NSCOM01

UDP-Based Application Protocols

Instructor: Dr. Marnel Peradilla

USER DATAGRAM PROTOCOL

- **The User Datagram Protocol (UDP) is a connectionless transport protocol used in TCP/IP networks**
- **Considered as a 'bare-bones' protocol that provides only the essential capabilities needed to transport a data segment between applications**
- **Features:**
  1. Unreliable – datagrams are not acknowledged
  2. No congestion control mechanism- datagrams sent as quickly as possible
  3. Stateless – Server does not keep track of status and session information of a client. Each request-response exchange with a client is treated as an independent transaction
  4. Unordered delivery – datagrams do not contain any sequencing information

WHEN TO USE UDP

- **Connectionless services are commonly used with applications where occasional data loss is tolerable in exchange for reduced protocol overhead:**

1. Inward Data Collection – periodic sampling of data sources such as sensors or automatic self-test reports from network equipment
2. Outward Data Dissemination – message broadcasting to nodes or distribution of data to a network
3. Request – Response – query-based applications that use a transaction service provided by a single server where a single request-response is typical
4. Real-time applications – applications with a degree of redundancy or real-time requirement e.g. voice, telemetry

APPLICATION PROTOCOLS

- **Several well-known application protocols use UDP as transport protocol to support their operations:**
  - System Logging Protocol
  - Network Time Protocol
  - Domain Name System
  - Dynamic Host Configuration Protocol
  - Trivial File Transfer Protocol
  - Simple Network Management Protocol

DNS

Domain Name System

PURPOSE OF NAMING

- ❑ Addresses are used to locate objects
- ❑ On networks, hosts are identified using their IP addresses, which are difficult to remember
- ❑ DNS created in 1983 by Paul Mockapetris (RFCs 1034 and 1035) is used as a general-purpose naming service for resources on the Internet

DNS

- ❑ **A lookup system for naming computers and resources connected to the Internet using a hierarchical database for translating names into numerical addresses**
- ❑ **A globally distributed, loosely coherent, scalable, reliable, dynamic database**
- ❑ **Comprised of three components**
  - A "name space"
  - Servers that host different parts of the name space
  - Resolvers (clients) which query the servers about the name space
- ❑ **Operates using a combination of UDP and TCP as the transport layer protocol on port 53**

FEATURES

❑ Global Distribution

- Parts of the namespace data are maintained locally on different servers, but the entire namespace is accessible globally
- Data may be cached on other servers for faster retrieval

❑ Loose Coherence

- Database is always internally consistent, and changes to the master copy of the database are replicated to or deleted from caches according to configuration of a server’s administrator

❑ Scalability and Reliability

- No limit to the size of the database and multiple queries can be handled simultaneously by replicating data and distributing among different servers

❑ Dynamicity

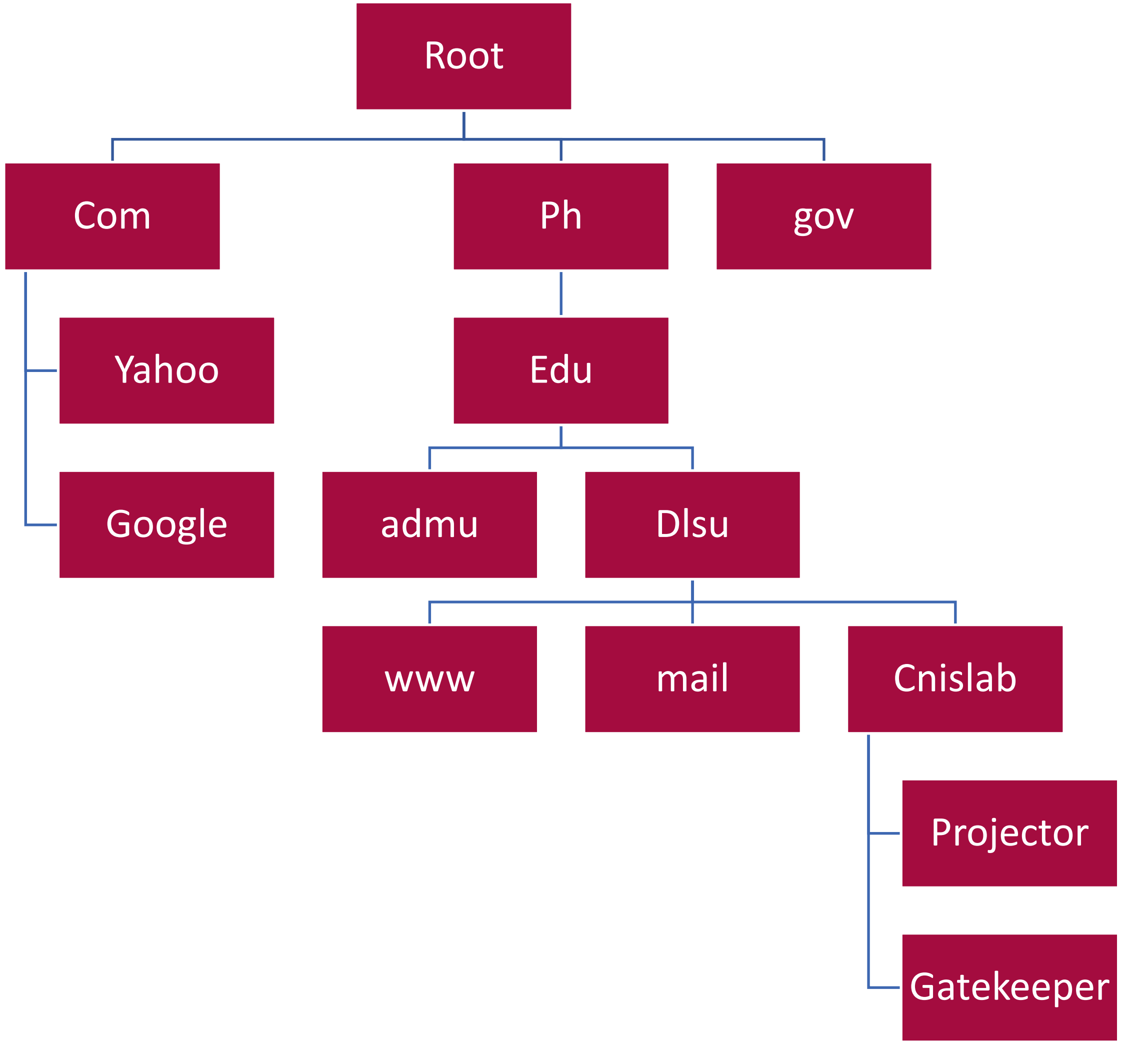
- Changes can be made anytime and replicated to other servers

DNS NAMES

- **The namespace needs to be made hierarchical to be able to scale.**
- **Fully Qualified Domain Name (FQDN) is the key used when fetching data from the DNS**
  - Labels separated by dots (i.e. www.dlsu.edu.ph)
  - DNS provides a mapping from FQDNs to resources of several types using resource records (RR)

www.dlsu.edu.ph	… A 103.231.241.180

- **Domain names can be mapped to a position in a tree-like database of RRs when each dot is a new branch and each leaf or node has a label**



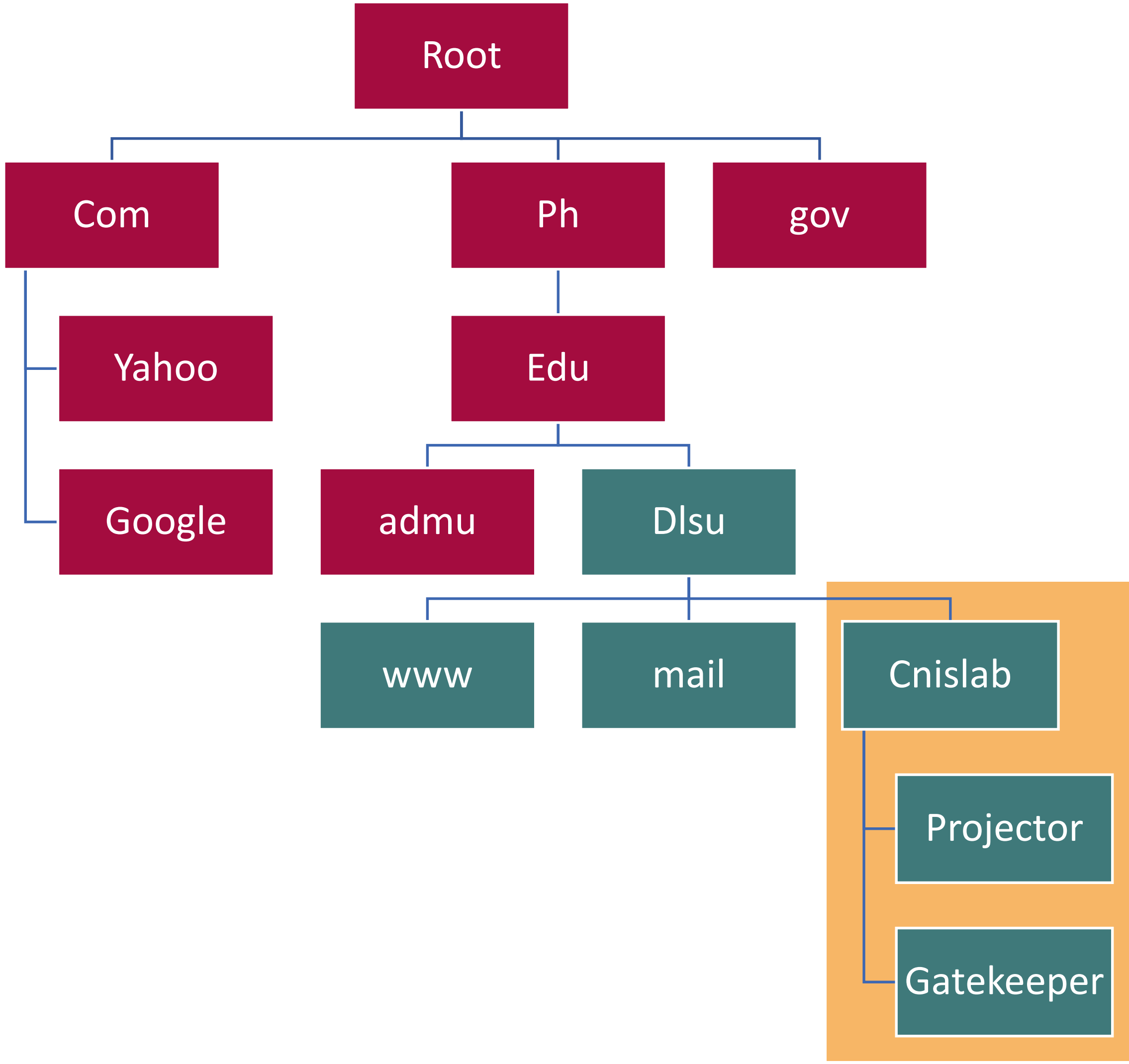
DOMAINS AND ZONES

❑ Domains are “namespaces”

- Everything below .ph is in the ph domain.
- Everything below edu.ph is in the edu.ph domain and in the ph domain.
- Administrators can create subdomains to group hosts according to geography, organization or any other criteria

❑ Zones are “administrative spaces”

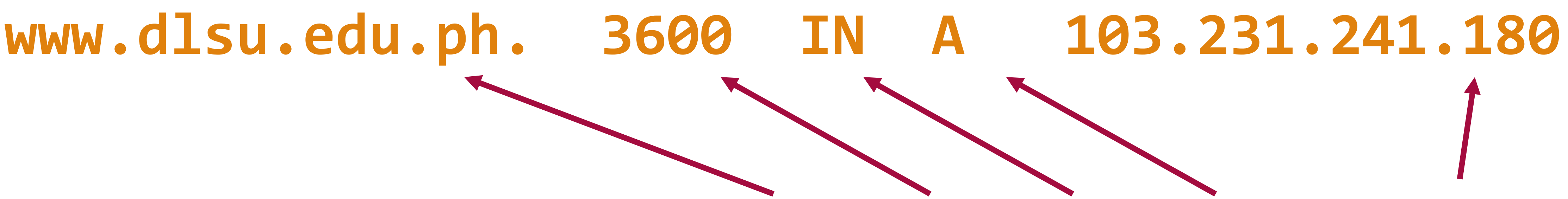
- Responsibility for managing a subdomain or portions of it can be delegated to another entity, creating a new administrative zone
- Zone administrators are responsible for portion of a domain’s name space
- The parent domain retains links to the delegated subdomain or zone



NAME SERVERS

- □ **Are server programs which hold the structure and set information about any part of the domain tree and respond to DNS queries**
- □ **Usually hold complete information for a subset of a domain space and pointers to other servers holding the rest of the tree**
- □ **An authoritative server holds complete domain information for one or more zones**
  - Master (primary) server contains locally stored record data loaded from a zone file
  - slave (secondary) server normally replicates the data from the master through a zone transfer
- □ **A recursive server perform lookups by querying the DNS in behalf of clients**
  - Answers are obtained from authoritative servers then forwarded to the clients
  - Answers are stored for future reference in the cache (a.k.a. caching forwarders)
- □ **Servers can be of mixed functionality – contain authoritative zone data while at the same time have the capability to perform recursive lookup with caching**

RESOURCE RECORDS



```
www.dlsu.edu.ph.  3600  IN  A   103.231.241.180
```

- **A resource records consist of a name, TTL, class, type and RDATA**
  - Name: label of the node
  - TTL : how long an entry may be used in seconds
  - Class: protocol type, usually ‘IN’ (Internet protocol)
  - Type: type of record contained
  - RDATA: data content

RESOURCE RECORDS

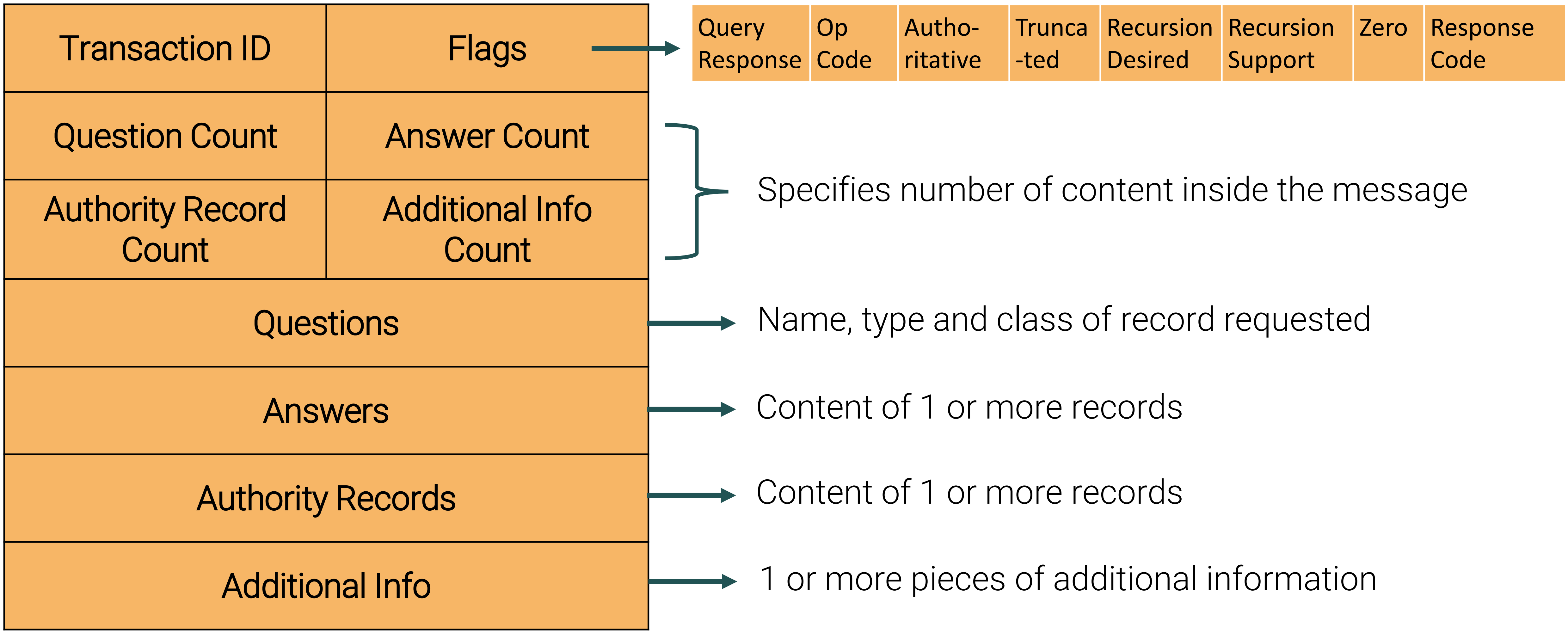
There are several RR types. The most common are:

1. Start of Authority (SOA) - Defines a zone name, its name server, an e-mail contact and various time and refresh values applicable to the zone
2. Address (A or AAAA) - Forward maps a host name to IPv4 (A) or IPv6 (AAAA) address
3. Mail Exchange (MX) - Name and preference of mail servers (mail exchangers) for the zone. Used primarily by external SMTP servers to send mail to the domain
4. Canonical Name (CNAME) - Maps a host alias or nickname to the real or Canonical host name which may lie outside the current zone.
5. Name Server (NS) - Defines the authoritative name server(s) for the specified domain or the subdomain. Used by DNS servers to make referrals
6. Pointer (PTR) - Reverse maps an IPv4 or IPv6 address to hostname

DNS RESOLVERS

- ❑ Programs that query information from name servers on behalf of applications in response to client requests.
- ❑ Must be able to access at least one name server and use that name server's information to answer a query directly, or pursue the query using referrals to other name servers
- ❑ Are usually services provided by the operating system or may be a standalone utility such as **nslookup**

DNS MESSAGE FORMAT



Transaction ID	Flags
Question Count	Answer Count
Authority Record Count	Additional Info Count
Questions	
Answers	
Authority Records	
Additional Info	

Query Response	Op Code	Autho-ritative	Trunca-ted	Recursion Desired	Recursion Support	Zero	Response Code

Specifies number of content inside the message

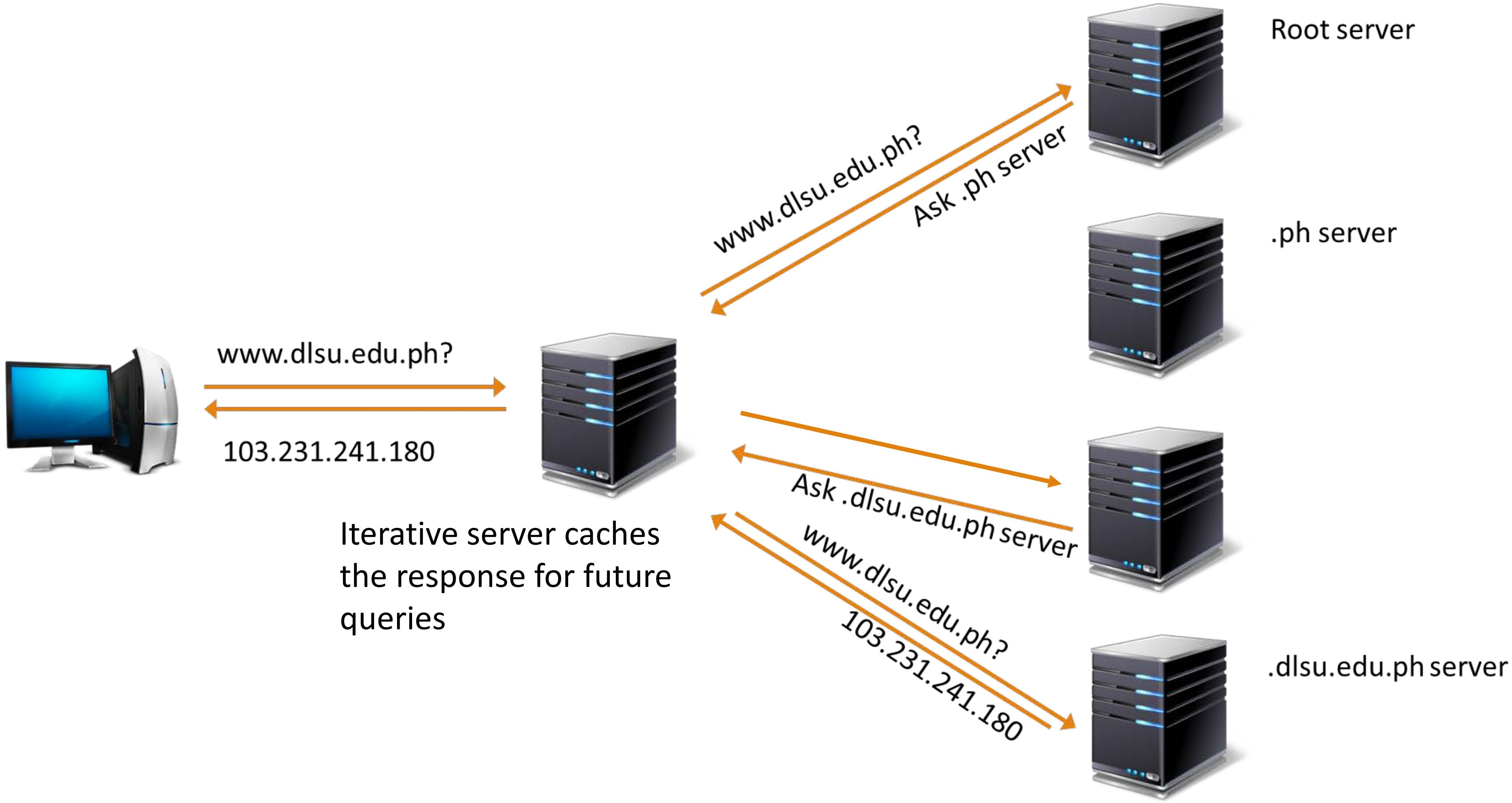
Name, type and class of record requested

Content of 1 or more records

Content of 1 or more records

1 or more pieces of additional information

QUERY AND RESOLVING PROCESS



Root server

.ph server

.dlsu.edu.ph server

www.dlsu.edu.ph?

103.231.241.180

www.dlsu.edu.ph?

Ask .ph server

Ask .dlsu.edu.ph server

www.dlsu.edu.ph?

103.231.241.180

Iterative server caches the response for future queries

CACHING/UPDATING DNS RECORDS

- **once (any) name server learns mapping, it *caches* mapping**
  - cache entries timeout (disappear) after some time (TTL)
  - TLD servers typically cached in local name servers
    - thus root name servers not often visited
- **cached entries may be *out-of-date* (best-effort name-to-address translation!)**
  - if name host changes IP address, may not be known Internet-wide until all TTLs expire!
- **update/notify mechanisms proposed IETF standard**
  - RFC 2136

INSERTING RECORDS INTO DNS

Example: new startup “Network Utopia”

- ❑**register name networkuptopia.com at *DNS registrar* (e.g., Network Solutions)**
  - provide names, IP addresses of authoritative name server (primary and secondary)
  - registrar inserts NS, A RRs into .com TLD server:

```
(networkutopia.com, dns1.networkutopia.com, NS)
(dns1.networkutopia.com, 212.212.212.1, A)
```

- ❑**create authoritative server locally with IP address** `212.212.212.1`
  - type A record for www.networkuptopia.com
  - type MX record for networkutopia.com

DNS SECURITY

DDoS attacks

- ❑ **bombard root servers with traffic**
  - not successful to date
  - traffic filtering
  - local DNS servers cache IPs of TLD servers, allowing root server bypass
- ❑ **bombard TLD servers**
  - potentially more dangerous

Redirect attacks

- ❑ **man-in-middle**
  - intercept DNS queries
- ❑ **DNS poisoning**
  - send bogus relies to DNS server, which caches
- ❑ **Exploit DNS for DDoS**
  - send queries with spoofed source address: target IP
  - requires amplification

MESSAGE FROM DPO

"The information and data contained in the online learning modules, such as the content, audio/visual materials or artwork are considered the intellectual property of the author and shall be treated in accordance with the IP Policies of DLSU. They are considered confidential information and intended only for the person/s or entities to which they are addressed. They are not allowed to be disclosed, distributed, lifted, or in any way reproduced without the written consent of the author/owner of the intellectual property."