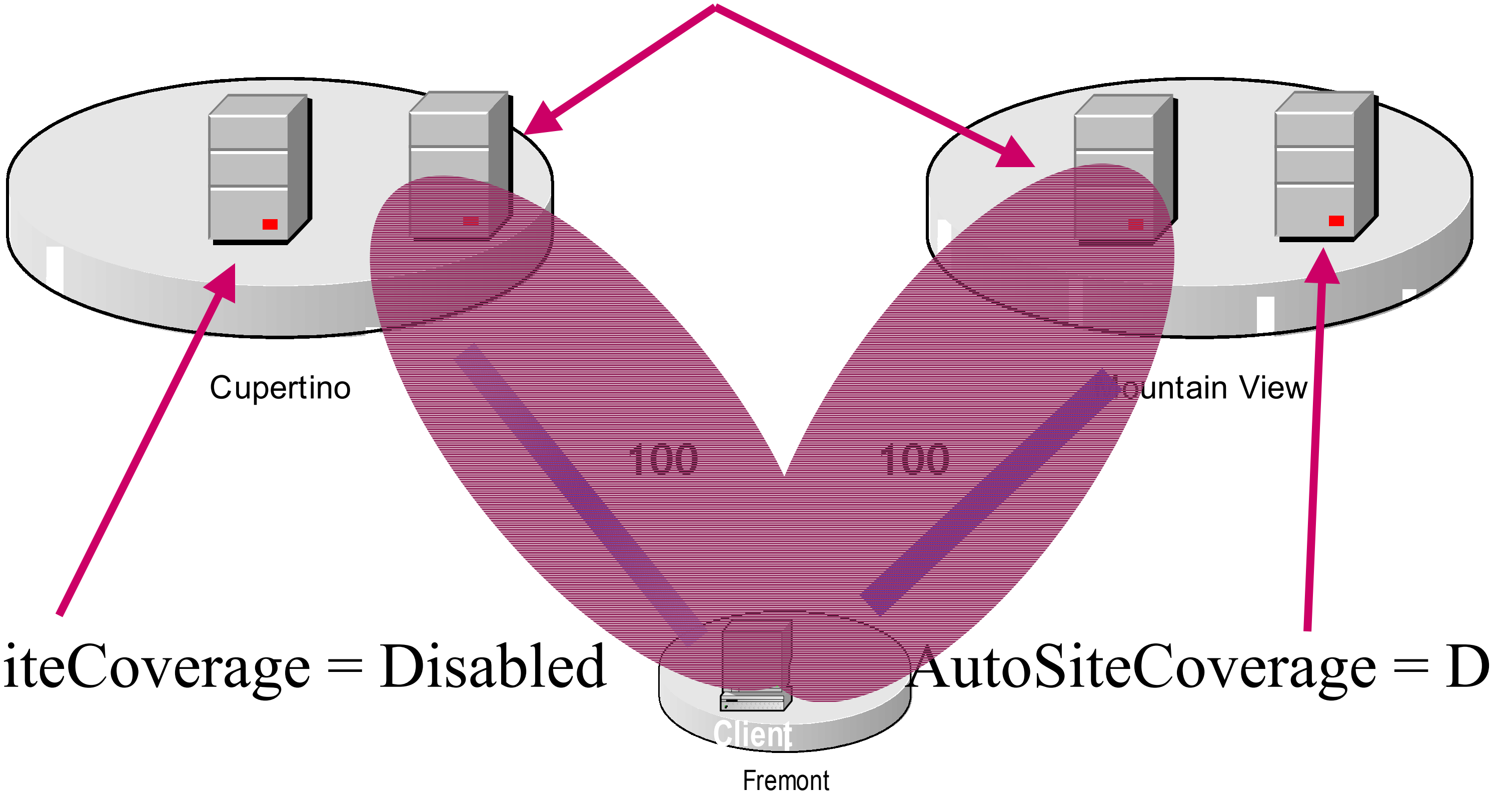
Site Coverage: Example

- AutoSiteCoverage = Enabled
- Selection process
  - Site Link cost
  - Site with larger number of DC/GC
  - Site sorted in alphabetical order
- In our example, Cupertino will cover Fremont site



Site Coverage: Example

AutoSiteCoverage = Disabled
SiteCoverage = Fremont



AutoSiteCoverage = Disabled

AutoSiteCoverage = Disabled

Priority on SRV records

- _Service._Protocol ….. [Priority] [Weight]
- Set preference for target host specified in the Target Field
- Weight is used to set preference when two SRV records have same priority

Priority in SRV records

- Windows 2000

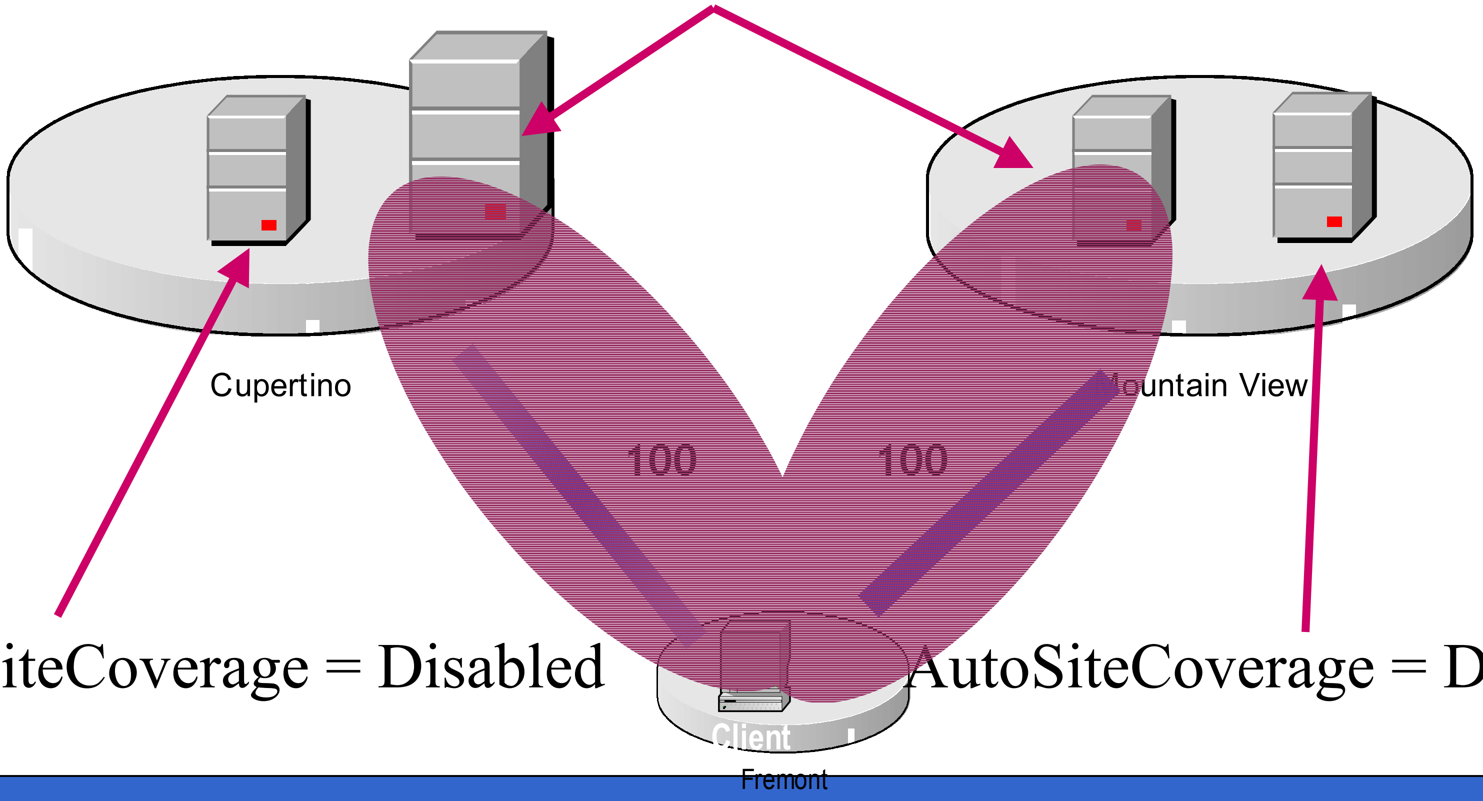
`HKLM\CCS\Services\NetLogon\Parameters\`
`LdapSrvPriority` = [0, 65535]

Windows .NET
Computer Configuration\Administrative Templates\System\Netlogon\<Dynamic Registration of the DC Locator DNS Records>

LdapSrvPriority = [0, 65535]

Priority in SRV records: Example

AutoSiteCoverage = Disabled
SiteCoverage = Fremont



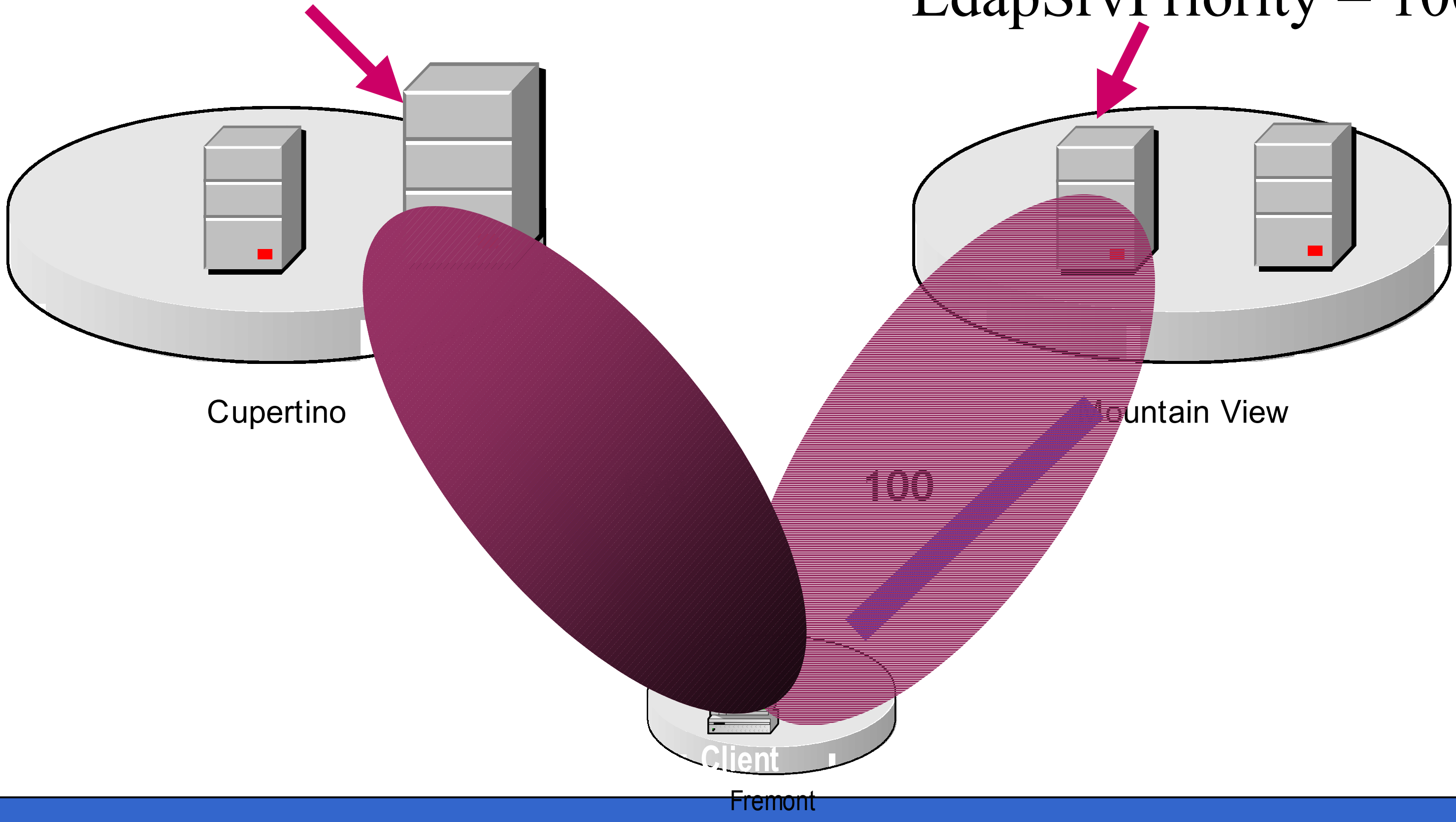
AutoSiteCoverage = Disabled

AutoSiteCoverage = Disabled

Priority in SRV records: Example

LdapSrvPriority = 200

LdapSrvPriority = 100



Site Coverage for GC

- Windows 2000: HKLM\CCS\Services\NetLogon\

  Parameters

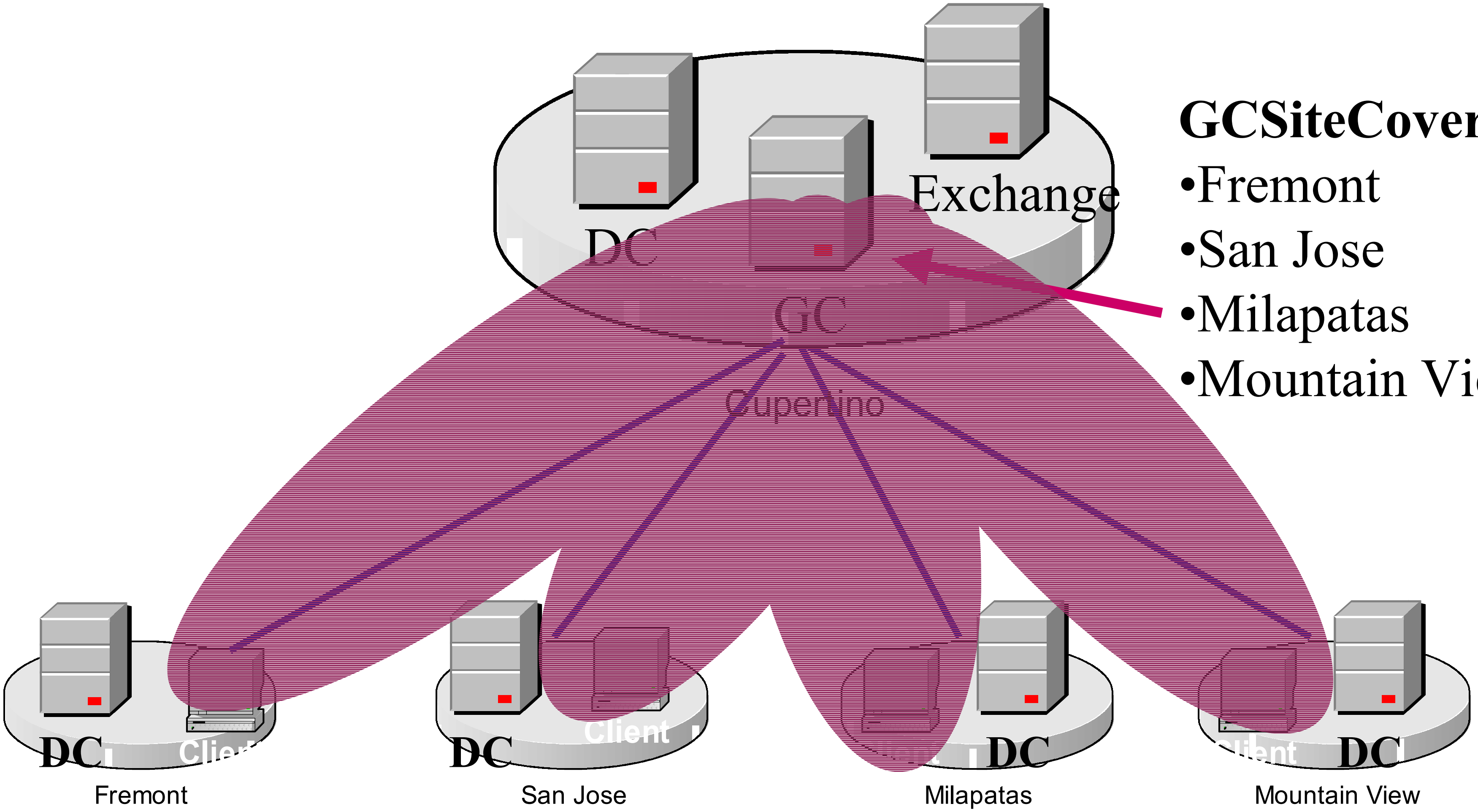
  GCSiteCoverage = *List of site names to be covered*

- Windows .NET

  Computer Configuration -> Administrative Templates -> System-> NetLogon

  GCSiteCoverage = *List of site names to be covered*

GC SiteCoverage: Example



GCSiteCoverage

- Fremont
- San Jose
- Milapatas
- Mountain View

Generic SRV records

- Used by clients when they cannot find AD servers in their sites
- Each DC/GC registers generic SRV records
  - DC specific records
  - GC specific records

Generic SRV Records for DC

Mnemonic	Type	DNS Record
LdapIPAddress	A	<DNSDomainName>
DcByGUID	SRV	_ldap._tcp.<DomainGuid>.domains._msdcs.<DnsForestName>
Kdc	SRV	_kerberos._tcp.dc._msdcs.<DnsDomainName>
Dc	SRV	_ldap._tcp.dc._msdcs.<DnsDomainName>
Rfc1510Kdc	SRV	_kerberos._tcp.<DnsDomainName>
Rfc1510UdpKdc	SRV	_kerberos._udp.<DnsDomainName>
Rfc1510Kpwd	SRV	_kpasswd._tcp.<DnsDomainName>
Rfc1510UdpKpwd	SRV	_kpasswd._udp.<DnsDomainName>

Generic SRV Records for GC

Mnemonic	Type	DNS Record
GcIpAddress	A	Gc._msdcs.<DNSForestName>
GenericGc	SRV	_ldap._tcp.gc._msdcs.<DnsForestName>
Gc	SRV	_ldap._tcp.gc._msdcs.<DnsForestName>

Generic SRV records: Optimization

- Settings to prevent DC/GC to register specific SRV records
- Available with Windows 2000 SP2

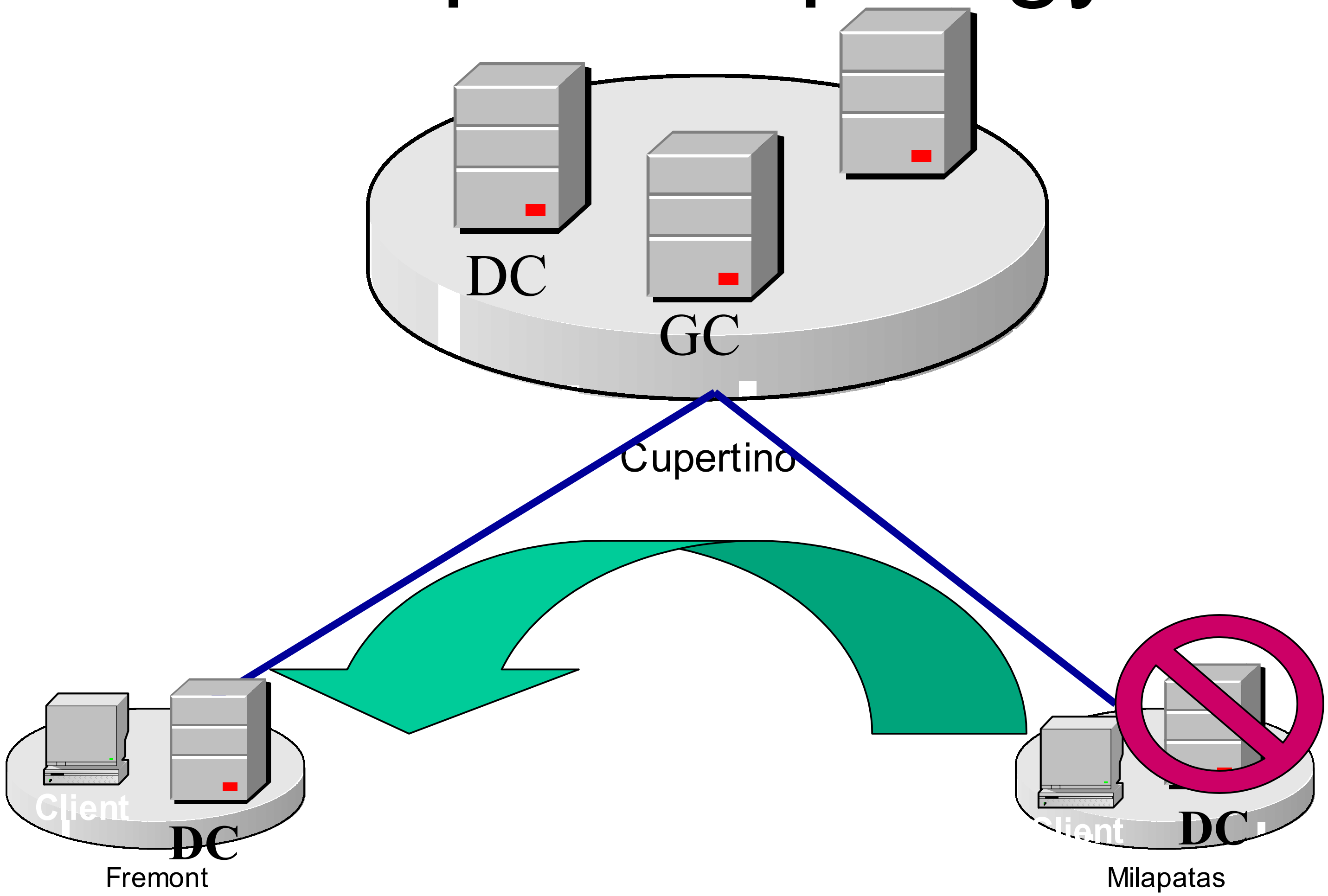
- Prevent local DC/GC to serve remote clients over the WAN
  - Hub-Spoke topology
  - Network Operating Centers (NOC) sites

Generic SRV records

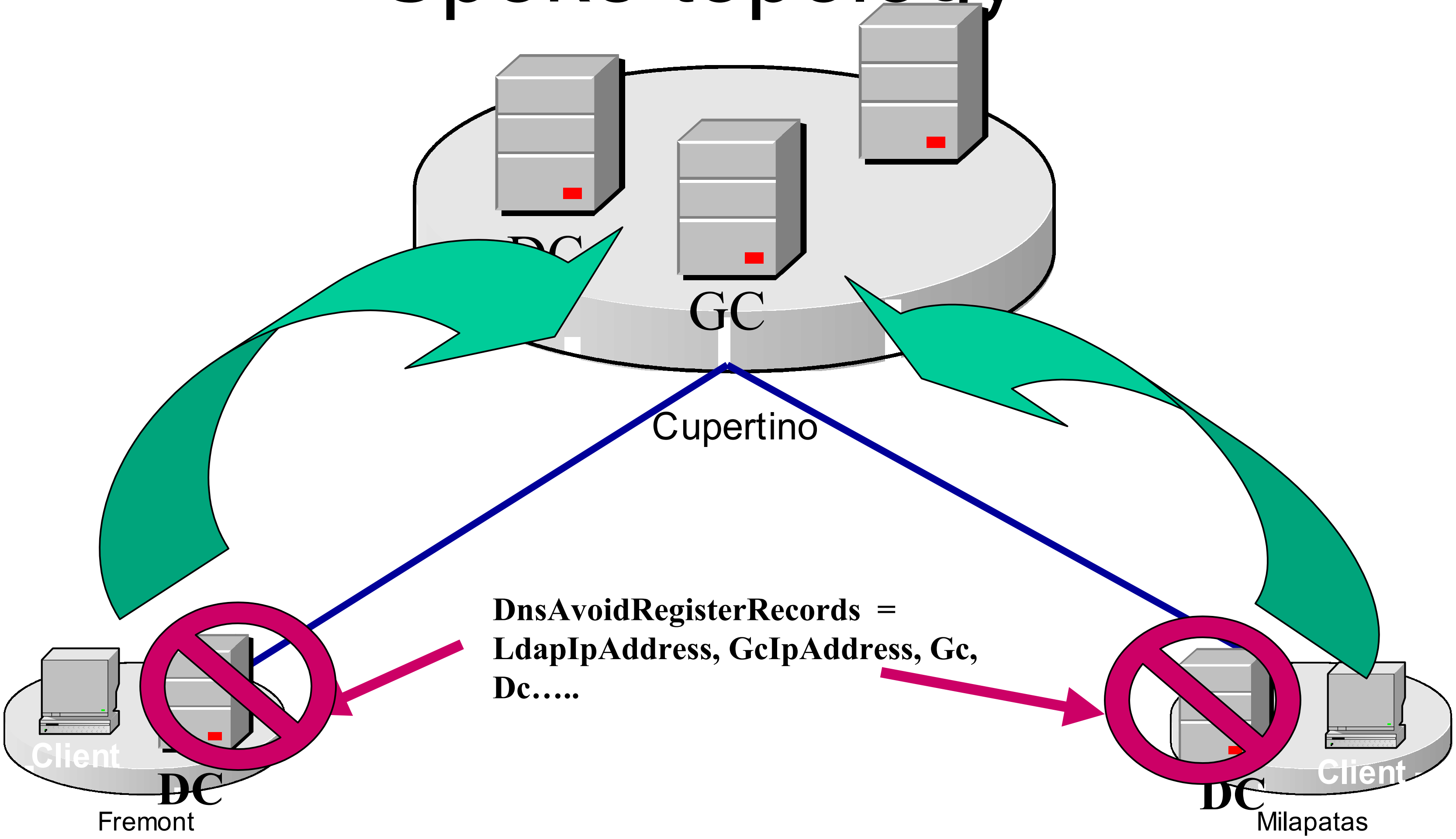
- Windows 2000: HKLM\CCS\Services\NetLogon\Parameters DnsAvoidRegisterRecords = *List of mnemonics*
- Windows .NET

  Computer Configuration -> Administrative Templates -> System-> NetLogon
  <u>DNS records not registered by the domain controllers</u> = *List of mnemonics*

Generic SRV Records: Hub-Spoke topology



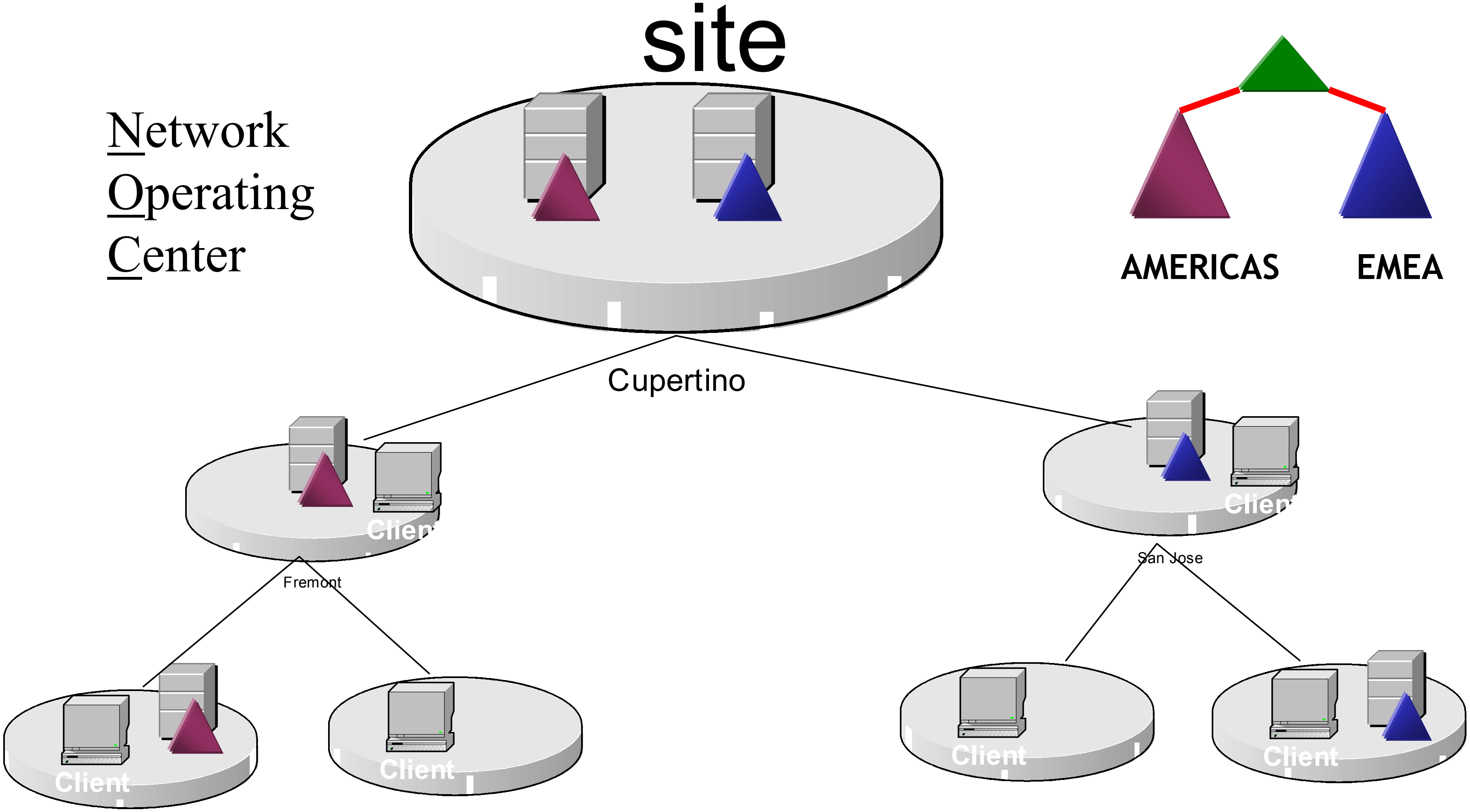
Generic SRV Records: Hub-Spoke topology



DnsAvoidRegisterRecords = LdapIpAddress, GcIpAddress, Gc, Dc…..

Generic SRV Records: NOC site

Network
Operating
Center



Network Operating Center

- Requirements:
  - Used only for centralized backup operations
  - Must not serve clients for authentication or directory lookup
  - Must not be disconnected from the network

- Solutions:
  - Turn off Automatic Site Coverage feature
  - DnsAvoidRegisterRecords has all mnemonics except DcByGUID

Summary

- The NetLogon service plays a fundamental role by:
  - Locating AD servers on the client side
  - Publishing service records on the server side
- Customized settings:
  - Windows 2000: registry keys
  - Windows .NET: GPO
- Optimize the discovery process of AD servers by clients
- Reduce impact of AD topology on the network

Questions?