

Figure 2.1 The distributed hierarchical nature of DNS.

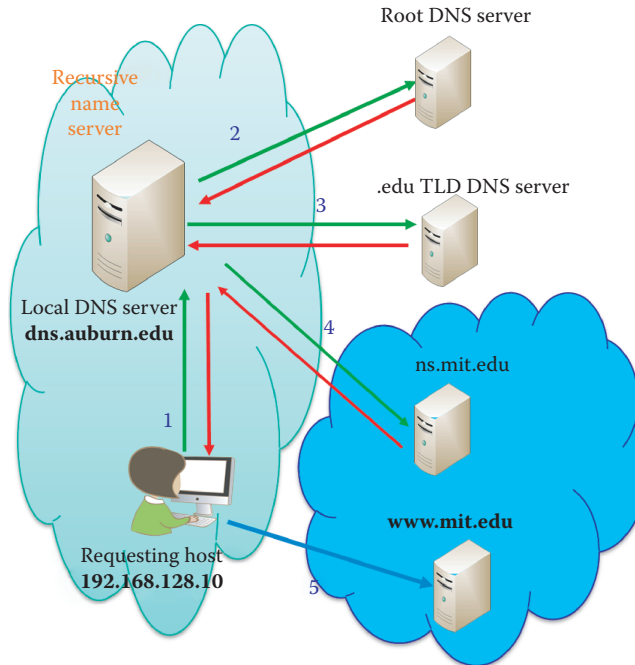


Figure 2.2 DNS queries include both recursive and iterative queries.

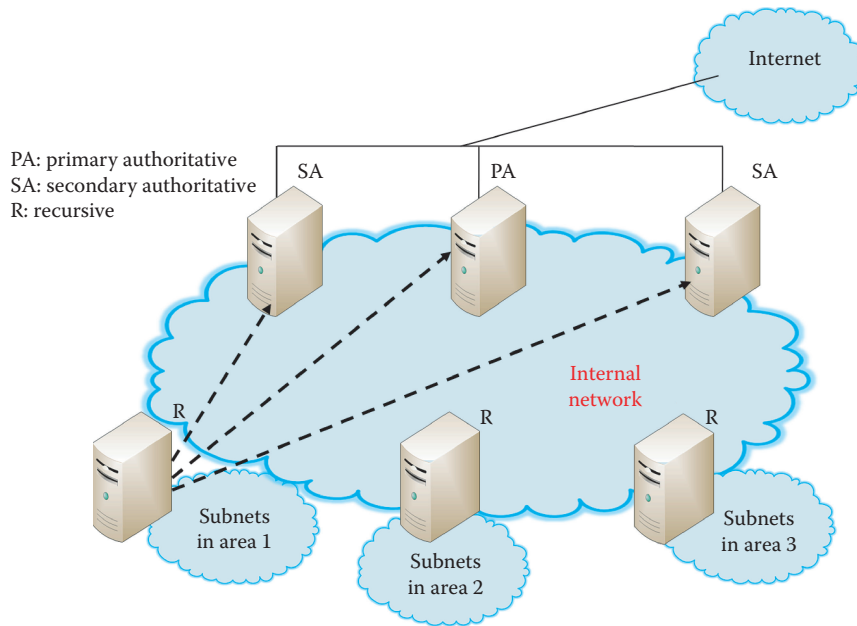


Figure 2.3 DNS hierarchy in a zone.

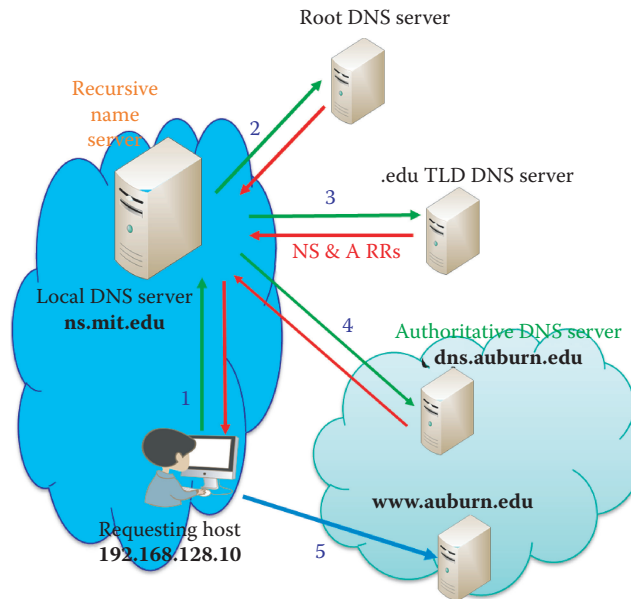
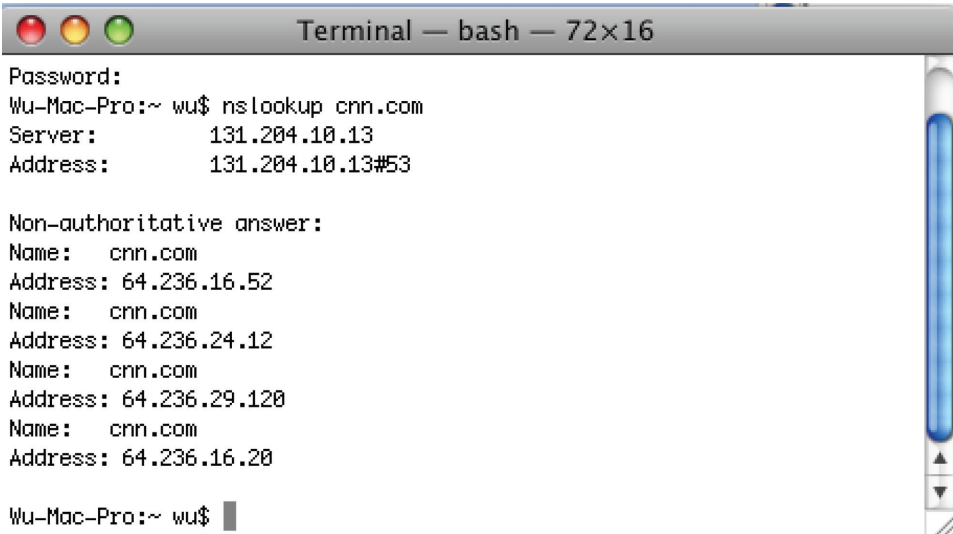


Figure 2.4 How to make DNS work for Auburn University's web and mail servers.

A screenshot of a macOS Terminal window titled "Terminal — bash — 72x16". The window has a standard macOS title bar with red, yellow, and green window control buttons. The terminal content shows a user at the "Wu-Mac-Pro" prompt running the command "nslookup cnn.com". The output shows a successful connection to a DNS server at 131.204.10.13, returning an authoritative answer for "cnn.com" with IP address 131.204.10.13#53. It then shows a "Non-authoritative answer:" section with five entries, each listing the name "cnn.com" and a different IP address: 64.236.16.52, 64.236.24.12, 64.236.29.120, and 64.236.16.20. The terminal ends with the prompt "Wu-Mac-Pro:~ wu\$ " and a cursor. A vertical scrollbar is visible on the right side of the terminal window.

```
Terminal — bash — 72x16
Password:
Wu-Mac-Pro:~ wu$ nslookup cnn.com
Server:      131.204.10.13
Address:     131.204.10.13#53

Non-authoritative answer:
Name:   cnn.com
Address: 64.236.16.52
Name:   cnn.com
Address: 64.236.24.12
Name:   cnn.com
Address: 64.236.29.120
Name:   cnn.com
Address: 64.236.16.20

Wu-Mac-Pro:~ wu$
```

Figure 2.5 The use of nslookup.

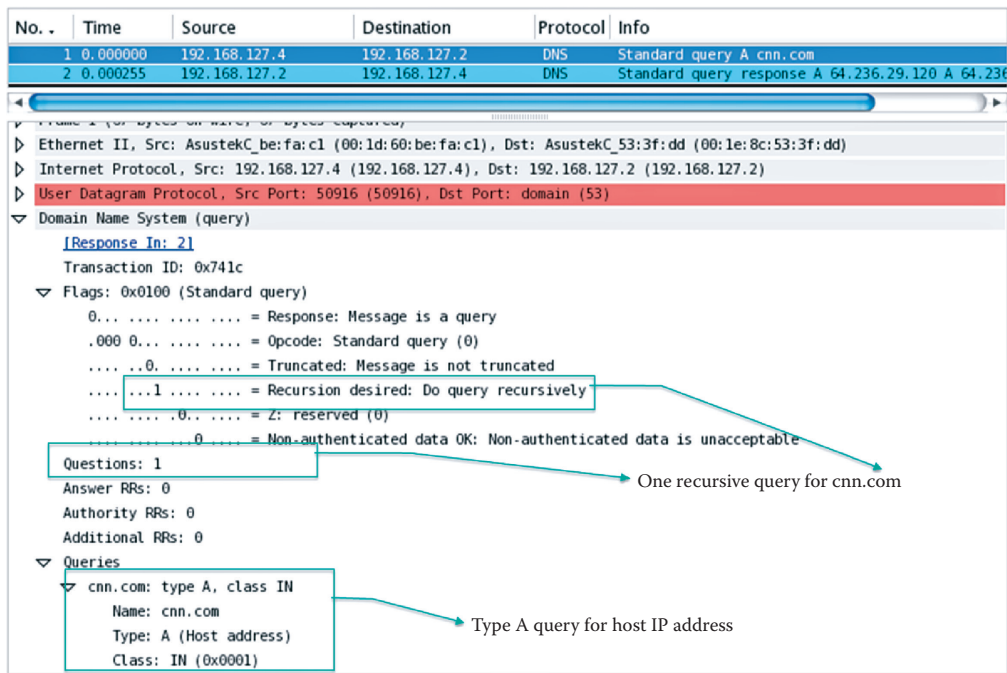
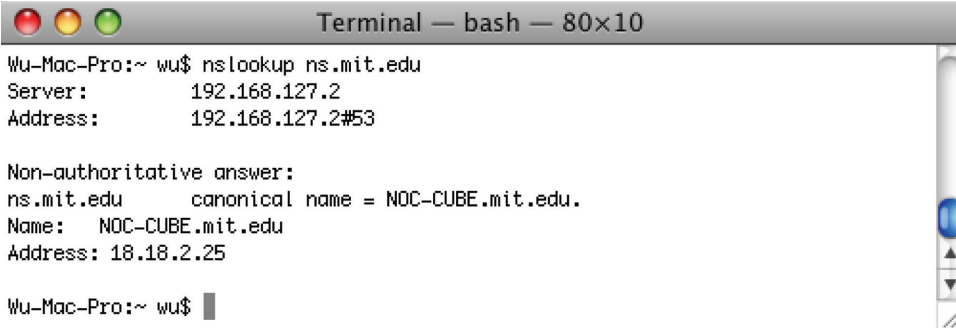


Figure 2.6 A DNS query.

A screenshot of a macOS Terminal window titled "Terminal — bash — 80x10". The window has a standard macOS title bar with red, yellow, and green window control buttons. The terminal text shows a user at the "Wu-Mac-Pro" prompt running the command "nslookup ns.mit.edu". The output displays the server IP as 192.168.127.2 and the address as 192.168.127.2#53. It then shows a "Non-authoritative answer:" for ns.mit.edu with a canonical name of NOC-CUBE.mit.edu, and its IP address as 18.18.2.25. The prompt returns to "Wu-Mac-Pro:~ wu\$".

```
Wu-Mac-Pro:~ wu$ nslookup ns.mit.edu
Server:          192.168.127.2
Address:         192.168.127.2#53

Non-authoritative answer:
ns.mit.edu       canonical name = NOC-CUBE.mit.edu.
Name:   NOC-CUBE.mit.edu
Address: 18.18.2.25

Wu-Mac-Pro:~ wu$
```

Figure 2.7 Finding a name server's IP address.

```

Mac-Pro:~ wu$ nslookup
> 131.204.10.13
Server:      131.204.10.13
Address:     131.204.10.13#53

Non-authoritative answer:
13.10.204.131.in-addr.arpa      name = dns.eng.auburn.edu.

Authoritative answers can be found from:
10.204.131.in-addr.arpa nameserver = dns.eng.auburn.edu.
dns.eng.auburn.edu      internet address = 131.204.10.13
> set q=mx
> auburn.edu
Server:      131.204.10.13
Address:     131.204.10.13#53

Non-authoritative answer:
auburn.edu      mail exchanger = 10 aumail.duc.auburn.edu.

Authoritative answers can be found from:
auburn.edu      nameserver = dns.auburn.edu.
auburn.edu      nameserver = dns.eng.auburn.edu.
auburn.edu      nameserver = dns.duc.auburn.edu.
aumail.duc.auburn.edu internet address = 131.204.2.83
dns.auburn.edu internet address = 131.204.41.3
dns.eng.auburn.edu internet address = 131.204.10.13
dns.duc.auburn.edu internet address = 131.204.2.10
> █

```

Figure 2.8 A query of auburn.edu's mail RR.

<u>google.com</u>	mail exchanger = 10 smtp4.google.com.
<u>google.com</u>	mail exchanger = 10 smtp1.google.com.
<u>google.com</u>	mail exchanger = 10 smtp2.google.com.
<u>google.com</u>	mail exchanger = 10 smtp3.google.com.
<u>google.com</u>	<u>nameserver</u> = ns2.google.com.
<u>google.com</u>	<u>nameserver</u> = ns3.google.com.
<u>google.com</u>	<u>nameserver</u> = ns4.google.com.
<u>google.com</u>	<u>nameserver</u> = ns1.google.com.
smtp1.google.com	internet address = 209.85.237.25
smtp2.google.com	internet address = 64.233.165.25
smtp3.google.com	internet address = 64.233.183.25
smtp4.google.com	internet address = 72.14.221.25
ns4.google.com	internet address = 216.239.38.10
ns1.google.com	internet address = 216.239.32.10
ns2.google.com	internet address = 216.239.34.10
ns3.google.com	internet address = 216.239.36.10

Figure 2.9 A query of google.com's MX RRs.

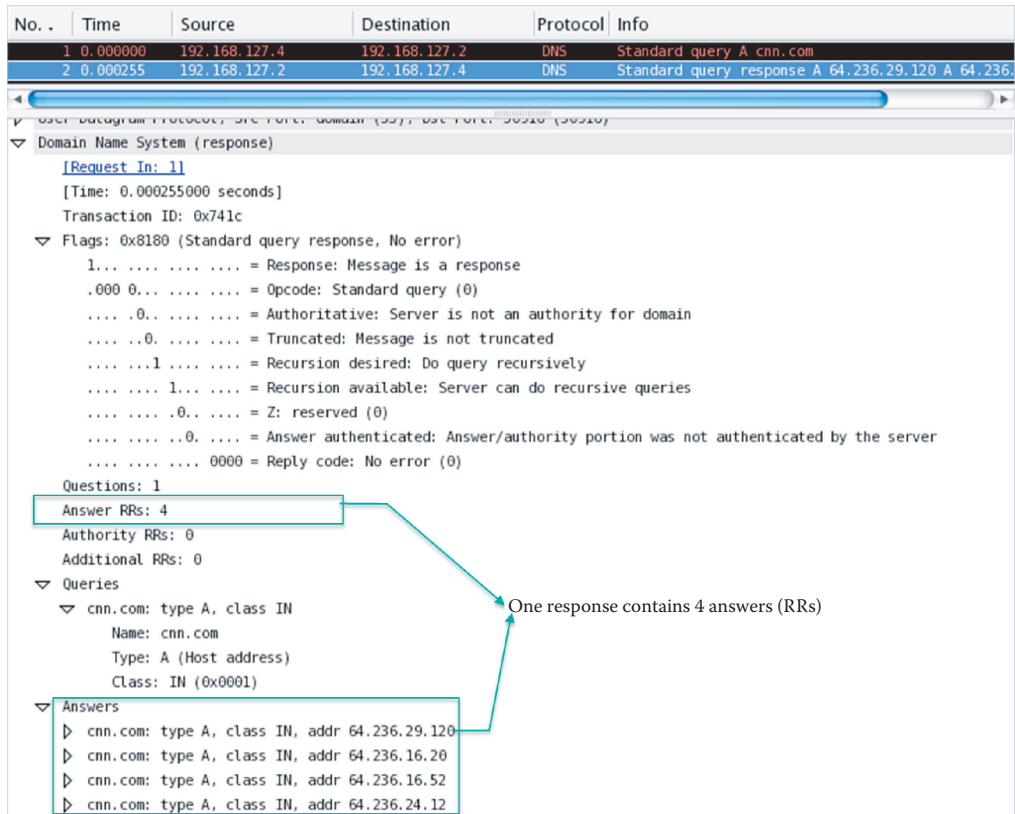


Figure 2.10 A DNS response.

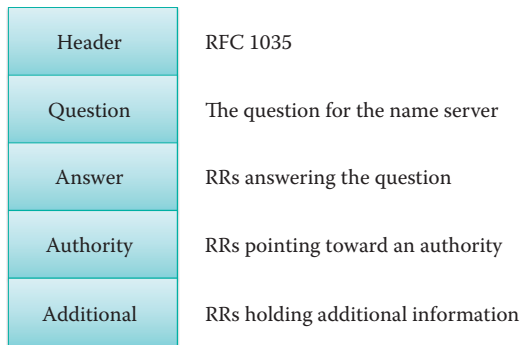


Figure 2.11 The DNS message format.

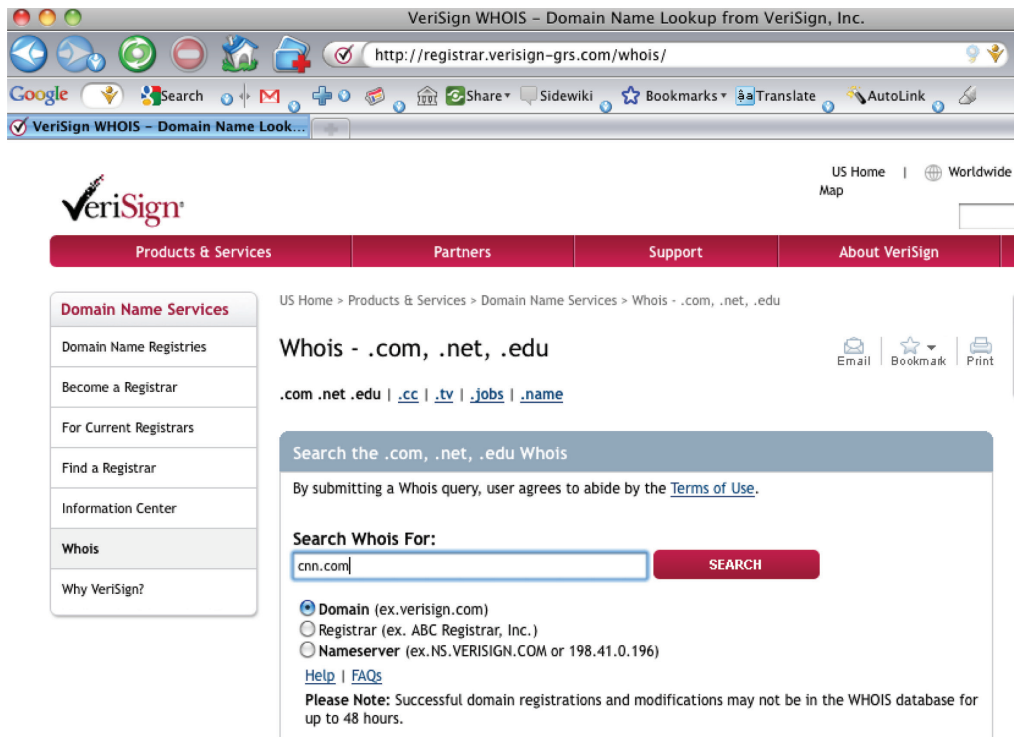


Figure 2.12 The use of Whois service.

Search the .com, .net, .edu Whois

By submitting a Whois query, user agrees to abide by the [Terms of Use](#).

Search Whois For:

☒ Domain (ex.verisign.com)
☐ Registrar (ex. ABC Registrar, Inc.)
☐ Nameserver (ex.NS.VERISIGN.COM or 198.41.0.196)

[Help](#) | [FAQs](#)

Please Note: Successful domain registrations and modifications may not be in the WHOIS database for up to 48 hours.

Whois Server Version 2.0

Domain names in the .com and .net domains can now be registered with many different competing registrars. Go to <http://www.internic.net> for detailed information.

```
Domain Name: CNN.COM
Registrar: CSC CORPORATE DOMAINS, INC.
Whois Server: whois.corporatedomains.com
Referral URL: http://www.cscglobal.com
Name Server: NS1.TIMEWARNER.NET
Name Server: NS3.TIMEWARNER.NET
Name Server: NS5.TIMEWARNER.NET
Status: clientTransferProhibited
Updated Date: 04-feb-2010
Creation Date: 22-sep-1993
Expiration Date: 21-sep-2018
```

cnn.com uses
Timewarner to host its
authoritative DNS servers

Details about cnn.com

>>> Last update of whois database: Tue, 09 Mar 2010 21:23:26 UTC <<<

Figure 2.13 Whois query response.

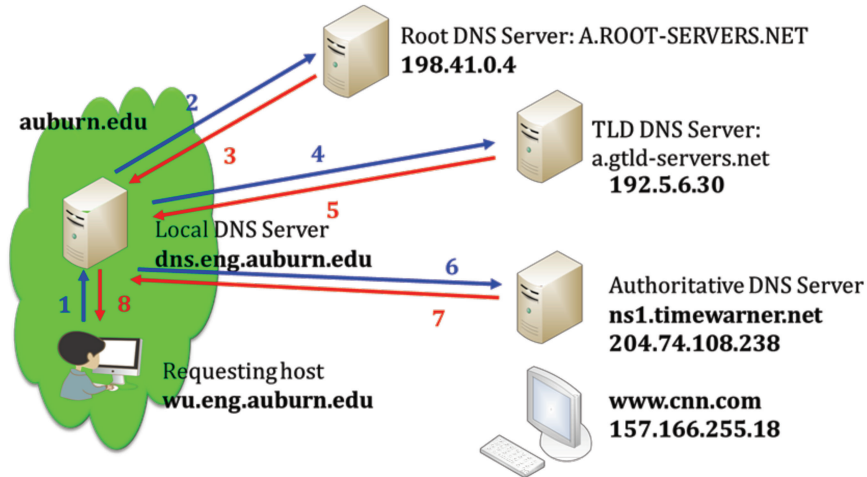


Figure 2.14 Local DNS server to client.

```
Mac-Pro:~ wu$ nslookup 74.125.45.100
Server:      131.204.10.13
Address:     131.204.10.13#53

Non-authoritative answer:
100.45.125.74.in-addr.arpa      name = yx-in-f100.google.com.

Authoritative answers can be found from:
125.74.in-addr.arpa    nameserver = ns1.google.com.
125.74.in-addr.arpa    nameserver = ns2.google.com.
125.74.in-addr.arpa    nameserver = ns3.google.com.
125.74.in-addr.arpa    nameserver = ns4.google.com.
ns1.google.com internet address = 216.239.32.10
ns2.google.com internet address = 216.239.34.10
ns3.google.com internet address = 216.239.36.10
ns4.google.com internet address = 216.239.38.10
```

Figure 2.15 A reverse DNS lookup example.

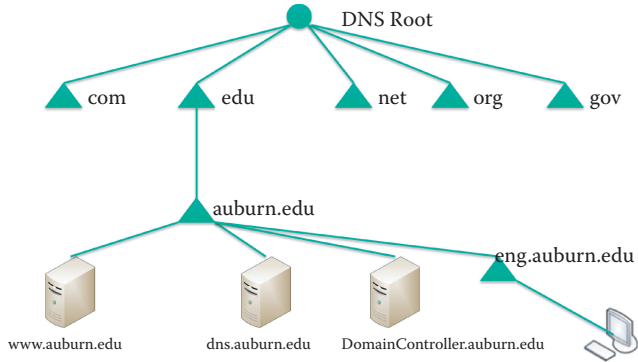


Figure 2.16 A DNS hierarchical structure.

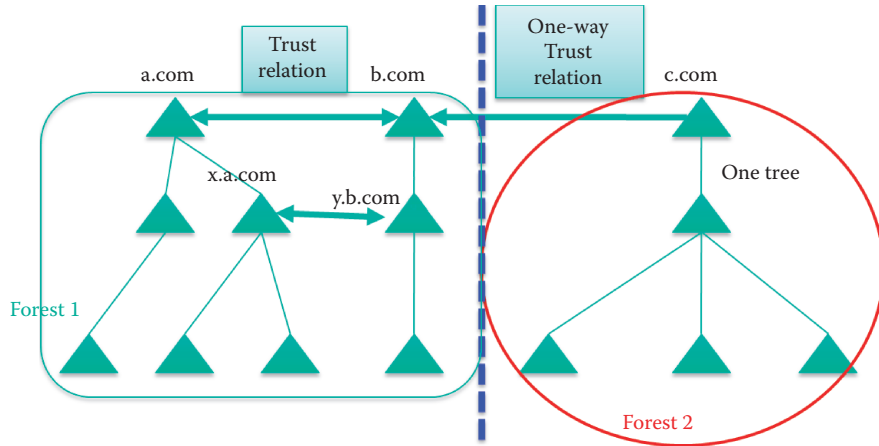


Figure 2.17 Forest at pinnacle of hierarchical structure.

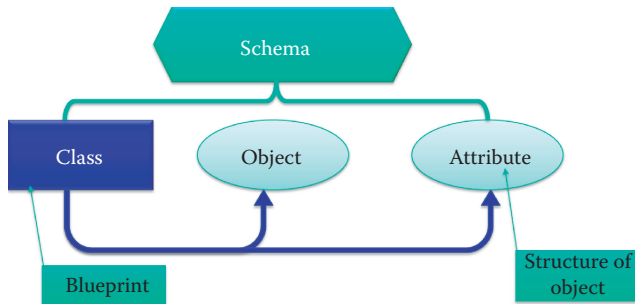


Figure 2.18 The relationship of class, object and attribute of a schema.

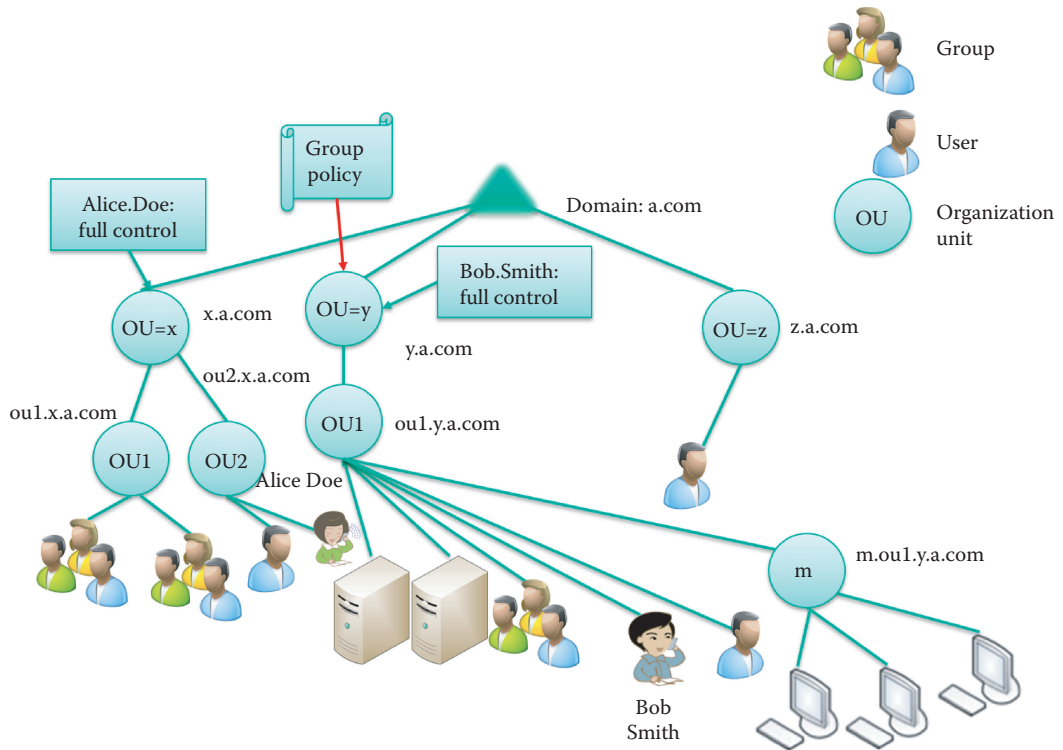


Figure 2.19 An AD domain.

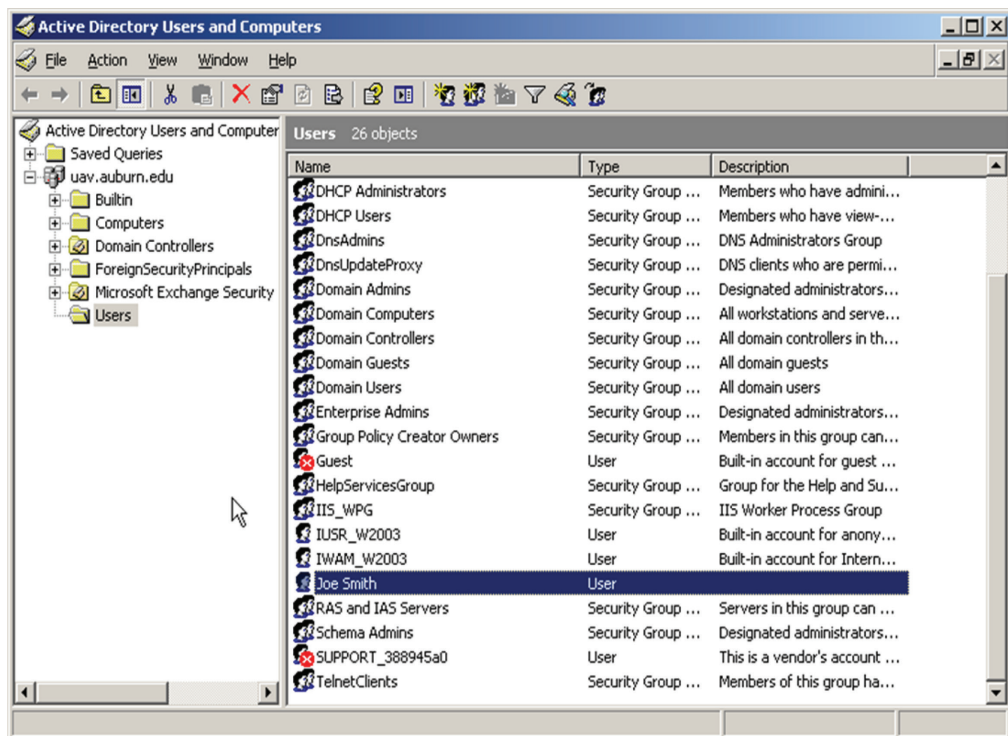


Figure 2.20 Active directory for users.

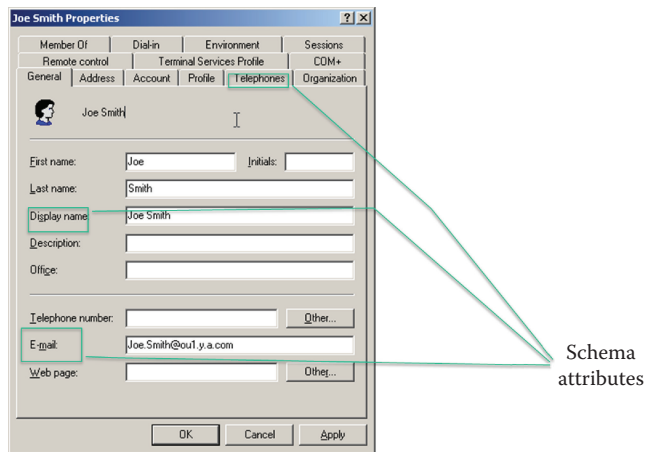


Figure 2.21 A user object in active directory.

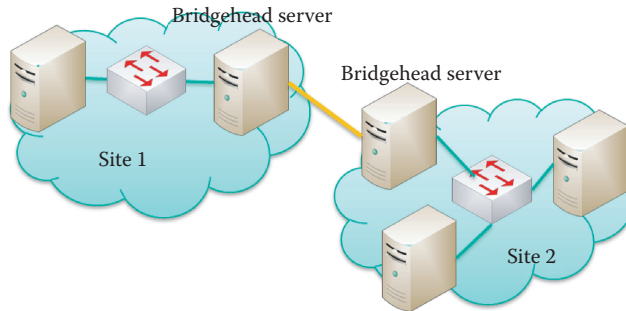


Figure 2.22 Sites within an AD network.

The diagram shows an SRV record: `http.tcp.www SRV 0 0 80 webserver.auburn.edu.`. Blue curly braces and arrows link the fields to labels below. The first brace under `http.tcp.www` points to `Service.Proto.Name`. The second brace under `SRV` points to `TTL`. The third brace under `0` points to `Class`. The fourth brace under `0` points to `SRV`. The fifth brace under `80` points to `Priority`. The sixth brace under `webserver.auburn.edu.` points to `Weight`. The seventh brace under `webserver.auburn.edu.` points to `Port`. The eighth brace under `webserver.auburn.edu.` points to `Target`.

<code>http.tcp.www</code>	<code>SRV</code>	<code>0</code>	<code>0</code>	<code>80</code>	<code>webserver.auburn.edu.</code>
Service.Proto.Name	TTL	Class	SRV	Priority	Weight
				Port	Target

Figure 2.23 A SRV RR for HTTP (www) service at auburn.edu domain.