



**ICS361 :10.0**

# **Data Communications and Networking**

Lecturer: Toby Daniel

# Network Services

- DHCP
- DNS
- SNMP

# DHCP

## Dynamic Host Configuration Protocol

- DHCP is a means to configure TCP/IP settings on computers from a central server.
- Without DHCP every computer on a TCP/IP network has to have the IP address information configured manually.
  - Dynamic = can be changed on demand
  - Host = any computer/node on the network
  - Configuration = the TCP/IP settings
  - Protocol = standard rules to allow dynamic settings

# Why do we need DHCP?

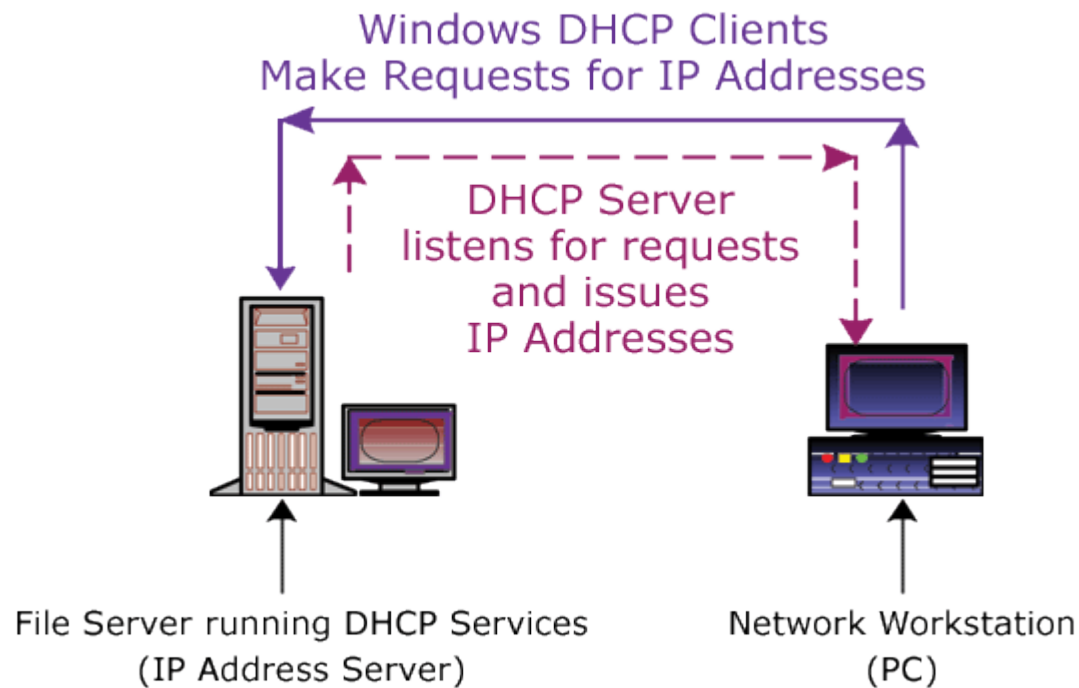
- What reasons can you think of for having a dynamic and central place to configure IP information?
- What type of networks would use DHCP?



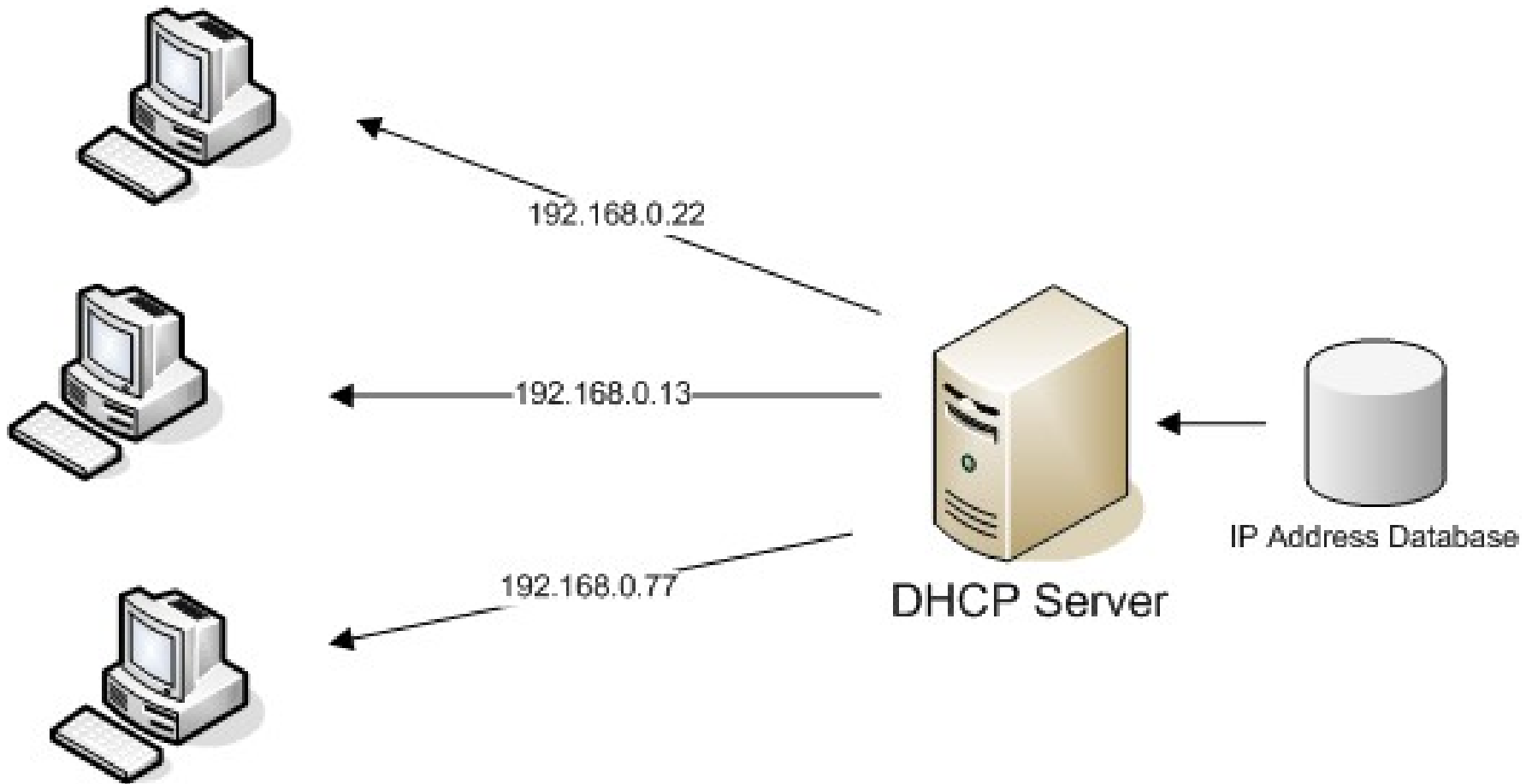
# DHCP

DHCP requires the following:

- specialized server (DHCP services server)
- a communications protocol (DHCP)
- a client application (DHCP client)



# DHCP



# How DHCP works..

- The DHCP client is responsible for requesting an IP address from any available DHCP server.
- DHCP clients are built into all common NOS.
- If the user would like to obtain an IP address automatically, they just have to configure their computer to use DHCP.
- The DHCP server has to be configured to give out the correct IP information.

# Configuring a Windows DHCP client

**Internet Protocol (TCP/IP) Properties** [?] [X]

**General**

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

Obtain an IP address automatically

Use the following IP address:

IP address: [ . . . ]

Subnet mask: [ . . . ]

Default gateway: [ . . . ]

Obtain DNS server address automatically

Use the following DNS server addresses:

Preferred DNS server: [ 128 . 101 . 101 . 101 ]

Alternate DNS server: [ 134 . 84 . 84 . 84 ]

[ Advanced... ]

[ OK ] [ Cancel ]

# Dynamic Address Allocation

- Using dynamic allocation the DHCP server assigns an IP address to a requesting client on a **temporary** basis.
- The IP address is **leased** to the DHCP client for a specified duration of time.
- When this lease expires, the IP address is **revoked** from the client and the client is required to stop using the address.
- If the DHCP client still needs an IP address to perform its functions, it can request another IP address.

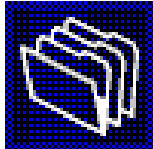
# DHCP Server

- The DHCP server is configured with a range or **scope** of IP addresses that it can lease to the clients.
- DHCP also configures the IP information about the:
  - subnet mask
  - default gateway
  - DNS servers that the client should use.
- Along with the scope of IP addresses there will also be the **lease duration** of each IP address.

# DHCP Server Scope Configuration

**New Scope Wizard**

**IP Address Range**  
You define the scope address range by identifying a set of consecutive IP addresses.



Enter the range of addresses that the scope distributes.

Start IP address:

End IP address:

A subnet mask defines how many bits of an IP address to use for the network/subnet IDs and how many bits to use for the host ID. You can specify the subnet mask by length or as an IP address.

Length:

Subnet mask:

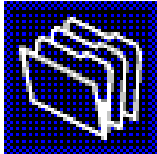
< Back      Next >      Cancel

# DHCP Server Lease Duration

**New Scope Wizard**

**Lease Duration**

The lease duration specifies how long a client can use an IP address from this scope.



Lease durations should typically be equal to the average time the computer is connected to the same physical network. For mobile networks that consist mainly of portable computers or dial-up clients, shorter lease durations can be useful. Likewise, for a stable network that consists mainly of desktop computers at fixed locations, longer lease durations are more appropriate.

Set the duration for scope leases when distributed by this server.

Limited to:

Days:

Hours:

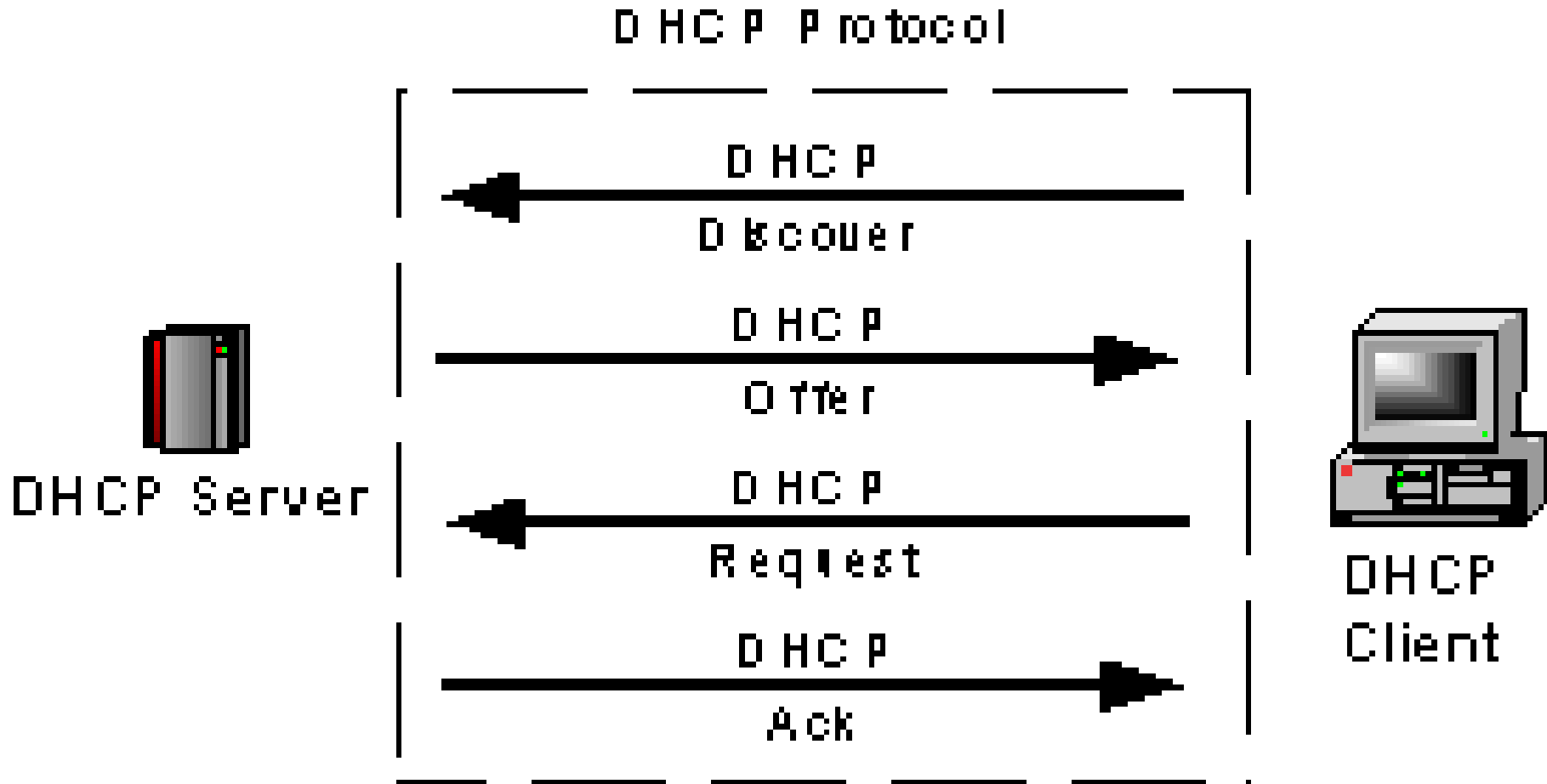
Minutes:

< Back    Next >    Cancel

# The DHCP Handshake

- To use DHCP to get an IP address the client and server have to go through a four step process:
  1. DHCP Discover
  2. DHCP Offer
  3. DHCP Request
  4. DHCP Ack

# DHCP Handshake



# 1. DHCP Discover

- Clients try to find a DHCP server on the network.
- Remember, the client does not have an IP address yet, so it must use a broadcast request using its MAC address to identify itself.

## 2. DHCP Offer

- Any DHCP server that receives this message makes a decision on whether to respond.
- The DHCP server will check its IP scope and make a temporary IP address assignment.
- It will respond with an offer of the new IP address to the client.
- It will also contain other IP address information (lease duration, subnet mask, default gateway, dns)

# 3. DHCP Request

- The client will then make a formal request to the DHCP server for the IP address.

# 4. DHCP Ack

- The server will then respond with an acknowledgement:

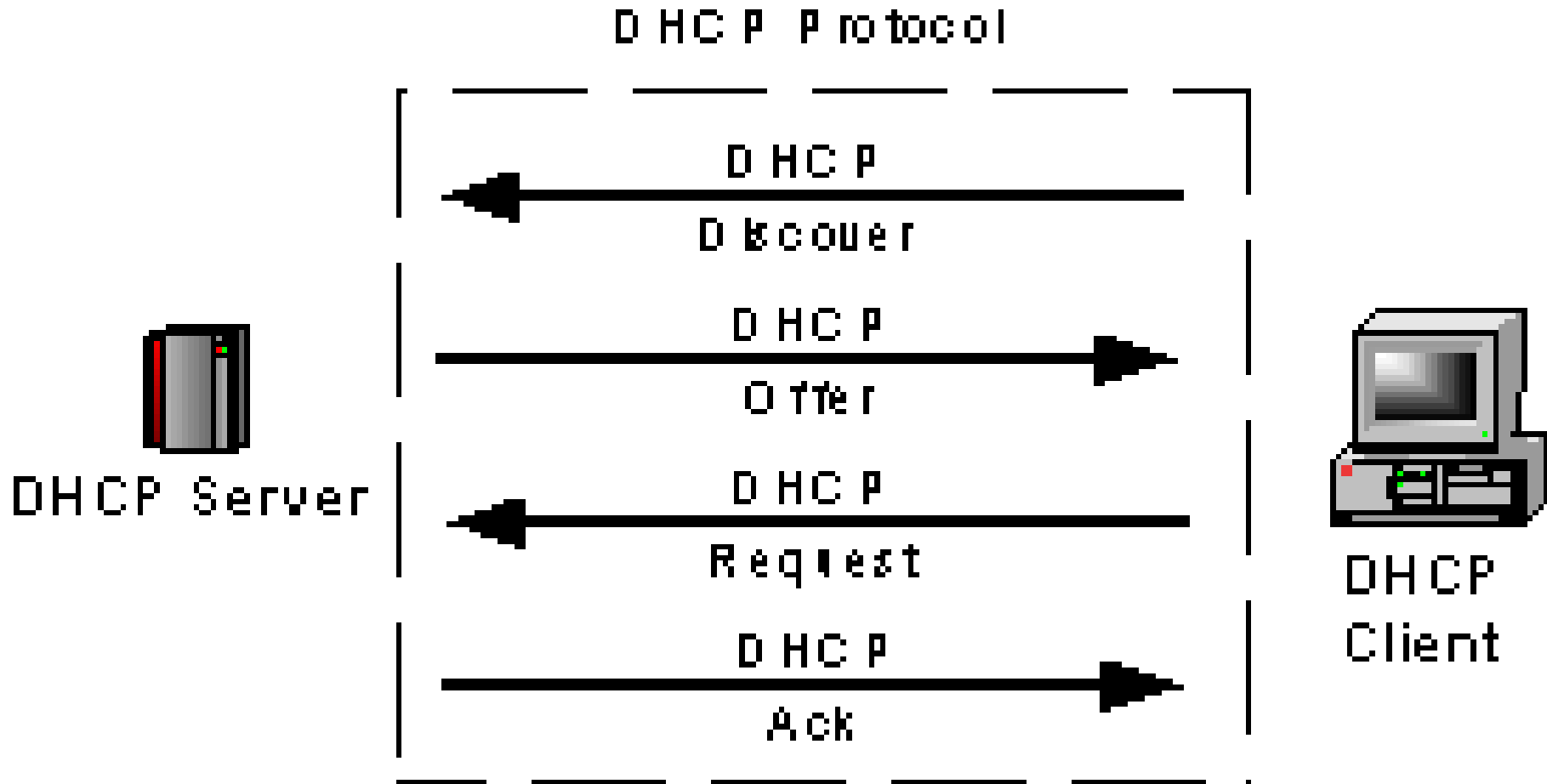
Ack (yes)

or

NAck (no)

- and give it a lease duration.

# DHCP Handshake



# Additional Server Configuration

## Exclusions

- Some hosts on the network might need to have a static IP address that is configured by hand (web servers, DHCP servers, DNS servers etc)
- The DHCP scope should include these IP addresses as **exclusions** – IP address that are excluded from those that are handed out.

# Additional Server Configuration

## Reservations

- Just as some Hosts might need to be manually configured, others might need to use the same IP address every time.
- DHCP servers can configure **reservations**, where an IP address is reserved for use by a specified computer.
- Each time that computer uses DHCP it will get its reserved IP address.

# Creating a DHCP reservation

The image shows a 'New Reservation' dialog box with a title bar containing a question mark and a close button. The main area contains the following fields and options:

- Instruction: Provide information for a reserved client.
- Reservation name: [Empty text box]
- IP address: [192 . 168 . .]
- MAC address: [Empty text box]
- Description: [Empty text box]
- Supported types section with three radio buttons:
  - Both
  - DHCP only
  - BOOTP only

At the bottom right, there are two buttons: 'Add' and 'Close'.

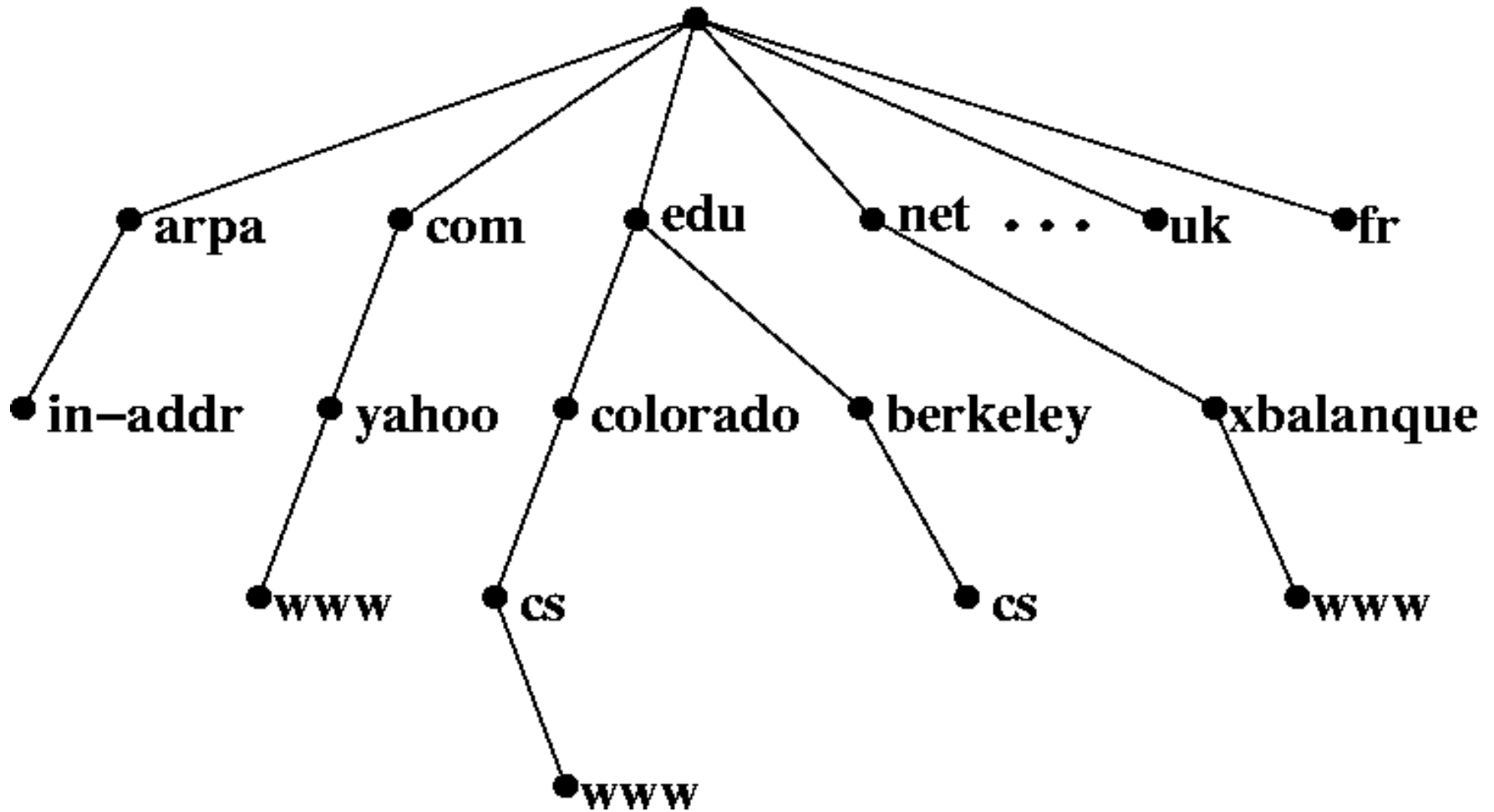
# DHCP Lease Duration

Imagine you are setting up DHCP on a LAN.

- What lease duration would you use for office desktop computers that are connected using Ethernet cables?
- What lease duration would you use for personal laptop computers that employees connect using WiFi?



# DNS

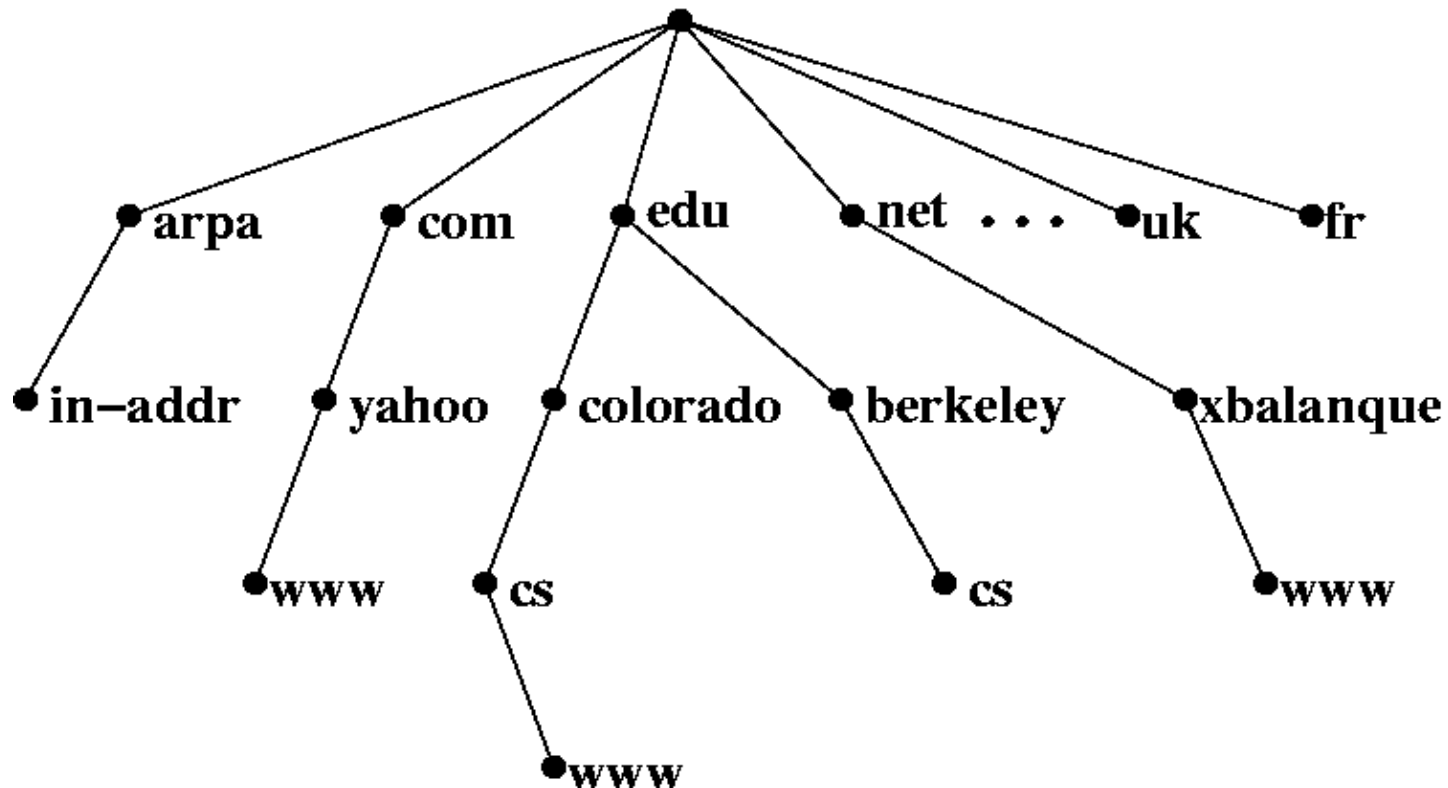


# Domain Name System

- DNS is a system for converting host names and domain names into IP addresses on the Internet or on local networks that use the TCP/IP protocol.
- For example, when a Web site address is given to the DNS either by typing a URL in a browser or behind the scenes from one application to another, DNS servers return the IP address of the server associated with that name.

# DNS

- The DNS system is a hierarchy of database servers that start with the root servers for all the top level domains

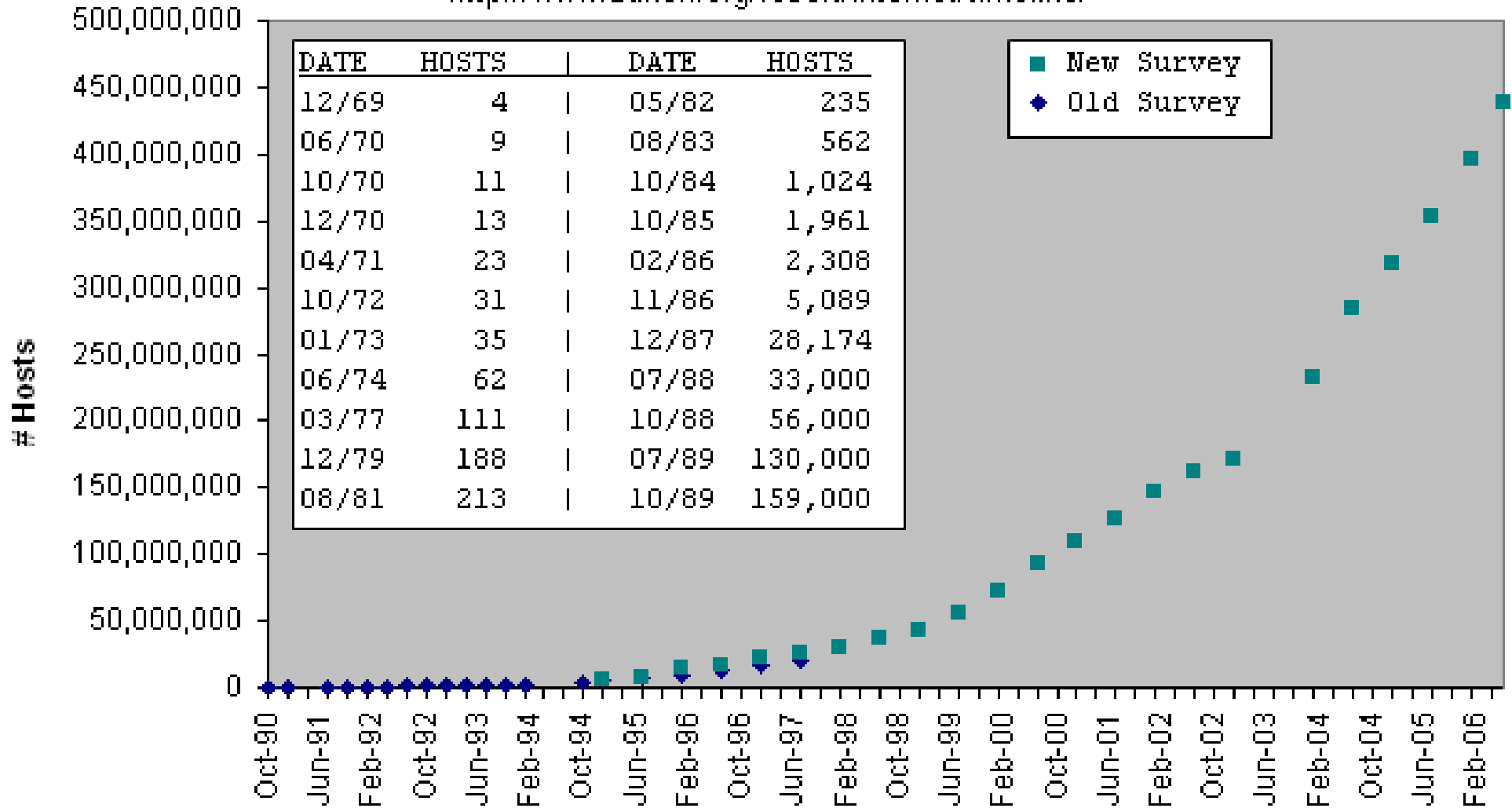


# Brief History of DNS

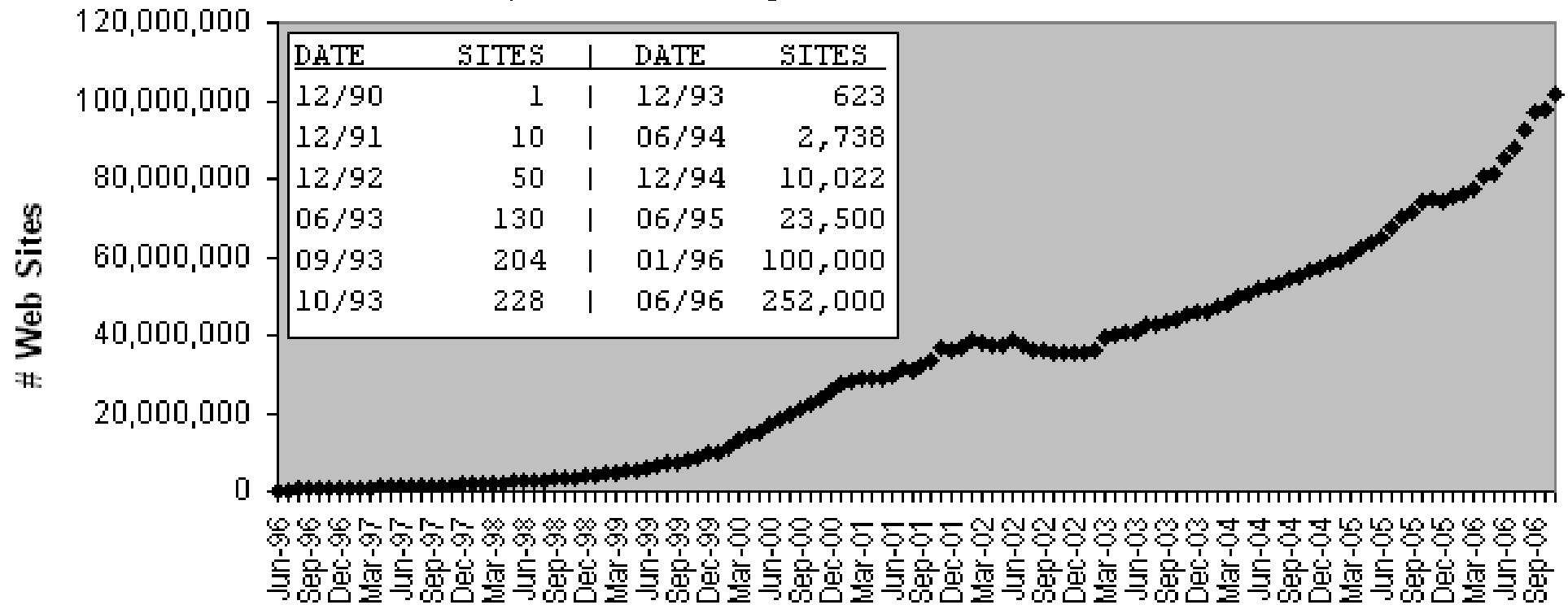
- The Domain Name System was proposed in the early 80's to address the problem of name resolution.
- Prior to the middle 1980's all machines connected to the “Internet” used a common HOSTS.TXT file that provided all the hostnames and addresses in use.
- The file was flat and hostnames had to be unique in the file. As the number of hosts attached to the internet began to grow at an increasing rate, the central HOSTS.TXT file became more and more of a problem.

Hobbes' Internet Timeline Copyright ©2006 Robert H Zakon

<http://www.zakon.org/robert/internet/timeline/>



Hobbes' Internet Timeline Copyright ©2006 Robert H Zakon  
<http://www.zakon.org/robert/internet/timeline/>



# A Globally Distributed Database

- No single machine stores all the data.
- This solves both the **large hosts file** problem AND the **single machine bottleneck** problem
- Individual organizations are responsible for their own portion of the database.
- Special forwarding information is needed to connect the various portions of the name space.

# Fully-Qualified Domain Names (FQDNs)

- Each node name from a leaf node to the root within the DNS is concatenated with dots.

ic.payap.ac.th

- Officially, the root node has a name of the NULL string:

ic.payap.ac.th.NULL

- There can be a maximum of 127 nodes in an FQDN.

# DNS Queries

- DNS Clients contact local DNS Name Servers for host address resolution.
- These queries specify a hostname or IP address and expect the opposite value in return
- Local DNS Servers may be authoritative for local names and addresses.
- If they are, they respond directly to the queries with the relevant answers.
- All other queries must be re-transmitted to name servers that are authoritative for the information requested.

# Recursive Queries

- Recursive Queries are made by clients.
- The client makes a query and expects an answer or an error returned back.
- These queries are called recursive because it is expected that if the name server contacted doesn't already know the answer, then it will ask some other name servers until it gets the answer.
- DNS Servers listen on TCP port 53

# Non-recursive Queries / Referrals

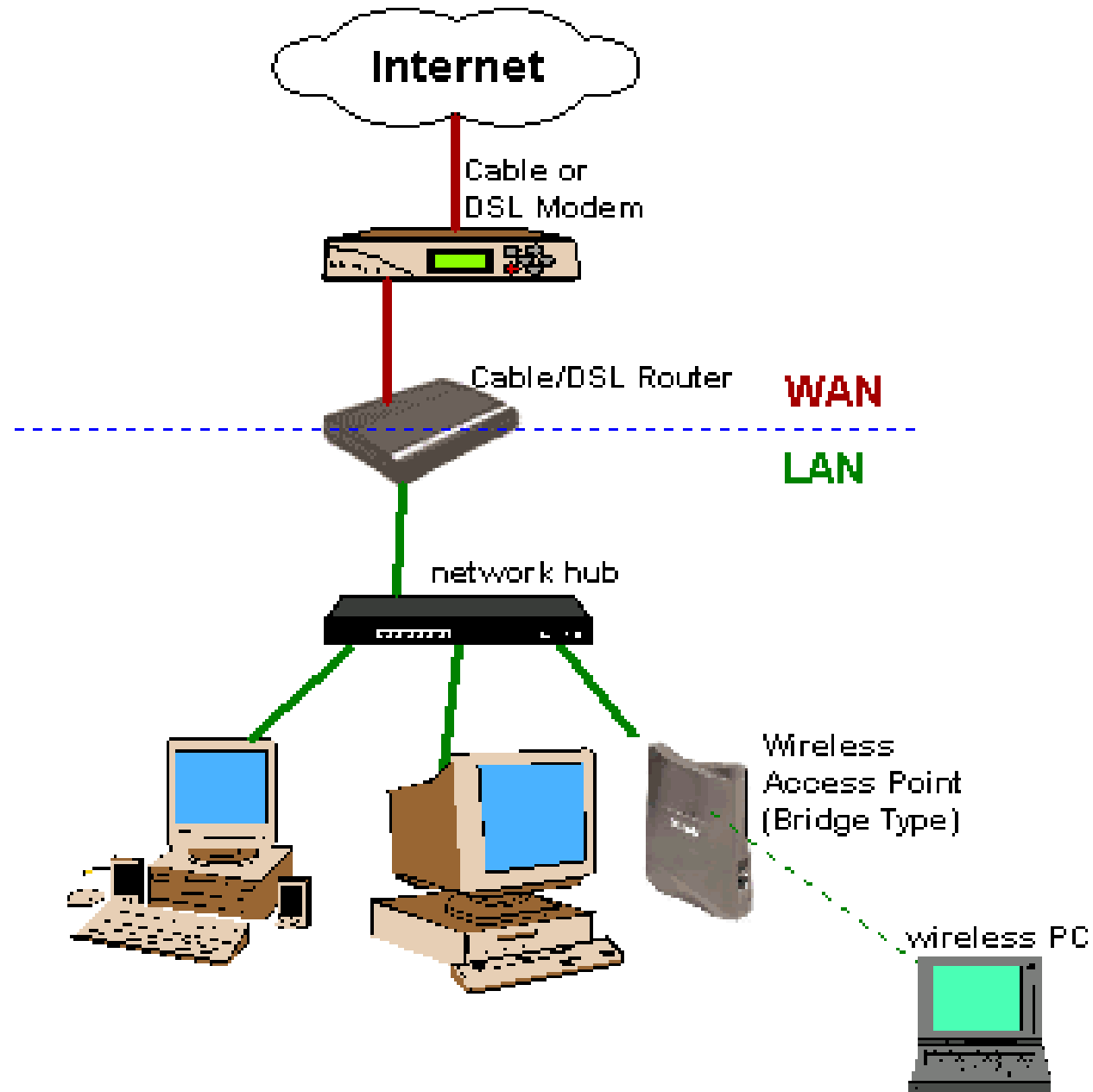
- Non-recursive queries are made by DNS Servers.
- Instead of an answer to their query the name server may get a **referral**.
- A referral means “I don't know the answer, but here is the address of a name server that might know”.
- The name server then follows the referral and sends its query to the indicated address.

# nslookup

- The `nslookup` command is used to retrieve Resource Records (RRs) from DNS servers.

```
nslookup domainname
```

# SNMP



# SNMP

- The Simple Network Management Protocol (SNMP) forms part of the TCP/IP protocol suite.
- SNMP is used in network management systems to monitor network-attached devices.
- By using SNMP network administrators can more easily manage network performance, find and solve network problems, and plan for network growth.

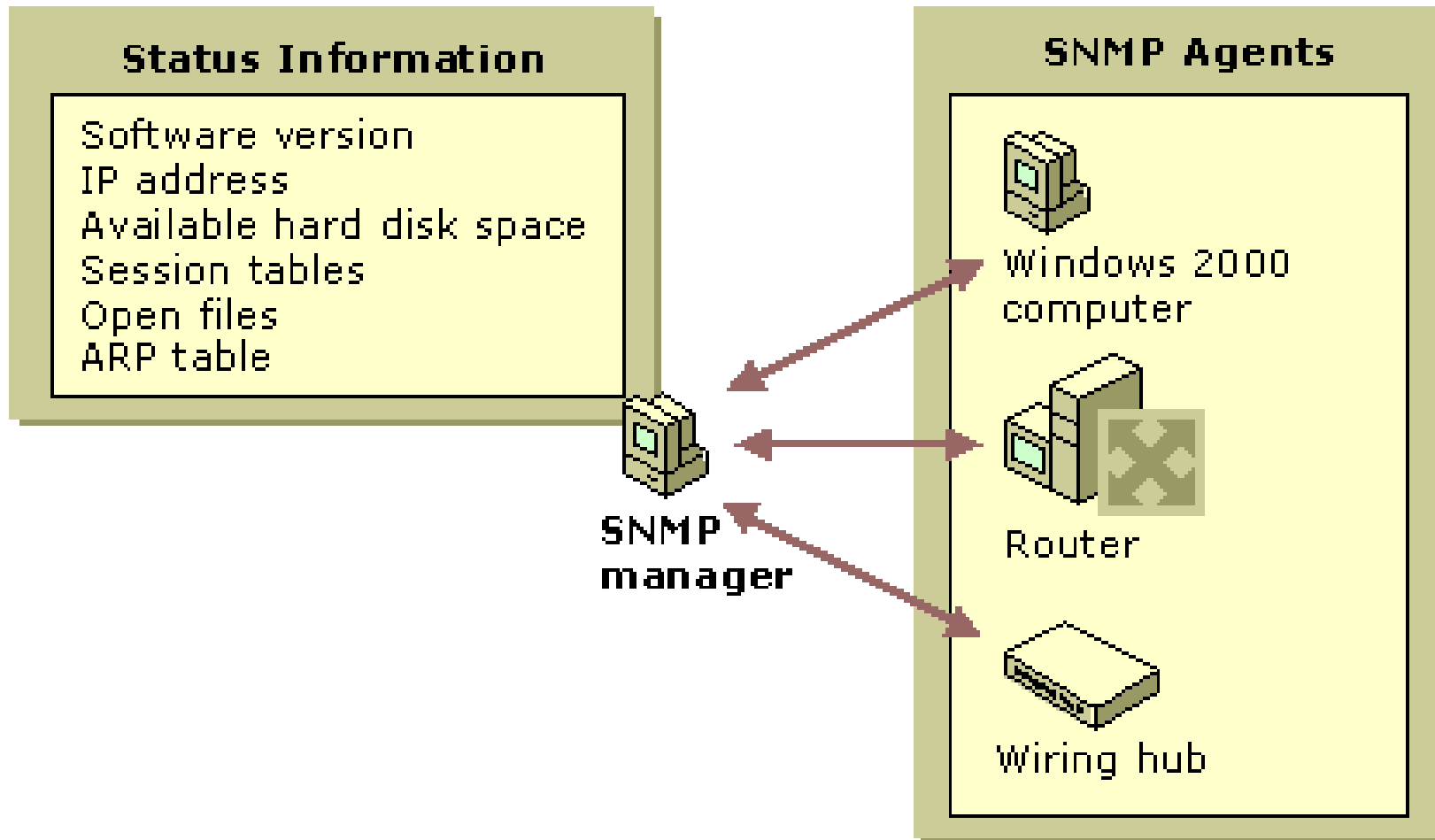
# SNMP

- SNMP is used to report on the performance of network components and can give information such as:
  - system name
  - free memory
  - running processes
  - default route
  - packets per second
  - network error rates
- For: workstations, servers, routers, bridges, hubs.

# How SNMP works..

- SNMP is based on the manager/agent model consisting of:
  - an SNMP manager
  - an SNMP agent
  - a database of management information
  - managed SNMP devices
  - network protocol

# SNMP



# SNMP Messages

- SNMP uses five basic messages:
  - GET
  - GET-NEXT
  - GET-RESPONSE
  - SET
  - TRAP

to communicate between the SNMP manager and the SNMP agent.

# GET & GET-NEXT

- The GET and GET-NEXT messages allow the manager to request information for a specific variable.
- The agent, upon receiving a GET or GET-NEXT message, will issue a GET-RESPONSE message to the SNMP manager with either the information requested or an error indication as to why the request cannot be processed.

# SET

- A SET message allows the SNMP manager to request a change be made to the value of a specific variable.
- The SNMP agent will then respond with a GET-RESPONSE message indicating the change has been made or an error indication as to why the change cannot be made.

# TRAP

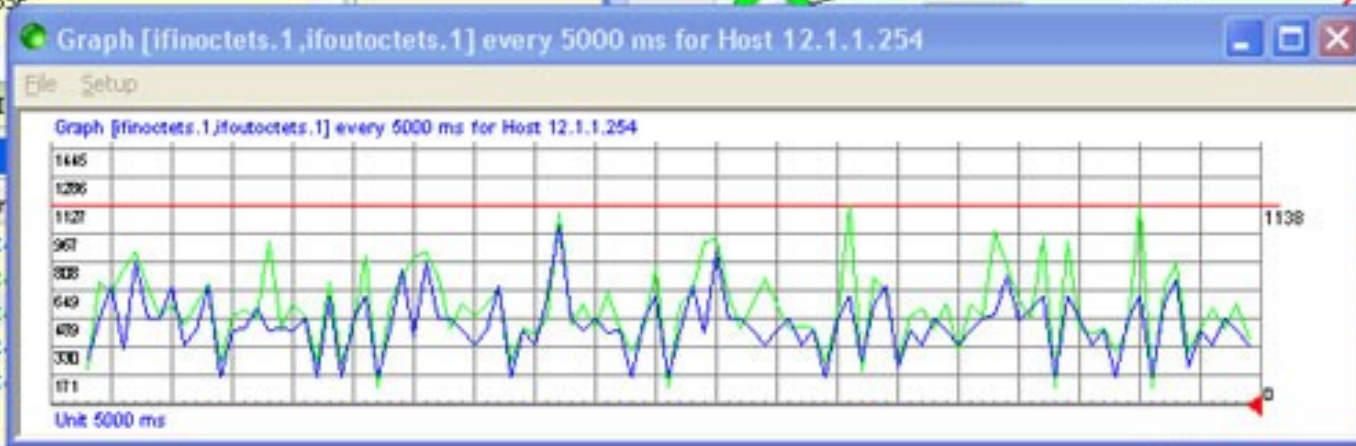
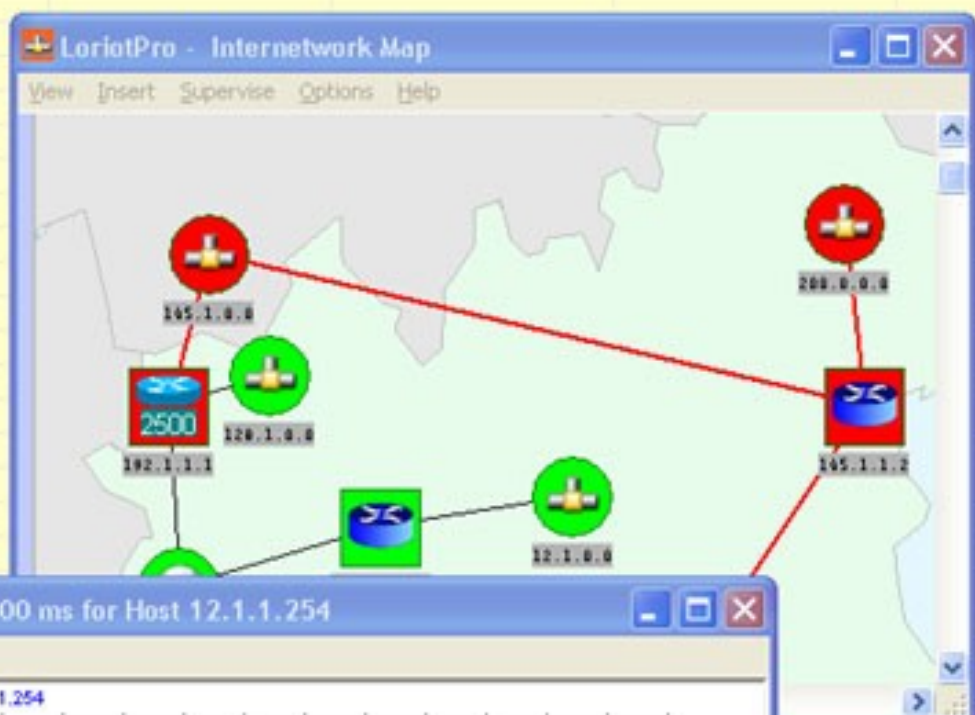
- The SNMP TRAP message allows the agent to spontaneously inform the SNMP manager of an "important" event.



World

- LoriotPro
  - MyOrganisation
    - Local\_Network\_12.1.0.0
      - MEDUSE
        - Active View - noName [C:\LOR...
        - Interface Monitor : MEDUSE 12
        - plug-in/interfacemonitor.:
        - Poll Host [12.1.1.254:80] Stop
        - Graph [ifinocets.1,ifoutocets...
        - plug-in/loriotgraphcounte
      - TITAN
      - ULYSSE

Agent Name	IP address	SysName	SysObjectID	Mac Address
Health Control Center	[Just DClick one contain...			



Events

TimeStamp	Loc
▲ Fri Sep 16 11:47:16 2...	Loc
▲ Fri Sep 16 11:47:16 2...	Loc
▲ Fri Sep 16 11:45:15 2...	Loc
▲ Fri Sep 16 11:45:14 2...	Loc
▲ Fri Sep 16 11:45:13 2...	Loc