System and Network Administration

A·P·U
ASIA PACIFIC UNIVERSITY
OF TECHNOLOGY & INNOVATION

Core Services:
DNS and DHCP

Configuring for Network Services

Networks are made of

- Hosts that act as clients and servers
  - **Servers share resources with AUTHORISED Clients**
- Media and Equipment that interconnect hosts
- Protocols that govern connections
- Users

Networks allow cooperation

Cooperation leads to communities of users

Names, Addresses, Routes

Hosts and their services need an identity

These definitions are inevitably mentioned:

- a name identifies what you want, and is generally a text string for human interpretation;
- an address identifies where it is, and is generally in a machine readable form;
- a route identifies a way to get there, generally as a list of names or addresses.

Administrators maintain these

Dynamic Allocation

At boot, the system knows its MAC address

- What is the IP address? Netmask?
- What is the route to other hosts?

Static Allocation – host configuration file

- `ifconfig`
- `route add default gw`

Dynamic Allocation – configuration server

- need a request/reply protocol
- need a server listening on a TCP/UDP port

Static Vs. Dynamic Addressing

- Many networks use a combination of static and dynamic addressing.
  - Static addresses for servers, routers, and network management systems.
  - Dynamic addresses for end systems, including workstations and IP phones.
- The number of end systems
  - 30+ use dynamic
- The importance of tracking addresses
  - Static provides a consistent audit trail

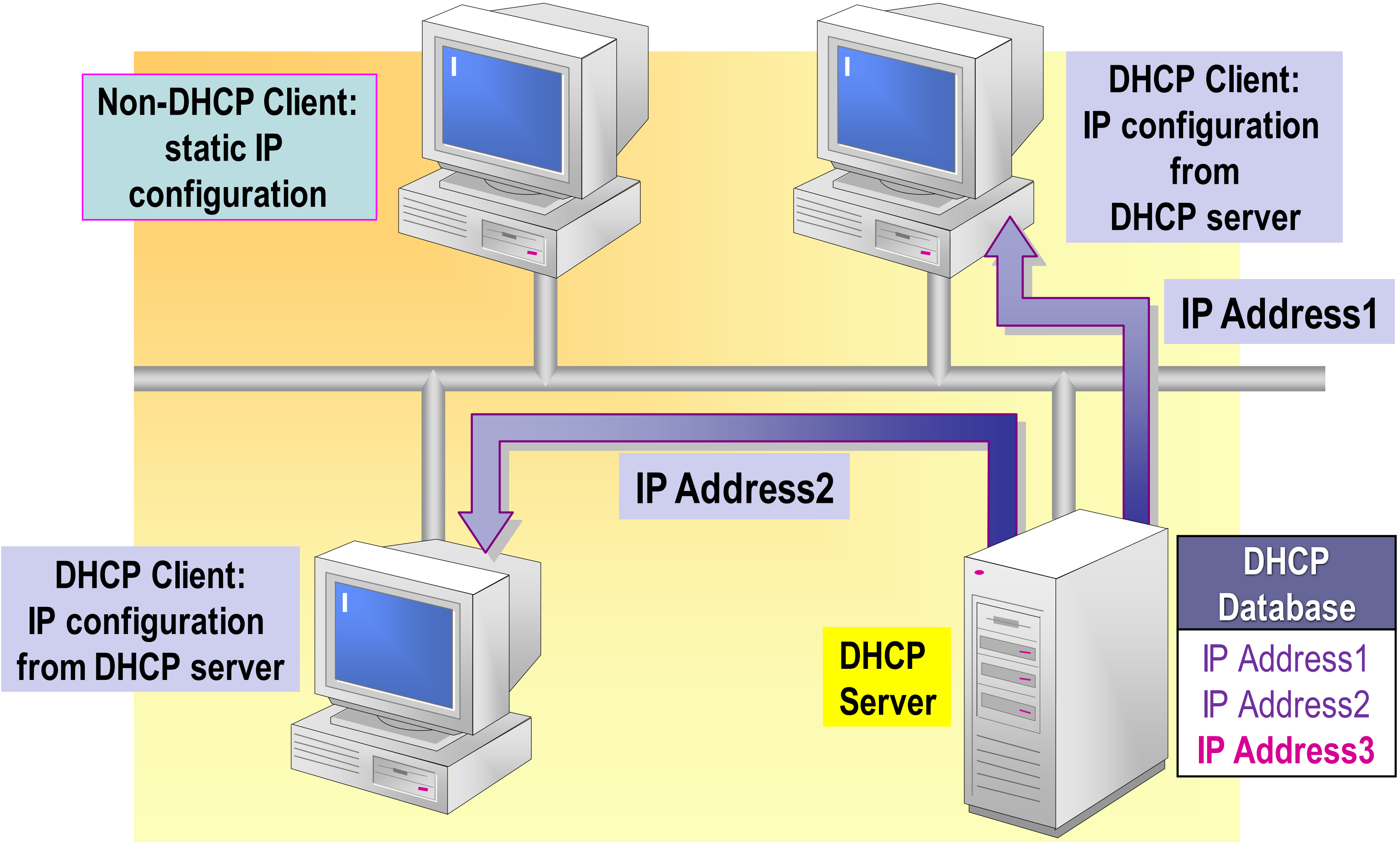
Q
&
A

Dynamic Host Configuration Protocol (DHCP)

- Centralized administration, superset of BootP
- Servers allocate network layer addresses and save information about which addresses have been allocated.
- *All* communication initiated by the client
- Uses UDP on port 68 for client, port 67 for server
  - One DHCP session has a common xid ("transaction ID"), randomly selected by the client

Dynamic Addressing: DHCP

- Server offers IP address and network parameters for a limited time (called a *lease*)
- Addresses offered can be
  - Fixed addresses allocated to particular computers
  - From a pool of reusable IP addresses (supports hosts that are not online all the time - more hosts than addresses)
- client can renew or relinquish the lease
- address can be requested again when the lease expires
- Lease renewal efforts occur at two intervals: 1/2 of the lease has been used and 7/8 of the lease has been used



Non-DHCP Client:
static IP
configuration

DHCP Client:
IP configuration
from
DHCP server

IP Address1

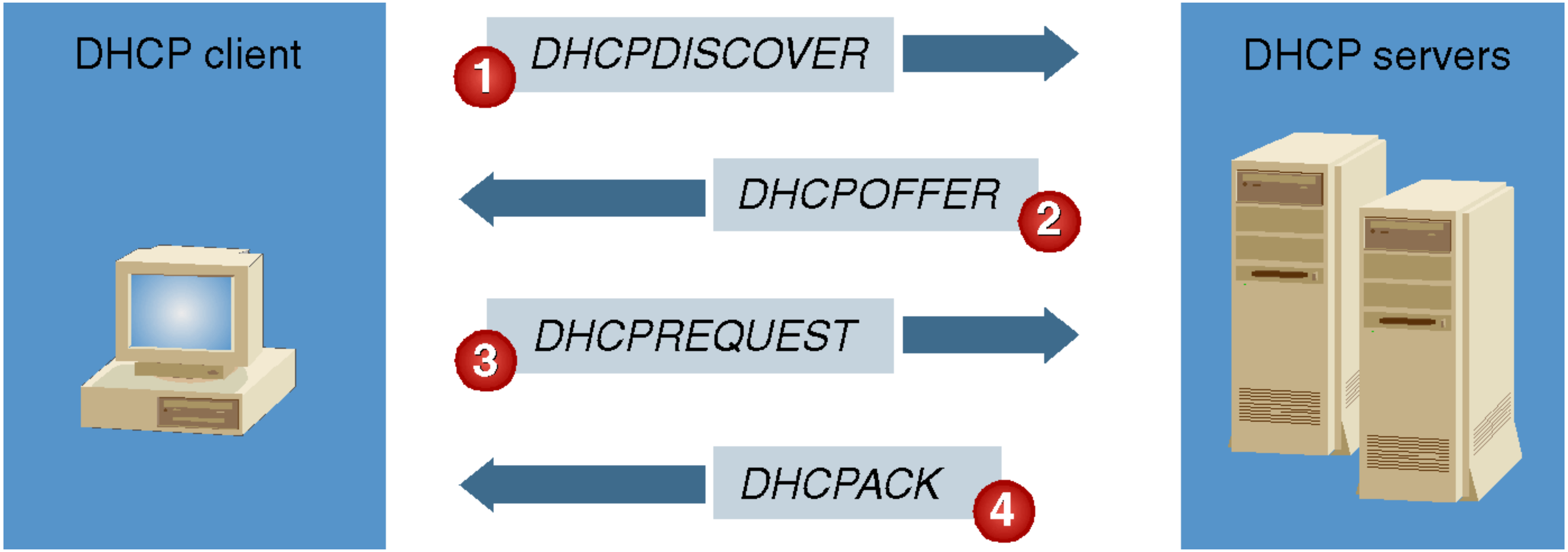
IP Address2

DHCP Client:
IP configuration
from DHCP server

DHCP
Server

DHCP Database
IP Address1
IP Address2
IP Address3

The DHCP Lease Process



DHCP: Messages

1. DHCP client broadcasts a DHCPDISCOVER message to its subnet (255.255.255.255)
   – A *DHCP relay agent* is configured to pass this request to DHCP servers not on the same physical subnet within the campus or enterprise

2. **All** DHCP servers that receive a DHCPDISCOVER request may send an DHCPOFFER
   – Contains an IP address and possibly other configuration information (subnet mask, DNS servers, default gateway, etc)
   – since a client typically does not need > 1 IP address, more messages needed

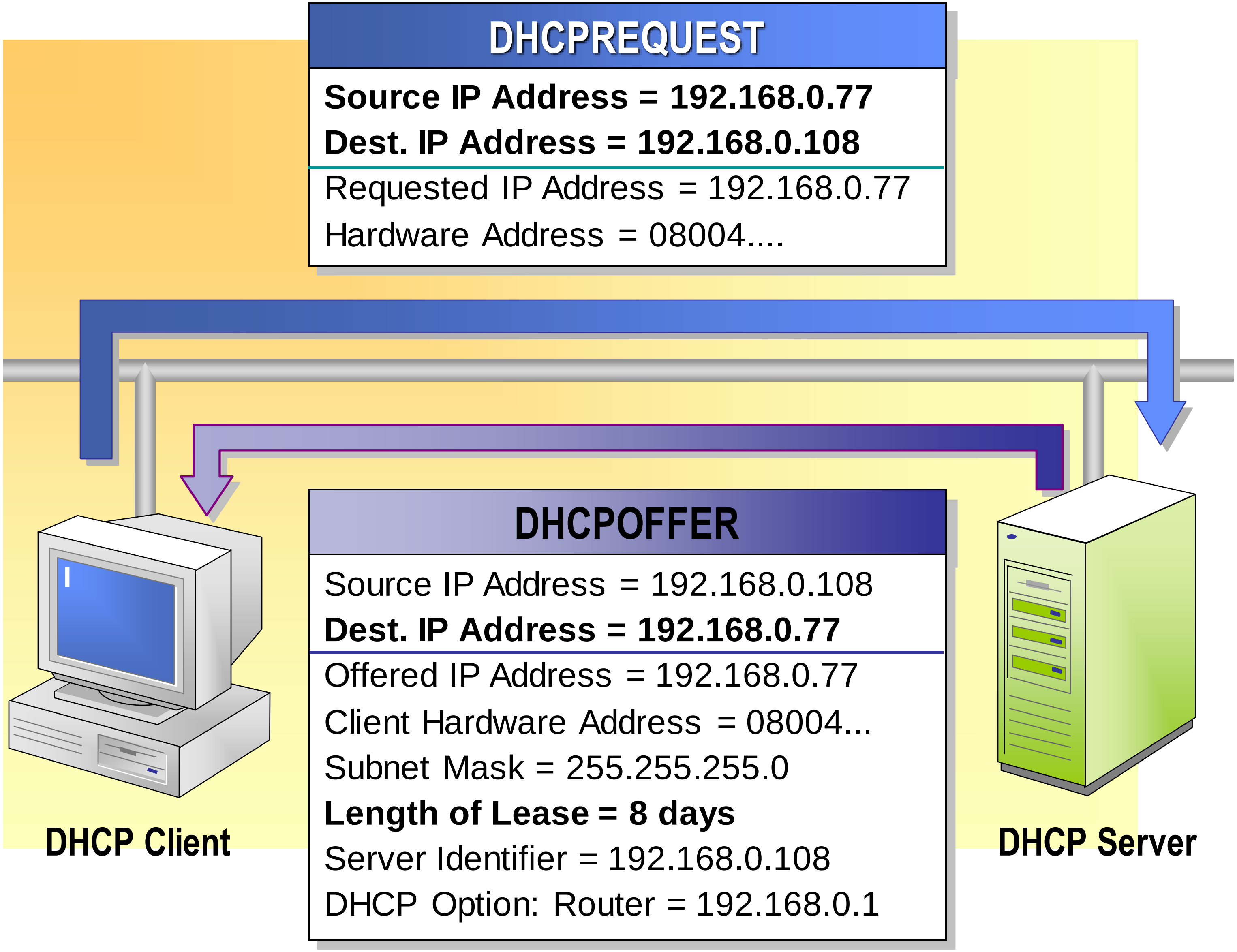
DHCP: Messages

3. DHCPREQUEST sent by client to request a certain IP address
   - Usually the one sent by an DHCPOFFER
   - also used to renew leases and to try to get same address after a reboot
   - message is broadcast since a client typically does not need more than one IP address but may get more than one DHCPOFFER

4. Response by server is DHCPAK or DHCPNAK

   ACK: acknowledged, accepted

   NACK: something is wrong (for example client requested an IP address it is not supposed to have)



DHCPREQUEST

Source IP Address = 192.168.0.77

Dest. IP Address = 192.168.0.108

Requested IP Address = 192.168.0.77

Hardware Address = 08004....

DHCPOFFER

Source IP Address = 192.168.0.108

Dest. IP Address = 192.168.0.77

Offered IP Address = 192.168.0.77

Client Hardware Address = 08004...

Subnet Mask = 255.255.255.0

Length of Lease = 8 days

Server Identifier = 192.168.0.108

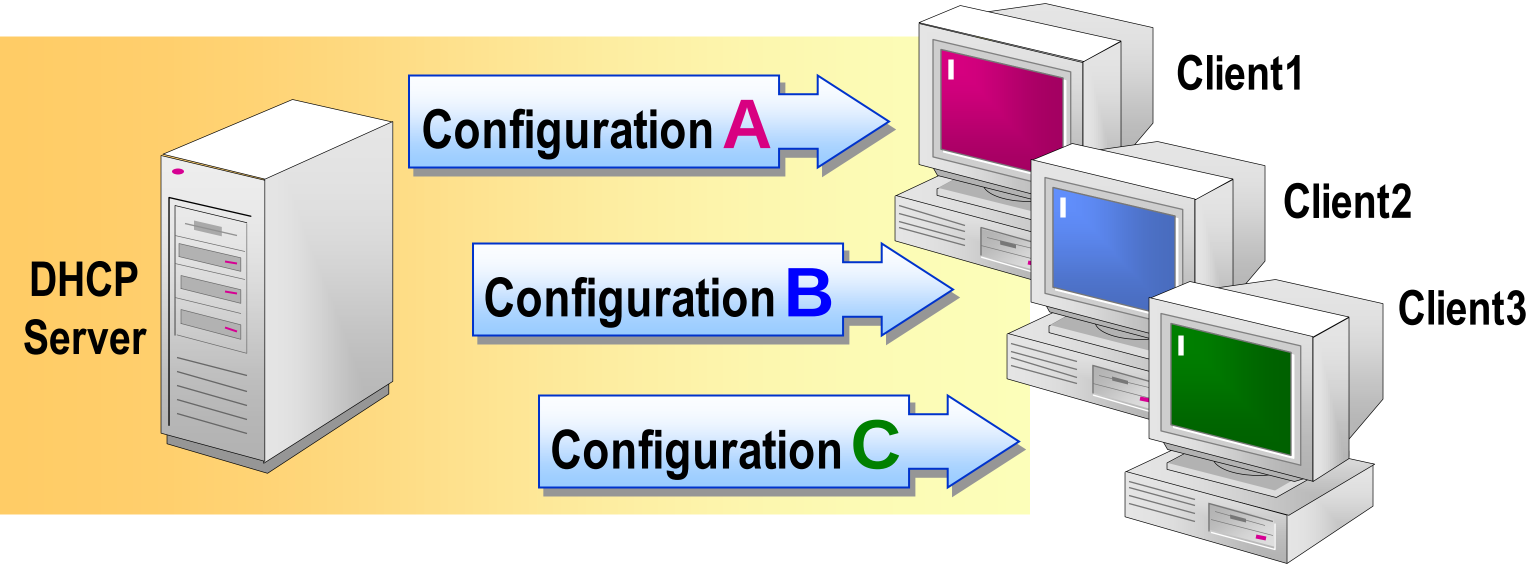
DHCP Option: Router = 192.168.0.1

DHCP Client

DHCP Server

Using Option Classes

- Vendor-defined Classes Manage DHCP Options Identified by Operating System Vendor Type
- User-defined Classes Manage DHCP Options with Common Configuration Requirements



Commonly used dhcp options

- option domain-name domain ;
  - Defines the domain part of the host name
- option subnet-mask mask ;
  - Specifies the subnet mask in dotted decimal notation. If the subnet mask option is not provided, dhcpd uses the network mask from the subnet statement.
- option broadcast-address address ;
  - Defines the broadcast address for the client's subnet.
- option static-routes destination gateway [, gateway ...] ;
  - Lists the static routes the client should use. The default route cannot be specified in this manner. Use the routers option for the default route.
- option routers address [, address ...] ;
  - Lists the routers the client should use, in order of preference.
- option domain-name-servers address [, address ...] ;
  - Lists the Domain Name System (DNS) name servers the client should use, in order of preference.

Unauthorised Server Trouble

- Unauthorised DHCP server on your subnet giving DHCPOFFER to all requests
  - since most will send a REQUEST for the first OFFER they receive by default, may *ignore* OFFERs from enterprise DHCP relays
- Unauthorised DNS server on your subnet giving response to all requests
  - may *ignore* the enterprise servers
  - extra/confusing traffic
  - USING SAME IP RANGE??

Q
&
A
dreamstime.com

Names for Hosts

- a name identifies what you want: a text string for human interpretation
- an address identifies where it is: usually machine readable (numeric)

- /etc/HOSTNAME
  defines the official name of the host *(can see it in the command prompt)*
- /etc/hosts
  defines local static layer 3 addresses and aliases *(localhost)*
- /proc/sys/net/ …
  records the interface names & addresses known to the kernel

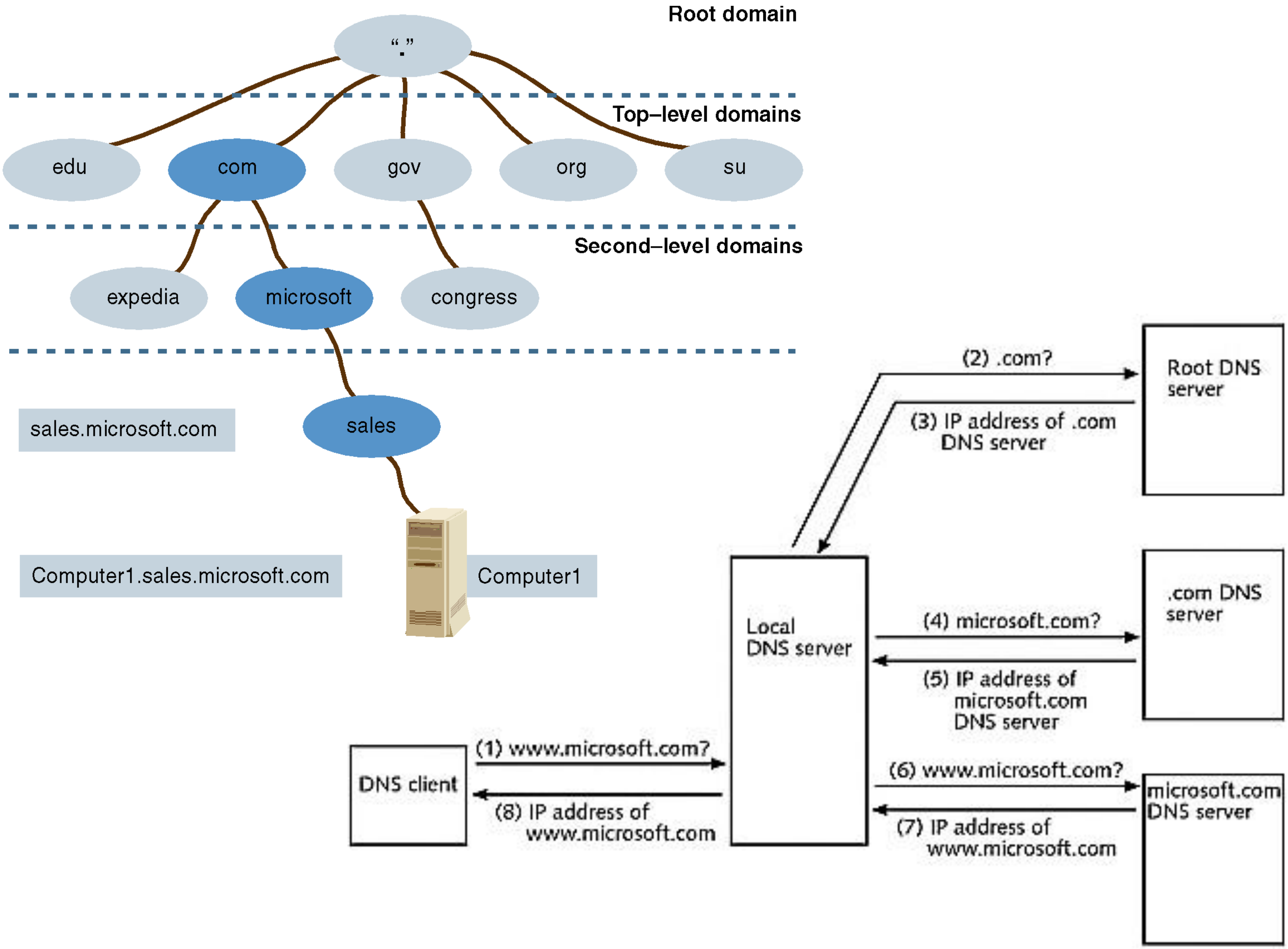
Domain Name Service

- The Internet DNS (Domain Name Service) provides translation between (*binds*) the IP address in numeric format and the user-oriented domain name
  - given a domain name a DNS server will return a numeric IP address;
  - given an IP address, the server *may* return a domain name (this service, known as a *reverse-lookup*, is actually optional).
- Provides machine independent names (address can change while the name stays the same)
- The DNS is only one example of network directory services; there are other naming, addressing, and directory systems in use.

Domain Name System

- The DNS is a hierarchy of ***nameservers***, each with local knowledge about the names and addresses in its ***zone of authority***.
- There is no global map of zones of authority. The DNS relies on the idea of ***delegation***: transfer of authority for a domain beginning with root or "." (dot) servers

  `example.org is a delegation from org.`
- Every server knows how to reach servers that are ***authoritative*** for names further down the hierarchy.
- With a series of queries, a nameserver can follow ***referrals*** from servers with more general knowledge to find the server with the specific answer it needs.



Root domain

"."

Top–level domains

edu

com

gov

org

su

Second–level domains

expedia

microsoft

congress

sales

sales.microsoft.com

Computer1.sales.microsoft.com

Computer1

Root DNS server

.com DNS server

microsoft.com DNS server

Local DNS server

DNS client

(1) www.microsoft.com?

(2) .com?

(3) IP address of .com DNS server

(4) microsoft.com?

(5) IP address of microsoft.com DNS server

(6) www.microsoft.com?

(7) IP address of www.microsoft.com

(8) IP address of www.microsoft.com

Delegation

- Need to register with next highest level
  - all the way up to the root or “.”
  - these are known as Top-Level Domains (TLDs)
- Identify organization and responsible persons
- create pointers to authoritative server
  - *[somebody needs to point to you!!]*
- A ***host name*** is the leftmost portion of the ***fully qualified domain name (FQDN),*** which describes the exact position of a host within the domain hierarchy.
- DNS uses a host’s FQDN to resolve a name to an IP address.

DNS - /etc/services

Standard DNS traffic uses UDP port 53

- if DNS requests don’t fit into a UDP response (typically 512 bytes) then it will try again using TCP;
- **A client computer will always send a DNS Query using UDP Protocol over Port 53. If a client computer does not get response from a DNS Server, it will re-transmit the query using the TCP after some interval.**
- By default, modern DNS servers use random ports above 1024 to query other nameservers. However, some firewalls expect all nameservers to communicate using only port 53.

Q
&
A
dreamstime.com

Name Server software

- Internet Software Consortium ISC makes *reference implementations* of DNS, DHCP
- Available from http://www.isc.org/
  - Implemented by people directly involved with the standardisation process
  - standards compliant, very robust feature-rich implementations
  - Scalable: used for the global root nameservers

Name Server software

DNS on UNIX systems generally use Berkeley Internet Name Daemon (BIND) /usr/sbin/named

BIND usually runs as the process ***named*** *(pronounced name d)*

`/etc/named.conf` – sets general parameters and points to domain database (local files or remote servers)

`/var/named/*` – working directory for zone, statistic, and cache files

- `/var/named/named.ca` – *initial cache,* points to the root domain servers

`/etc/resolv.conf` – client configuration, points to domain servers

`/etc/host.conf` – client configuration general parameters

Resource Record Types

Text name	Type	Function
Start of authority	SOA	Defines the zone and zone parameters
Name Server	NS	Identifies the nameserver for the domain
Address	A	Converts a hostname to an IPv4 address
Pointer	PTR	Converts an IPv4 address to a hostname
Canonical Name	CNAME	Defines another name (alias) for a host
Mail Exchanger	MX	Where to deliver mail for a domain
Text	TXT	Arbitrary text strings

Others types are defined, but not commonly used

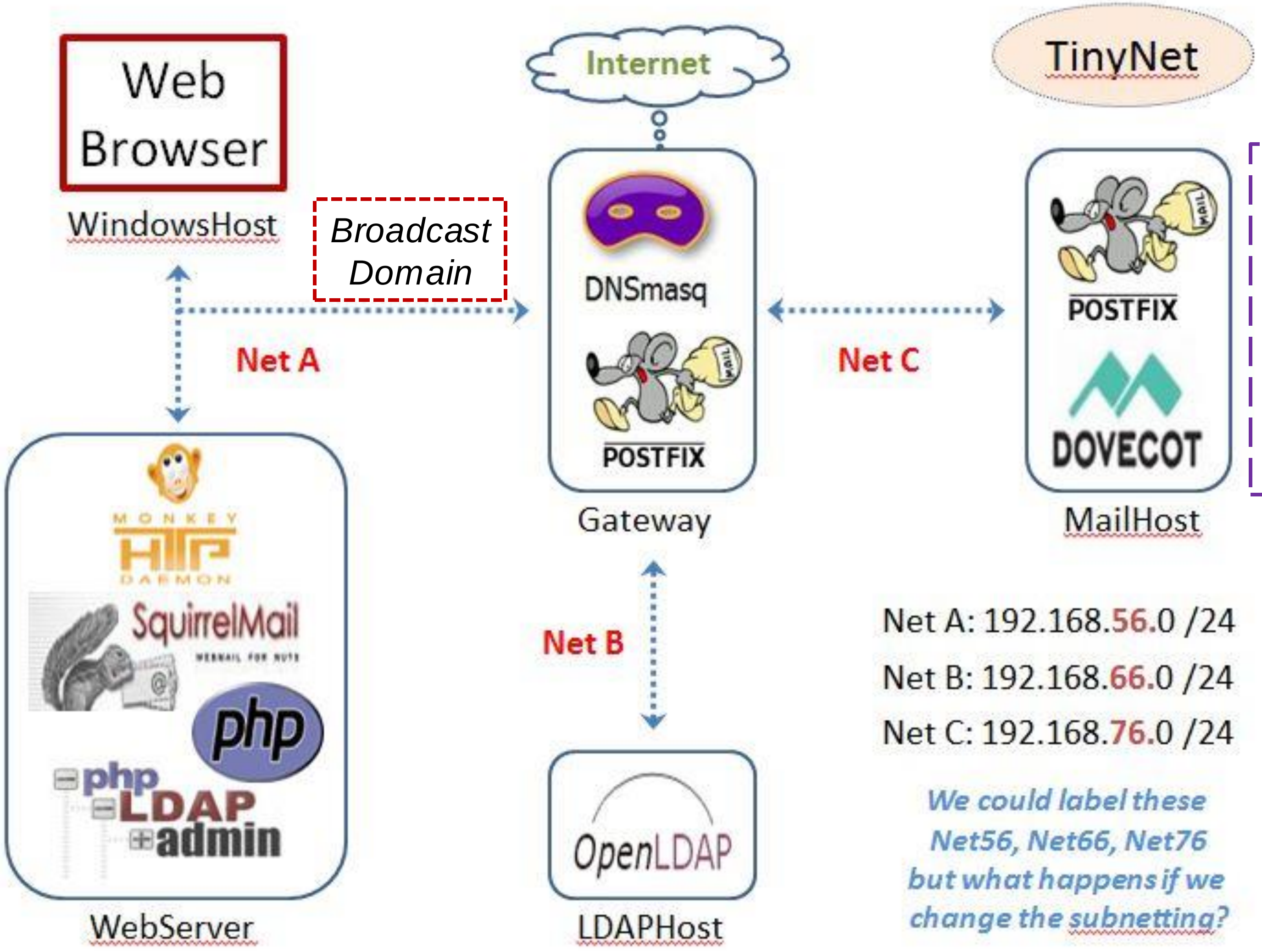
TinyNet: DNSMASQ

- syntax is different, but function is the same
- integrated, simpler, suitable for small networks

- preconfigured – isolated from enterprise services
- auto-update (harder to do in ISC Bind/DHCP)

- Has examples of everything we cover in this lecture

Gateway:
One interface for each subnet



Broadcast Domain

Net A: 192.168.56.0 /24

Net B: 192.168.66.0 /24

Net C: 192.168.76.0 /24

We could label these Net56, Net66, Net76 but what happens if we change the subnetting?

HOSTNAME
Is registered
With dnsmasq
Via DHCP

Matched to
Configured
cnames

Resource Records: A and CNAME

A (address record) specifies an IP address assigned to a name.

The A record binds a hostname to an IP address, while a CNAME record points another name to it (creates an *alias*): **CNAMEs point to hostnames not IP addresses**

/etc/dnsmasq/cnames

Resource Records: MX

MX (Mail eXchanger) tells where mail sent to a particular namespace in this zone should go.

- The lowest preference-value is preferred; having multiple servers with the same value will distribute traffic evenly.
- The email-server-name may be a hostname or FQDN.

Troubleshooting the DNS Service

- `nslookup` and `dig`
- Run in debug mode
- Restart after updates
- Check the logs to familiarise yourself with what it says when it starts
- Ensure that the process is running,and listening on UDP (and TCP) port 53 (the domain port)

Requires skills of

– Mechanic

– Sociologist

– Researcher

Q&A