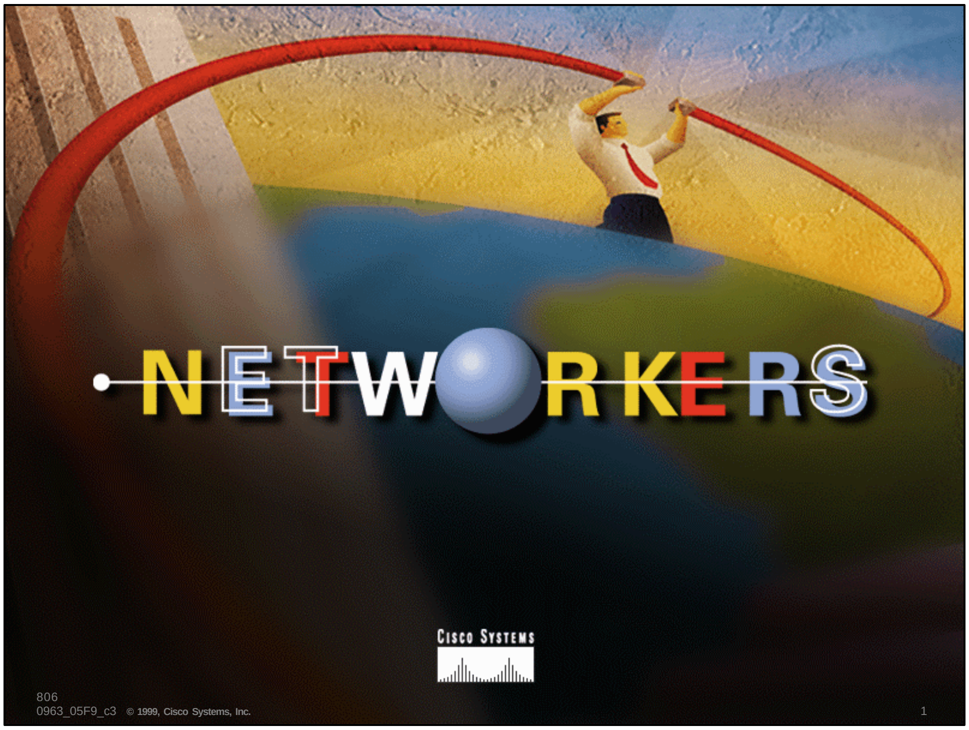


NETWORKERS

Cisco Systems

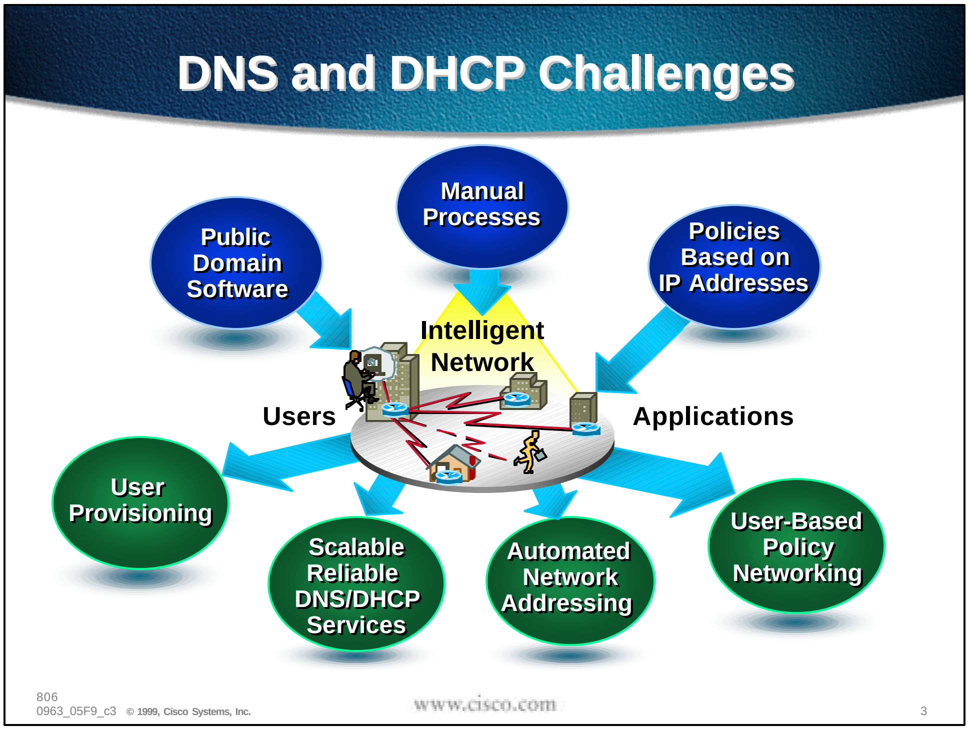
806
0963_05F9_c3 © 1999, Cisco Systems, Inc. 1

DNS, DHCP, and IP Address Management

Session 806

Cisco Systems

806
0963_05F9_c3 © 1999, Cisco Systems, Inc. 2



DNS and DHCP Challenges

Public Domain Software

Manual Processes

Policies Based on IP Addresses

Intelligent Network

Users

Applications

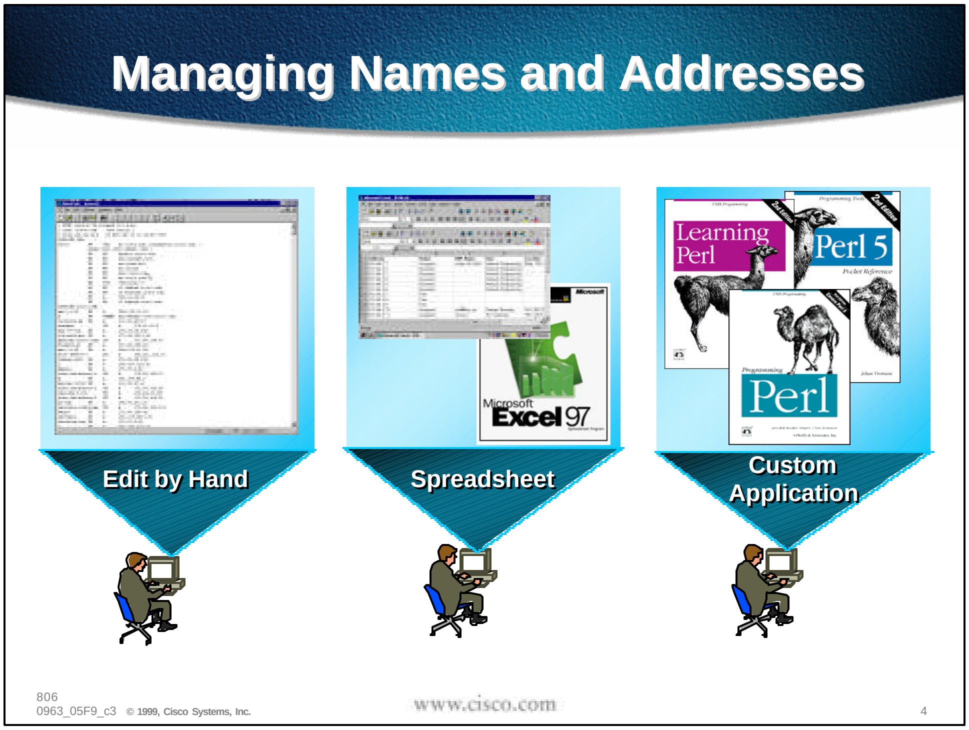
User Provisioning

Scalable Reliable DNS/DHCP Services

Automated Network Addressing

User-Based Policy Networking

806
0963_05F9_c3 © 1999, Cisco Systems, Inc. www.cisco.com 3



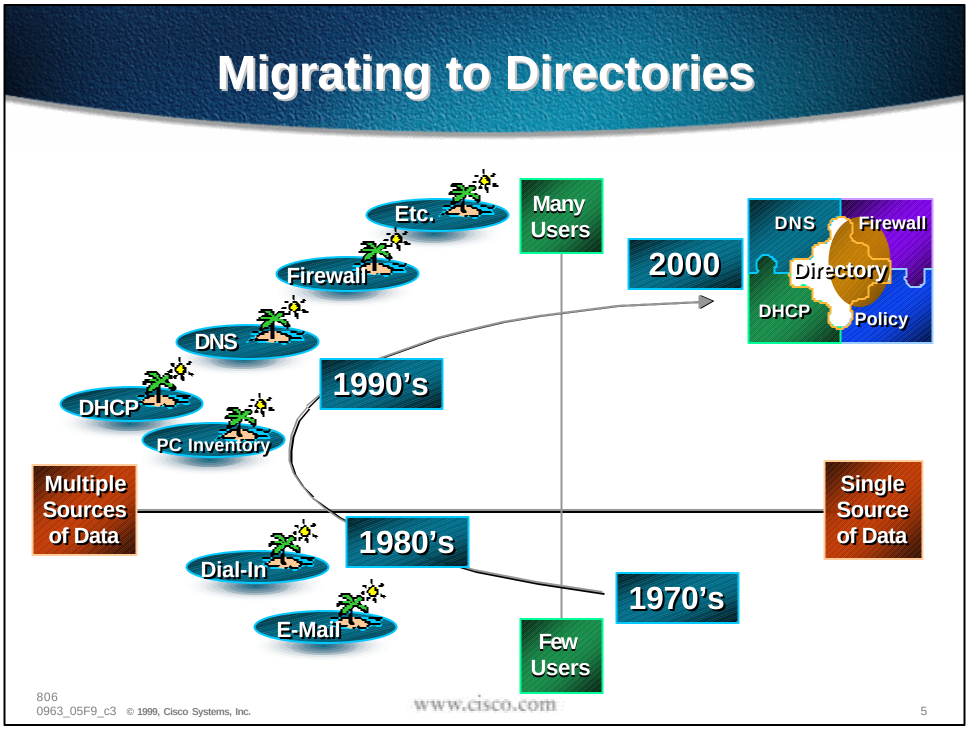
Managing Names and Addresses

Edit by Hand

Spreadsheet

Custom Application

806
0963_05F9_c3 © 1999, Cisco Systems, Inc. www.cisco.com 4



Migrating to Directories

Etc.

Firewall

DNS

DHCP

PC Inventory

Many Users

2000

DNS

Firewall

Directory

DHCP

Policy

1990's

Multiple Sources of Data

Single Source of Data

1980's

Dial-In

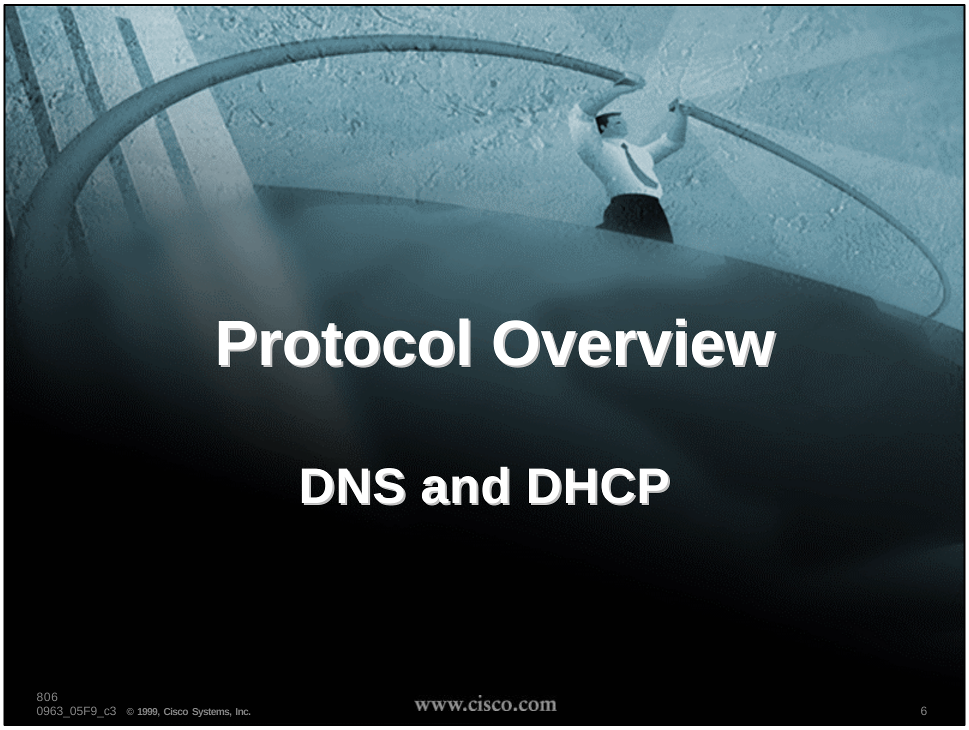
E-Mail

1970's

Few Users

806
0963_05F9_c3 © 1999, Cisco Systems, Inc.

www.cisco.com

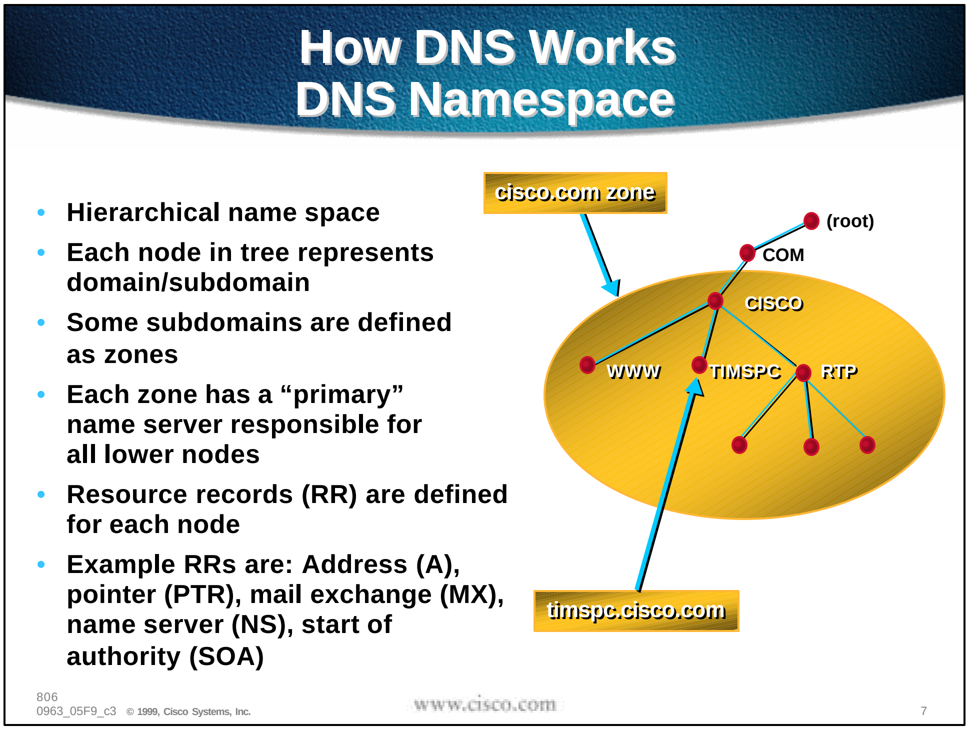


Protocol Overview

DNS and DHCP

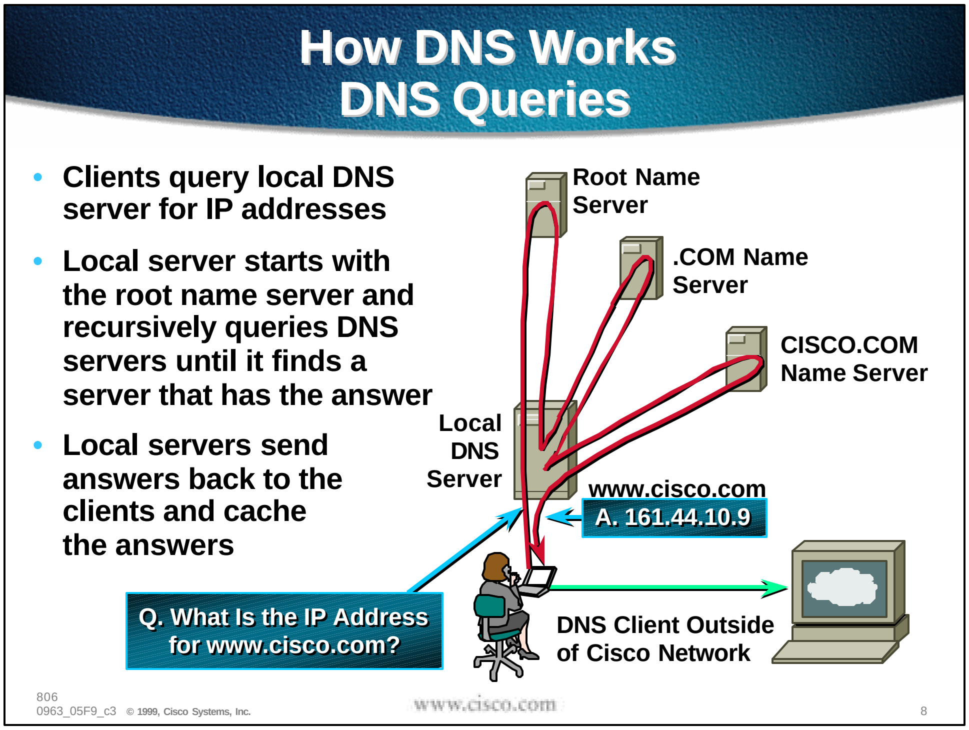
806
0963_05F9_c3 © 1999, Cisco Systems, Inc.

www.cisco.com



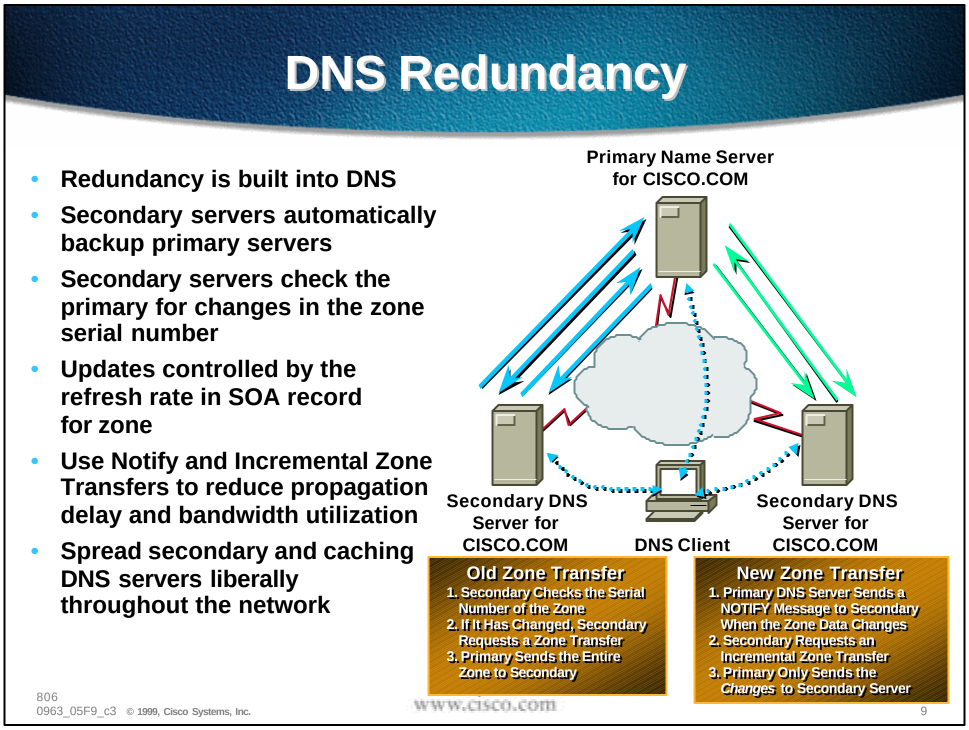
How DNS Works
DNS Namespace

- Hierarchical name space
- Each node in tree represents domain/subdomain
- Some subdomains are defined as zones
- Each zone has a “primary” name server responsible for all lower nodes
- Resource records (RR) are defined for each node
- Example RRs are: Address (A), pointer (PTR), mail exchange (MX), name server (NS), start of authority (SOA)



How DNS Works
DNS Queries

- Clients query local DNS server for IP addresses
- Local server starts with the root name server and recursively queries DNS servers until it finds a server that has the answer
- Local servers send answers back to the clients and cache the answers



DNS Redundancy

- Redundancy is built into DNS
- Secondary servers automatically backup primary servers
- Secondary servers check the primary for changes in the zone serial number
- Updates controlled by the refresh rate in SOA record for zone
- Use Notify and Incremental Zone Transfers to reduce propagation delay and bandwidth utilization
- Spread secondary and caching DNS servers liberally throughout the network

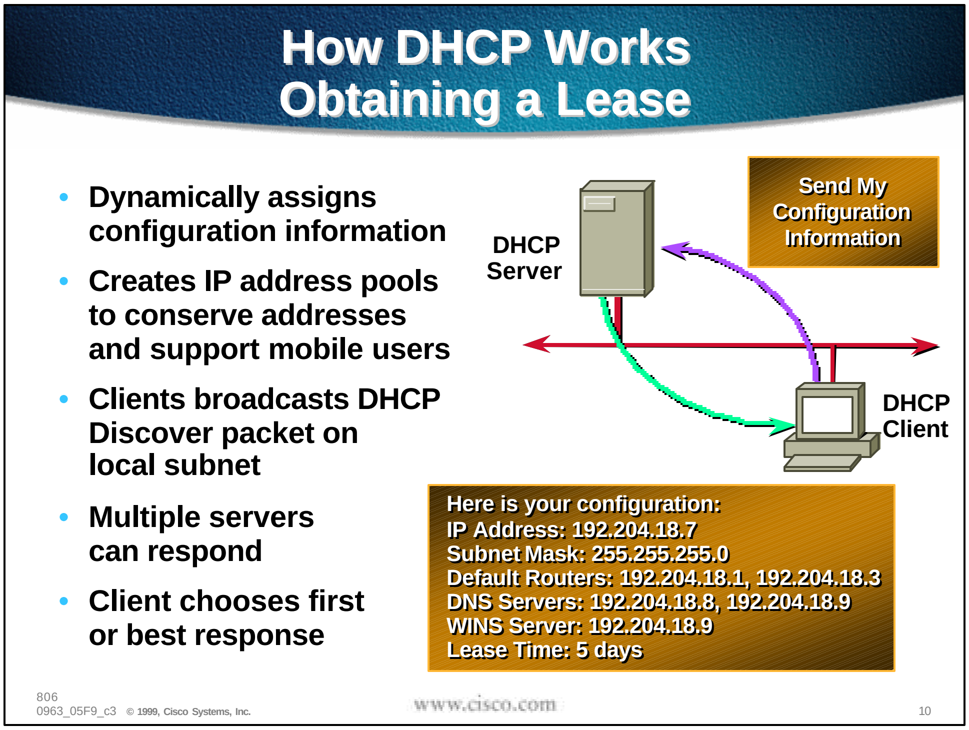
Primary Name Server for CISCO.COM
Secondary DNS Server for CISCO.COM
DNS Client
Secondary DNS Server for CISCO.COM

Old Zone Transfer

1. Secondary Checks the Serial Number of the Zone
2. If It Has Changed, Secondary Requests a Zone Transfer
3. Primary Sends the Entire Zone to Secondary

New Zone Transfer

1. Primary DNS Server Sends a NOTIFY Message to Secondary When the Zone Data Changes
2. Secondary Requests an Incremental Zone Transfer
3. Primary Only Sends the *Changes* to Secondary Server

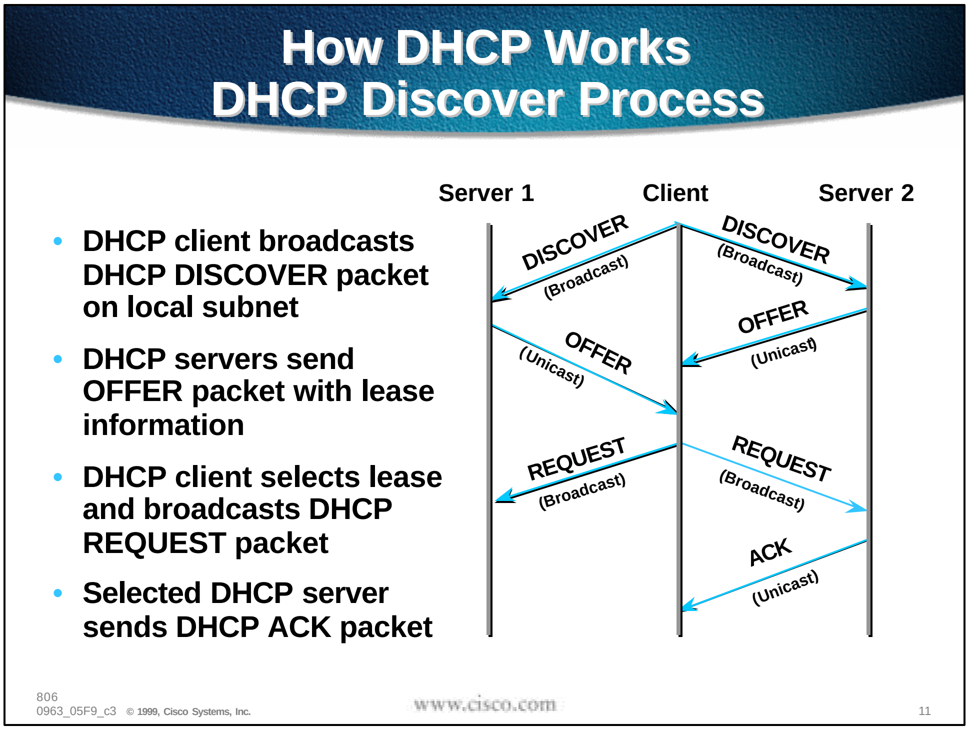


How DHCP Works Obtaining a Lease

- Dynamically assigns configuration information
- Creates IP address pools to conserve addresses and support mobile users
- Clients broadcasts DHCP Discover packet on local subnet
- Multiple servers can respond
- Client chooses first or best response

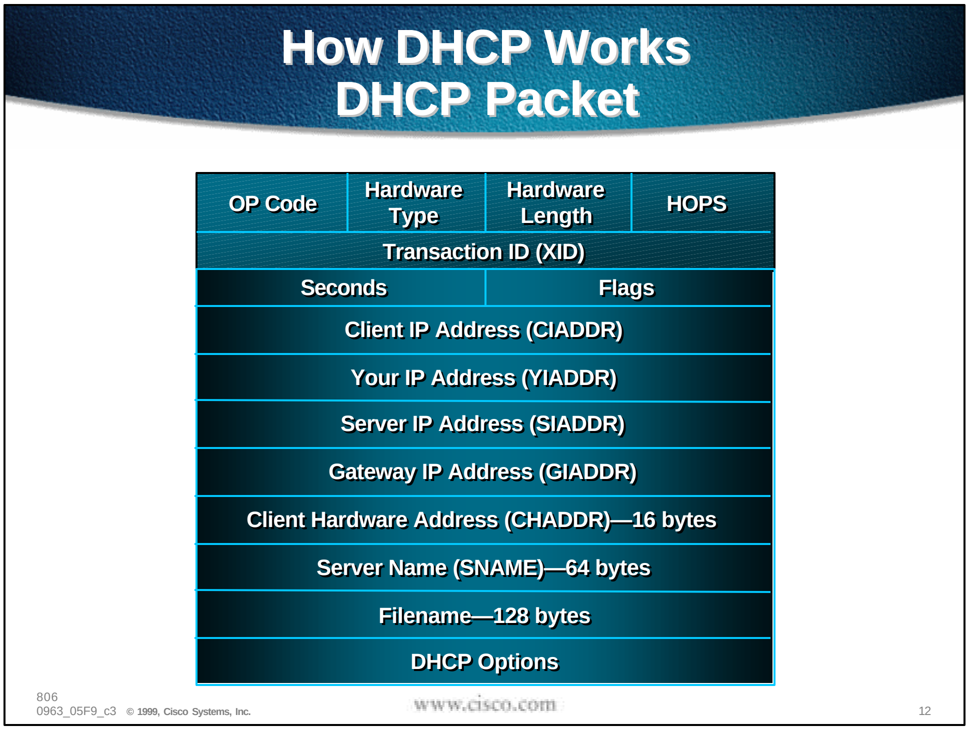
Send My Configuration Information

Here is your configuration:
IP Address: 192.204.18.7
Subnet Mask: 255.255.255.0
Default Routers: 192.204.18.1, 192.204.18.3
DNS Servers: 192.204.18.8, 192.204.18.9
WINS Server: 192.204.18.9
Lease Time: 5 days



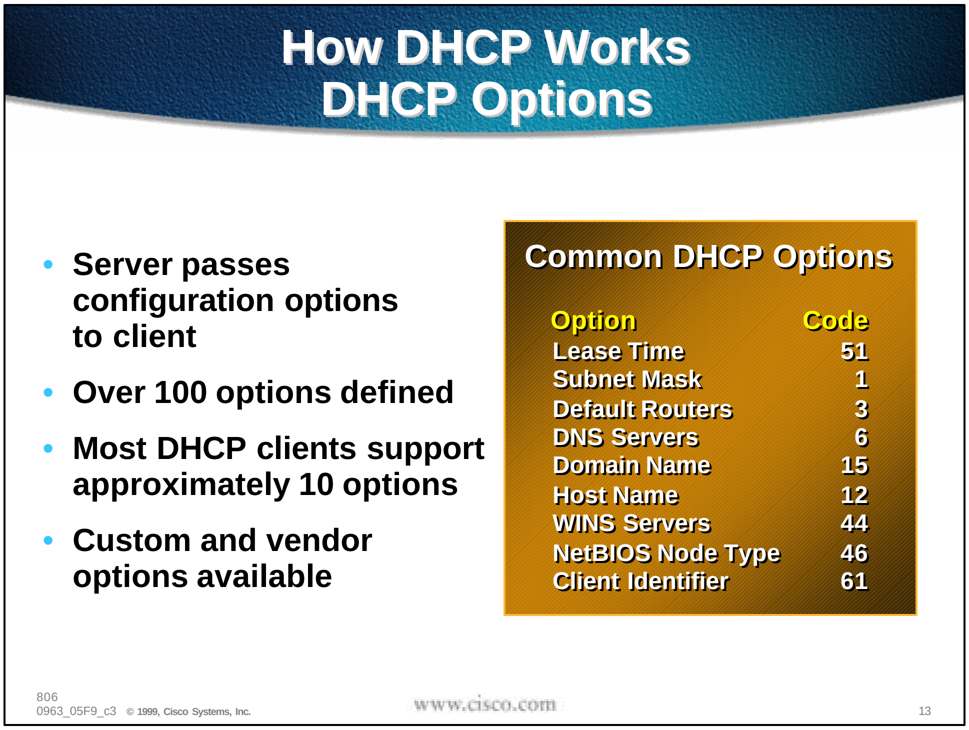
How DHCP Works
DHCP Discover Process

- DHCP client broadcasts DHCP DISCOVER packet on local subnet
- DHCP servers send OFFER packet with lease information
- DHCP client selects lease and broadcasts DHCP REQUEST packet
- Selected DHCP server sends DHCP ACK packet



How DHCP Works
DHCP Packet

OP Code	Hardware Type	Hardware Length	HOPS
Transaction ID (XID)			
Seconds		Flags	
Client IP Address (CIADDR)			
Your IP Address (YIADDR)			
Server IP Address (SIADDR)			
Gateway IP Address (GIADDR)			
Client Hardware Address (CHADDR)—16 bytes			
Server Name (SNAME)—64 bytes			
Filename—128 bytes			
DHCP Options			

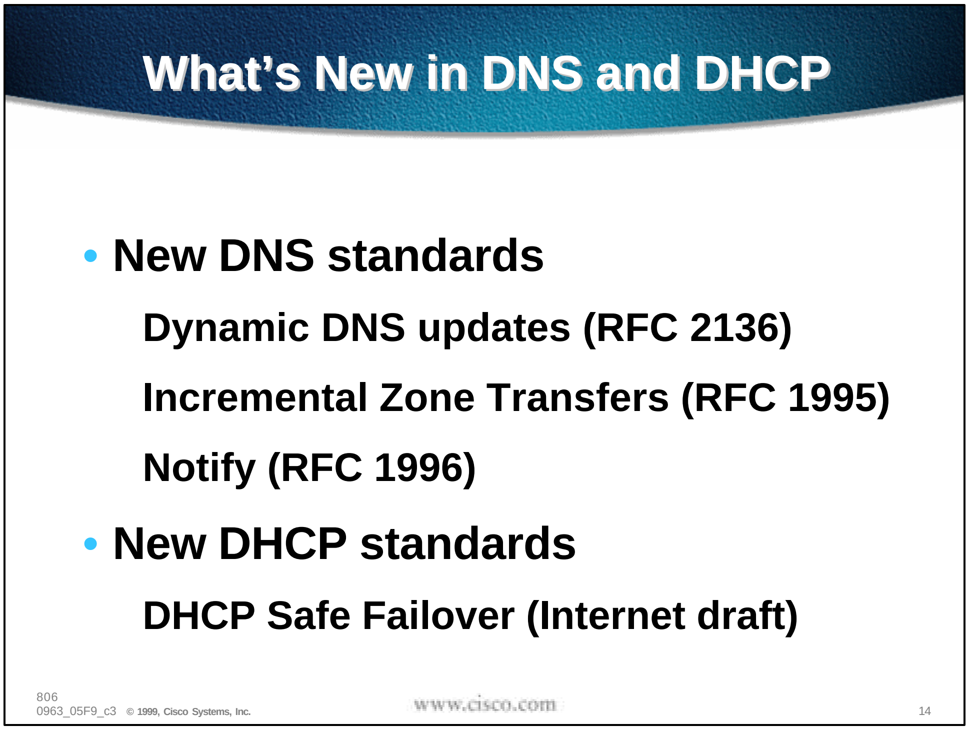


How DHCP Works
DHCP Options

- Server passes configuration options to client
- Over 100 options defined
- Most DHCP clients support approximately 10 options
- Custom and vendor options available

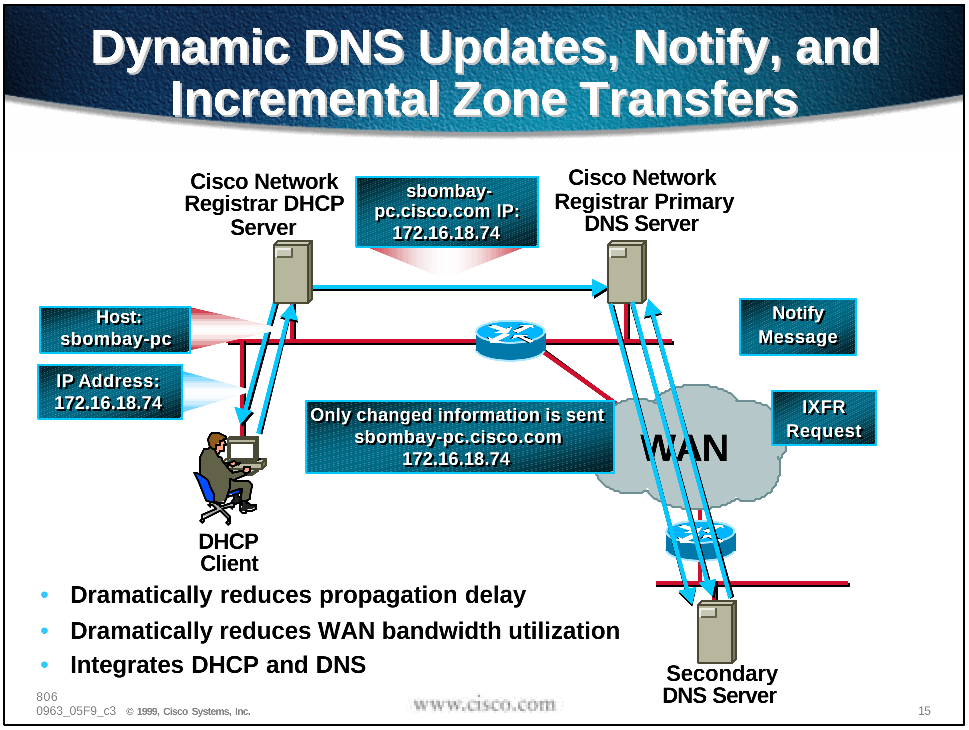
Common DHCP Options

Option	Code
Lease Time	51
Subnet Mask	1
Default Routers	3
DNS Servers	6
Domain Name	15
Host Name	12
WINS Servers	44
NetBIOS Node Type	46
Client Identifier	61



What's New in DNS and DHCP

- New DNS standards
  - Dynamic DNS updates (RFC 2136)
  - Incremental Zone Transfers (RFC 1995)
  - Notify (RFC 1996)
- New DHCP standards
  - DHCP Safe Failover (Internet draft)



Dynamic DNS Updates, Notify, and Incremental Zone Transfers

Cisco Network Registrar DHCP Server

sbombay-pc.cisco.com IP: 172.16.18.74

Cisco Network Registrar Primary DNS Server

Host: sbombay-pc

IP Address: 172.16.18.74

Notify Message

IXFR Request

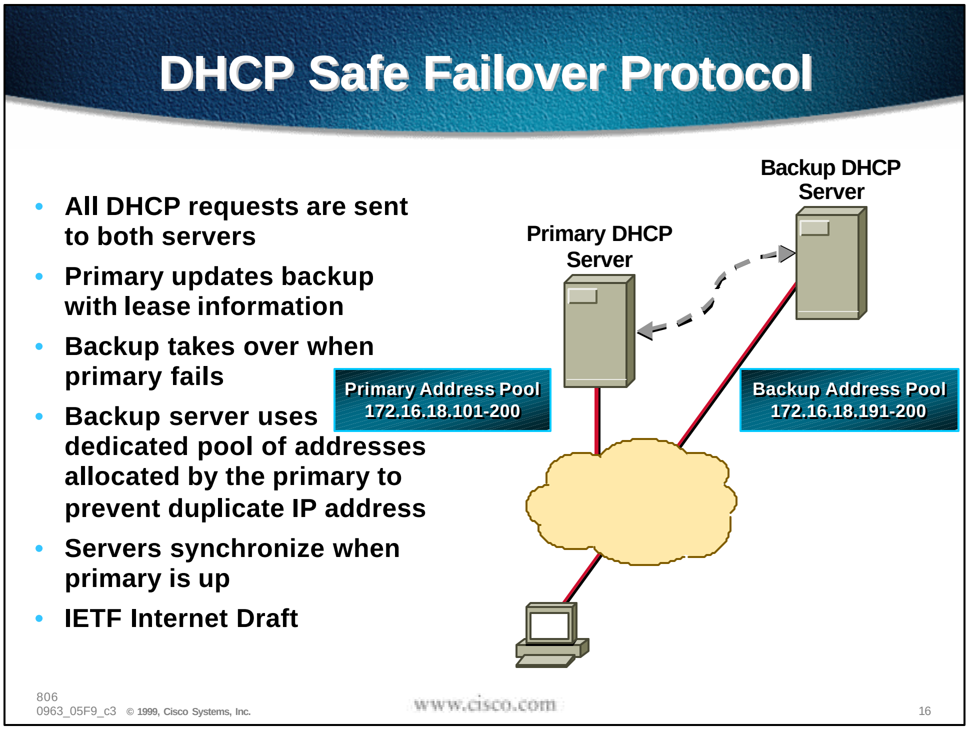
Only changed information is sent sbombay-pc.cisco.com 172.16.18.74

WAN

DHCP Client

- Dramatically reduces propagation delay
- Dramatically reduces WAN bandwidth utilization
- Integrates DHCP and DNS

Secondary DNS Server



DHCP Safe Failover Protocol

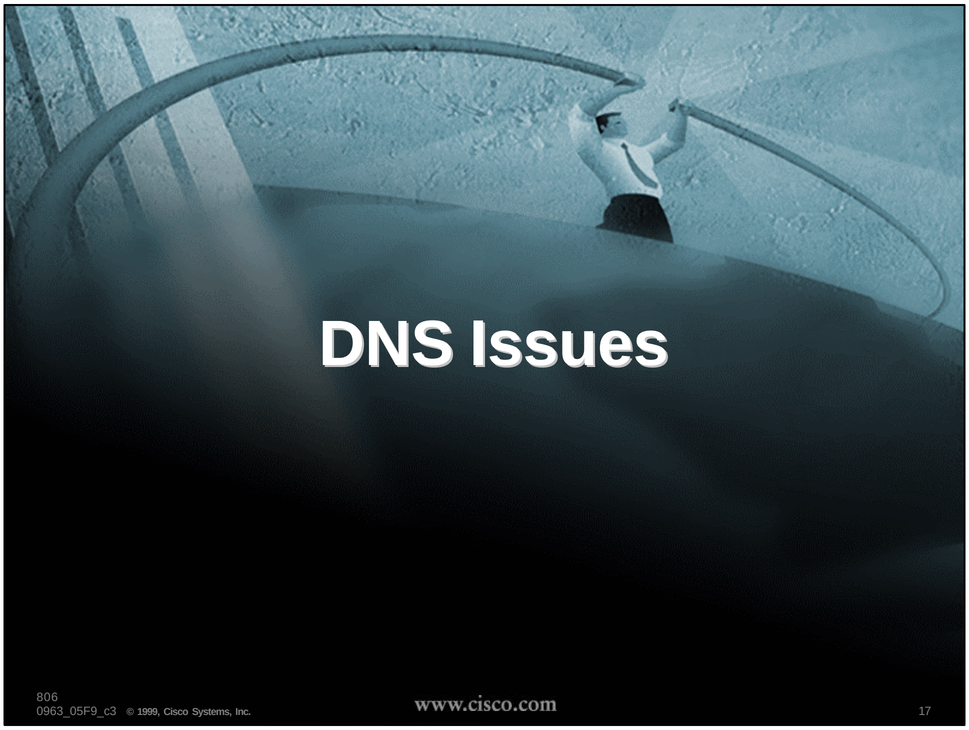
- All DHCP requests are sent to both servers
- Primary updates backup with lease information
- Backup takes over when primary fails
- Backup server uses dedicated pool of addresses allocated by the primary to prevent duplicate IP address
- Servers synchronize when primary is up
- IETF Internet Draft

Backup DHCP Server

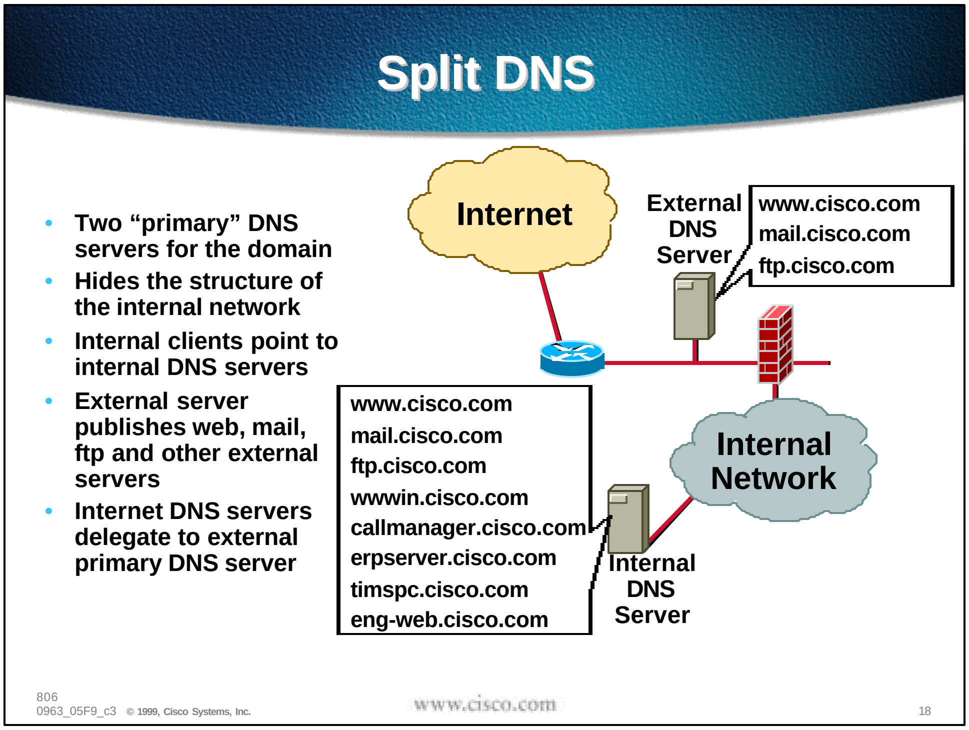
Primary DHCP Server

Primary Address Pool 172.16.18.101-200

Backup Address Pool 172.16.18.191-200



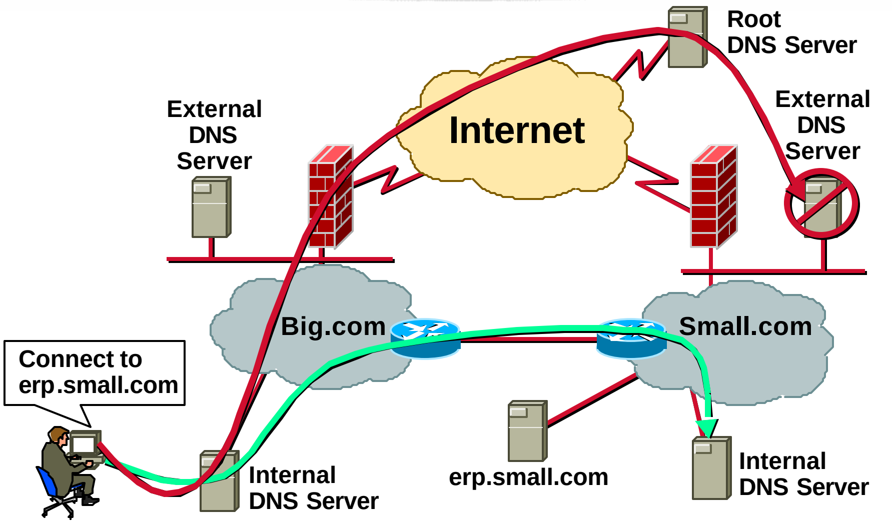
DNS Issues



Split DNS

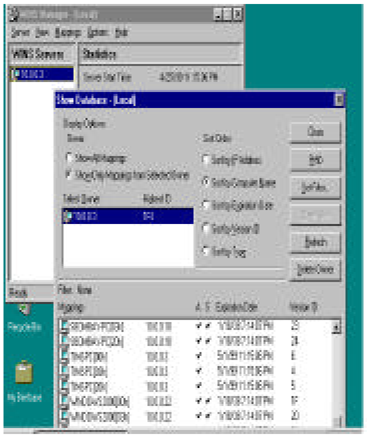
- Two “primary” DNS servers for the domain
- Hides the structure of the internal network
- Internal clients point to internal DNS servers
- External server publishes web, mail, ftp and other external servers
- Internet DNS servers delegate to external primary DNS server

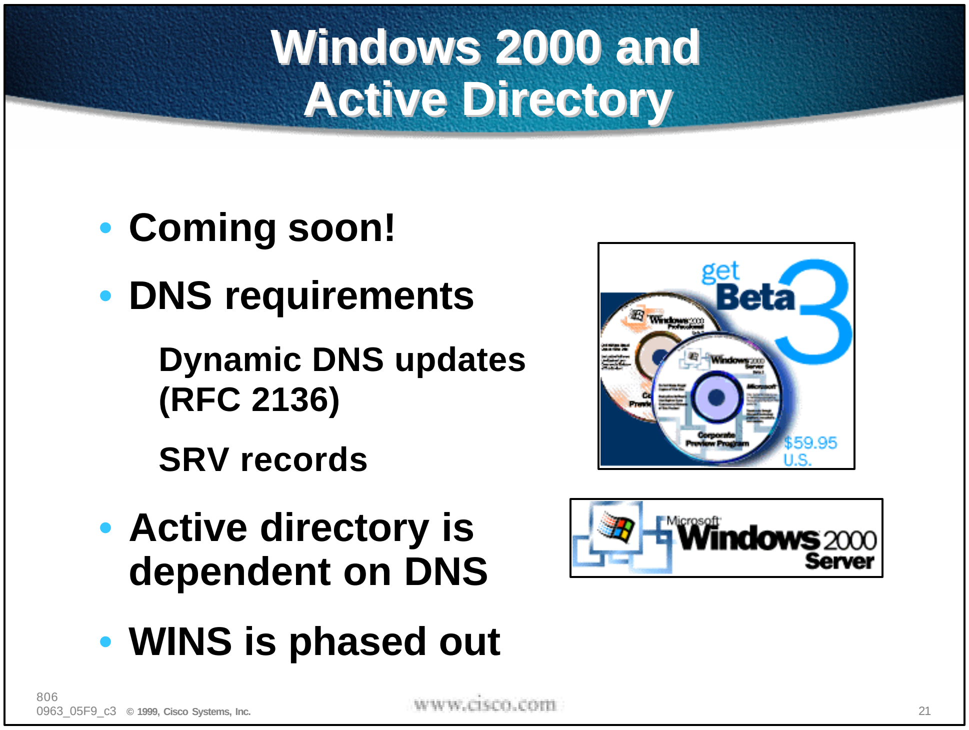
Selective Forwarders



WINS

- Windows Internet Names Service (WINS)
  - NetBIOS Names Service (NBNS)
  - Windows NT file and print services
  - Flat name space
- Coexists with DNS
- Scaling problems in large networks
- Going away with Windows 2000!




get
Beta 3
$59.95 U.S.
Microsoft Windows 2000 Server

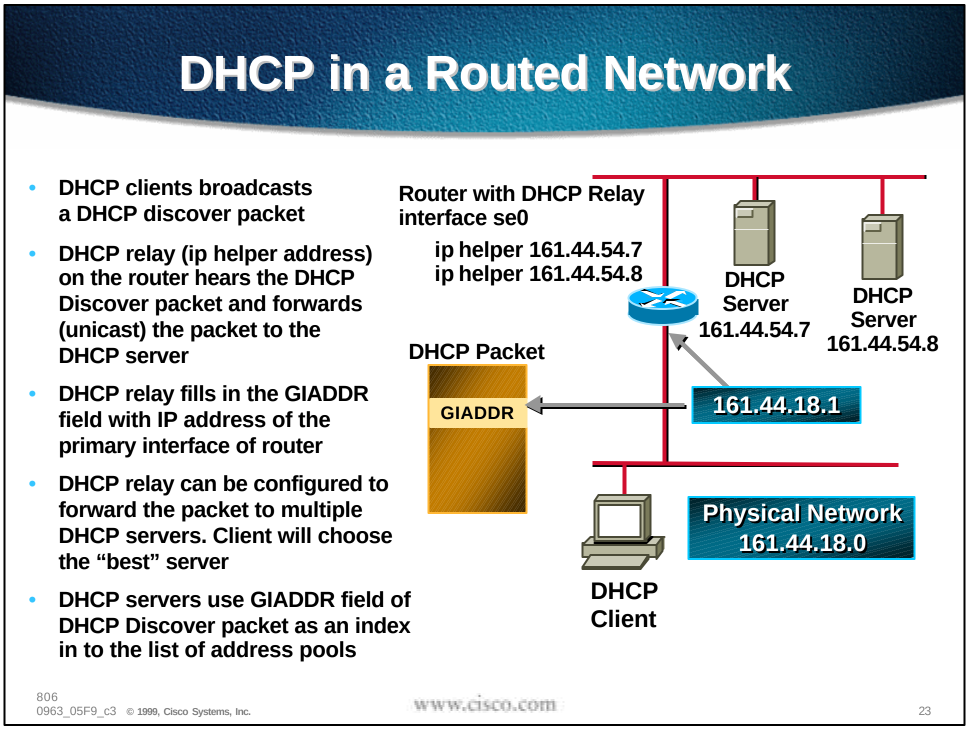
Windows 2000 and Active Directory

- Coming soon!
- DNS requirements

  Dynamic DNS updates (RFC 2136)

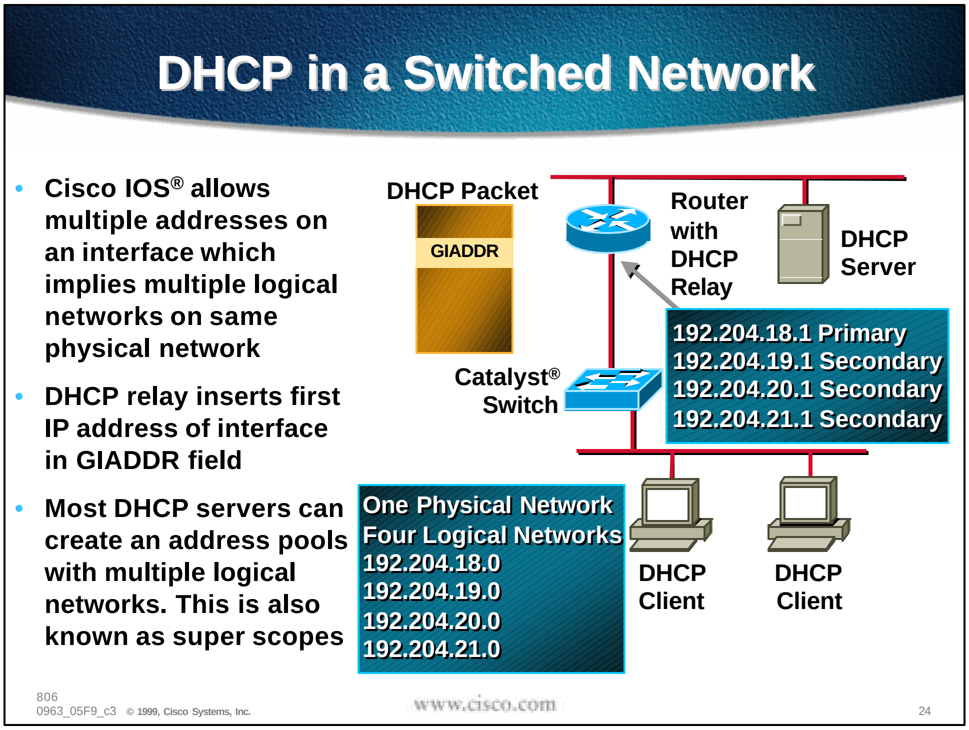
  SRV records
- Active directory is dependent on DNS
- WINS is phased out

DHCP Issues



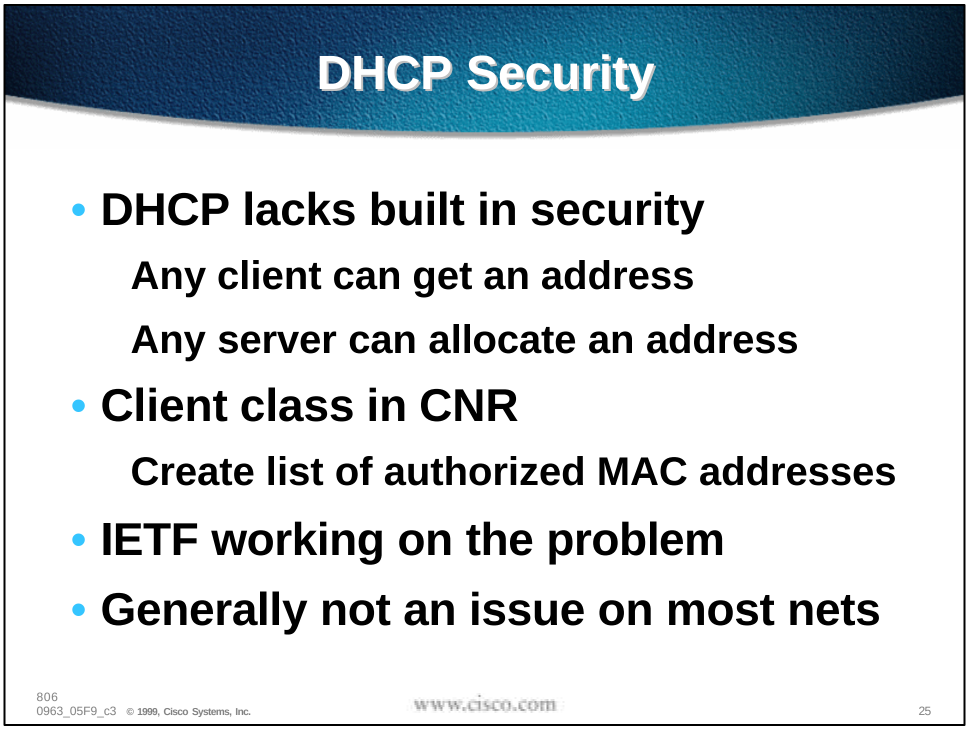
DHCP in a Routed Network

- DHCP clients broadcasts a DHCP discover packet
- DHCP relay (ip helper address) on the router hears the DHCP Discover packet and forwards (unicast) the packet to the DHCP server
- DHCP relay fills in the GIADDR field with IP address of the primary interface of router
- DHCP relay can be configured to forward the packet to multiple DHCP servers. Client will choose the “best” server
- DHCP servers use GIADDR field of DHCP Discover packet as an index in to the list of address pools



DHCP in a Switched Network

- Cisco IOS® allows multiple addresses on an interface which implies multiple logical networks on same physical network
- DHCP relay inserts first IP address of interface in GIADDR field
- Most DHCP servers can create an address pools with multiple logical networks. This is also known as super scopes



DHCP Security

- DHCP lacks built in security

  Any client can get an address

  Any server can allocate an address

- Client class in CNR

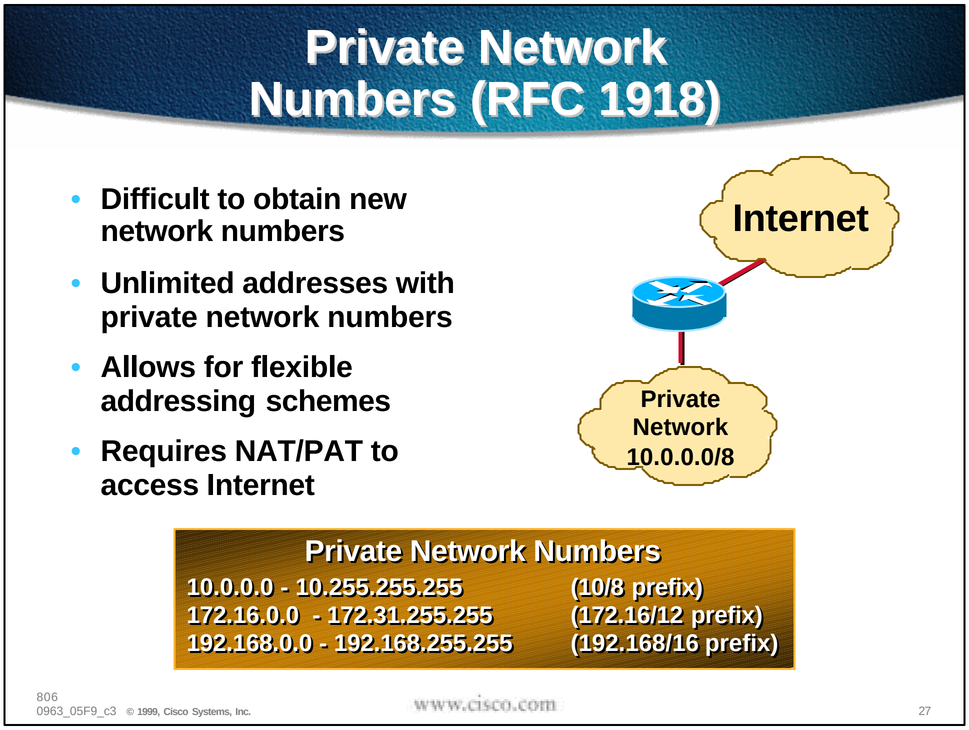
  Create list of authorized MAC addresses

- IETF working on the problem
- Generally not an issue on most nets

806
0963_05F9_c3 © 1999, Cisco Systems, Inc. www.cisco.com 25

IP Address Management Issues

806
0963_05F9_c3 © 1999, Cisco Systems, Inc. www.cisco.com 26



Private Network Numbers (RFC 1918)

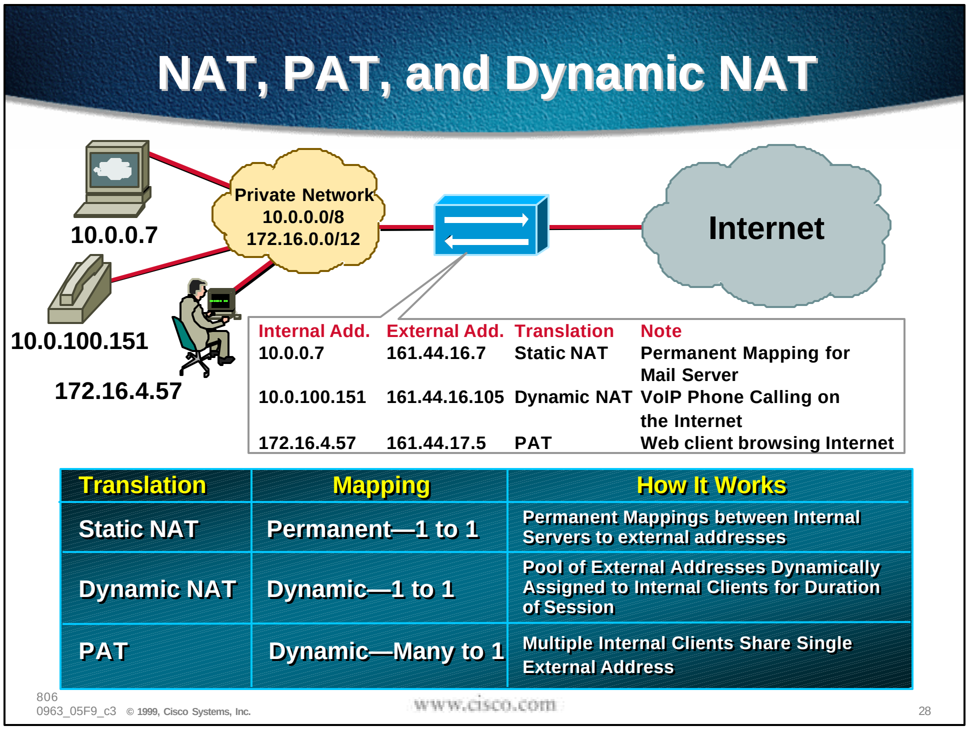
- Difficult to obtain new network numbers
- Unlimited addresses with private network numbers
- Allows for flexible addressing schemes
- Requires NAT/PAT to access Internet

Internet
Private Network 10.0.0.0/8

Private Network Numbers

10.0.0.0 - 10.255.255.255	(10/8 prefix)
172.16.0.0 - 172.31.255.255	(172.16/12 prefix)
192.168.0.0 - 192.168.255.255	(192.168/16 prefix)

806
0963_05F9_c3 © 1999, Cisco Systems, Inc. www.cisco.com 27



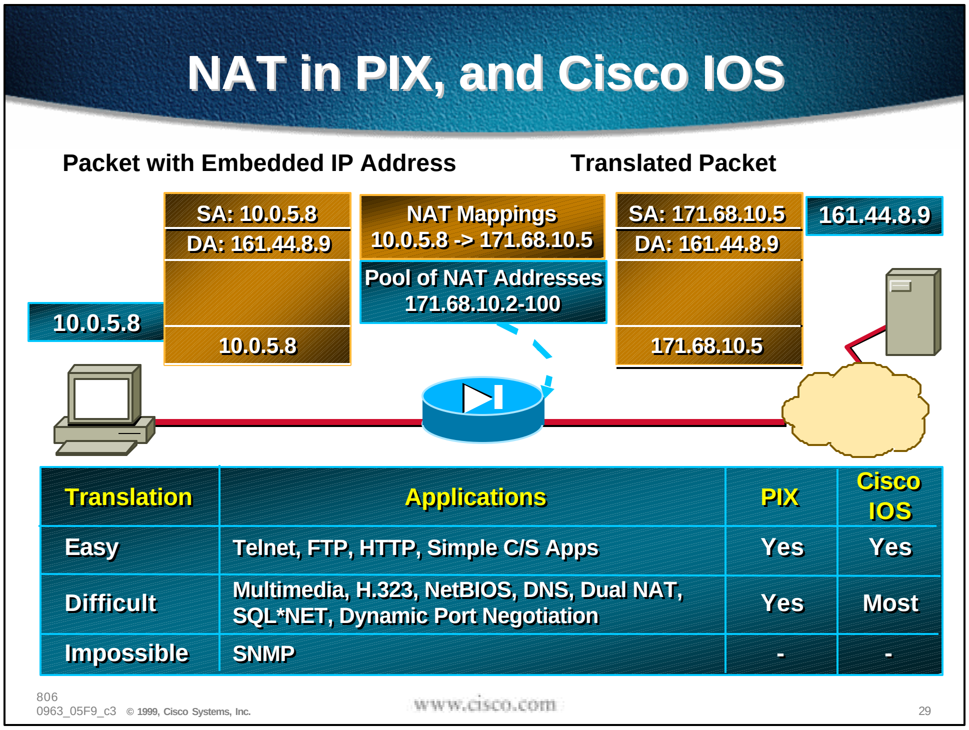
NAT, PAT, and Dynamic NAT

10.0.0.7
10.0.100.151
172.16.4.57
Private Network
10.0.0.0/8
172.16.0.0/12
Internet

Internal Add.	External Add.	Translation	Note
10.0.0.7	161.44.16.7	Static NAT	Permanent Mapping for Mail Server
10.0.100.151	161.44.16.105	Dynamic NAT	VoIP Phone Calling on the Internet
172.16.4.57	161.44.17.5	PAT	Web client browsing Internet

Translation	Mapping	How It Works
Static NAT	Permanent—1 to 1	Permanent Mappings between Internal Servers to external addresses
Dynamic NAT	Dynamic—1 to 1	Pool of External Addresses Dynamically Assigned to Internal Clients for Duration of Session
PAT	Dynamic—Many to 1	Multiple Internal Clients Share Single External Address

806
0963_05F9_c3 © 1999, Cisco Systems, Inc. www.cisco.com 28



NAT in PIX, and Cisco IOS

Packet with Embedded IP Address

Translated Packet

SA: 10.0.5.8
DA: 161.44.8.9
10.0.5.8

NAT Mappings
10.0.5.8 -> 171.68.10.5

Pool of NAT Addresses
171.68.10.2-100

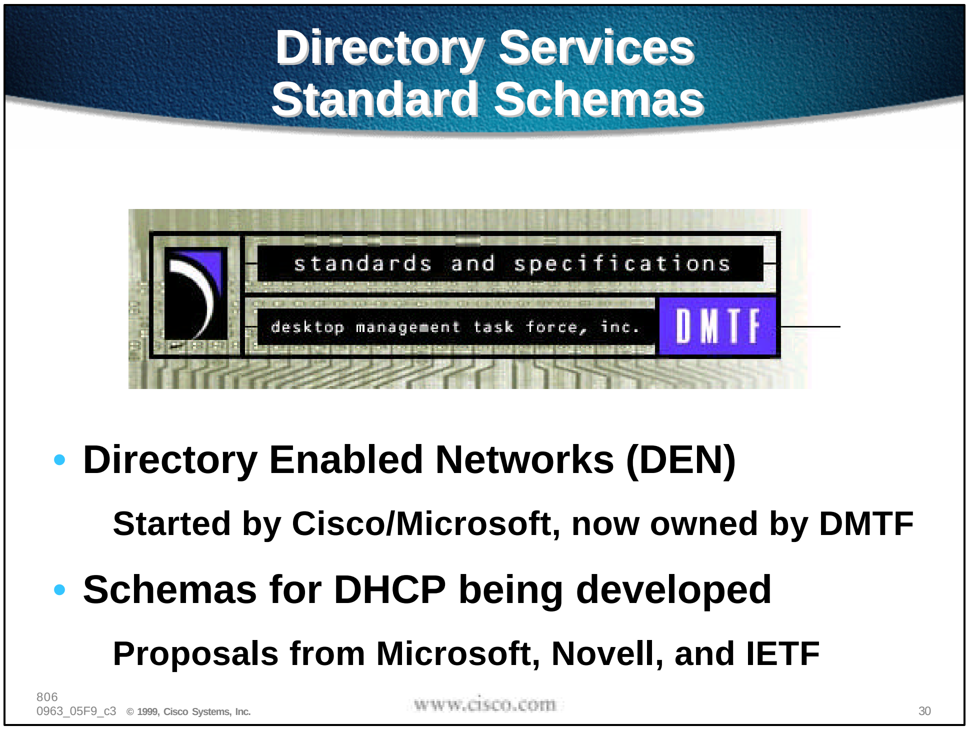
SA: 171.68.10.5
DA: 161.44.8.9
171.68.10.5

10.0.5.8

161.44.8.9

Translation	Applications	PIX	Cisco IOS
Easy	Telnet, FTP, HTTP, Simple C/S Apps	Yes	Yes
Difficult	Multimedia, H.323, NetBIOS, DNS, Dual NAT, SQL*NET, Dynamic Port Negotiation	Yes	Most
Impossible	SNMP	-	-

806
0963_05F9_c3 © 1999, Cisco Systems, Inc. www.cisco.com 29



Directory Services Standard Schemas

standards and specifications
desktop management task force, inc.
DMTF

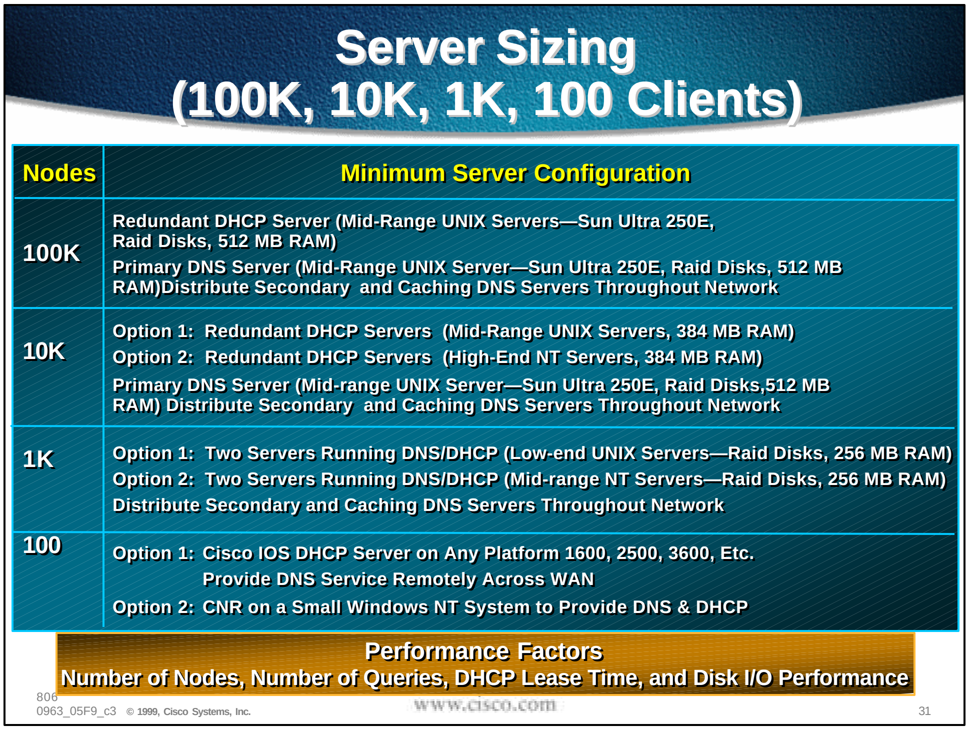
- Directory Enabled Networks (DEN)

  Started by Cisco/Microsoft, now owned by DMTF

- Schemas for DHCP being developed

  Proposals from Microsoft, Novell, and IETF

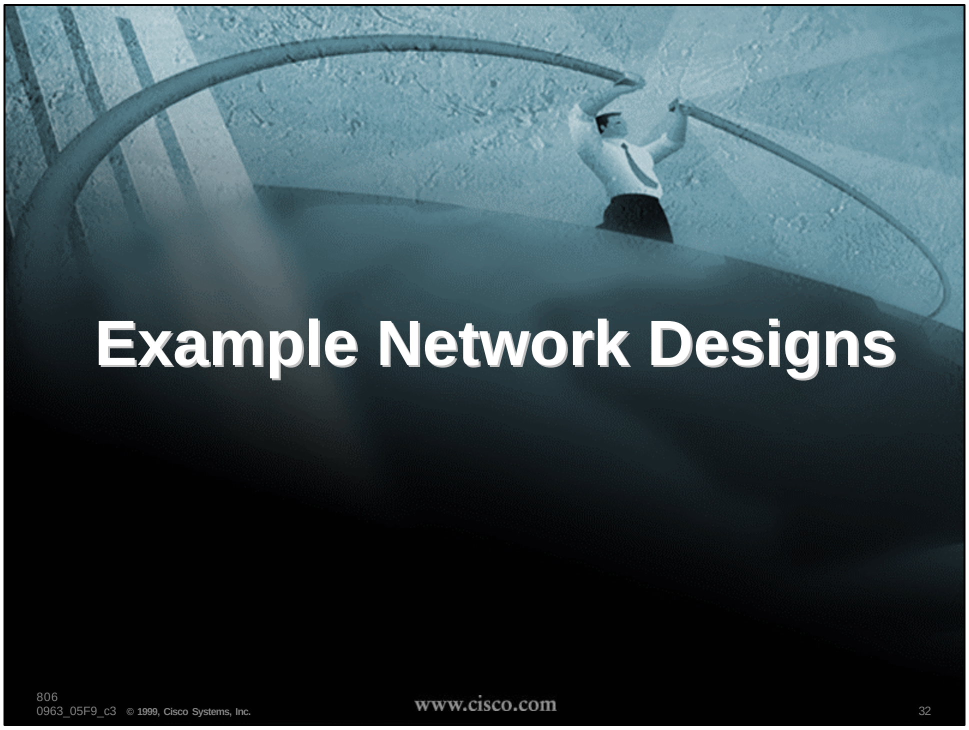
806
0963_05F9_c3 © 1999, Cisco Systems, Inc. www.cisco.com 30



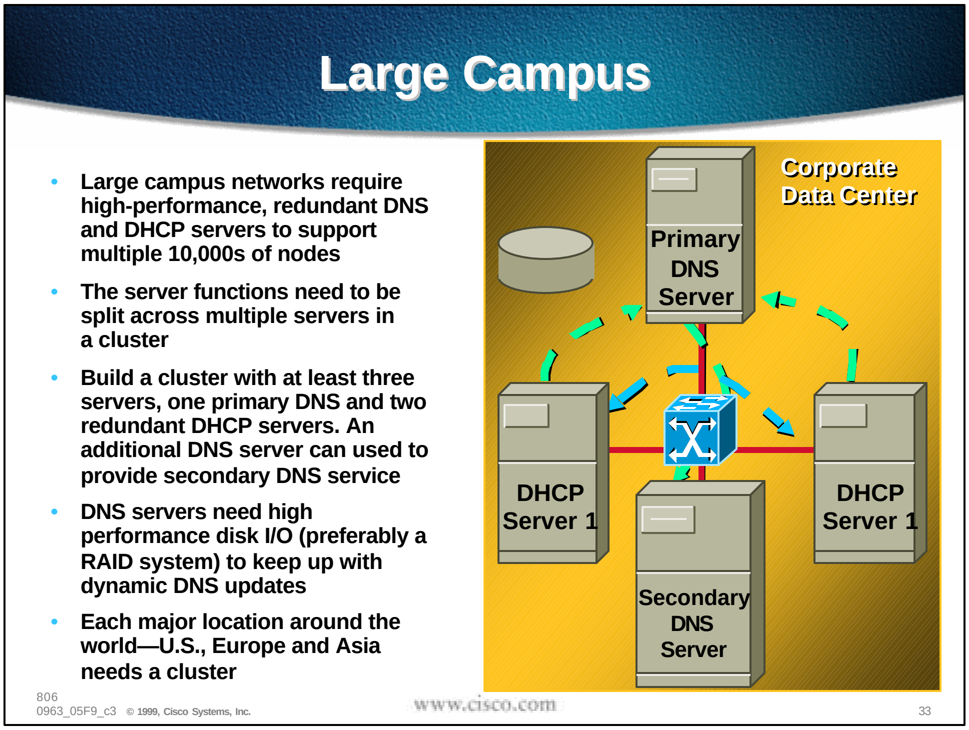
Server Sizing (100K, 10K, 1K, 100 Clients)

Nodes	Minimum Server Configuration
100K	Redundant DHCP Server (Mid-Range UNIX Servers—Sun Ultra 250E, Raid Disks, 512 MB RAM) Primary DNS Server (Mid-Range UNIX Server—Sun Ultra 250E, Raid Disks, 512 MB RAM)Distribute Secondary and Caching DNS Servers Throughout Network
10K	Option 1: Redundant DHCP Servers (Mid-Range UNIX Servers, 384 MB RAM) Option 2: Redundant DHCP Servers (High-End NT Servers, 384 MB RAM) Primary DNS Server (Mid-range UNIX Server—Sun Ultra 250E, Raid Disks,512 MB RAM) Distribute Secondary and Caching DNS Servers Throughout Network
1K	Option 1: Two Servers Running DNS/DHCP (Low-end UNIX Servers—Raid Disks, 256 MB RAM) Option 2: Two Servers Running DNS/DHCP (Mid-range NT Servers—Raid Disks, 256 MB RAM) Distribute Secondary and Caching DNS Servers Throughout Network
100	Option 1: Cisco IOS DHCP Server on Any Platform 1600, 2500, 3600, Etc. Provide DNS Service Remotely Across WAN Option 2: CNR on a Small Windows NT System to Provide DNS & DHCP

Performance Factors
Number of Nodes, Number of Queries, DHCP Lease Time, and Disk I/O Performance

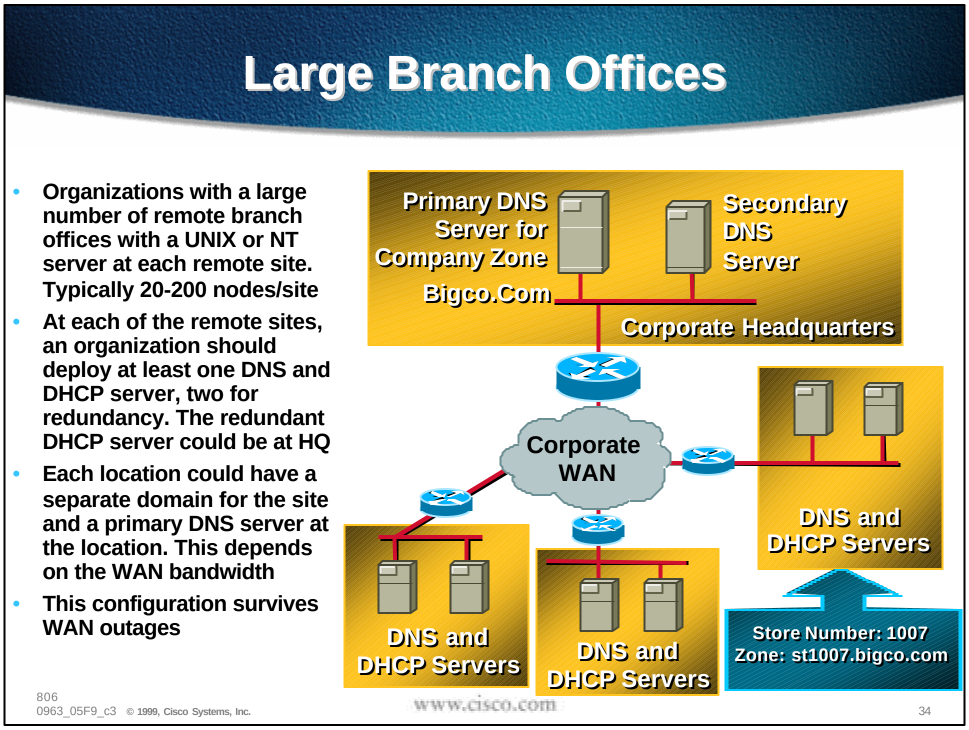


Example Network Designs



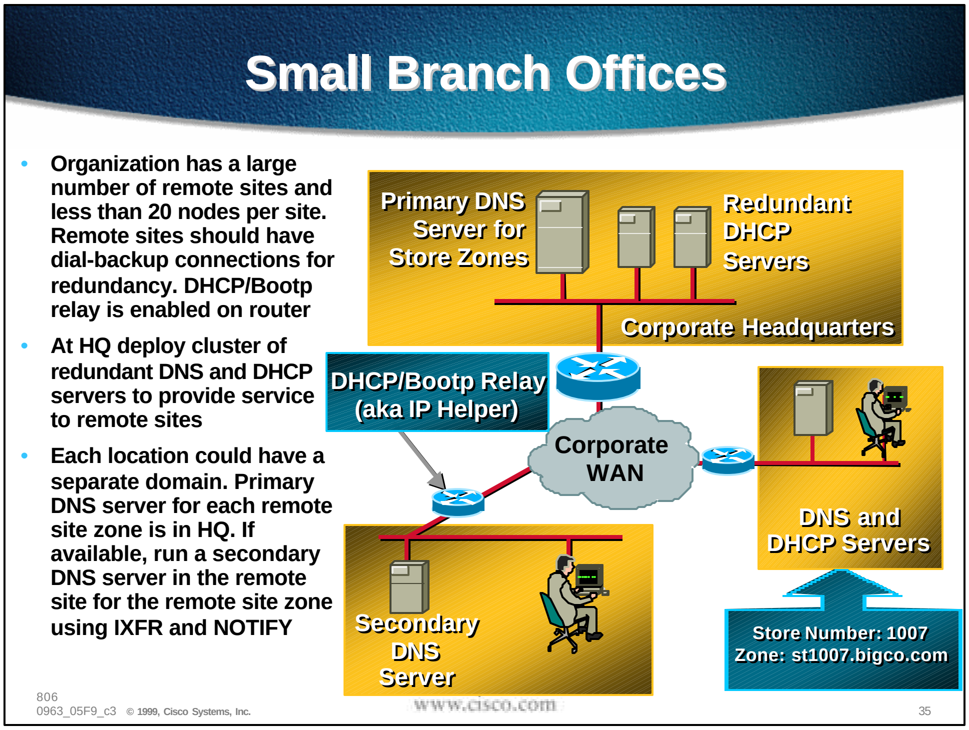
Large Campus

- Large campus networks require high-performance, redundant DNS and DHCP servers to support multiple 10,000s of nodes
- The server functions need to be split across multiple servers in a cluster
- Build a cluster with at least three servers, one primary DNS and two redundant DHCP servers. An additional DNS server can used to provide secondary DNS service
- DNS servers need high performance disk I/O (preferably a RAID system) to keep up with dynamic DNS updates
- Each major location around the world—U.S., Europe and Asia needs a cluster



Large Branch Offices

- Organizations with a large number of remote branch offices with a UNIX or NT server at each remote site. Typically 20-200 nodes/site
- At each of the remote sites, an organization should deploy at least one DNS and DHCP server, two for redundancy. The redundant DHCP server could be at HQ
- Each location could have a separate domain for the site and a primary DNS server at the location. This depends on the WAN bandwidth
- This configuration survives WAN outages

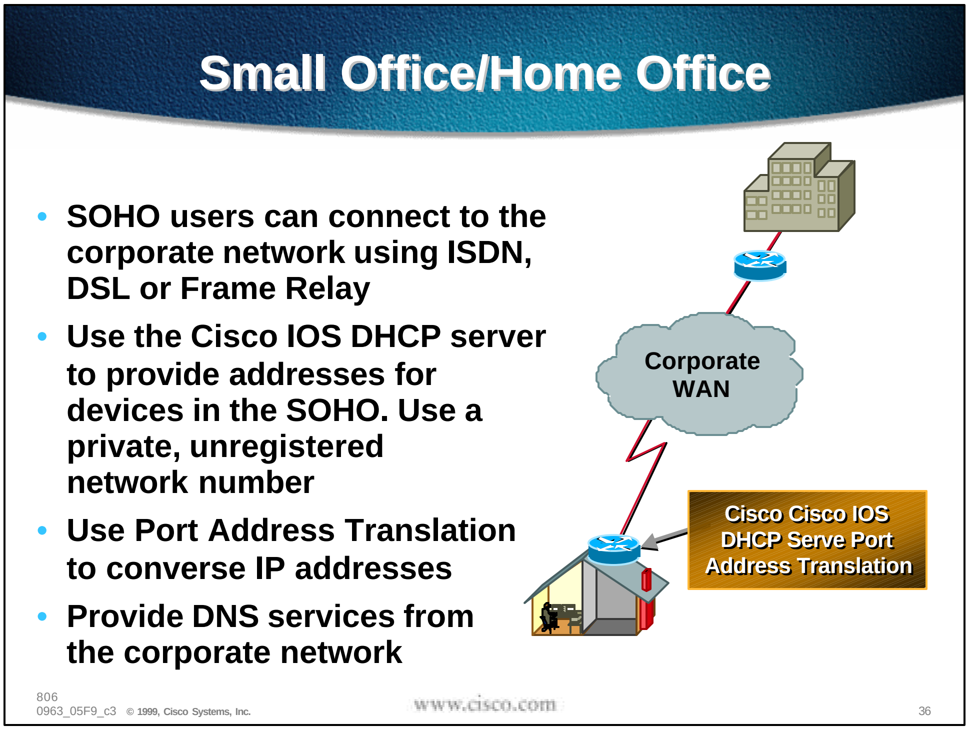


Small Branch Offices

- Organization has a large number of remote sites and less than 20 nodes per site. Remote sites should have dial-backup connections for redundancy. DHCP/Bootp relay is enabled on router
- At HQ deploy cluster of redundant DNS and DHCP servers to provide service to remote sites
- Each location could have a separate domain. Primary DNS server for each remote site zone is in HQ. If available, run a secondary DNS server in the remote site for the remote site zone using IXFR and NOTIFY

Primary DNS Server for Store Zones
Redundant DHCP Servers
Corporate Headquarters
DHCP/Bootp Relay (aka IP Helper)
Corporate WAN
DNS and DHCP Servers
Secondary DNS Server
Store Number: 1007 Zone: st1007.bigco.com

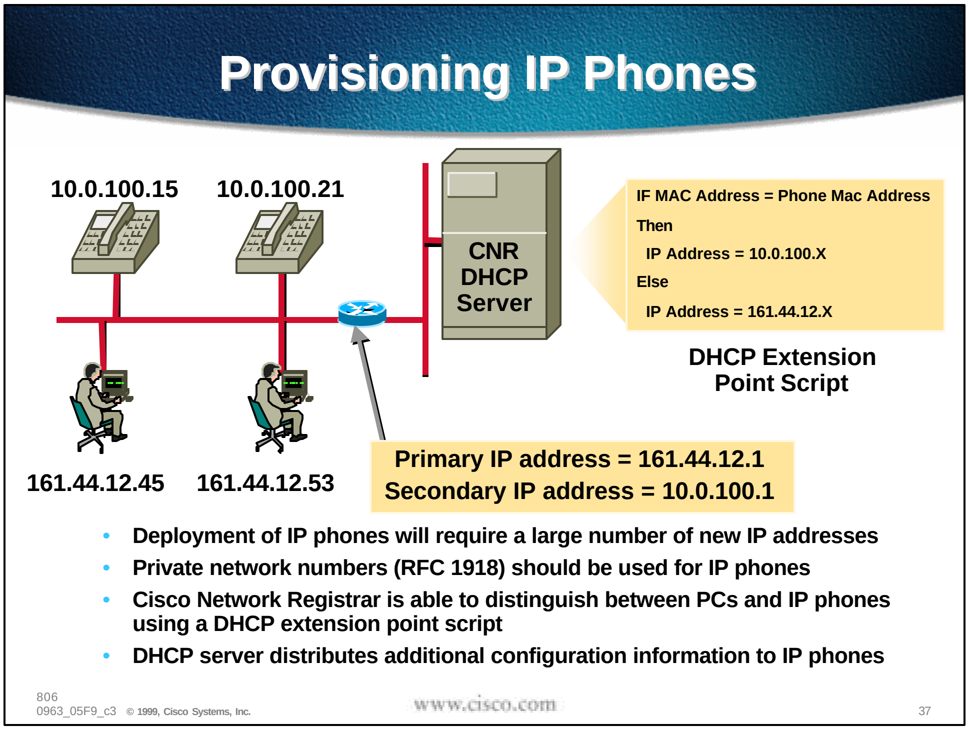
806
0963_05F9_c3 © 1999, Cisco Systems, Inc.
www.cisco.com
35



Small Office/Home Office

- SOHO users can connect to the corporate network using ISDN, DSL or Frame Relay
- Use the Cisco IOS DHCP server to provide addresses for devices in the SOHO. Use a private, unregistered network number
- Use Port Address Translation to converse IP addresses
- Provide DNS services from the corporate network

806
0963_05F9_c3 © 1999, Cisco Systems, Inc.
www.cisco.com
36



Provisioning IP Phones

10.0.100.15

10.0.100.21

CNR DHCP Server

IF MAC Address = Phone Mac Address
Then
IP Address = 10.0.100.X
Else
IP Address = 161.44.12.X

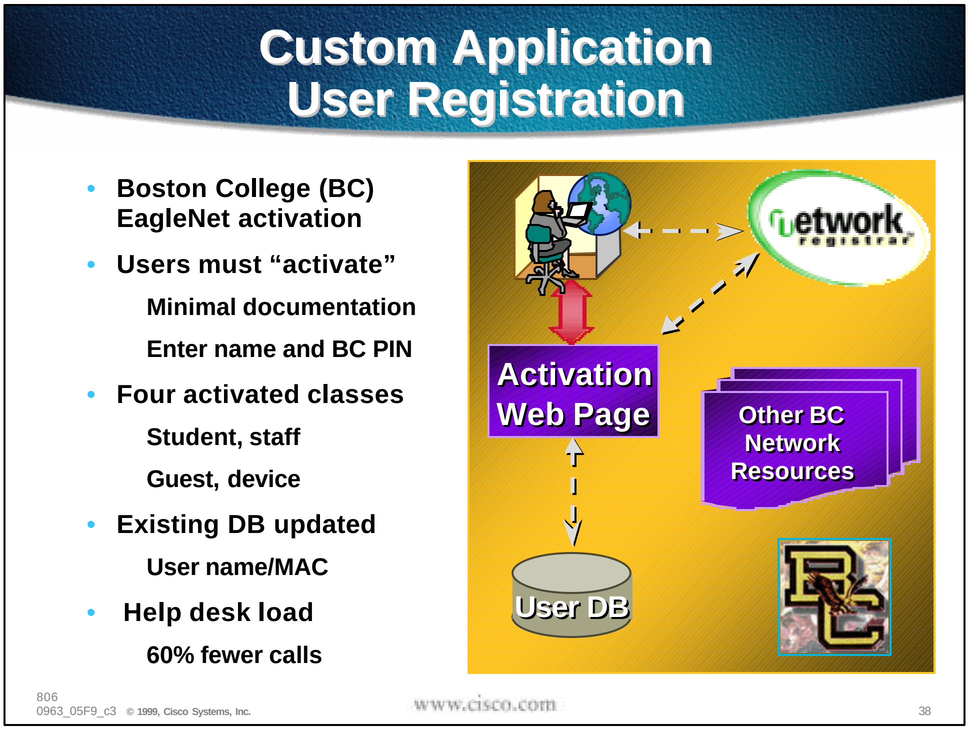
DHCP Extension Point Script

161.44.12.45

161.44.12.53

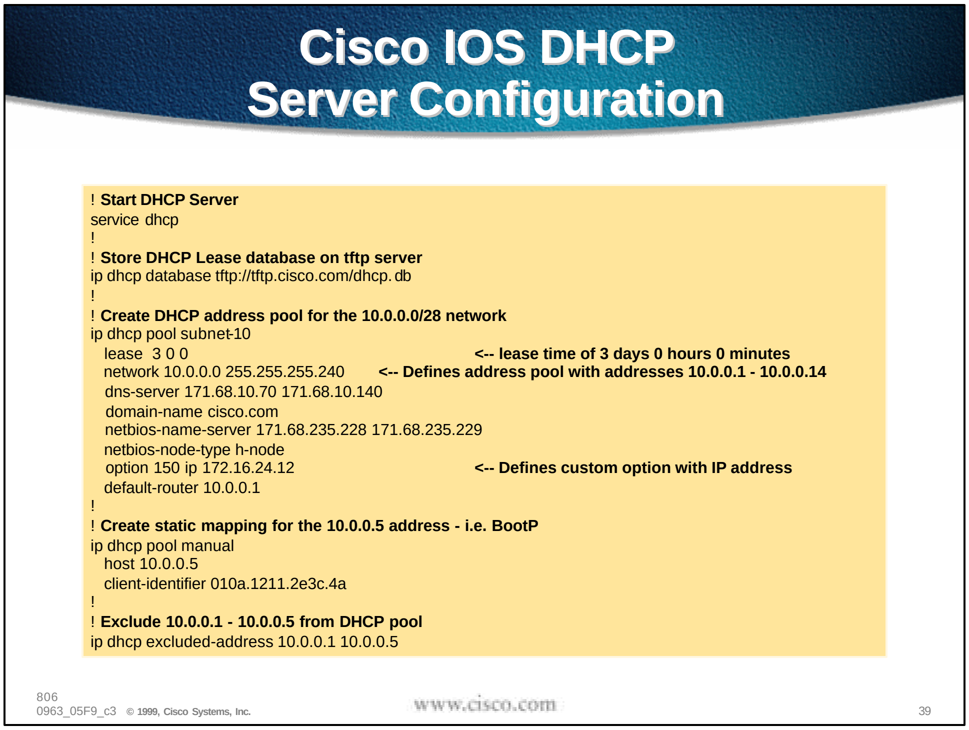
Primary IP address = 161.44.12.1
Secondary IP address = 10.0.100.1

- Deployment of IP phones will require a large number of new IP addresses
- Private network numbers (RFC 1918) should be used for IP phones
- Cisco Network Registrar is able to distinguish between PCs and IP phones using a DHCP extension point script
- DHCP server distributes additional configuration information to IP phones



Custom Application User Registration

- Boston College (BC) EagleNet activation
- Users must “activate”
  - Minimal documentation
  - Enter name and BC PIN
- Four activated classes
  - Student, staff
  - Guest, device
- Existing DB updated
  - User name/MAC
- Help desk load
  - 60% fewer calls



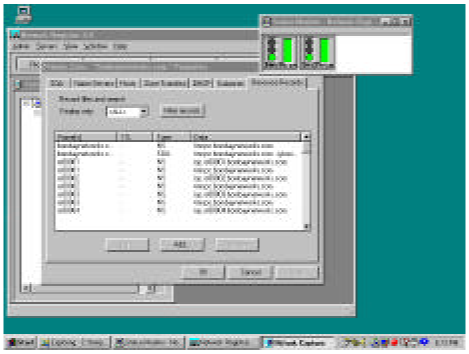
Cisco IOS DHCP Server Configuration

```
! Start DHCP Server
service dhcp
!
! Store DHCP Lease database on tftp server
ip dhcp database tftp://tftp.cisco.com/dhcp. db
!
! Create DHCP address pool for the 10.0.0.0/28 network
ip dhcp pool subnet-10
   lease  3 0 0                                    <-- lease time of 3 days 0 hours 0 minutes
   network 10.0.0.0 255.255.255.240       <-- Defines address pool with addresses 10.0.0.1 - 10.0.0.14
   dns-server 171.68.10.70 171.68.10.140
   domain-name cisco.com
   netbios-name-server 171.68.235.228 171.68.235.229
   netbios-node-type h-node
   option 150 ip 172.16.24.12                      <-- Defines custom option with IP address
   default-router 10.0.0.1
!
! Create static mapping for the 10.0.0.5 address - i.e. BootP
ip dhcp pool manual
   host 10.0.0.5
   client-identifier 010a.1211.2e3c.4a
!
! Exclude 10.0.0.1 - 10.0.0.5 from DHCP pool
ip dhcp excluded-address 10.0.0.1 10.0.0.5
```

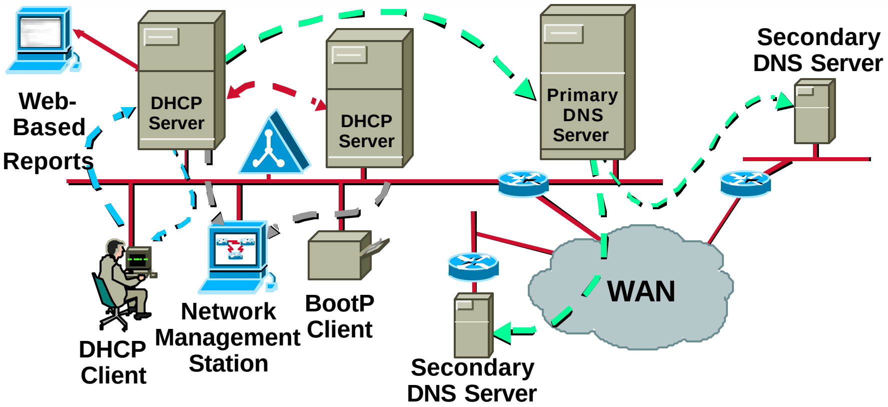
Product Update

Cisco Network Registrar 3.0

- Reliable and scalable services
  - DHCP Safe Failover
  - DDNS, IXFR and notify
  - Multithreaded servers
  - SNMP traps
  - Web reporting tool
  - Solaris, NT, HP-UX and AIX
- Flexible integration
  - LDAP integration
  - CLI and API
- Policy networking
  - Client class
  - LDAP integration

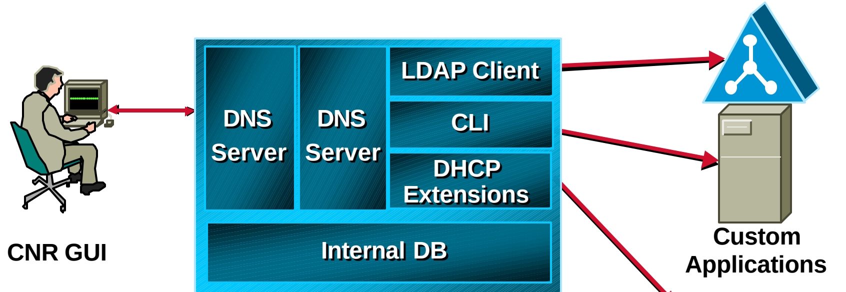


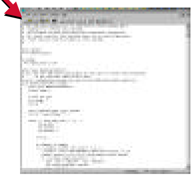
Reliable and Scalable Services



- Redundant DHCP and DNS services
- Integration with Network Management Systems
- Web-based reporting tools
- High-performance, multithreaded servers

Integrating CNR with Existing Management Applications

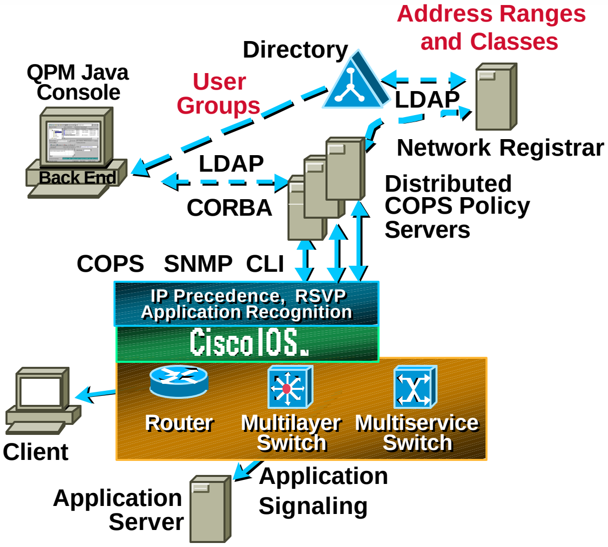


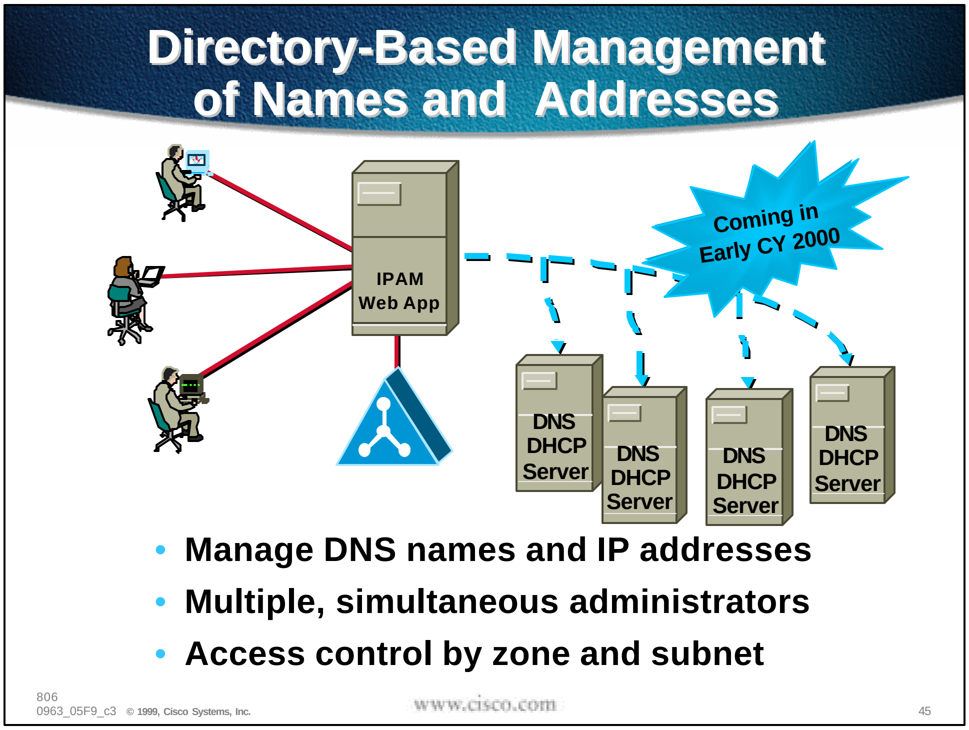


- Build custom network management and provisioning applications using the CLI
- Custom DHCP processing using the DHCP extension points
- Build custom web UI using CLI and Perl

CiscoAssure Policy Networking

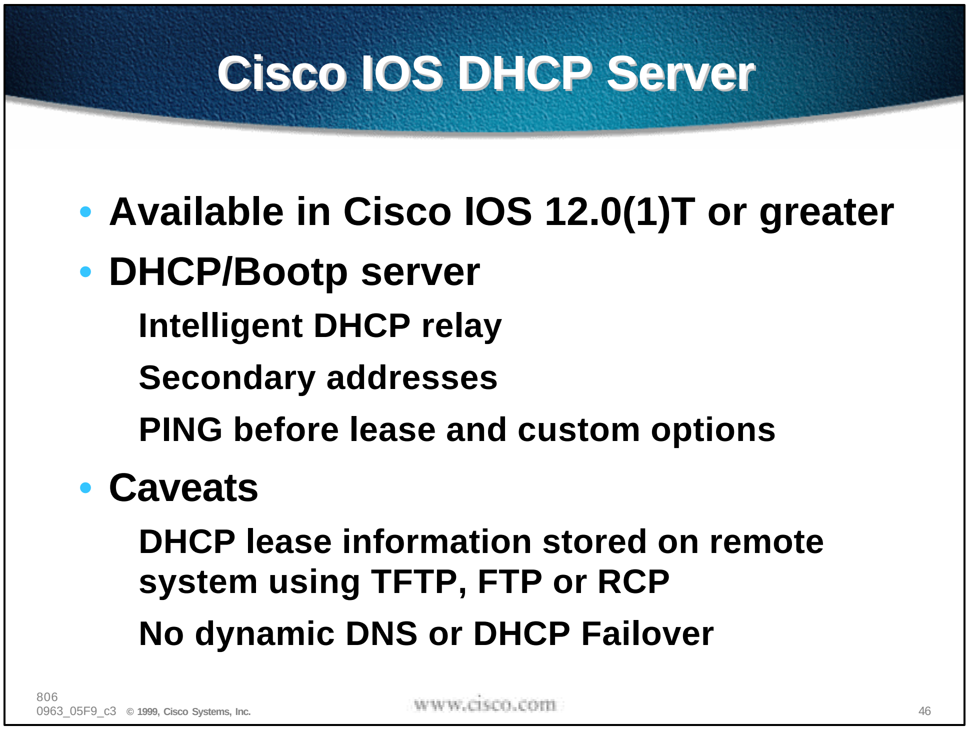
- QoS and security policies enforced in the network
- Polices based on applications
- Policies based on users and groups
- Integrated with directory services
- Integrate third party applications





Directory-Based Management of Names and Addresses

- Manage DNS names and IP addresses
- Multiple, simultaneous administrators
- Access control by zone and subnet



Cisco IOS DHCP Server

- Available in Cisco IOS 12.0(1)T or greater
- DHCP/Bootp server

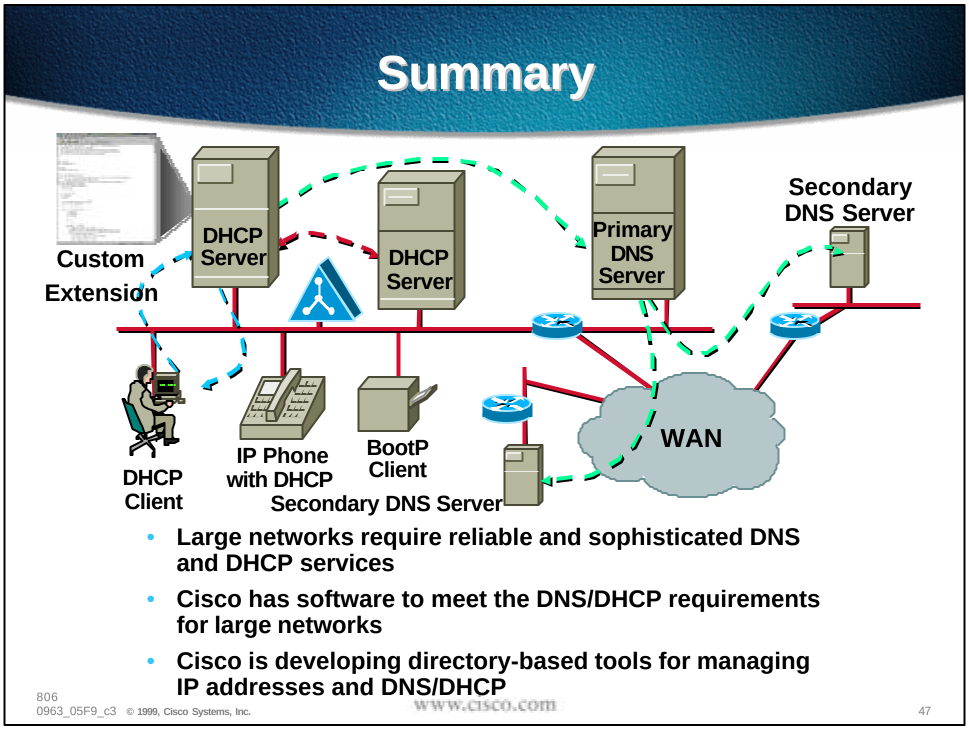
  Intelligent DHCP relay

  Secondary addresses

  PING before lease and custom options
- Caveats

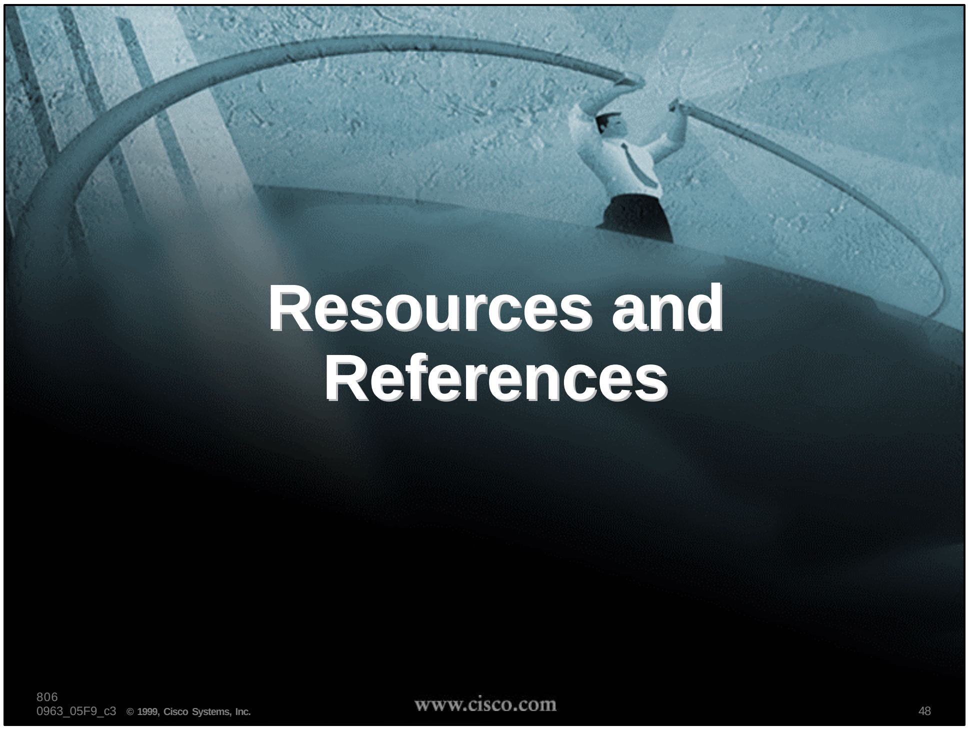
  DHCP lease information stored on remote system using TFTP, FTP or RCP

  No dynamic DNS or DHCP Failover

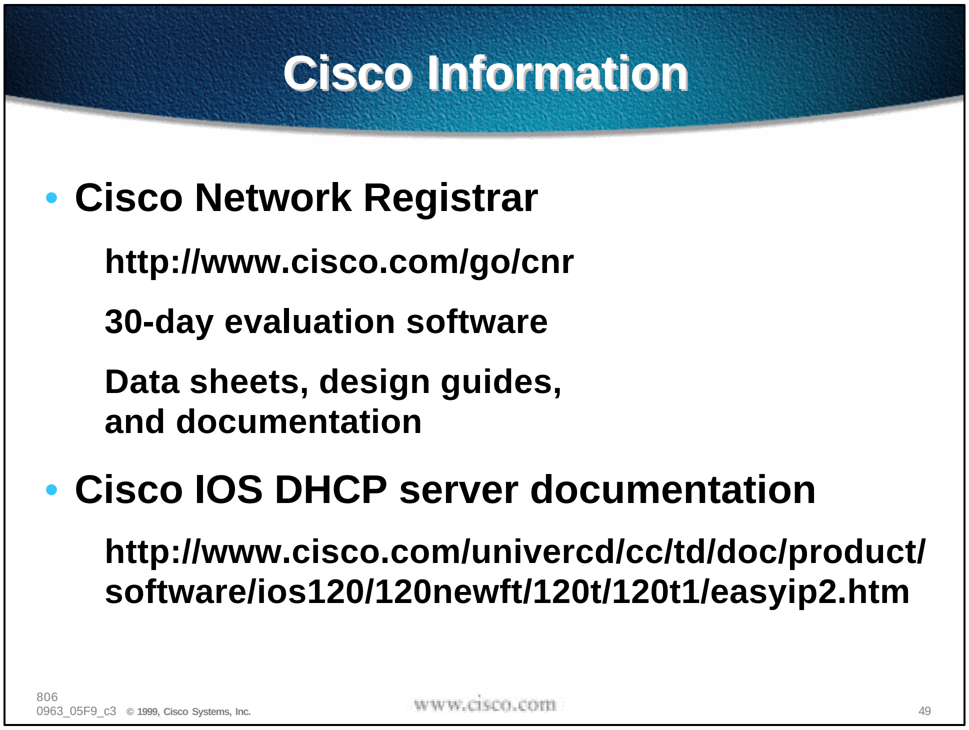


Summary

- Large networks require reliable and sophisticated DNS and DHCP services
- Cisco has software to meet the DNS/DHCP requirements for large networks
- Cisco is developing directory-based tools for managing IP addresses and DNS/DHCP



Resources and References



Cisco Information

- Cisco Network Registrar

  http://www.cisco.com/go/cnr

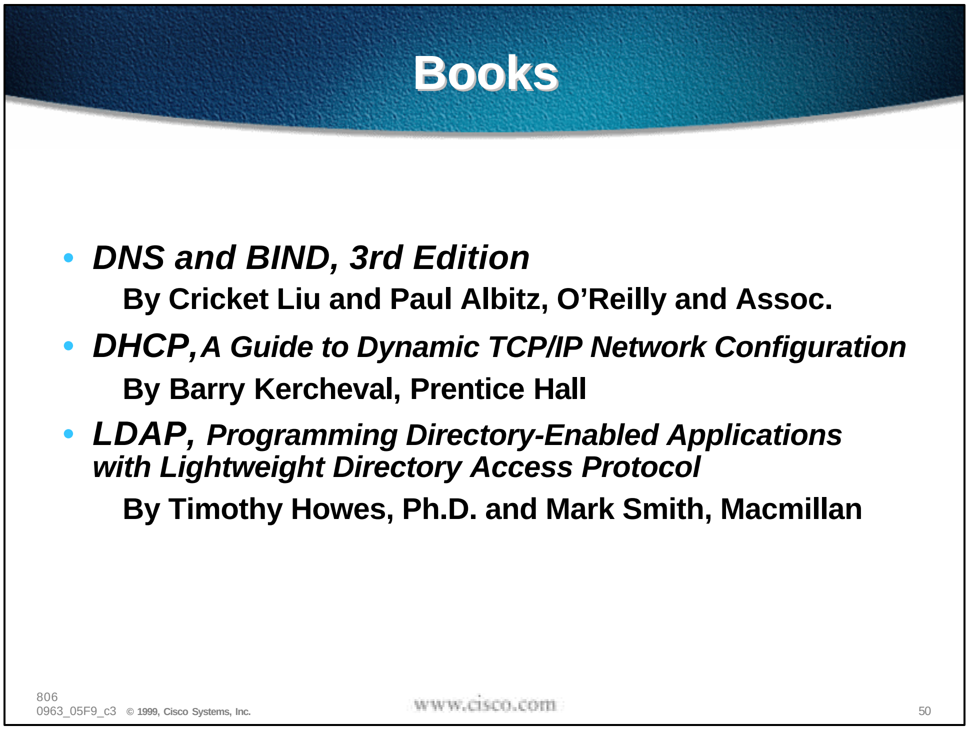
  30-day evaluation software

  Data sheets, design guides,
  and documentation

- Cisco IOS DHCP server documentation

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t1/easyip2.htm

806
0963_05F9_c3 © 1999, Cisco Systems, Inc. www.cisco.com 49



Books

- *DNS and BIND, 3rd Edition*

  By Cricket Liu and Paul Albitz, O'Reilly and Assoc.

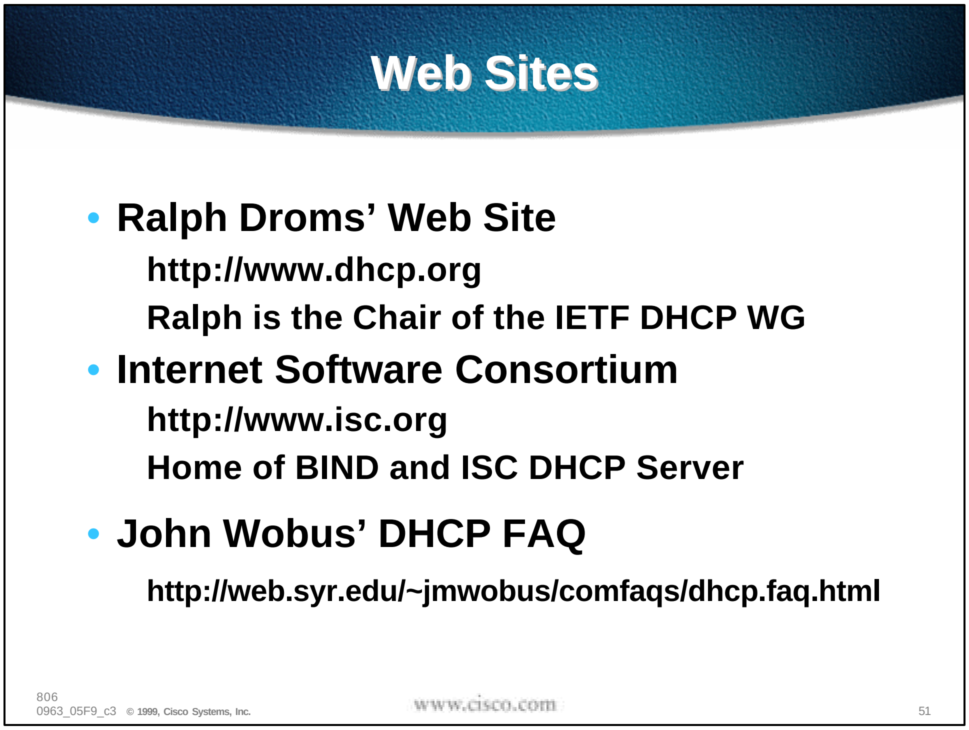
- *DHCP, A Guide to Dynamic TCP/IP Network Configuration*

  By Barry Kercheval, Prentice Hall

- *LDAP, Programming Directory-Enabled Applications with Lightweight Directory Access Protocol*

  By Timothy Howes, Ph.D. and Mark Smith, Macmillan

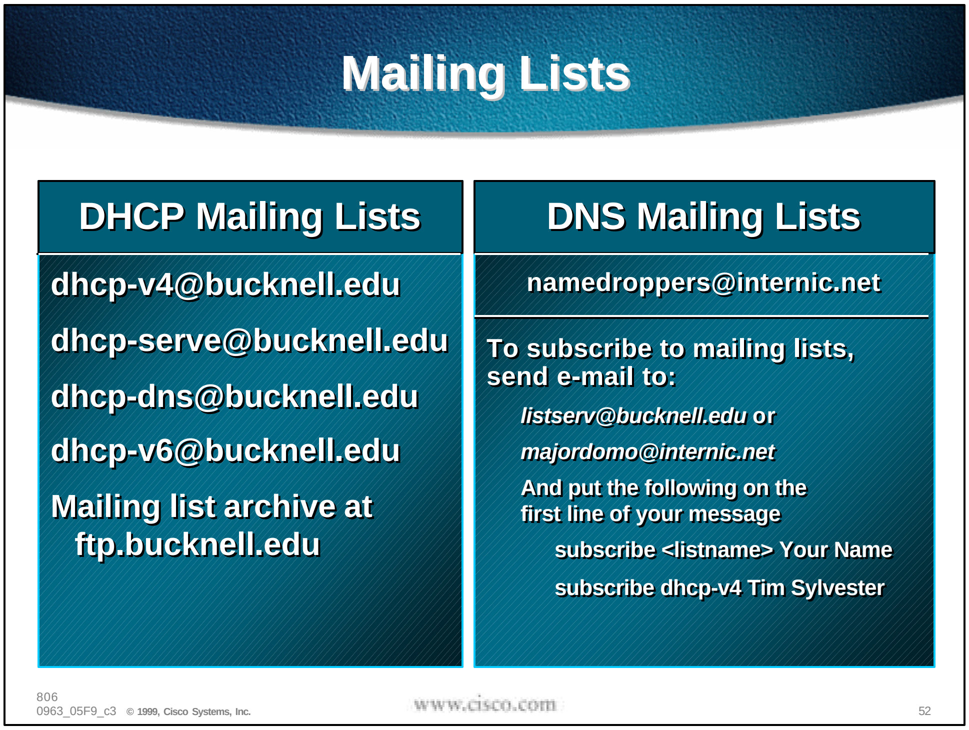
806
0963_05F9_c3 © 1999, Cisco Systems, Inc. www.cisco.com 50



Web Sites

- Ralph Droms' Web Site
  http://www.dhcp.org
  Ralph is the Chair of the IETF DHCP WG
- Internet Software Consortium
  http://www.isc.org
  Home of BIND and ISC DHCP Server
- John Wobus' DHCP FAQ
  http://web.syr.edu/~jmwobus/comfaqs/dhcp.faq.html

806
0963_05F9_c3 © 1999, Cisco Systems, Inc. www.cisco.com 51



Mailing Lists

DHCP Mailing Lists

dhcp-v4@bucknell.edu

dhcp-serve@bucknell.edu

dhcp-dns@bucknell.edu

dhcp-v6@bucknell.edu

Mailing list archive at
ftp.bucknell.edu

DNS Mailing Lists

namedroppers@internic.net

To subscribe to mailing lists, send e-mail to:

listserv@bucknell.edu or

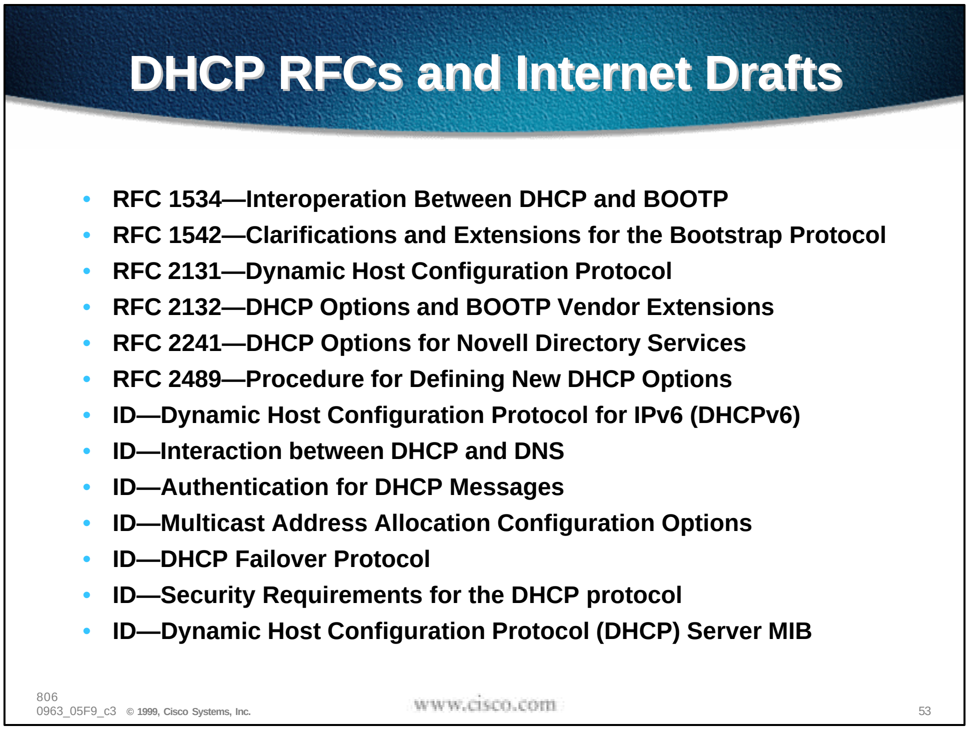
majordomo@internic.net

And put the following on the first line of your message

subscribe <listname> Your Name

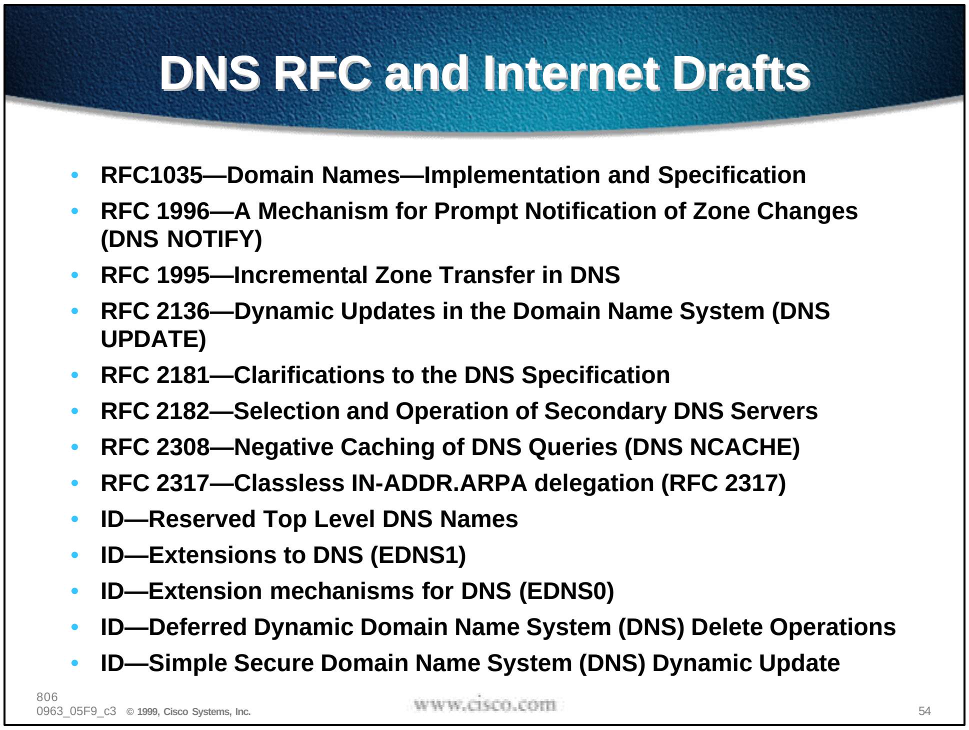
subscribe dhcp-v4 Tim Sylvester

806
0963_05F9_c3 © 1999, Cisco Systems, Inc. www.cisco.com 52



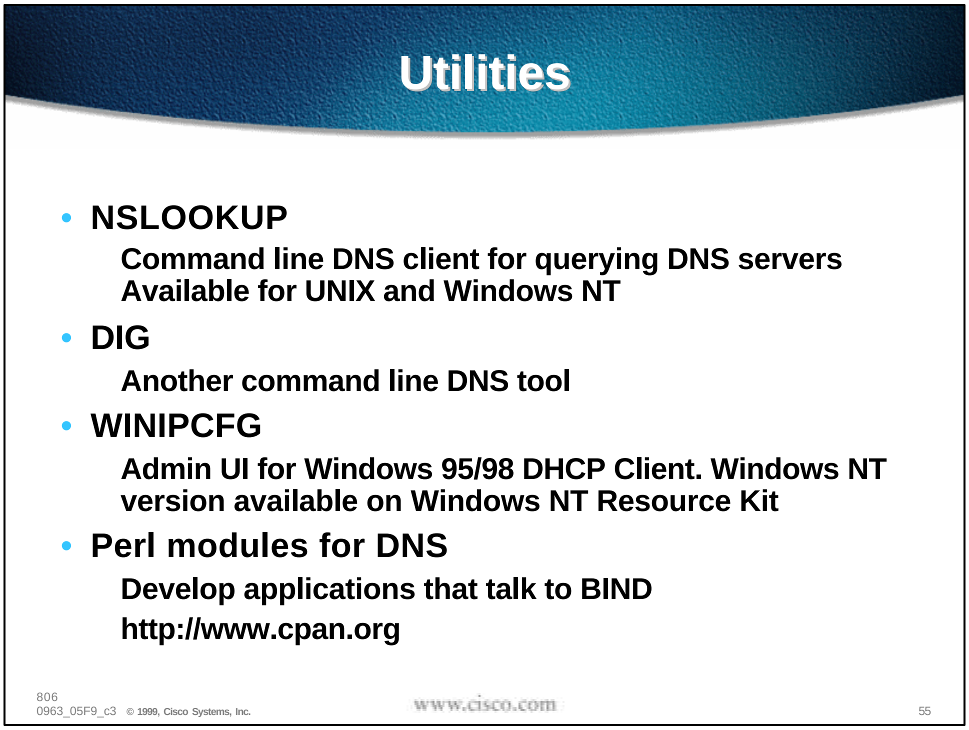
DHCP RFCs and Internet Drafts

- RFC 1534—Interoperation Between DHCP and BOOTP
- RFC 1542—Clarifications and Extensions for the Bootstrap Protocol
- RFC 2131—Dynamic Host Configuration Protocol
- RFC 2132—DHCP Options and BOOTP Vendor Extensions
- RFC 2241—DHCP Options for Novell Directory Services
- RFC 2489—Procedure for Defining New DHCP Options
- ID—Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
- ID—Interaction between DHCP and DNS
- ID—Authentication for DHCP Messages
- ID—Multicast Address Allocation Configuration Options
- ID—DHCP Failover Protocol
- ID—Security Requirements for the DHCP protocol
- ID—Dynamic Host Configuration Protocol (DHCP) Server MIB



DNS RFC and Internet Drafts

- RFC1035—Domain Names—Implementation and Specification
- RFC 1996—A Mechanism for Prompt Notification of Zone Changes (DNS NOTIFY)
- RFC 1995—Incremental Zone Transfer in DNS
- RFC 2136—Dynamic Updates in the Domain Name System (DNS UPDATE)
- RFC 2181—Clarifications to the DNS Specification
- RFC 2182—Selection and Operation of Secondary DNS Servers
- RFC 2308—Negative Caching of DNS Queries (DNS NCACHE)
- RFC 2317—Classless IN-ADDR.ARPA delegation (RFC 2317)
- ID—Reserved Top Level DNS Names
- ID—Extensions to DNS (EDNS1)
- ID—Extension mechanisms for DNS (EDNS0)
- ID—Deferred Dynamic Domain Name System (DNS) Delete Operations
- ID—Simple Secure Domain Name System (DNS) Dynamic Update



Utilities

- NSLOOKUP

  Command line DNS client for querying DNS servers
  Available for UNIX and Windows NT

- DIG

  Another command line DNS tool

- WINIPCFG

  Admin UI for Windows 95/98 DHCP Client. Windows NT version available on Windows NT Resource Kit

- Perl modules for DNS

  Develop applications that talk to BIND

  http://www.cpan.org

Please Complete Your Evaluation Form

Session 806

Cisco Systems ®
Empowering the Internet Generation SM