Configuring BIND DNS for Microsoft's® Active Directory

Michele Beveridge, UGA, EITS
Mark Plaksin, Board of Regents, OIIT

What is Active Directory?

- LDAP-based directory service released in January of 2000
- Required Upgrade Path for Windows NT 4 Domains
- The Only Way to Enjoy the Great New Features of Windows 2000

What Microsoft Wants
The Overview

- 4 _Zones (underscore!).
- Dynamic updates.
- SRV records.
- It's own namespace in the DNS domain, one Active Directory per DNS domain.
- Be The Domain!

Why Would the BIND Guys Care?

- AD requires integration with DNS namespace for Microsoft's domain structure and for service location.
- AD Requires Dynamic Updates, SRV records, and underscores in DNS.
- AD requires CHANGES (Oh My!) in most existing DNS configurations.

Until Recently, Most BIND DNS Implementations….

- Did not accept Dynamic Updates
- Did not accept underscores
- What is an SRV record#!$!$
- UGA's BIND configuration was no exception. It had lived comfortably in a world without Microsoft since the beginning….

Now What Do I Do? Search the Web!

- Of course, Active Directory was still fairly new.
- Microsoft had some good White Papers on how to do it *their* way.
- There were a few resources on the web by folks (Universities) who were running AD. Most of them used Microsoft's DNS or made BIND dynamic, of course.

What I Found

- In the end, I came up with 5 different ways that we could change our DNS to accommodate AD.
- One was just a hopeful guess.
- Some were easier on the BIND guys than others.

Option 1
Use Windows 2000 Dynamic DNS?

- No! Was the resounding cry from the masses of *nix guys within earshot. At least they didn't throw anything.
- Seriously, retraining was an issue and although Microsoft has offered a DNS product in the past, BIND had been doing the job well for years.
- And why spend the money to change an infrastructure that is already solid for one that no one knows, despite the fact that it offered Secure Updates for it own kind?
- I did make them sweat a little though. ;-)

Option 2
Make BIND Dynamic!

- Upgrade our BIND infrastructure to accept dynamic updates for the UGA zones
- This sounded like a BIG security hole to everyone concerned, especially the BIND guys.
- BIND didn't offer a secure protocol for dynamic updates from the clients.

Option 3
Do BOTH…MS marries BIND

- Set up Windows 2000 DNS in addition to BIND.
- MS DNS gets dynamic updates from AD.
- BIND does static DNS for everything else.
- MS hosts a separate zone for each department (ad.chem.uga.edu) or one zone for a central AD (ad.uga.edu). Alternatively, MS can host *just* the underscore zones for any/all AD.
- All but one of these scenarios create naming issues...

Issues with Option 3

MS Hosts:	BIND hosts:
ad.chem.uga.edu	chem.uga.edu
ad.uga.edu	uga.edu
_zones (chem.uga.edu)	chem.uga.edu
_zones (uga.edu)	uga.edu

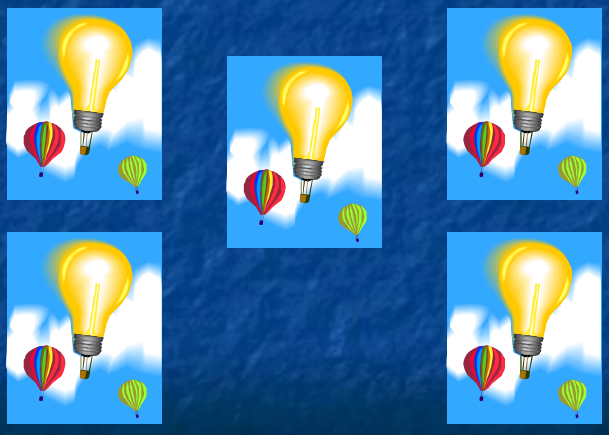
Issues With Option 3

- Either way, we'd have to implement a separate set of name servers to do this.

Option 4
Roll Your Own DNS

- Departments run their own DNS if they want AD.
- They would have their own namespace!
- Staffing problems, one more thing to learn
- Our DNS crew would probably end up with more consulting calls.
- We would be the laughing stock of the DNS world if we had, say, 30 different DNS implementations on campus. DNS is, for good reasons, a *central* service.

And The Winner is…..
Option 5



Unfortunately

- This was the 'hopeful' option.
- It was the solution we knew the LEAST about.
- I had read about it, but not found anyone who had actually DONE it.
- But, it seemed like it would have the least effect on Bind AND the AD namespace issues and was the best option.

Option 5
The Only *Real* Option for UGA

- Keep our existing BIND configuration.
- Add the required _zones to each child domain within the .uga.edu namespace.
- Allow the BIND servers to accept dynamic updates *only* for those zones.
- It's kinda dymanic. This allows the _zones to be the *only* BIND zones updated by Microsoft which we felt would eliminate collateral damage.

Why It Works for UGA And Makes the BIND Guys Happy (no pun intended)

- Only the _zones are dynamic.
- BIND doesn't care about those _zones
- Even if something went terribly wrong within those files, it would not affect the uga.edu domain name service (DNS).
- It also meant that we could 'allow updates' only from registered Domain Controllers (This doesn't prevent IP spoofing, but the security risk is not great, considering the limited damage that could be done , and only to the _zone files.)

What Microsoft Wants

Let's go into a bit more detail about exactly what Microsoft wants…

What Microsoft Wants Dynamic Updates (RFC 3007)

- BIND servers would need to be configured to accept changes dynamically from Microsoft's Domain Controllers (DC's).
- Dynamic updates are essential, because the DC's use this method to register Service Resource Records (SRV records) for certain zones.

What Microsoft Wants SRV Records (RFC 2782)

- SRV records (Service Resource Records) are used to list resources by service name and protocol, rather than by a specific server name.
- DNS becomes a 'directory of services'.
- This is a requirement for AD.
- And no, Microsoft did not invent SRV records, although they are fairly new.

Clients Want to Be Dynamic Too

- All Windows 2000 clients are also configured to register an A record for themselves.
- Client updates are not a required and can be disabled.

What Microsoft Wants New Subdomains

- Four new subdomains in each zone for SRV records:

  _msdcs.subdomain.uga.edu

  _sites.subdomain.uga.edu

  _tcp.subdomain.uga.edu

  _udp.subdomain.uga.edu
- AD Domain Controllers dynamically update SRV records in these zones and use them to locate services for client requests.

What Microsoft Wants
The Use of Underscores

- The use of underscores also had to be allowed in the BIND zones.

Let's Try IT

- We created a test BIND server.
- Allowed it to host a test subdomain for uga.edu.
- We called it dev.uga.edu.
- We set up the Windows 2000 Server.
- Promoted it to a Domain Controller.
- It failed.

We Dig a Little Deeper

- Cricket Liu only had a half a page dedicated to this and we read it a thousand times!
- We e-mailed him and every other DNS guy we could find.
- No one had done it or could help.
- So we called in the 'Sniffer'.

EtherPeek to the Rescue!

- We set up a sniffer on the Domain Controller.
- Between EtherPeek and the DNS logs we found a couple of things…

Windows 2000 Uses Dynamic Ports For (UDP) DNS Requests:

- Windows 2000 doesn't use Port 53 as its Source Port for DNS queries.
- It uses dynamic UDP ports for all its standard queries.
- It affected how we set the filters to get the trace.
- You can change the port it uses. This registry change used to be broken. (http://support.microsoft.com/default.aspx?scid=kb;EN-US;q260186)

BE THE DOMAIN!

- Active Directory Domain Controller Tries (and retries and retries) To BE the Domain:
- DC tries to register an A record for the domain name (chem.uga.edu), which the BIND server will not allow, since we were only allowing updates to the _zones.
- This makes the DCPROMO process look like it is failing.

Promoting the DC
What it looks like to the MS admin

- Run DCPROMO
- The Domain Controller looks for a DNS which is configured to accept dynamic updates for the zone which AD will be configured for.
- During the process, it will show you an error saying that a DNS server could not be contacted and ask you if you want to configure DNS on the Domain Controller. (just say no)
- DCPROMO will finish.
- When you reboot, AD will be installed.

What the DNL's have to do

- DNL's use a web page to request IP's at UGA.
- They use the same tool to request that their DC's are allowed to make dynamic updates.
- Make sure A record for DC and client are already in zone.

Now That It Is Working

- Mark wrote some scripts to automate the process for the subdomains.

The BIND Details

- Add an A (host) record for the DC to the child domain's zone file.
- Add the underscore zones to the named.conf file.
- Add an A record for the gc to the _msdcs zone (gc 10M IN A x.x.x.x).
- Allow updates to the _zones in the conf file.
- Allow underscores.

BIND configuration

- Create 4 subzones of dev.uga.edu for AD:
  - _udp.dev.uga.edu
  - _tcp.dev.uga.edu
  - _sites.dev.uga.edu
  - _msdcs.dev.uga.edu
- Tell BIND (version 8) to ignore underscores:
  check-names master ignore;
  check-names slave ignore;

BIND configuration (2)

- named.conf:

```
acl dc_dev { 128.192.45.46; 128.192.45.47; }
zone "_tcp.dev.uga.edu" {
   type master;
   file "dev_tcp";
   allow-update { dc_dev; };
};
```

- Also add zone stanzas for _msdcs.dev.uga.edu, _sites.dev.uga.edu, and _udp.dev.uga.edu.

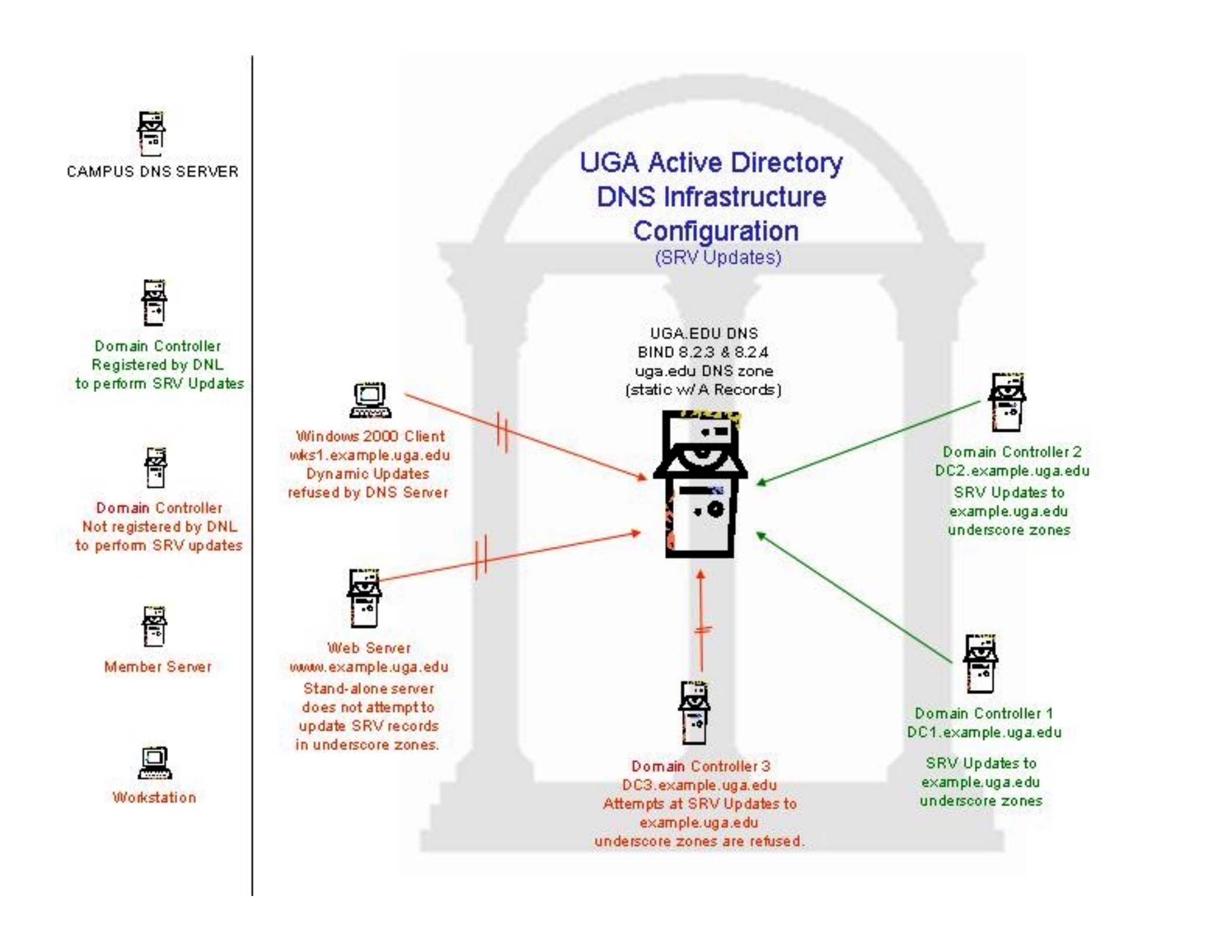
BIND configuration (3)

- Add A record called gc to _msdcs.dev.uga.edu which points to AD Global Catalog machine.
- Add an A record for the gc to the _msdcs zone (gc 10M IN A x.x.x.x).

BIND Configuration (3)

- You can Script It!
- The scripts that we used for UGA are located here: http://www.eits.uga.edu/nt2000/add_ad_to_zone.txt
- Of course, everybody is different.
- E-mail Happy if you want help.

happy@usg.edu


CAMPUS DNS SERVER
Domain Controller
Registered by DNL
to perform SRV Updates
Domain Controller
Not registered by DNL
to perform SRV updates
Member Server
Workstation
UGA Active Directory
DNS Infrastructure
Configuration
(SRV Updates)
UGA.EDU DNS
BIND 8.2.3 & 8.2.4
uga.edu DNS zone
(static w/ A Records)
Windows 2000 Client
wks1.example.uga.edu
Dynamic Updates
refused by DNS Server
Web Server
www.example.uga.edu
Stand-alone server
does not attempt to
update SRV records
in underscore zones.
Domain Controller 3
DC3.example.uga.edu
Attempts at SRV Updates to
example.uga.edu
underscore zones are refused.
Domain Controller 2
DC2.example.uga.edu
SRV Updates to
example.uga.edu
underscore zones
Domain Controller 1
DC1.example.uga.edu
SRV Updates to
example.uga.edu
underscore zones

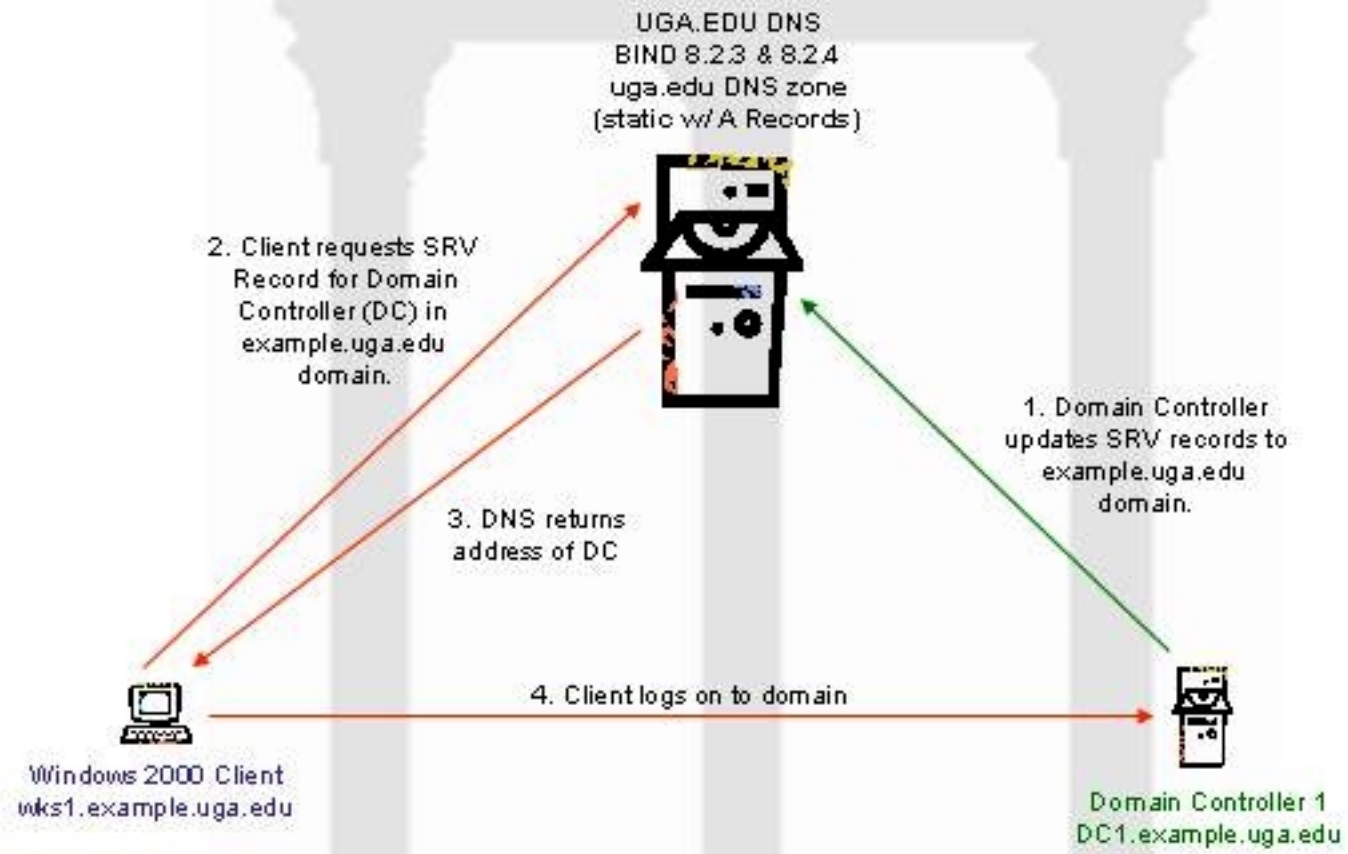
CAMPUS DNS SERVER

Domain Controller

Member Server

Workstation

UGA Active Directory
Client Service Request



Any Questions?

- No?
- Good!
- Have fun at the party!

Thanks for Coming!

- http://www.eits.uga.edu/nt2000/ad.html
- http://www.eits.uga.edu/nt2000/adandbind.htm