DNS/DHCP on CISCO IOS ROUTER

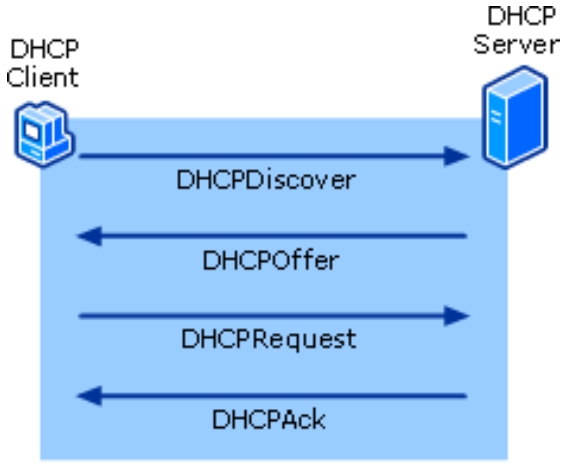
Kyuhwan Kim, CISCO TAC

Overview

- DHCP Overview
- DHCP Config / Debug
- DNS Overview
- IOS DNS Config / Debug
- DDNS with HTTP update
- DDNS with DHCP option 81
- SPLIT-DNS with DNS View
- DHCP option 82 with ip helper-address
- Useful PC TIP

DHCP Overview

How DHCP Works



- Dynamic Host Configuration Protocol , RFC 2131
- Obtain configuration information for operation in an Internet Protocol network, not just IP address
- The DHCP client requests an IP address by broadcasting a DHCPDiscover message, UDP, 255.255.255.255 or subnet broadcast address, to the local subnet.
  - Client can ask its old address in option DHCP option 50, and server will grant if it is still available
- DHCP server responds with a DHCPOffer message containing an IP address and configuration information for lease to the client.
  - Contains client's MAC, IP that the server is offering, the subnet mask, the lease duration, and the IP of the DHCP server making the offer.
  - If no DHCP server responds to the client request, the client sends DHCPDiscover messages at intervals of 0, 4, 8, 16, and 32 seconds
- The client indicates acceptance of the offer by selecting the offered address and broadcasting a DHCPRequest message in response.
- DHCP server broadcasts a DHCPAck message in response, finalizing the terms of the lease.

How DHCP renew

- **DHCP client first attempts to renew its lease when 50 percent of the original lease time, known as *T1*, has passed.**

  DHCP client sends a unicast DHCPRequest to DHCP server

  If the server is available, and the lease is still available, the server responds with a unicast DHCPAck

  If the original DHCP server is available, but the client's current lease is no longer available, the DHCP server responds with a DHCPNack

  Client immediately starts the process to obtain a new lease.

- **If there is no response from the DHCP server, the client waits until 87.5 percent of the lease time has passed (known as *T2*).**

  At T2, the client enters the rebinding state, and broadcasts a DHCPRequest message to attempt to renew the lease from any available DHCP server.

  If no DHCP server is available by the time the lease expires, the client immediately unbinds itself from the existing lease and starts the process to obtain a new lease,

DHCP Config/Debug

DHCP Server Config Example

```
ip dhcp excluded-address 10.10.10.1 → mostly, server addresses, avoid duplicated address
ip dhcp excluded-address 10.0.2.1 10.0.2.10
ip dhcp pool sdm-pool
   import all                          → import other options, like DNS, from ISP assigned DHCP address
   network 10.10.10.0 255.255.255.0
   default-router 10.10.10.1
   lease 0 2 1                         → year day hour
ip dhcp pool client vrf test           → only newer IOS supports, old IOS just recognize by IP Address
   network 10.0.2.0 255.255.255.0
   default-router 10.0.2.1
   dns-server 4.2.2.2
ip dhcp pool fedi                      → static DHCP entry, MAC is important
    host 192.168.200.206 255.255.255.240
    hardware-address 000f.fe83.bca9
    dns-server 208.67.220.220 208.67.222.222
int f4
   ip address dhcp
int vlan 1
   ip address 10.10.10.1 255.255.255.0
int vlan 2
   ip vrf for test
   ip add  10.0.2.0 255.255.255.0
```

How to verify DHCP import

sjc-kyukim-871#sh ip dhcp import
Address Pool Name: Home
Domain Name Server(s): 68.87.76.178
68.87.78.130
Domain Name Option:
hsd1.ca.comcast.net.

DHCP Server Commands

- **clear ip dhcp binding <address>**

  This command deletes an automatic address binding from the DHCP database

- **show ip dhcp binding 10.1.0.11**

```
IP address  Hardware address    Lease expiration          Type
10.1.0.11      00a0.9802.14b6     Feb 01 1998 12:00 AM Automatic
```

- **sh ip dhcp pool – displays all DHCP Pool informaiton**

```
Pool sdm-pool :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 0
 Pending event                  : none
 1 subnet is currently in the pool :
 Current index       IP address range                  Leased addresses
 10.10.10.1          10.10.10.1       - 10.10.10.254      0
```

- **debug ip dhcp server packet / debug ip dhcp server event**

  Use both commands to get detailed debug

Ddebug ip dhcp server event / packet

008629: Jun 3 17:25:10.929 PDT: DHCPD: DHCPDISCOVER received from client 0100.1558.8362.a1 on int BVI1.
008630: Jun 3 17:25:10.929 PDT: DHCPD: Seeing if there is an internally specified pool class:
>>> Identifying which pool to use
008631: Jun 3 17:25:10.929 PDT: DHCPD: htype 1 chaddr 0015.5883.62a1
008632: Jun 3 17:25:10.929 PDT: DHCPD: remote id 020a00000a130291f10000000000
008633: Jun 3 17:25:10.929 PDT: DHCPD: circuit id 00000000
008634: Jun 3 17:25:12.928 PDT: DHCPD: client requests 10.19.2.148.
008635: Jun 3 17:25:12.928 PDT: DHCPD: Adding binding to radix tree (10.19.2.148)
008636: Jun 3 17:25:12.928 PDT: DHCPD: Adding binding to hash tree
008637: Jun 3 17:25:12.928 PDT: DHCPD: assigned IP address 10.19.2.148 to client 0100.1558.8362.a1.
008638: Jun 3 17:25:12.928 PDT: DHCPD: Sending DHCPOFFER to client 0100.1558.8362.a1 (10.19.2.148).
008639: Jun 3 17:25:12.928 PDT: DHCPD: creating ARP entry (10.19.2.148, 0015.5883.62a1).
008640: Jun 3 17:25:12.928 PDT: DHCPD: unicasting BOOTREPLY to client 0015.5883.62a1 (10.19.2.148).
008641: Jun 3 17:25:12.940 PDT: DHCPD: DHCPREQUEST received from client 0100.1558.8362.a1.
008642: Jun 3 17:25:12.940 PDT: DHCPD: Sending notification of ASSIGNMENT:
008643: Jun 3 17:25:12.940 PDT: DHCPD: address 10.19.2.148 mask 255.255.255.240
008644: Jun 3 17:25:12.940 PDT: DHCPD: htype 1 chaddr 0015.5883.62a1
008645: Jun 3 17:25:12.940 PDT: DHCPD: lease time remaining (secs) = 172800
008646: Jun 3 17:25:12.944 PDT: DHCPD: Appending default domain from pool
008647: Jun 3 17:25:12.944 PDT: DHCPD: Using hostname 'kyukim-wxp.cisco.com' for dynamic update (from hostname option)
008648: Jun 3 17:25:12.944 PDT: DHCPD: Sending DHCPACK to client 0100.1558.8362.a1 (10.19.2.148).
008649: Jun 3 17:25:12.944 PDT: DHCPD: creating ARP entry (10.19.2.148, 0015.5883.62a1).
008650: Jun 3 17:25:12.944 PDT: DHCPD: Changing arp entry 10.19.2.148 to secure arp entry
008651: Jun 3 17:25:12.944 PDT: DHCPD: unicasting BOOTREPLY to client 0015.5883.62a1 (10.19.2.148)
008652: Jun 3 17:25:24.797 PDT: DHCPD: checking for expired leases.

DHCP Client Commands

- **Show dhcp binding**

```
Temp IP addr: 76.125.48.68  for peer on Interface: FastEthernet4
Temp  sub net mask: 255.255.252.0
   DHCP Lease server: 68.87.76.23, state: 3 Bound
   DHCP transaction id: 1FE8
   Lease: 345600 secs,  Renewal: 172800 secs,  Rebind: 302400 secs
Temp default-gateway addr: 76.125.48.1
   Next timer fires after: 16:59:18
   Retry count: 0   Client-ID: cisco-001e.be7c.efad-Fa4
   Client-ID hex dump: 636973636F2D303031652E626537632E
                       656661642D466134
```

- **Show dhcp server**

```
sjc-kyukim-871#sh dhcp server
   DHCP server: ANY (255.255.255.255)
    Leases:   5
    Offers:   1      Requests: 5     Acks : 5     Naks: 0
    Declines: 0      Releases: 0     Query: 0     Bad: 0
    DNS0:   68.87.76.178,   DNS1:  68.87.78.130
    Subnet: 255.255.252.0   DNS Domain: hsd1.ca.comcast.net.
```

Debug dhcp detail – for dhcp client activity

```
*Jun 11 19:38:47.875: DHCP: DHCP client process started: 10
*Jun 11 19:38:47.879: RAC: Starting DHCP discover on FastEthernet0/1
*Jun 11 19:38:47.879: DHCP: Try 1 to acquire address for FastEthernet0/1
*Jun 11 19:38:47.879: DHCP: allocate request
*Jun 11 19:38:47.879: DHCP: zapping entry in DHC_PURGING state for Fa0/1
*Jun 11 19:38:47.879: DHCP: deleting entry 45BBFFEC 192.168.150.101 from list
*Jun 11 19:38:47.879: Temp IP addr: 192.168.150.101  for peer on Interface: Fa0/1
*Jun 11 19:38:47.879: Temp  sub net mask: 255.255.255.0
*Jun 11 19:38:47.879:  DHCP Lease server: 192.168.150.1, state: 9 Purging
*Jun 11 19:38:47.879:  DHCP transaction id: 19B
*Jun 11 19:38:47.879:   Lease: 86400 secs,  Renewal: 43200 secs,  Rebind: 75600
*Jun 11 19:38:47.879:   Next timer fires after: 00:00:24
*Jun 11 19:38:47.879:   Retry count: 0   Client-ID: cisco-001f.cab6.4dc9-Fa0/1
*Jun 11 19:38:47.879:   Client-ID hex dump: 636973636F2D303031662E636162362E
*Jun 11 19:38:47.883:                       346463392D4661302F31
*Jun 11 19:38:47.883:    Hostname: R4
*Jun 11 19:38:47.883: DHCP: new entry. add to queue, interface FastEthernet0/1
*Jun 11 19:38:47.883: DHCP: SDiscover attempt # 1 for entry:
*Jun 11 19:38:47.883: Temp IP addr: 0.0.0.0  for peer on Interface: FastEthernet0/1
*Jun 11 19:38:47.883: Temp  sub net mask: 0.0.0.0
*Jun 11 19:38:47.883:    DHCP Lease server: 0.0.0.0, state: 1 Selecting
*Jun 11 19:38:47.883:    DHCP transaction id: 1A74
*Jun 11 19:38:47.883:    Lease: 0 secs,  Renewal: 0 secs,  Rebind: 0 secs
*Jun 11 19:38:47.883:    Next timer fires after: 00:00:04
*Jun 11 19:38:47.883:    Retry count: 1   Client-ID: cisco-001f.cab6.4dc9-Fa0/1
*Jun 11 19:38:47.883:    Client-ID hex dump: 636973636F2D303031662E636162362E
*Jun 11 19:38:47.883:                        346463392D4661302F31
*Jun 11 19:38:47.883:    Hostname: R4
*Jun 11 19:38:47.883: DHCP: SDiscover: sending 291 byte length DHCP packet
*Jun 11 19:38:47.883: DHCP: SDiscover 291 bytes
*Jun 11 19:38:47.883:              B'cast on FastEthernet0/1 interface from 0.0.0.0
```

```
*Jun 11 19:38:49.887: DHCP: Scan: Rebind time: 75600
*Jun 11 19:38:49.887: DHCP: Scan: Subnet Address Option: 255.255.255.0
*Jun 11 19:38:49.887: DHCP: Scan: Router Option: 192.168.150.1
*Jun 11 19:38:49.887: DHCP: Scan: DNS Name Server Option: 12.1.1.2
*Jun 11 19:38:49.887: DHCP: rcvd pkt source: 192.168.150.1,  destination:  255.255.255.255
*Jun 11 19:38:49.887:    UDP  sport: 43,  dport: 44,  length: 308
*Jun 11 19:38:49.887:    DHCP op: 2, htype: 1, hlen: 6, hops: 0
*Jun 11 19:38:49.887:    DHCP server identifier: 192.168.150.1
*Jun 11 19:38:49.887:        xid: 1A74, secs: 0, flags: 8000
*Jun 11 19:38:49.887:        client: 0.0.0.0, your: 192.168.150.102
*Jun 11 19:38:49.887:        srvr:   0.0.0.0, gw: 0.0.0.0
*Jun 11 19:38:49.887:        options block length: 60
*Jun 11 19:38:49.887: DHCP Offer Message   Offered Address: 192.168.150.102
*Jun 11 19:38:49.887: DHCP: Lease Seconds: 86400    Renewal secs:  43200 Rebind secs:
*Jun 11 19:38:49.887: DHCP: Server ID Option: 192.168.150.1
*Jun 11 19:38:49.887: DHCP: offer received from 192.168.150.1
*Jun 11 19:38:49.887: DHCP: SRequest attempt # 1 for entry:
*Jun 11 19:38:49.887: Temp IP addr: 192.168.150.102  for peer on Interface: FastEthernet0/1
*Jun 11 19:38:49.887: Temp  sub net mask: 255.255.255.0
*Jun 11 19:38:49.891:    DHCP Lease server: 192.168.150.1, state: 2 Requesting
*Jun 11 19:38:49.891:    DHCP transaction id: 1A74
*Jun 11 19:38:49.891:    Lease: 86400 secs,  Renewal: 0 secs,  Rebind: 0 secs
*Jun 11 19:38:49.891:    Next timer fires after: 00:00:03
*Jun 11 19:38:49.891:    Retry count: 1   Client-ID: cisco-001f.cab6.4dc9-Fa0/1
*Jun 11 19:38:49.891:    Client-ID hex dump: 636973636F2D303031662E636162362E
*Jun 11 19:38:49.891:    Hostname: R4
*Jun 11 19:38:49.891: DHCP: SRequest- Server ID option: 192.168.150.1
*Jun 11 19:38:49.891: DHCP: SRequest- Requested IP addr option: 192.168.150.102
*Jun 11 19:38:49.891: DHCP: SRequest placed lease len option: 86400
*Jun 11 19:38:49.891:           B'cast on FastEthernet0/1 interface from 0.0.0.0
```

*Jun 11 19:38:49.895: DHCP: Received a BOOTREP pkt
*Jun 11 19:38:49.895: DHCP: Scan: Message type: DHCP Ack
*Jun 11 19:38:49.895: DHCP: Scan: Server ID Option: 192.168.150.1 = C0A89601
*Jun 11 19:38:49.895: DHCP: Scan: Lease Time: 86400
*Jun 11 19:38:49.895: DHCP: Scan: Renewal time: 43200
*Jun 11 19:38:49.895: DHCP: Scan: Rebind time: 75600
*Jun 11 19:38:49.895: DHCP: Scan: Subnet Address Option: 255.255.255.0
*Jun 11 19:38:49.895: DHCP: Scan: Router Option: 192.168.150.1
*Jun 11 19:38:49.895: DHCP: Scan: DNS Name Server Option: 12.1.1.2
*Jun 11 19:38:49.895: DHCP: rcvd pkt source: 192.168.150.1, destination: 255.255.255.255
*Jun 11 19:38:49.895: UDP sport: 43, dport: 44, length: 308
*Jun 11 19:38:49.895: DHCP op: 2, htype: 1, hlen: 6, hops: 0
*Jun 11 19:38:49.895: DHCP server identifier: 192.168.150.1
*Jun 11 19:38:49.895: xid: 1A74, secs: 0, flags: 8000
*Jun 11 19:38:49.895: client: 0.0.0.0, your: 192.168.150.102
*Jun 11 19:38:49.895: srvr: 0.0.0.0, gw: 0.0.0.0
*Jun 11 19:38:49.895: options block length: 60
*Jun 11 19:38:49.895: DHCP Ack Message
*Jun 11 19:38:49.895: DHCP: Lease Seconds: 86400 Renewal secs: 43200 Rebind secs: 75600
*Jun 11 19:38:49.895: DHCP: Server ID Option: 192.168.150.1
*Jun 11 19:38:52.895: DHCP: Releasing ipl options:
*Jun 11 19:38:52.895: DHCP: Applying DHCP options:
*Jun 11 19:38:52.895: Setting default_gateway to 192.168.150.1
*Jun 11 19:38:52.895: Adding default route 192.168.150.1
*Jun 11 19:38:53.895: Adding DNS server address 12.1.1.2
*Jun 11 19:38:53.895: DHCP Client Pooling: ***Allocated IP address: 192.168.150.102
*Jun 11 19:38:53.899: Allocated IP address = 192.168.150.102 255.255.255.0
*Jun 11 19:38:53.899: %DHCP-6-ADDRESS_ASSIGN: Interface FastEthernet0/1 assigned DHCP address 192.168.150.102, mask 255.255.255.0, hostname R4If IOS router is not getting IP address from ISP modem

DHCP Problem example

- **RP only handles DHCP server on IOS**
- **First team who received DHCP client case must handle as there is no keyword**
- **Recently, there were several DHCP client issues on router to connect to cable or DSL modem/router**
  - Most ot cases, it is caused by inspect rule or ACL blocking DHCP traffic
  - But sometimes, it is new feature on cable modem like below.
  - Solution was making ISP DHCP server as approved DHCP server by adding “ip dhcp server 10.247.64.1”

*Mar 3 01:48:05.027: DHCP: Received a BOOTREP pkt Not for us..: xid: 0xBED70ABC
*Mar 3 01:48:05.699: DHCP: SDiscover attempt # 3 for entry:
*Mar 3 01:48:05.699: DHCP: SDiscover: sending 294 byte length DHCP packet
*Mar 3 01:48:05.699: DHCP: SDiscover 294 bytes
*Mar 3 01:48:05.699: B'cast on FastEthernet4 interface from 0.0.0.0
*Mar 3 01:48:05.771: DHCP: Received a BOOTREP pkt
*Mar 3 01:48:05.775: DHCP: offer received from 10.247.64.1
*Mar 3 01:48:05.775: DHCP: offer: server 10.247.64.1 not in approved list%Unknown DHCP problem.. No allocation possible
*Mar 3 01:48:18.543: DHCP: Waiting for 60 seconds on interface FastEthernet4

DNS Overview

How DNS works

- **Name Resolution in Computer world**

  You don't want to remember all IP addresses of servers

  So, all APP are programmed to use names, not ip address

  DNS for Internet, WINS for Microsoft

- **DNS is**

  - Domain Name Servers translate domain names, like www.cisco.com or @hotmail.com to IP addresses, 4.2.2.2
  - DNS system is a big layered **database** of whole Internet world
    - Top level domain - .com .gov .kr .uk
    - Second level domain – yahoo cisco
    - Sub level domain – bbc.co.uk chosun.co.kr
    - Host name – www.yahoo.com ftp.cisco.com

- **DNS does**

  - Answer the DNS Query with an IP because it already knows
  - Contact another name server and try to find if it doesn't know
    - Start its search by contacting one of the **root name servers**.
    - Root servers knows the IP addresses of the name servers handling the several hundred top-level domains.
    - Root server return the IP for top-level domain server to your DNS

DNS Records

- DNS Domain and Zone
  - Zone is a portion of domain name space
  - NS can be authoritative for a zone. (has full info of Zone)
- DNS is a database
  - Consists of resource records (RR)
  - Each RR identifies a particular resource
  - SOA - Specifies authoritative server for the zone
  - NS - Specifies address of domain's name server(s)
  - A - Maps host name to an address
  - PTR - Maps address to a host name for reverse lookup
  - CNAME - Creates alias name for specified host name
    - Multiple CNAMEs for A RR
  - MX - Mail exchange server for domain

DNS Server Types

- Master (Primary) NS

  contains one or more zone files for which this DNS is **Authoritative**

- Slave (secondary) NS

  Gets its zone file information from a zone master

- Caching (hint) NS

  Obtains information from another server (a Zone Master) in response to a host query and then saves (caches) the data locally.

- Forwarding (proxy, client, or remote) NS

  Simply forwards all requests to another DNS and caches the results.

  CISCO ISO router is FWD NS

  http://www.zytrax.com/books/dns/ch4/

IOS DNS

CISCO IOS DNS Server Config

- DNS lookup has to be enabled with the **ip domain-lookup** command
- Upstream DNS server has to be defined with the **ip name-server *x.x.x.x***
- Optionally, the local domain suffix (like *example.com*) has to be defined on the router with the **ip domain name *suffix*** or **ip domain list** *suffix*
- DNS server is started with the **ip dns server**
- Make host use IOS router as DNS resolver
  - Configure DHCP Pool's DNS option points to IOS router
  - or manually config DNS option on host

IOS DNS Config Example

- **IOS DNS CONFIG Example**

  ip domain name company.com → for incomplete FQDN queries, will add domain name

  ip name-server 10.0.0.1 → NS server to forward DNS query

  ip name-server 4.2.2.2 → the most well known public DNS

  ip dns server → must have

  ip host sjck-access-isc1.cisco.com 10.17.8.8 → create DNS cache

  ip host sjck-access-cert1.cisco.com 10.17.8.6

  Ip dhcp pool test

  dns-server 10.1.1.1 → router's own IP address

- **Show host – displays DNS cache**

  router#**show hosts** → clear hosts all * to clear cache on router

  Default domain is nil.com

  Name/address lookup uses domain service

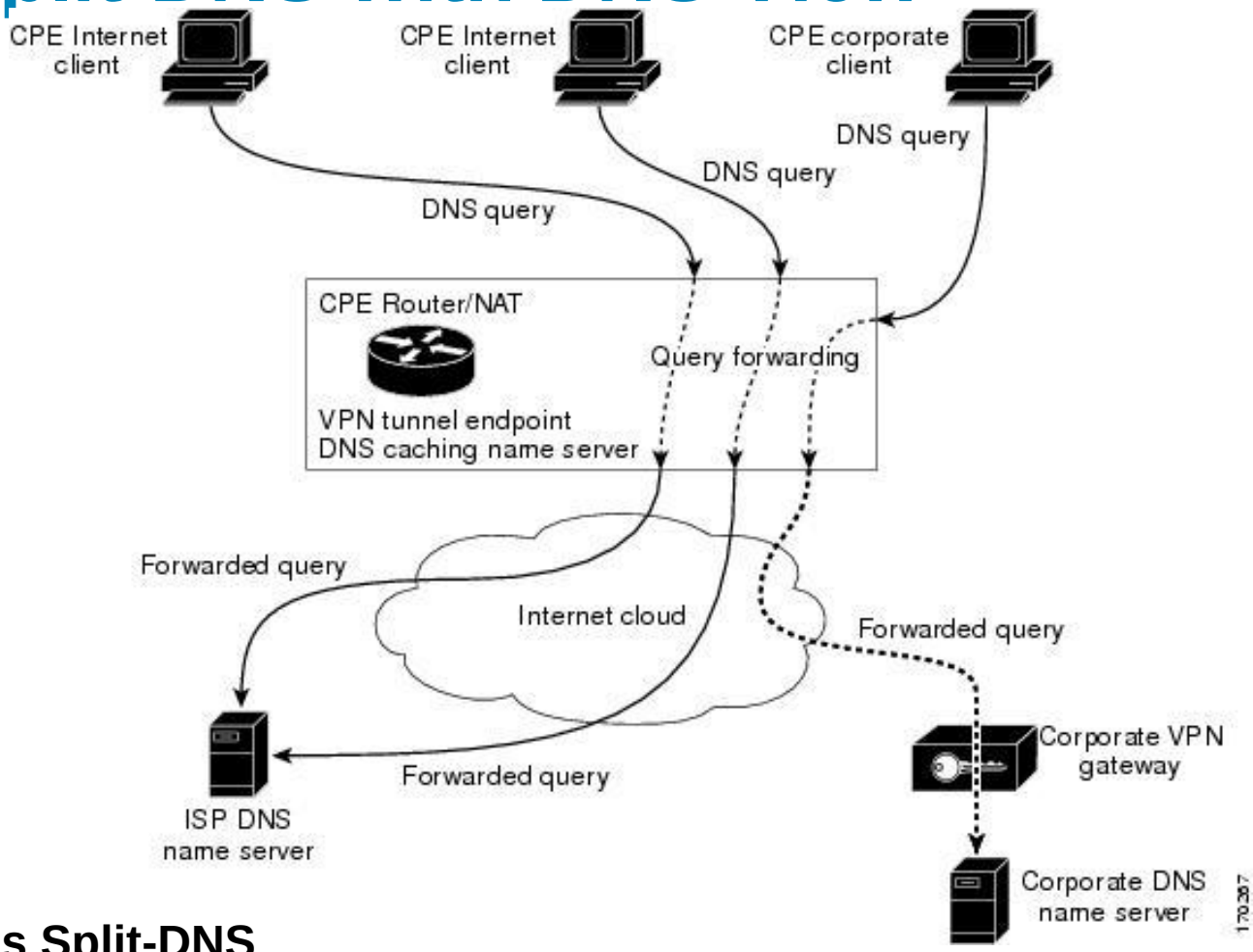
  Name servers are 10.0.0.1, 10.0.0.2

Host	Port	Flags	Age	Type	Address(es)
ns1.cisco.com	None	(temp, OK)	4	IP	128.107.241.185
www.cisco.com	None	(temp, OK)	0	IP	198.133.219.25
sj-inbound-d.cisco.com	None	(temp, OK)	4	IP	128.107.243.13
cisco.com	NA	(temp, EX)	0	MX	25 syd-inbound-a.cisco.com
					10 sj-inbound-a.cisco.com
					10 sj-inbound-b.cisco.com

CISCO IOS DNS/DHCP
Part II

Kyuhwan Kim, TAC SJ RP

Split-DNS with DNS View



What is Split-DNS

- A method of spliting a DNS zone when use one domain name for internal/external
- Direct internal host to internal zone and external hosts to external
- Cisco implements this with DNS View

Split-DNS Config Example

ip dns view Teva → parameters for how to handle a DNS query
logging → enable DNS logging
domain name cisco.com → to complete unqualified hostnames
dns forwarder 192.168.3.240 → **order: local cache, dns fwd, domain ns, broadcast**
dns forwarding source-interface Vlan2 → DNS query is FWD and sourced from
domain name-server 171.70.168.183 → to resolve internally generated DNS Q
ip domain lookup source-interface vlan2
ip dns view default → used for int without dns view or query not match any view
logging
ip dns view-list dvl-Test → Usage restrictions can be specified for views
view Teva 1
restrict name-group 2 → name group uses DNS name list
restrict access-group 99 → source IP address of the DNS query matches
view default 2 → rest of queried that didn't match with view 1
ip dns name-list 2 permit .*.CO.KR → All other access implicitly denied
access-list 99 permit ip 10.1.1.0 0.0.0.255 any
int vlan 2
ip dns view-group dvl-Test → apply on inerface

if DNS Q source from ACL 99 and look for *.co.kr, use

Split-DNS Logging / Debug domain

- Split DNS logging

  *Sep 19 10:37:23.938: %DNS-6-LOG_ACCESS: DNS View Teva used for client 10.225.1.2/54394, querying A 'www.chosun.co.kr‘

  *Sep 19 10:38:52.078: %DNS-6-LOG_ACCESS: DNS View default used for client 10.225.1.2/58174, querying A 'www.yahoo.com‘

- Debug domain

*Sep 19 10:39:27.082: DNS: Incoming UDP query (id#29)

*Sep 19 10:39:27.082: DNS: Type 1 DNS query (id#29) for host 'www.chosun.co.kr' from 10.225.1.2(51997)

*Sep 19 10:39:27.082: %DNS-6-LOG_ACCESS: DNS View Teva used for client 10.225.1.2/51997, querying A 'www.chosun.co.kr'

*Sep 19 10:39:27.082: DNS: Servicing request using view Teva

*Sep 19 10:39:27.082: Domain: Using source interface BVI1

*Sep 19 10:39:27.082: DNS: Re-sending DNS query (type 1, id#29) to 171.70.168.183

DDNS/DHCP option 81

Dynamic DNS

- DDNS to update your internal NS, DHCP option 81
  - Since W2K, MS introduced DDNS function to Active Directory DNS server
  - AD DNS replaces WINS, famous old netbios name resolution (\\vanguard\c$)
  - As AD rely on DNS, all hostname and IP address should be updated dynamically
  - DDNS on IOS router enables the DHCP server to support a new FQDN DHCP option 81
  - Only AD authorized DHCP server can update AD DDNS server
- DDNS HTTP Update to update Internet A record
  - If you don’t have static internet IP, you can’t register your domain name for your server (especially, in Asia)
  - DDNS vendors, like dyndns.org, support the new way of updating A record automatically from CU router

DDNS HTTP Update

- Split DNS logging

```
ip ddns update method mytest
  ddns
  http
    add http://test:test@members.dyndns.org/nic/update?system=dyndns&hostname=<h>&myip=<a>
   interval maximum 1 0 0 0
interface F4
   ip ddns update hostname abc.dyndns.org
   ip ddns update mytest
    ip address dhcp
```

→ what A record you want to update

Press the control (Ctrl) key and the "v" key together to put ? in config mode

Different vendors are using different format of HTTP string. Please refer below.

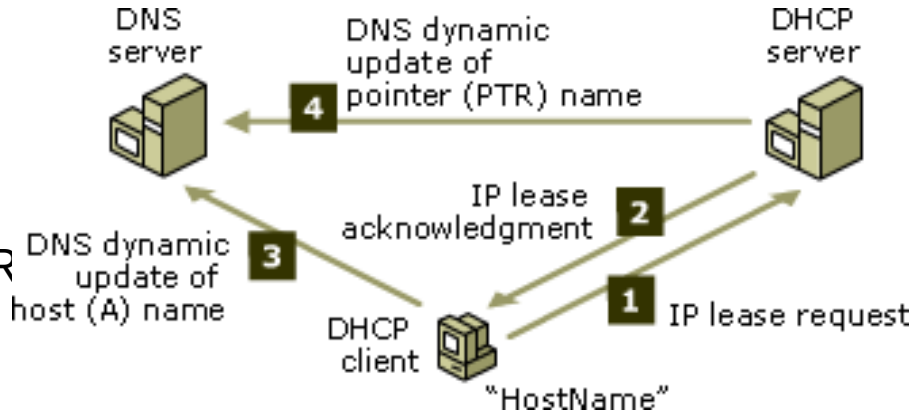
http://www.cisco.com/en/US/docs/ios/ipaddr/configuration/guide/iad_ddns_ps6441_TSD_Products_Configuration_Guide_Chapter.html

Debug ip ddns update

- Router# **debug ip ddns update**

00:04:35:%DHCP-6-ADDRESS_ASSIGN: Interface Ethernet1 assigned DHCP address 10.32.254.187, mask 255.255.255.240, hostname test.dyndns.org
00:04:35: DYNDNSUPD: Adding DNS mapping for test.dyndns.org <=> 10.32.254.187 server 10.208.196.94
00:04:35: DYNDNSUPD: Sleeping for 3 seconds waiting for interface Ethernet1 configuration to settle
00:04:38: HTTPDNS: Update add called for test.dyndns.org <=> 10.32.254.187
00:04:38: HTTPDNS: Update called for test.dyndns.org <=> 10.32.254.187
00:04:38: HTTPDNS: init
00:04:38: HTTPDNSUPD: Session ID = 0x7
00:04:38: HTTPDNSUPD: URL = 'http://test:test@10.208.196.94/nic/update?system=dyndns&hostname=test.dyndns.org&myip=10. 32.254.187'
00:04:38: HTTPDNSUPD: Sending request
00:04:40: HTTPDNSUPD: Response for update test.dyndns.org <=> 10.32.254.187
00:04:40: HTTPDNSUPD: DATA START good 10.32.254.187
00:04:40: HTTPDNSUPD: DATA END, Status is Response data received, successfully
00:04:40: HTTPDNSUPD: Call returned SUCCESS for update test.dyndns.org <=> 10.32.254.187
00:04:40: HTTPDNSUPD: Freeing response
00:04:40: DYNDNSUPD: Another update completed (outstanding=0, total=0)
00:04:40: HTTPDNSUPD: Clearing all session 7 info

DHCP Option 81



- Whenever IP address changed on host, NS must have update A RR and PTR RR
- DDNS enables DHCP client or server updates A RR and PTR RR dynamically
- By default, DHCP client updates A record and DHCP server updates PTR record if DDNS update is enabled on DHCP server/client
- DHCP client can specify if it wants DHCP server to update PTR or both in DHCP Request
- DHCP server can notify client

  It will update both or PTR as client requested

  Or it will update both by overriding client's request

- All this is done by FQDN option in DHCP packet, RFC 4072

  • A client sets the N bit to 0 in **DHCP REQ** to request that the server SHOULD perform PTR updates. (N bit to 1 means no update)

  • A server sets the "N" bit in **DHCP ACK** to indicate whether the server SHALL (0) or SHALL NOT (1) perform DNS updates.

Configure DHCP option 81 FQDN

- Client
  ip ddns update method testing
  ddns both
  int F4
  ip address dhcp
  ip ddns update testing host 10.1.78.7
  ip dhcp client update dns server both → instruct server to update A and PRT
  none → instruct server not to update any
- Server
  ip dhcp update → DHCP server will update RR unless client requests not to
  both → DHCP server will update A and RR unless client requests not to
  both override →DHCP server will update A and RR no matter what
  ip dhcp pool test
  update dns both | never
- http://tools.ietf.org/html/draft-ietf-dhc-fqdn-option-13
- I wouldn't much care this as IOS DHCP can't update windows AD DNS. Only authorized AD DHCP can update DNS.

Troubleshooting DHCP option 81

- Use same debug ip ddns update

  00:19:01: DDNS: Zone name for '10.0.0.11.in-addr.arpa.' is '10.in-addr.arpa'

  00:19:01: DDNS: Using server 10.19.192.32

  00:19:01: DDNS: Dynamic Update 1: (sending to server 10.19.192.32)

  00:19:01: DDNS: Zone = 10.in-addr.arpa

  00:19:01: DDNS: Prerequisite: 10.0.0.11.in-addr.arpa. not in use

  00:19:01: DDNS: Update: add 10.0.0.11.in-addr.arpa. IN PTR canada_reserved.hacks

  00:19:01: DDNS: Zone name for '10.0.0.11.in-addr.arpa.' is '10.in-addr.arpa'

  00:19:01: DDNS: Using server 10.0.0.1

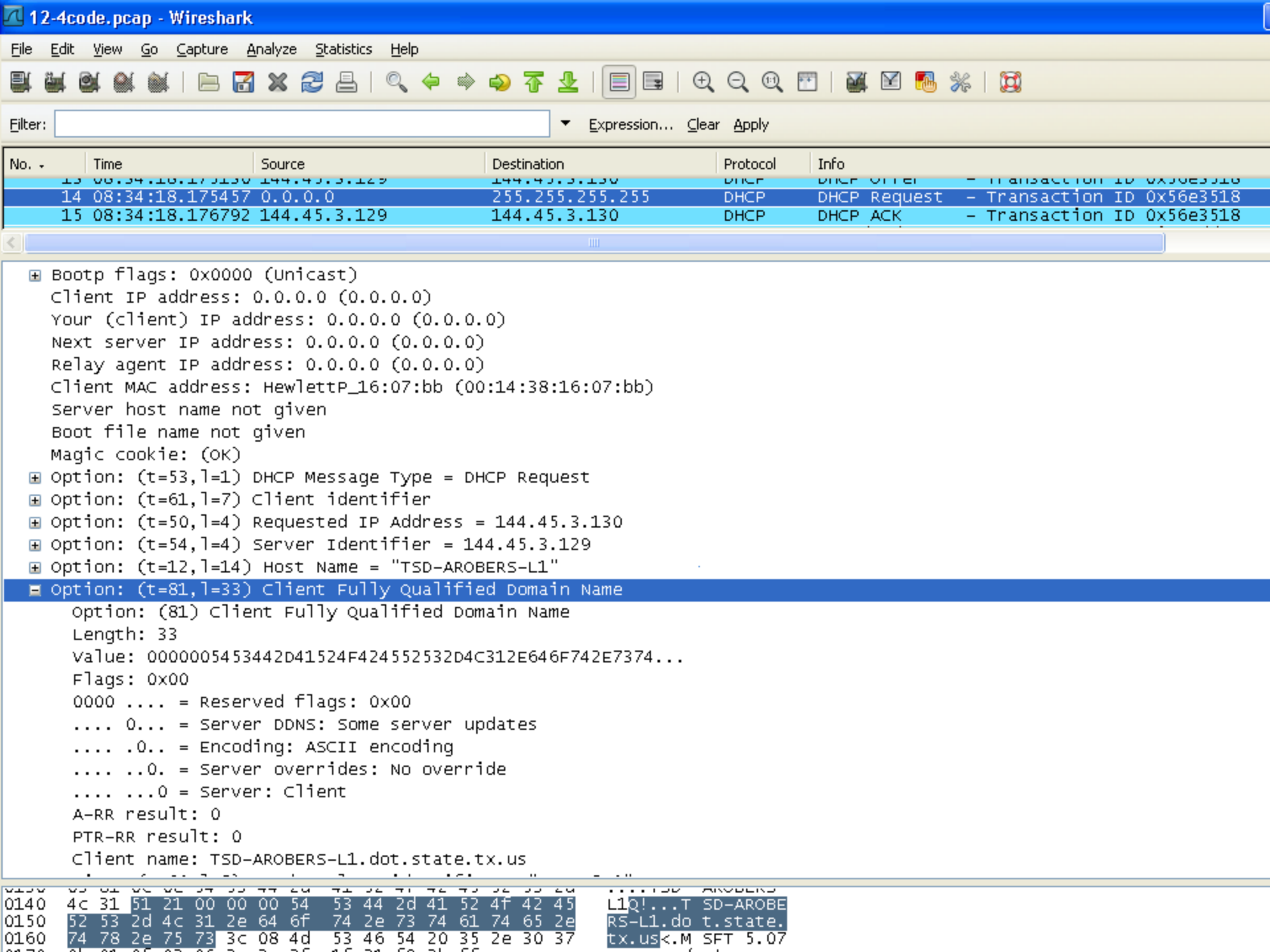
- Venky's case, 609672001

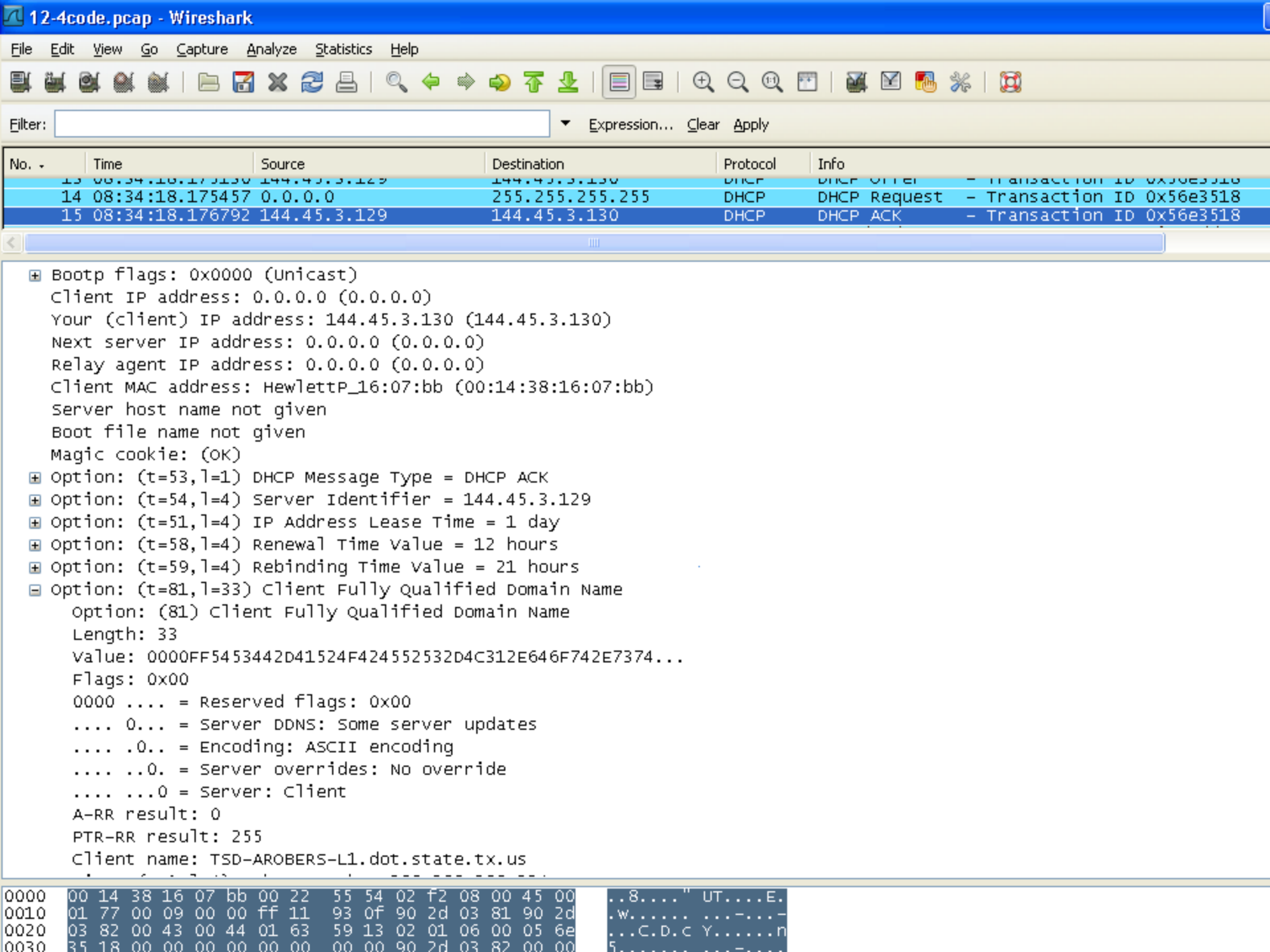
  • CU found PTR record is not updated on DNS after changing to 1811.

  • With no dynamic DNS configured, IOS router sends the DHCP Client a DHCP ACK message with Option 81 with the N flag bit set to 1

  • DHCP Client, Windows Vista, fails to understand this and does not do PTR update as it thinks Server will do it.

  • "update ddns never" under DHCP pool config should make IOS router not send option 81 at all


12-4code.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
14 08:34:18.175457 0.0.0.0 255.255.255.255 DHCP DHCP Request - Transaction ID 0x56e3518
15 08:34:18.176792 144.45.3.129 144.45.3.130 DHCP DHCP ACK - Transaction ID 0x56e3518
Bootp flags: 0x0000 (Unicast)
Client IP address: 0.0.0.0 (0.0.0.0)
Your (client) IP address: 0.0.0.0 (0.0.0.0)
Next server IP address: 0.0.0.0 (0.0.0.0)
Relay agent IP address: 0.0.0.0 (0.0.0.0)
Client MAC address: HewlettP_16:07:bb (00:14:38:16:07:bb)
Server host name not given
Boot file name not given
Magic cookie: (OK)
Option: (t=53,l=1) DHCP Message Type = DHCP Request
Option: (t=61,l=7) Client identifier
Option: (t=50,l=4) Requested IP Address = 144.45.3.130
Option: (t=54,l=4) Server Identifier = 144.45.3.129
Option: (t=12,l=14) Host Name = "TSD-AROBERS-L1"
Option: (t=81,l=33) Client Fully Qualified Domain Name
Option: (81) Client Fully Qualified Domain Name
Length: 33
Value: 0000005453442D41524F424552532D4C312E646F742E7374...
Flags: 0x00
0000 .... = Reserved flags: 0x00
.... 0... = Server DDNS: Some server updates
.... .0.. = Encoding: ASCII encoding
.... ..0. = Server overrides: No override
....0 = Server: Client
A-RR result: 0
PTR-RR result: 0
Client name: TSD-AROBERS-L1.dot.state.tx.us
0140 4c 31 51 21 00 00 00 54 53 44 2d 41 52 4f 42 45 L1Q!...T SD-AROBE
0150 52 53 2d 4c 31 2e 64 6f 74 2e 73 74 61 74 65 2e RS-L1.do t.state.
0160 74 78 2e 75 73 3c 08 4d 53 46 54 20 35 2e 30 37 tx.us<.M SFT 5.07


12-4code.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
14 08:34:18.175457 0.0.0.0 255.255.255.255 DHCP DHCP Request - Transaction ID 0x56e3518
15 08:34:18.176792 144.45.3.129 144.45.3.130 DHCP DHCP ACK - Transaction ID 0x56e3518
Bootp flags: 0x0000 (Unicast)
Client IP address: 0.0.0.0 (0.0.0.0)
Your (client) IP address: 144.45.3.130 (144.45.3.130)
Next server IP address: 0.0.0.0 (0.0.0.0)
Relay agent IP address: 0.0.0.0 (0.0.0.0)
Client MAC address: HewlettP_16:07:bb (00:14:38:16:07:bb)
Server host name not given
Boot file name not given
Magic cookie: (OK)
Option: (t=53,l=1) DHCP Message Type = DHCP ACK
Option: (t=54,l=4) Server Identifier = 144.45.3.129
Option: (t=51,l=4) IP Address Lease Time = 1 day
Option: (t=58,l=4) Renewal Time Value = 12 hours
Option: (t=59,l=4) Rebinding Time Value = 21 hours
Option: (t=81,l=33) Client Fully Qualified Domain Name
Option: (81) Client Fully Qualified Domain Name
Length: 33
Value: 0000FF5453442D41524F424552532D4C312E646F742E7374...
Flags: 0x00
0000 .... = Reserved flags: 0x00
.... 0... = Server DDNS: Some server updates
.... .0.. = Encoding: ASCII encoding
.... ..0. = Server overrides: No override
....0 = Server: Client
A-RR result: 0
PTR-RR result: 255
Client name: TSD-AROBERS-L1.dot.state.tx.us
0000 00 14 38 16 07 bb 00 22 55 54 02 f2 08 00 45 00
0010 01 77 00 09 00 00 ff 11 93 0f 90 2d 03 81 90 2d
0020 03 82 00 43 00 44 01 63 59 13 02 01 06 00 05 6e
0030 35 18 00 00 00 00 00 00 00 00 90 2d 03 82 00 00

DHCP Relay Agent / DHCP option 82

What is DHCP Relay Agent

- One big giant Subnet with one DHCP server, worked fine
- Now, you subnetted your network , can't put DHCP server into all subnets, what should I do for crying users?
- DHCP message are mostly UDP based broadcast
- So, we need a method of forwarding DHCP message to DHCP server located in other subnet
- Ip helper-address x.x.x.x

  Forwards TFTP, DNS, Time, NetBIOS, ND, BOOTP or DHCP packet, or a UDP port specified by the **ip forward-protocol udp**

- R9 f4----------f0 R8 f4----------f0 R7

```
int f4                  int f0                    int f0
  ip add dhcp             ip add 10.1.89.8 /24      ip add 10.1.78.7 /24
                           ip helper-add 10.1.78.7  ip dhcp pool test
                         int f4                      network 10.1.89.0 /24
                           ip add 10.1.78.8 /24      default-router 1.1.1.2
                                                      dns-server 4.2.2.2
```

Troubleshooting → debug ip dchp server packet/event on R3

On Client

*Jun 24 00:42:57.682: DHCP: Received a BOOTREP pkt
*Jun 24 00:42:57.682: DHCP: Scan: Message type: **DHCP Offer**
*Jun 24 00:42:57.682: DHCP: Scan: Server ID Option: 10.1.78.7 = A014E07
*Jun 24 00:42:57.682: DHCP: Scan: Lease Time: 86400
*Jun 24 00:42:57.682: DHCP: Scan: Renewal time: 43200
*Jun 24 00:42:57.682: DHCP: Scan: Rebind time: 75600
*Jun 24 00:42:57.682: DHCP: Scan: Subnet Address Option: 255.255.255.0
*Jun 24 00:42:57.682: DHCP: Scan: Router Option: 10.1.89.8
*Jun 24 00:42:57.682: DHCP: rcvd pkt source: **10.1.89.8**, destination: **255.255.255.255**
*Jun 24 00:42:57.682: UDP sport: 43, dport: 44, length: 308
*Jun 24 00:42:57.682: DHCP op: 2, htype: 1, hlen: 6, hops: 0
*Jun 24 00:42:57.682: DHCP server identifier: 10.1.78.7
*Jun 24 00:42:57.682: xid: DFF, secs: 0, flags: 8000
*Jun 24 00:42:57.682: client: 0.0.0.0, your: 10.1.89.2
*Jun 24 00:42:57.682: srvr: 0.0.0.0, gw: 10.1.89.8
*Jun 24 00:42:57.682: options block length: 60

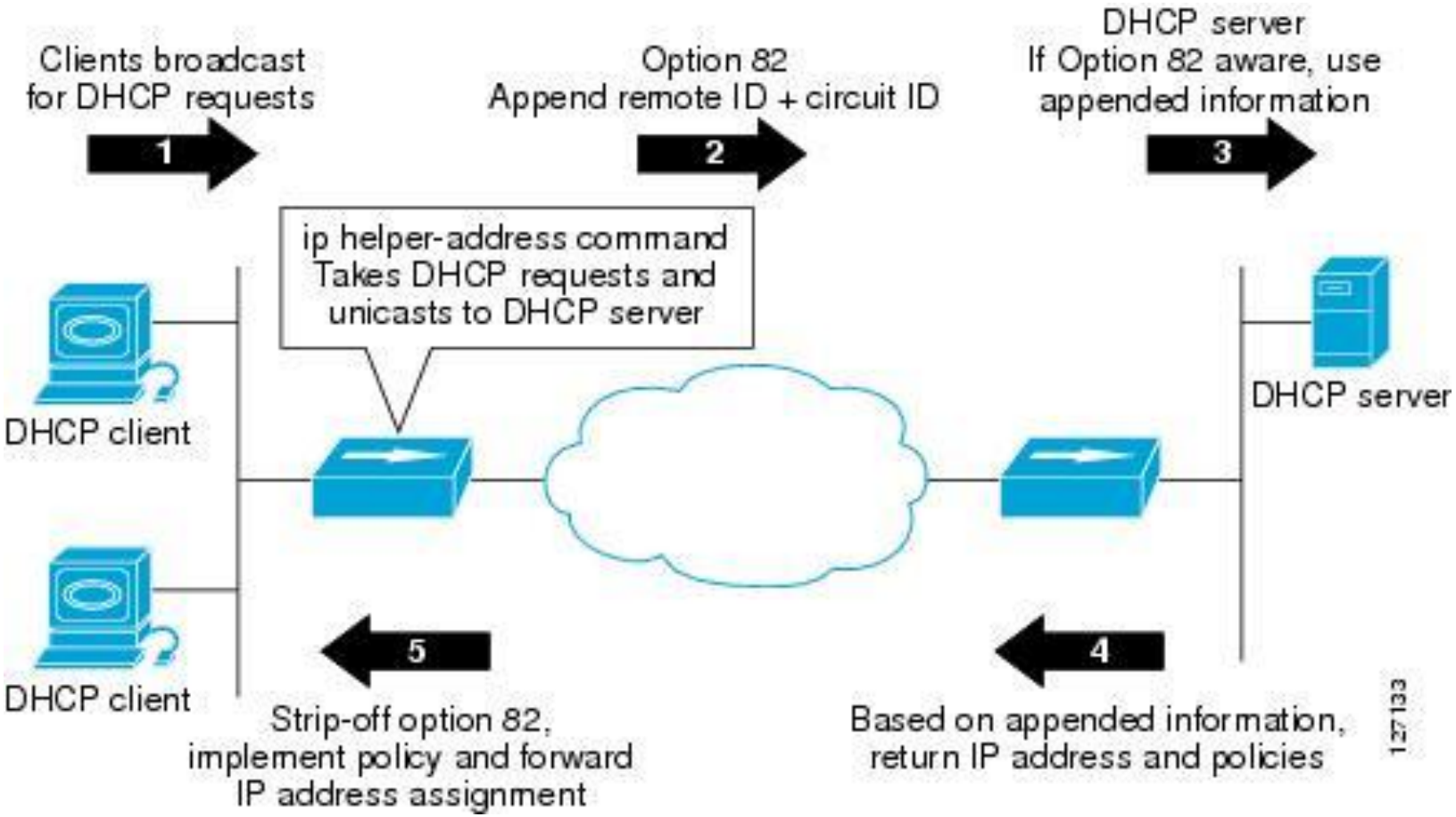
On Server

*Jun 24 00:36:02.046: DHCPD: **DHCPDISCOVER** received from client
0063.6973.636f.2d61.6162.622e.6363.3030.2e36.6430.302d.4574.302f.30 **through relay 10.1.89.8**.
*Jun 24 00:36:02.046: DHCPD: Seeing if there is an internally specified pool class:
*Jun 24 00:36:02.046: DHCPD: htype 1 chaddr aabb.cc00.6d00
*Jun 24 00:36:02.046: DHCPD: remote id 020a00000a014e0710000000
*Jun 24 00:36:02.046: DHCPD: circuit id 00000000
*Jun 24 00:36:02.046: DHCPD: Allocate an address without class information (10.1.89.0)
*Jun 24 00:36:04.058: DHCPD: Adding binding to radix tree (10.1.89.1)
*Jun 24 00:36:04.058: DHCPD: Adding binding to hash tree
*Jun 24 00:36:04.058: DHCPD: assigned IP address 10.1.89.1 to client
0063.6973.636f.2d61.6162.622e.6363.3030.2e36.6430.302d.4574.302f.30.
*Jun 24 00:36:04.058: DHCPD: Sending **DHCPOFFER** to client
0063.6973.636f.2d61.6162.622e.6363.3030.2e36.6430.302d.4574.302f.30 (10.1.89.1).
*Jun 24 00:36:04.058: DHCPD: unicasting BOOTREPLY for **client aabb.cc00.6d00 to relay 10.1.89.8**.
*Jun 24 00:36:04.062: DHCPD: DHCPREQUEST received from client
0063.6973.636f.2d61.6162.622e.6363.3030.2e36.6430.302d.4574.302f.30.

DHCP Option 82

- DHCP Relay Agent make it possible that you put one DHCP server and handles hundreds of subnets for your whole network
- Nice, but it brings one big problem – user identification
- DHCP option 82 is here to say some user-related information to the DHCP server
- DHCP server will use this user-related information to decide which DHCP pool or class to use
- Option 82 has two most used sub options which are
  - “Agent circuit id” sub option
  - “Agent remote id” sub option

DHCP Option 82 + DHCP Relay Agent



1. DHCP client generates a DHCP request and broadcasts it on the network.
2. DHCP relay agent intercepts DHCP request and inserts option 82 in the packet.
3. DHCP relay agent unicasts the DHCP packet to the DHCP server.
4. DHCP server receives packet and uses the suboptions to assign IP and FWD them back to the client.
5. The suboption fields are stripped off of the packet by the relay agent while forwarding to the client.

Config Example

- DHCP SERVER

```
ip dhcp class CLASS1
 relay agent information
  relay-information hex 01030a0b0c02050000000123
  relay-information hex 01030a0b0c02*
ip dhcp class CLASS2
 relay agent information
  relay-information hex 010401020304020202102
ip dhcp pool ABC
 network 10.0.20.0 255.255.255.0
 class CLASS1
  address range 10.0.20.1 10.0.20.100
class CLASS2
  address range 10.0.20.101 10.0.20.200
```

- DHCP Relay Agent

```
ip dhcp relay information option   → Enables the system to insert option 82
int f4
  ip helper-address 10.2.2.2
  ip dhcp relay information option   → automatically adds the circuit /remote id to d option 82
```

Useful PC Tips

- IPCONFIG/ALL – display all IP information, dns, wins, mac-address

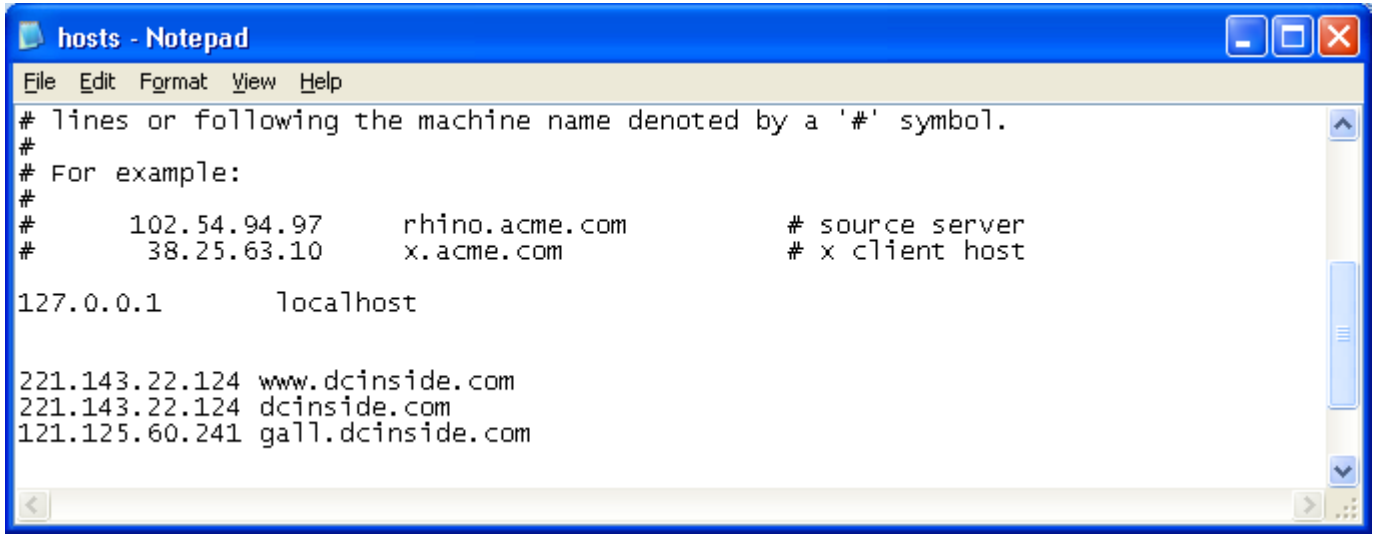
  /Release and Renew – release IP address or renew IP address

  /flushdns – Delete dns resolver cache on PC

  /registerdns - Refreshes all DHCP leases and re-registers DNS names

  /displaydns - Display the contents of the DNS Resolver Cache.

- HOSTS file
  - Manually create DNS Cache in file, the mappings of IP to host names
  - Located C:\windows\system32\drivers\etc\ hosts



- NSLOOKUP TOOL

C:\Documents and Settings\kyukim>**nslookup**
Default Server: dns-sj.cisco.com → your current primary NS server
Address: 171.70.168.183

> www.cisco.com → type any FQDN
Server: dns-sj.cisco.com
Address: 171.70.168.183
Name: origin-www.cisco.com → actual A record
Address: 198.133.219.25
Aliases: www.cisco.com, www.cisco.com.akadns.net

> server 4.2.2.2 → change name server to anyone you want to use
Default Server: vnsc-bak.sys.gtei.net → def server changed from cisco NS to gtei NS
Address: 4.2.2.2
> www.yahoo.com
Server: vnsc-bak.sys.gtei.net
Address: 4.2.2.2
Non-authoritative answer: → meaning GTEI NS is not owner
Name: www-real.wa1.b.yahoo.com
Address: 209.131.36.158
Aliases: www.yahoo.com, www.wa1.b.yahoo.com

> set type=mx → change search type to MX, (ex. A,ANY,CNAME,MX,NS,PTR,SOA,SRV)
> cisco.com
Server: vnsc-bak.sys.gtei.net
Address: 4.2.2.2
Non-authoritative answer:
cisco.com MX preference = 10, mail exchanger = sj-inbound-d.cisco.com
cisco.com MX preference = 10, mail exchanger = sj-inbound-e.cisco.com
cisco.com MX preference = 10, mail exchanger = sj-inbound-f.cisco.com
cisco.com MX preference = 15, mail exchanger = rtp-mx-01.cisco.com


CISCO