Microsoft Networking

Hussain Ali
hussain@ccse.kfupm.edu.sa
Department of Computer Engineering

M. Ghouseuddin
mghouse@ccse.kfupm.edu.sa
Department of Information & Computer Science

KFUPM, Dhahran, Saudi Arabia

Overview

- Windows NT Vs windows 95/98
- Network administration models
  - » Windows NT domains
  - » Workgroups
- Network subsystem
  - » Network services
  - » Protocols supported
- Network information services
  - » Computer browser
  - » DHCP
  - » DNS

dows NT VS Windows 95/98

Windows NT

- Supports multiprocessing
- Supports preemptive multitasking
- File level security
- Applications run in their own address space
- True 32 bit OS
- No plug & play support

Windows 95/98

- No multiprocessing support
- Interrupt driven multitasking
- No file level security
- Shared address space
- Contains some 16 bit code
- Plug & play support
- More hardware support

Common Features

- Same user interface
- Some Common applications

Workgroups and Domains

- Workgroup
  - » Is a logical grouping in which each computer :
  - » Is managed separately and has separate accounts
  - » Has per computer sharing and security policies
  - » User and share level security
- Domain
  - » Is a logical grouping in which there is a centralized accounts and security database, managed by a domain controller
  - » Management is centralized
  - » Users and machines both have accounts in the domain i.E you can control by granting or denying permissions in a centralized manner

Protocols Supported

- Windows 95, 98 and NT support following protocols by default
- TCP/IP
- IPX/SPX
- NetBEUI

- DLC (for printing purposes only)

mportant Network Services

Some important information exchange utilities of Windows NT

- Computer Browser
- Dynamic host configuration protocol (DHCP)
- Domain name system (DNS) for TCP/IP
- Dynamic DNS (DDNS)

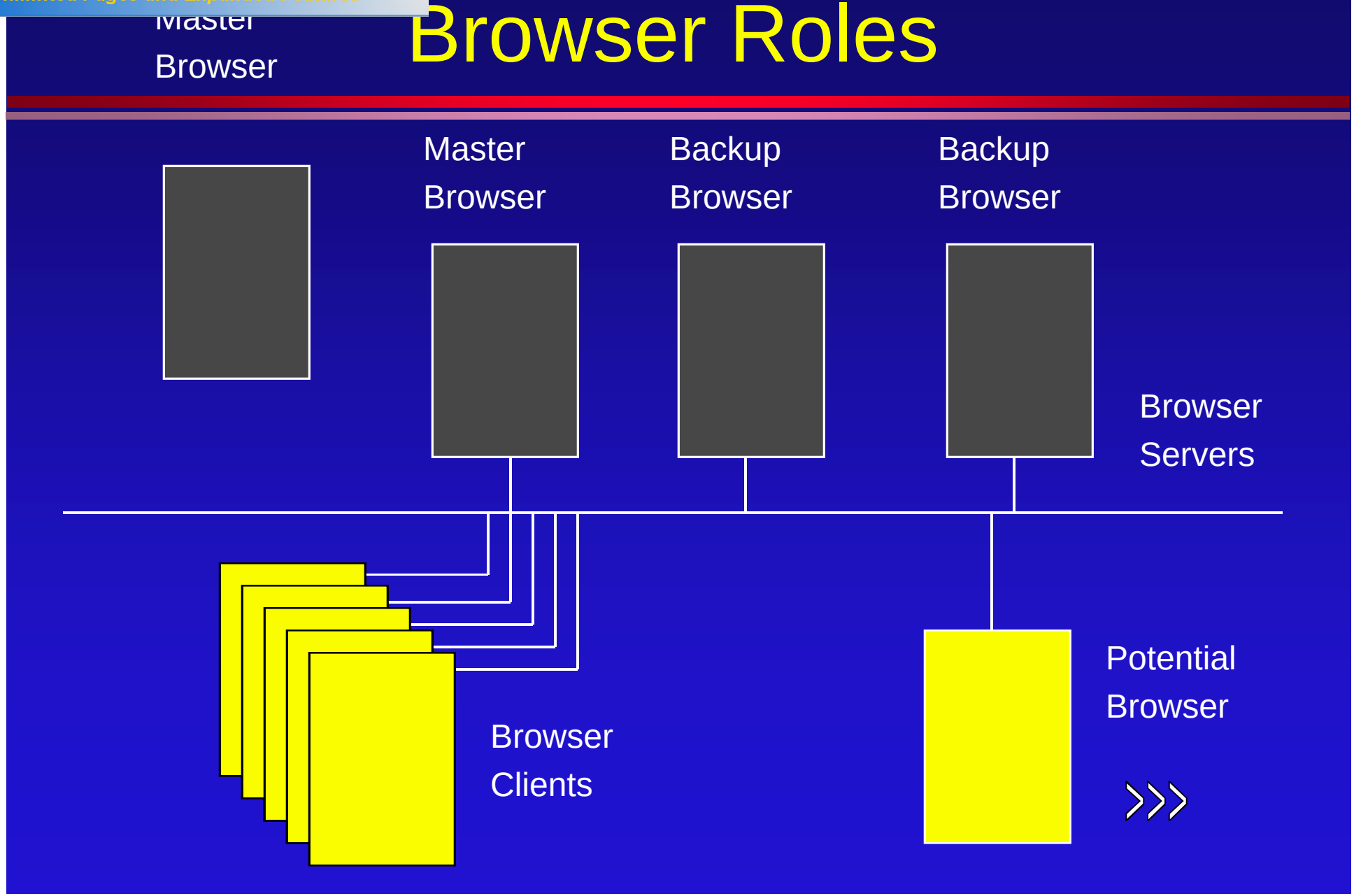
Browser Overview

- Browsing is a Windows default resource information system
- Resource database is maintained on a computer called a Master Browser. The database is called a *browse list*
- Each subnet must have its own (single) Master Browser at all times
- Master Browser is elected through an election process

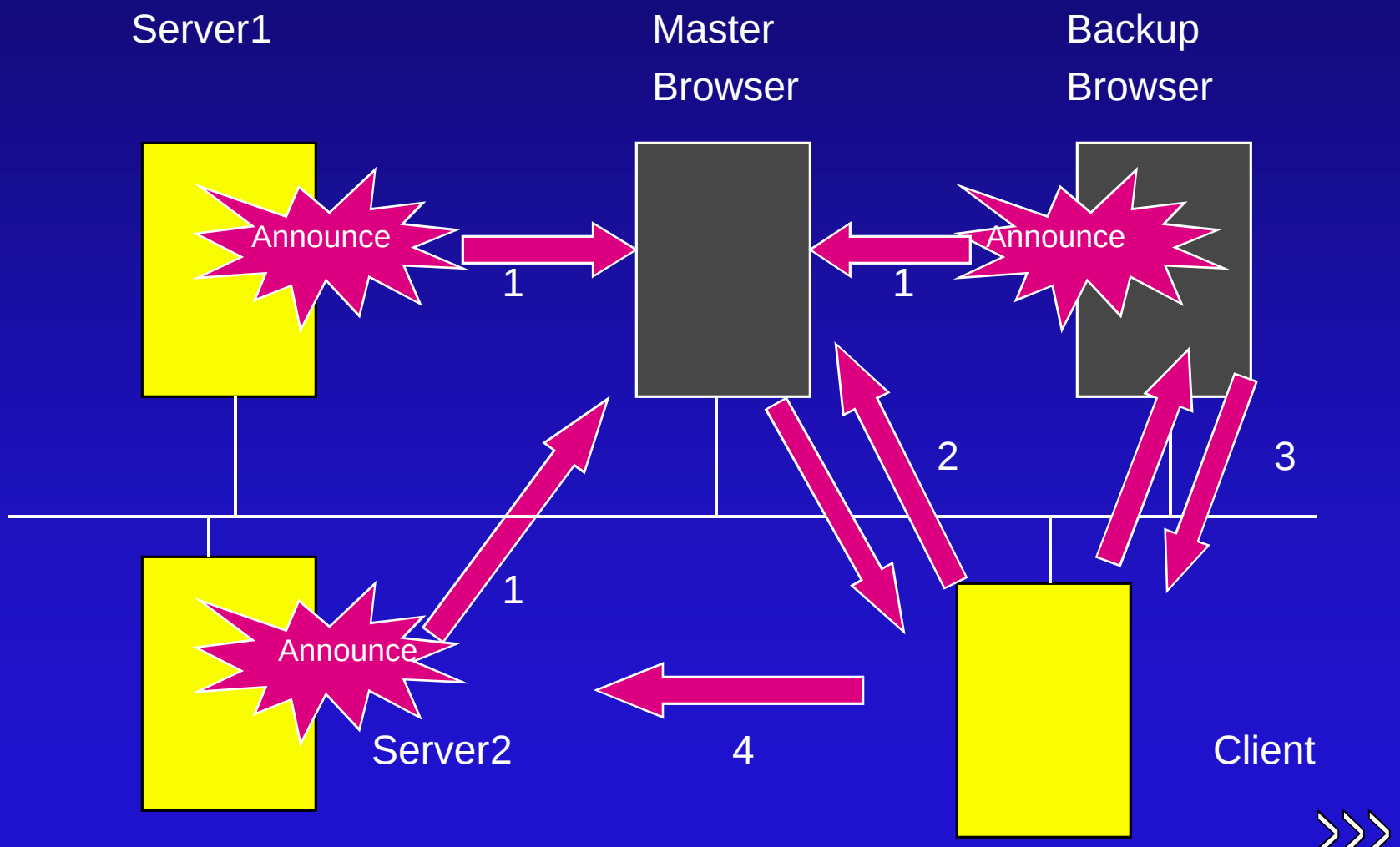
Advantages

- Reduces network traffic.
- Reduces CPU workload.
- Improves network performance.

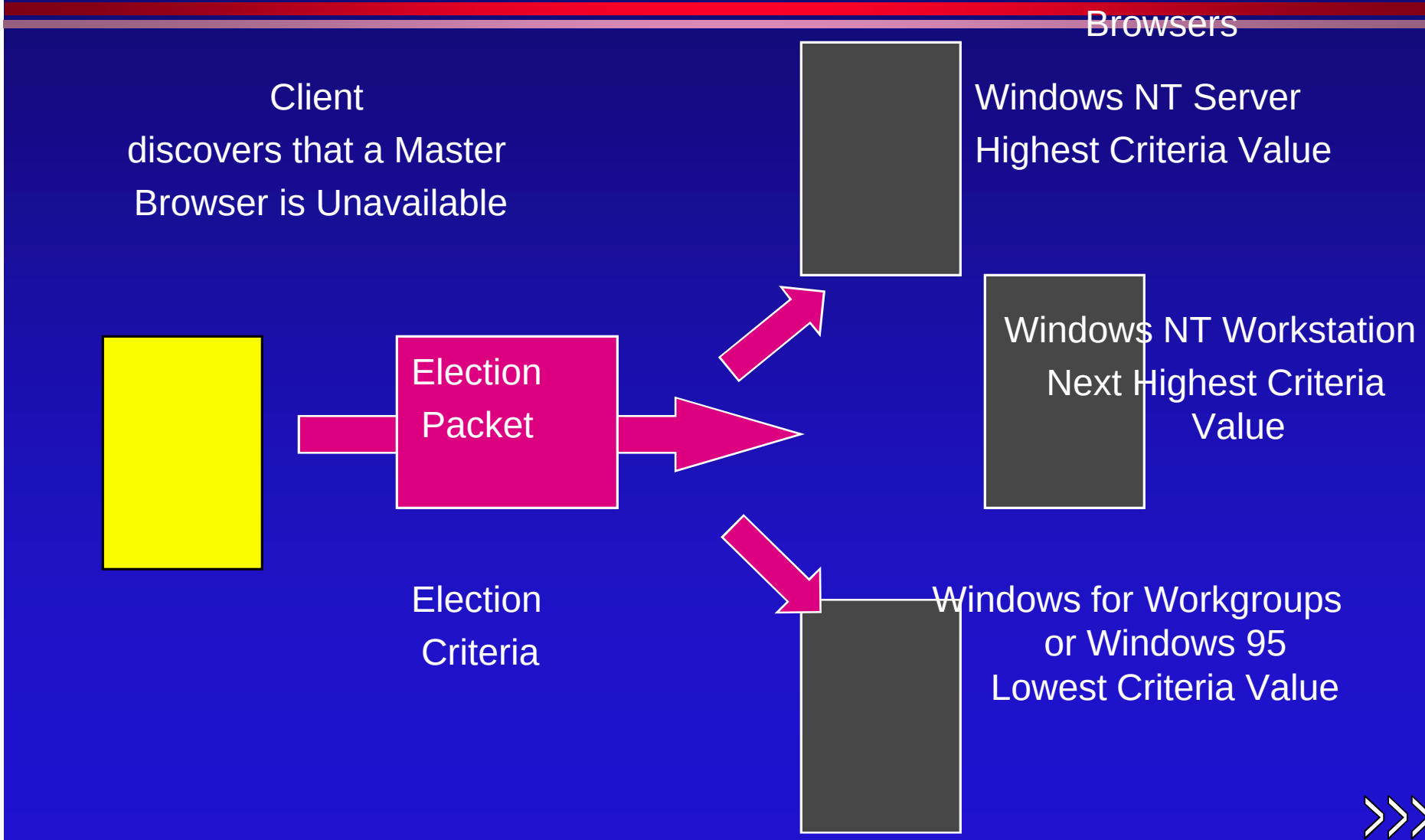
Browser Roles



Browse Process



Browser Election



Browser Criteria

- It determines the hierarchical order of the different types of computer systems in the workgroup or domain. The criteria includes:
  - The operating system like NT server, NT workstations, 95 or Windows for Workgroups
  - The operating system version
  - The configured role in the browsing environment like master, backup, potential, non browser etc

In Windows NT computers the browsing function is configurable

WINS Overview

WINS Server can only run on a computer running Windows NT, with TCP/IP installed

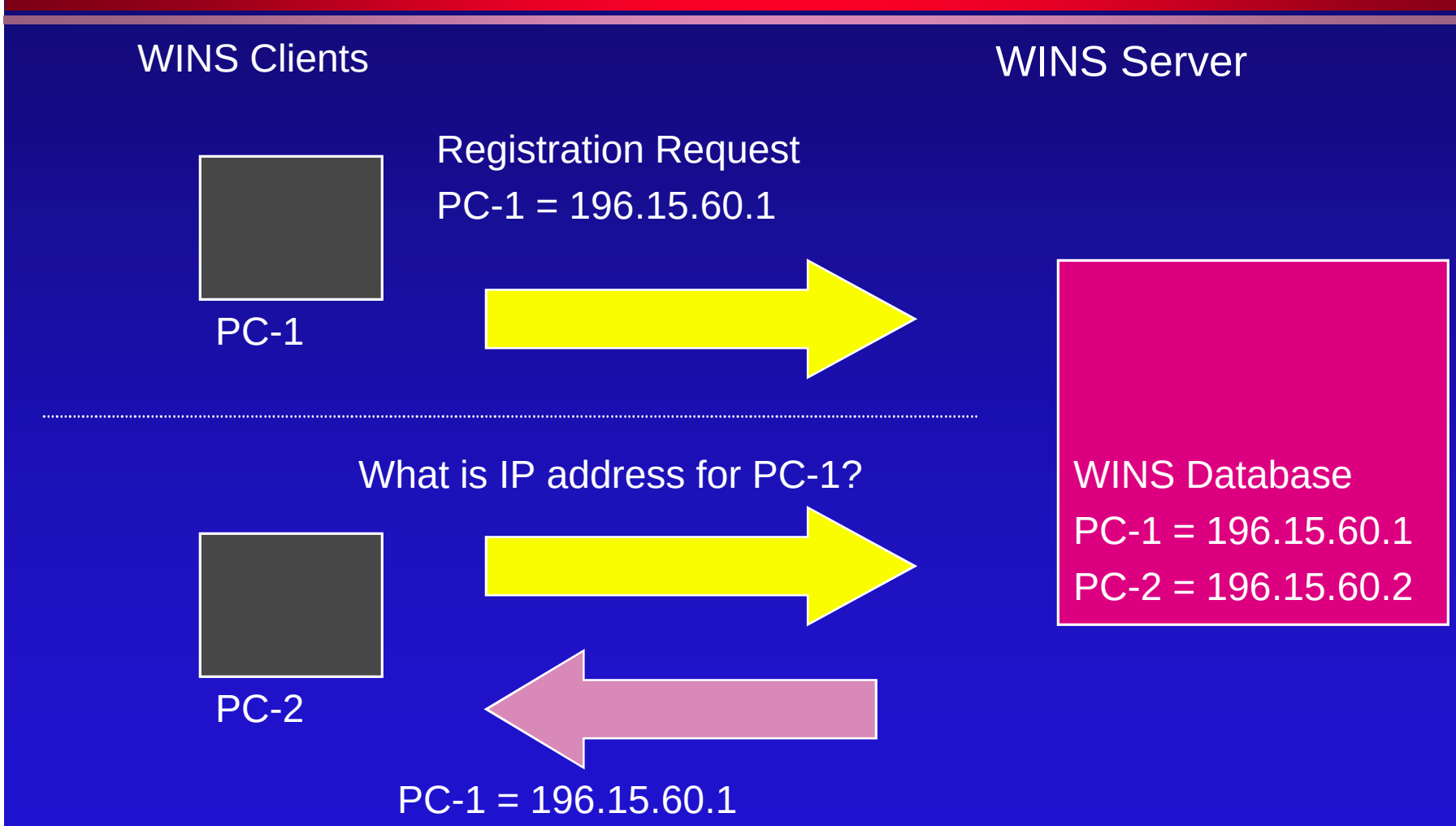
- WINS Server
  - » Maintains a dynamic database that maps the NetBIOS computer names of WINS clients to their IP addresses
  - » Handles name registration and queries
  - » resolves NetBIOS computer names to IP addresses

- WINS clients
  - » At system startup WINS clients, register their computer names and IP addresses with the WINS server

WINS Overview

- Windows-based WINS enabled networking clients can directly access WINS service.
- Non-WINS computers use may use WINS proxies.

WINS Overview



WINS Operation

- Each time a WINS client is started, it registers its NetBIOS name/IP address mapping with a designated WINS server.
- When a client initiates a NetBIOS command to communicate with another host, the name query is directly sent to the WINS server .
- If the server finds a NetBIOS name <--> IP address mapping for the destination host, it returns the IP address for the destination host to the WINS client.
- If the WINS server is unavailable the client may switch to b-node operation and send the query as a broadcast message on the local subnet.

WINS Partners

- WINS servers on different subnets can exchange information using ⊕Push℮and ⊕Pull℮mechanisms
- Push operation:
  - » Initiates exchange of information when specified number of new clients have been added to database
- Pull operation:
  - » Initiates exchange of information at a specified time during the day

DH

- Dynamic host configuration protocol
- Used for dynamic configuration of essential network parameters e.G. TCP/IP parameters
  - » TCP/IP parameters: IP address, DNS address, WINS address etc.
- DHCP clients request DHCP servers for network parameters using DHCP protocol

Why DHCP ?

- Large networks constitute of many hosts. Therefore configuring network parameters on all hosts is a time-consuming task.
- Network may have a small pool of addresses & lot of computers. Reuse of IP addresses is possible because only a few hosts are expected to use their IP address at a given time.
- Network restructuring may result in change of host subnets, thereby necessitating change in network parameters.
- Networks may have mobile computers.

Without DHCP, network parameters would need to be.

Configured manually.

DHCP Operation

Client.

- Client must be configured to use DHCP.
- Client broadcasts request for network parameters.
- Client gets network parameters from the DHCP server for specified lease times.

Server.

- Maintains database of network parameters for different machines or groups of machines (called scopes).
- Manages lease times for all machines.

DHCP Lease Times

- Lease period
  - » Amount of time a client can hold network parameters assigned by the DHCP server
  - » When this time expires client surrenders its IP address
- Renewal period
  - » = 0.5 x lease period
  - » On expiry, host starts trying to renew its lease
- Rebinding period
  - » = .875 x lease period
  - » On expiry host tries to get lease from other DHCP server over the network

IP Address Management

DHCP server uses three methods for IP address:

- Static allocation
  - » IP address is tied to MAC address of client
- Automatic allocation
  - » DHCP server assigns an IP address with an infinite lease period
- Dynamic allocation
  - » IP address assigned on a temporary basis (for lease period)
  - » Revokes the client on expiry of the lease
  - » Client can request for renewal or another IP address at end of lease period

Useful in an environments where temporary connections are Required or when IP addresses are scarce

Configuring DHCP Scopes

- Each subnet may be configured as a scope.
  - A scope is a grouping of DHCP clients.
  - All network parameters for computers of a given scope are the same.
  - A scope may be assigned a pool of IP addresses.
  - Scopes allow exclusion ranges within the scope.

DHCP Relay

- DHCP protocol uses a broadcast mechanism, and is therefore limited to a subnet.
- DHCP relay is used to pass DHCP request across a router(subnet).
- A DHCP relay listens to a broadcast on its segment, repackages the request in a point to point protocol and sends it to the server. On receipt of the response the relay passes the reply to the client.

DHCP Demo

Name Service Concepts

- A name defines what we seek
- An address indicates where it is
- A route indicates how to get there

Names & Addresses

- Names are there because they are easier for humans to remember
  - » Telnet ccse OR telnet 196.1.64.1
- Hostname can be assigned to any device that has an IP address
- Underlying software uses IP addresses
- Conversion from name to IP address
  - » Host table
  - » Domain name system (DNS)

Name Resolution for TCP/IP

- NETBIOS name resolution.
- WINS (client- server).
  - » WINS resolves 16 bit NetBIOS names to IP addresses. E.G.
  - » 196.1.67.240 < -- > ccsepdc.
- LMHOSTS (file).

- Internet domain name resolution.
- DNS (client- server).
  - » DNS resolves IP addresses to internet domain names. E.G.
  - » 196.1.64.2 < -- > razi.ccse.kfupm.edu.Sa.
- Hosts (file).

H o

- Simple text file that associates IP addresses with host names
  - » Aliases of names can also be given
- Commonly used in LANs
- Major problems with this approach in a huge internet
  - » Large size
    - ï Inefficient lookup
  - » Frequency of updates
    - ï No technique for automatically distributing information about newly registered hosts

Domain Name System

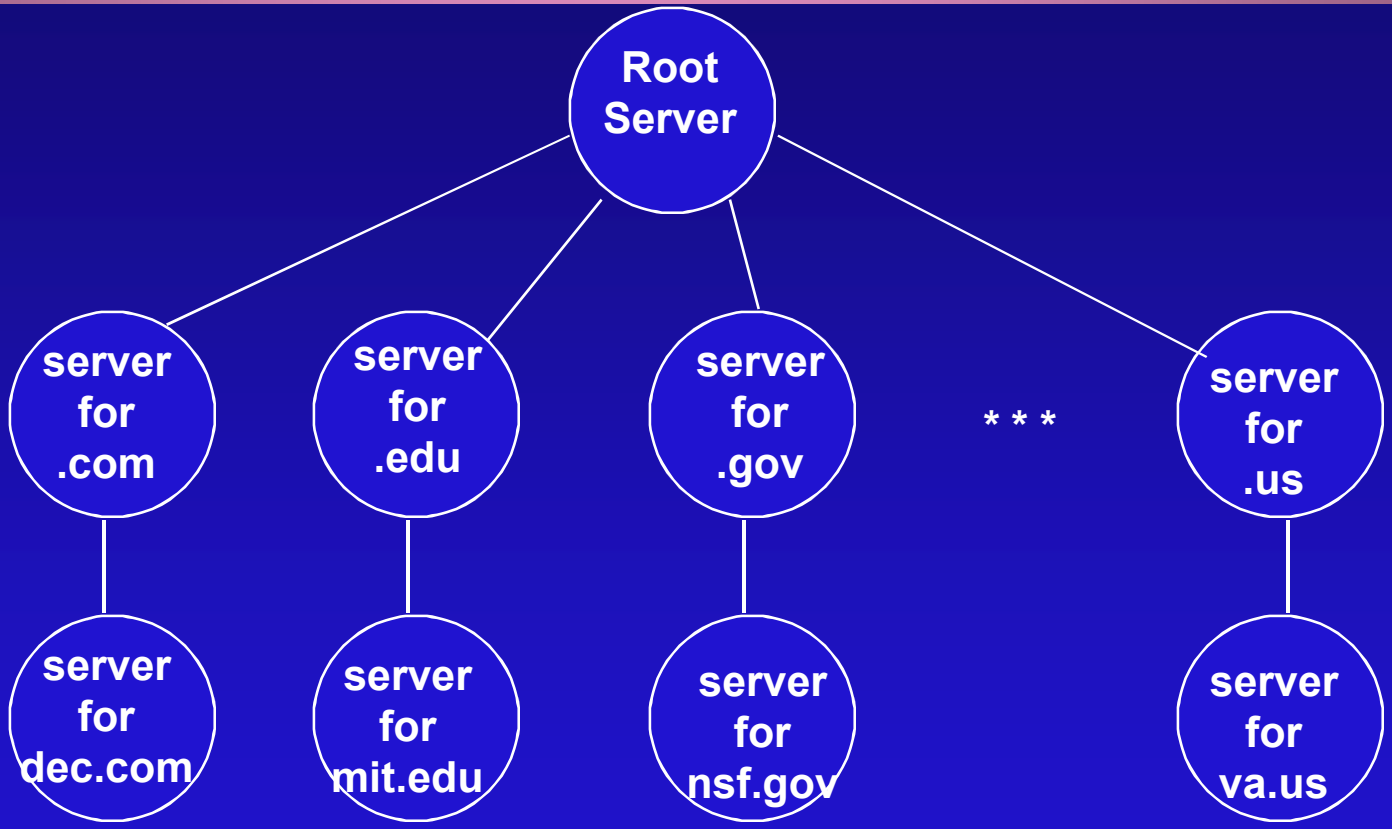
- Designed to overcome both major weaknesses of host table approach
- DNS scales well
  - » No single large table
  - » Distributed database system
- DNS guarantees that new host information will be disseminated to the rest of the network as needed
  - » Actually it is only sent to those who are interested

Domain Hierarchy

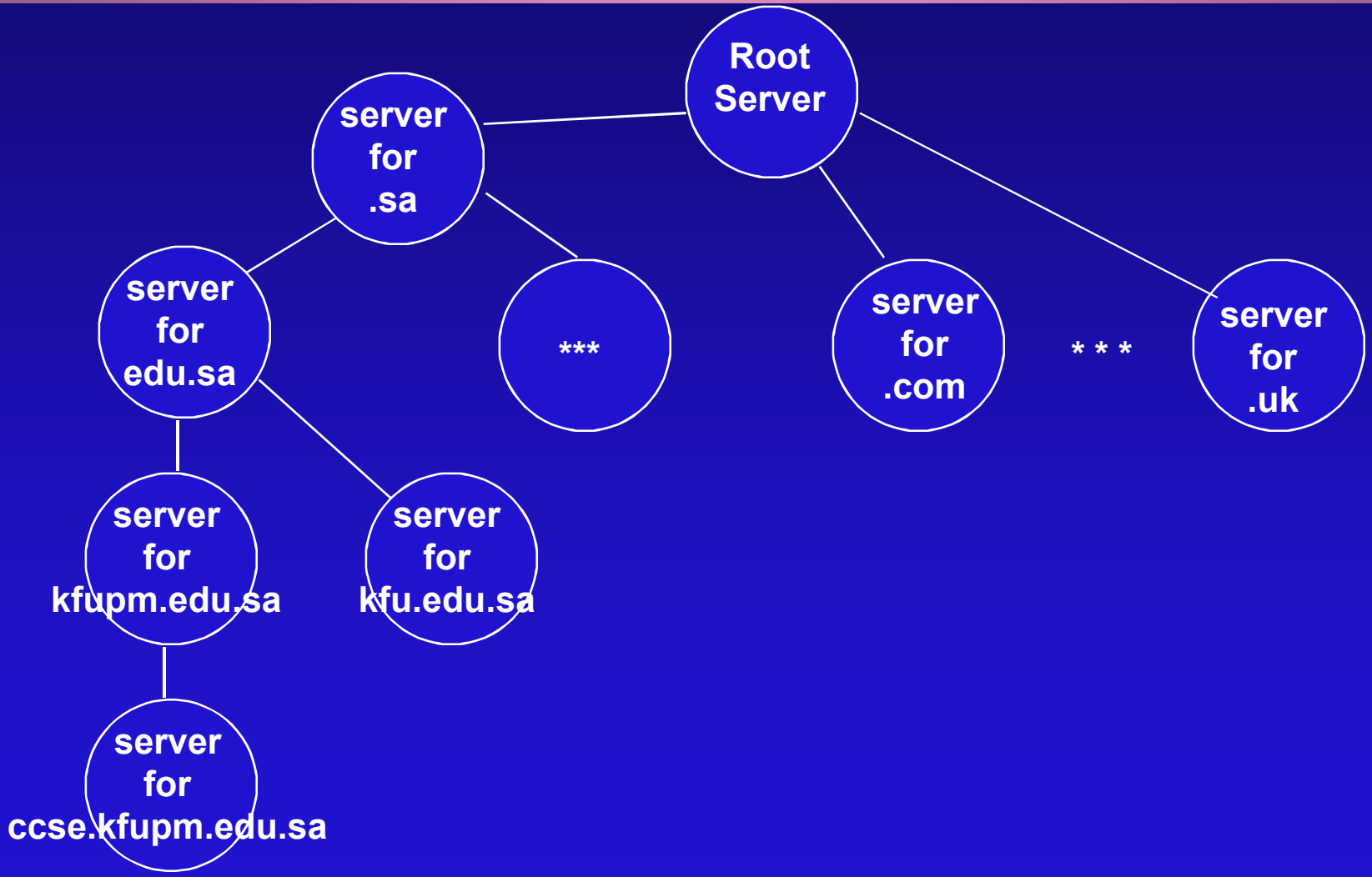
- DNS has no central database with all host information
- Thousands of name servers organized in an hierarchy
- Root domain
  - » Root servers
- Top level domains
  - » Organizational
  - » Geographic

Com	commercial
edu	educational
Gov	governmental
Mil	military
Org	other organizations
XX	two letter country code e.G. Sa for Saudi Arabia

DNS Hierarchy



DNS Resolution



Domain Names

- Domains and Subdomains
  - » Once domain is registered in parent domain, decision to create sub-domains is decentralized
- Domain names reflect the domain hierarchy
  - » Most specific to least specific
    - ï razi.kfupm.edu.Sa
    - ï hpkhan.fc.Hp.Com
    - ï nic.ddn.Mil
- Name lookup
  - » Recursive query
  - » Non-recursive query

MS DNS Server

- MS DNS server can be maintained using DNS files or in the windows registry
- When maintained in the registry a graphical tool -- ñDNS manageròis available for maintenance

MS DNS Server DEMO

DNS in W2000

- Introduction
- Dynamic DNS
  - » Need for DDNS
  - » Update Protocol
  - » Definitions
  - » DDNS operation
- Secure Dynamic Update
  - » Integration with Active Directory (Security)
  - » Update Policy
- Summary

Introduction

- DNS is a host name resolution process
- It has new features
  - » Active directory integration
  - » Dynamic/secure update
    - ï Dynamic DNS (DDNS)
    - ï Secure Update
  - » Incremental zone transfer
  - » Enhanced Domain Locator
  - » Caching Resolver Service
  - » DNS Manager
- Support for service location

Dynamic DNS

Why Dynamic DNS

- Designed to overcome weakness of Conventional DNS (C-DNS).
- C-DNS needs manual update of host information.
- Manual update takes lot of time even in small networks.
- C-DNS does not integrate with DHCP.
- C-DNS stores stale records.

Dynamic Update Protocol

- DDNS covers RFC 2136.
- A DNS client locates the authoritative server & zone for record update.
- Sends a message to check if registration exists.

Update Protocol(contd.)

- If no registration send the information.
- Otherwise reregister. Useful for avoiding corrupt records.
- If update fails then send the message to another authoritative server.
- Retry every 10 minutes.

Definitions

Definitions

- A record
  - » Maps Host name to IP Address.
    - ï Used for Forward name resolution.
- PTR Record
  - » Maps IP Address to Host name.
    - ï Used for Reverse name resolution.

Definitions (Contd.)

- DHCP Client
  - » A client machine which gets an IP Address from the DHCP server on a lease basis
- Static DHCP Client
  - » A client machine configured to use a static IP Address
- RAS Client
  - » Has no interaction with DHCP Server

DDNS Operation

- DNS dynamic updates are generated by the DHCP service at the client machine
- Functionality at both the client side & the DHCP server
- Operation varies by the type of client network configuration. Following configurations are explored
  - » DHCP client
  - » Static DHCP client
  - » RAS client

DDNS Operation (Contd.)

DHCP client ï At bootup

- Client proposes to update the A resource record
- DHCP Server updates the A & PTR record

DHCP client ï At shutdown or IP release

- DHCP server removes PTR R
- Removes A Record if configured for that

DDNS Operation (Contd.)

Static DHCP client ï At every bootup

- No communication with DHCP server
- Dynamically updates both A & PTR records
- Changes IP address at every bootup if needed

DDNS Operation (Contd.)

RAS client

- Similar to Static DHCP client
- RAS server deregisters the client in case of line failure (PTR record)
- At connection close
  - » Deletes both records (A & PTR)

Secure Update

Security

Integrates with Active Directory to provide security

- Active directory treats DNS zones as objects
- Hence provides ACLs (Access Control Lists) to secure the Zones
- Each ACL can contain a group of users who can have different access to different zones
- W2000 has a DNS Admins group on whom the ACLs can be defined

Secure Update Policy

The following approaches can be used by a W2000 client

- Attempt a non-secure update first and negotiate a secure update if it fails (Default)
- Always negotiate a secure dynamic update
- Attemp only a non-secure dynamic update

Summary

- Helps in automation of DNS updates for new hosts
- Obsolete information is not entertained
- Allows frequent changes in IP addresses

DNS Demo