Lecture 3 – DNS, Network Configurations

COMP1002 (Cybersecurity and Networks)

Outline

- Part 1: Application Layer - DNS
- Part 2: Network Configurations – based on CISCO devices

Part 1: Applications Layer - DNS

(Chapter 2 of the Textbook)

DNS: Domain Name System

people: many identifiers:

- SSN, name, passport #

Internet hosts, routers:

- IP address (32 bit) - used for addressing datagrams
- "name", e.g., www.yahoo.com - used by humans

Q: how to map between IP address and name, and vice versa ?

Domain Name System:

- *distributed database* implemented in hierarchy of many *name servers*
- *application-layer protocol:* hosts, name servers communicate to *resolve* names (address/name translation)

DNS: services, structure

DNS services

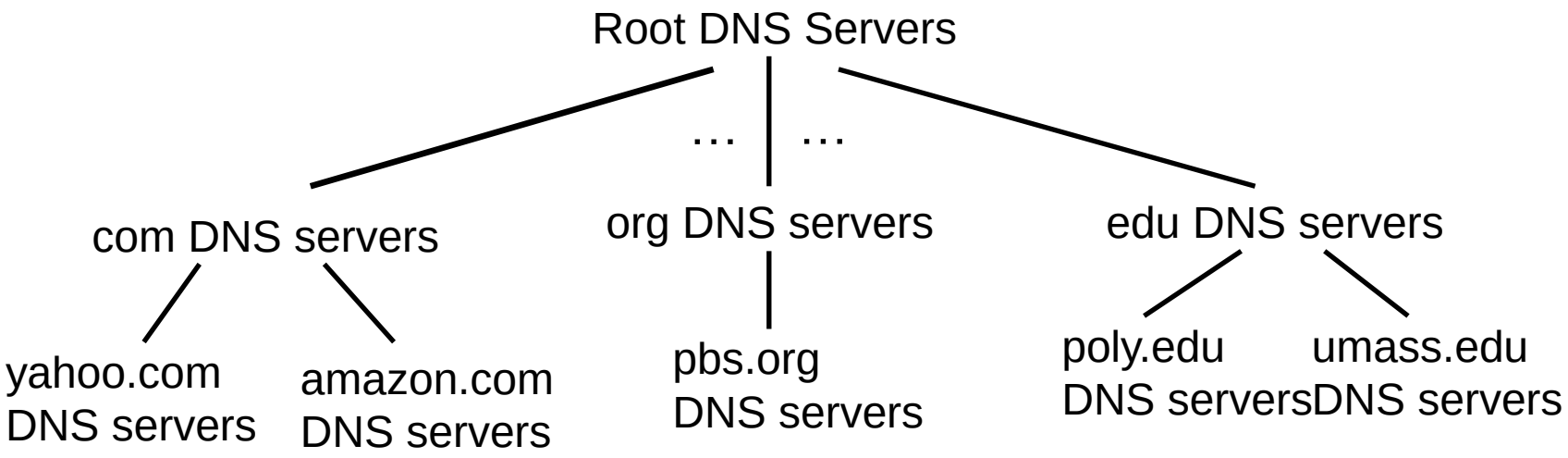
- hostname to IP address translation
- host aliasing
  - canonical, alias names
- mail server aliasing
- load distribution
  - replicated Web servers: many IP addresses correspond to one name

why not centralize DNS?

- single point of failure
- traffic volume
- distant centralized database
- maintenance

A: doesn't scale!

DNS: a distributed, hierarchical database

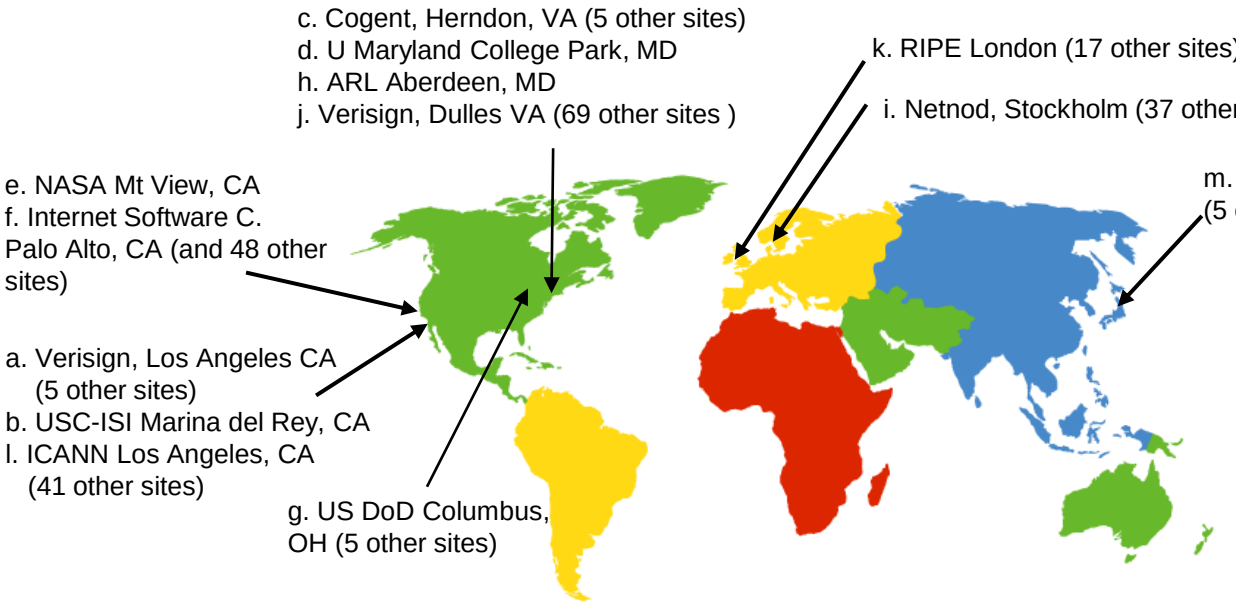


*client wants IP for **www.amazon.com**; 1st approximation:*

- client queries root server to find com DNS server
- client queries .com DNS server to get amazon.com DNS server
- client queries amazon.com DNS server to get IP address for www.amazon.com

DNS: root name servers

- contacted by local name server that can not resolve name
- root name server:
  - contacts authoritative name server if name mapping not known
  - gets mapping
  - returns mapping to local name server



13 logical root name "servers" worldwide

- *each "server" replicated many times*

TLD, authoritative servers

top-level domain (TLD) servers:

- responsible for com, org, net, edu, etc. and all top-level country domains, e.g.: uk, fr, ca, jp
- Network Solutions maintains servers for .com TLD
- Educause (sole registrar) for .edu TLD

authoritative DNS servers:

- organization's own DNS server(s), providing authoritative hostname to IP mappings for organization's named hosts
- can be maintained by organization or service provider

Local DNS name server

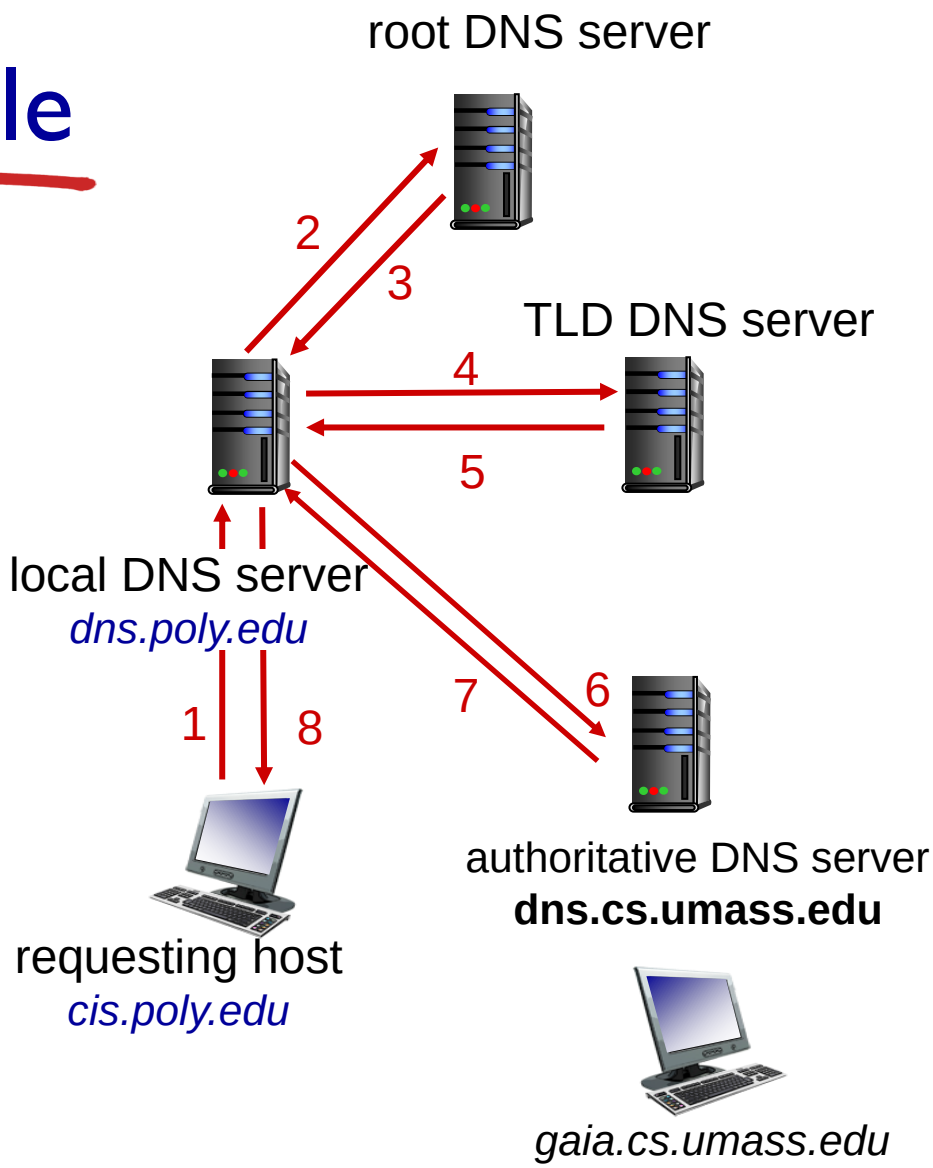
- does not strictly belong to hierarchy
- each ISP (residential ISP, company, university) has one
  - also called "default name server"
- when host makes DNS query, query is sent to its local DNS server
  - has local cache of recent name-to-address translation pairs (but may be out of date!)
  - acts as proxy, forwards query into hierarchy

DNS name resolution example

- host at cis.poly.edu wants IP address for gaia.cs.umass.edu

iterated query:

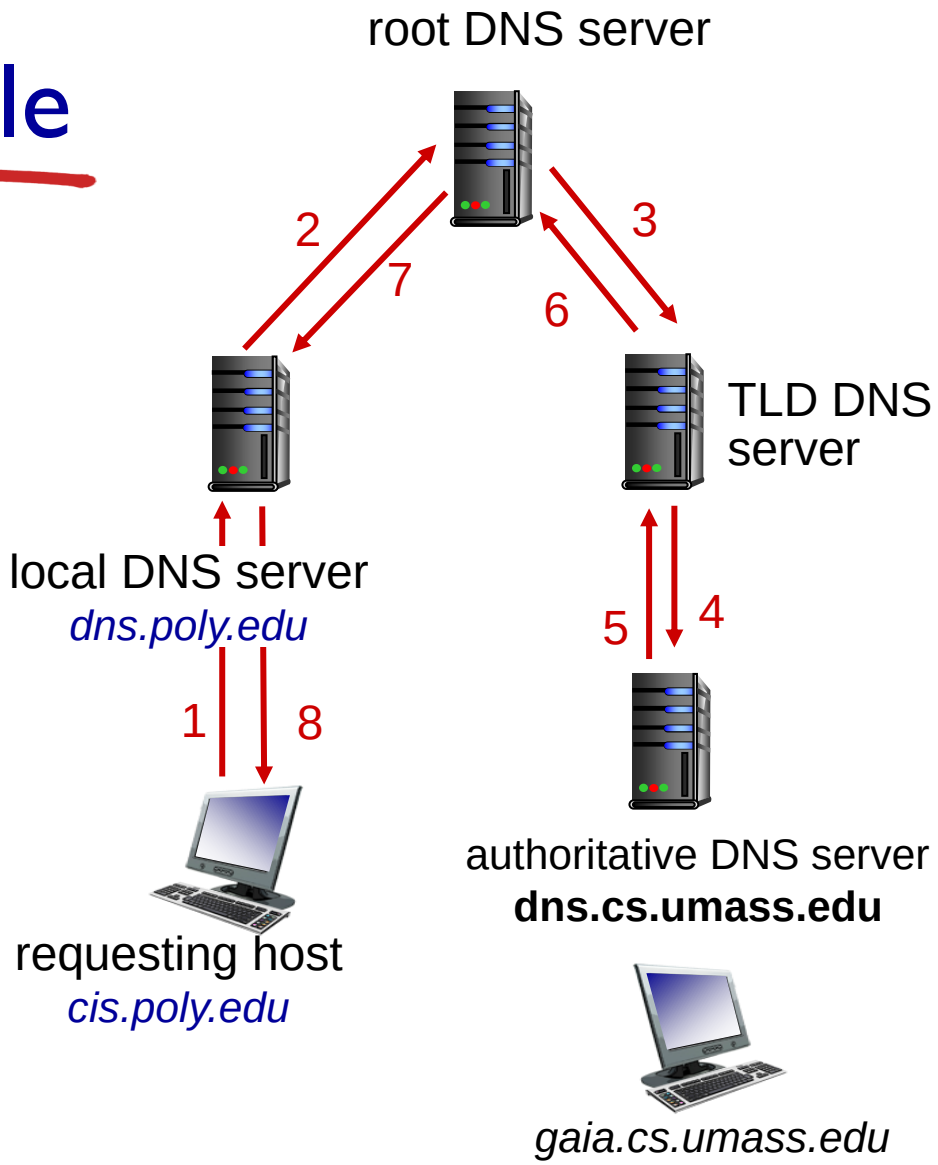
- contacted server replies with name of server to contact
- "I don't know this name, but ask this server"



DNS name resolution example

recursive query:

- puts burden of name resolution on contacted name server
- heavy load at upper levels of hierarchy?



DNS: caching, updating 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

NSLOOKUP - I

- Nslookup uses "resolver" software
- Allows you to make DNS queries and see responses

```
U:\>nslookup www.google.co.uk
Server:  ils022.uopnet.plymouth.ac.uk
Address:  141.163.201.222

Non-authoritative answer:
Name:    www.google.co.uk
Addresses:  2a00:1450:4009:80e::2003
          216.58.212.99


U:\>nslookup -type=NS google.co.uk
Server:  ils022.uopnet.plymouth.ac.uk
Address:  141.163.201.222

Non-authoritative answer:
google.co.uk    nameserver = ns1.google.com
google.co.uk    nameserver = ns2.google.com
google.co.uk    nameserver = ns4.google.com
google.co.uk    nameserver = ns3.google.com

ns1.google.com  internet address = 216.239.32.10
ns1.google.com  AAAA IPv6 address = 2001:4860:4802:32::a
ns2.google.com  internet address = 216.239.34.10
ns2.google.com  AAAA IPv6 address = 2001:4860:4802:34::a
ns4.google.com  internet address = 216.239.38.10
ns4.google.com  AAAA IPv6 address = 2001:4860:4802:38::a
ns3.google.com  internet address = 216.239.36.10
ns3.google.com  AAAA IPv6 address = 2001:4860:4802:36::a
```

NSLOOKUP-2

```
C:\Users\lsun>nslookup www.plymouth.ac.uk
Server:  CENT-0-007.uopnet.plymouth.ac.uk
Address:  10.7.4.7

Non-authoritative answer:
Name:    www.plymouth.ac.uk
Address:  37.128.134.101


C:\Users\lsun>ping www.plymouth.ac.uk

Pinging www.plymouth.ac.uk [37.128.134.101] with 32 bytes of data:
Reply from 37.128.134.101: bytes=32 time=8ms TTL=52
Reply from 37.128.134.101: bytes=32 time=8ms TTL=52
Reply from 37.128.134.101: bytes=32 time=8ms TTL=52
Reply from 37.128.134.101: bytes=32 time=8ms TTL=52

Ping statistics for 37.128.134.101:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 8ms, Maximum = 8ms, Average = 8ms

C:\Users\lsun>nslookup 37.128.134.101
Server:  CENT-0-007.uopnet.plymouth.ac.uk
Address:  10.7.4.7

Name:    www.plymouth.ac.uk
Address:  37.128.134.101
```

NSLOOKUP - 3

```
PS C:\Users\lsun> nslookup microsoft.com
Server:  bthub
Address:  192.168.1.254

Non-authoritative answer:
Name:    microsoft.com
Addresses:  20.103.85.33
          20.53.203.50
          20.112.52.29
          20.84.181.62
          20.81.111.85

PS C:\Users\lsun> nslookup -type=NS microsoft.com
Server:  bthub
Address:  192.168.1.254

Non-authoritative answer:
microsoft.com   nameserver = ns2-39.azure-dns.net
microsoft.com   nameserver = ns3-39.azure-dns.org
microsoft.com   nameserver = ns4-39.azure-dns.info
microsoft.com   nameserver = ns1-39.azure-dns.com
PS C:\Users\lsun>
PS C:\Users\lsun> nslookup -type=mx microsoft.com
Server:  bthub
Address:  192.168.1.254

Non-authoritative answer:
microsoft.com   MX preference = 10, mail exchanger = microsoft-com.mail.protection.outlook.com
PS C:\Users\lsun>
```

NSLOOKUP - 4

```
PS C:\Users\lsun> nslookup microsoft.com
Server:  bthub
Address:  192.168.1.254

Non-authoritative answer:
Name:    microsoft.com
Addresses:  20.84.181.62
          20.53.203.50
          20.103.85.33
          20.112.52.29
          20.81.111.85

PS C:\Users\lsun> nslookup microsoft.com 8.8.8.8
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
Name:    microsoft.com
Addresses:  20.112.52.29
          20.81.111.85
          20.84.181.62
          20.103.85.33
          20.53.203.50

PS C:\Users\lsun>
```

Query a public DNS server (e.g. 8.8.8.8) to get the answer

DNS records

DNS: distributed database storing resource records (RR)

RR format: `(name, value, type, ttl)`

type=A

- **`name`** is hostname
- **`value`** is IP address

type=NS

- **`name`** is domain (e.g., foo.com)
- **`value`** is hostname of authoritative name server for this domain

type=CNAME

- **`name`** is alias name for some "canonical" (the real) name
- **`www.ibm.com`** is really **`servereast.backup2.ibm.com`**
- **`value`** is canonical name

type=MX

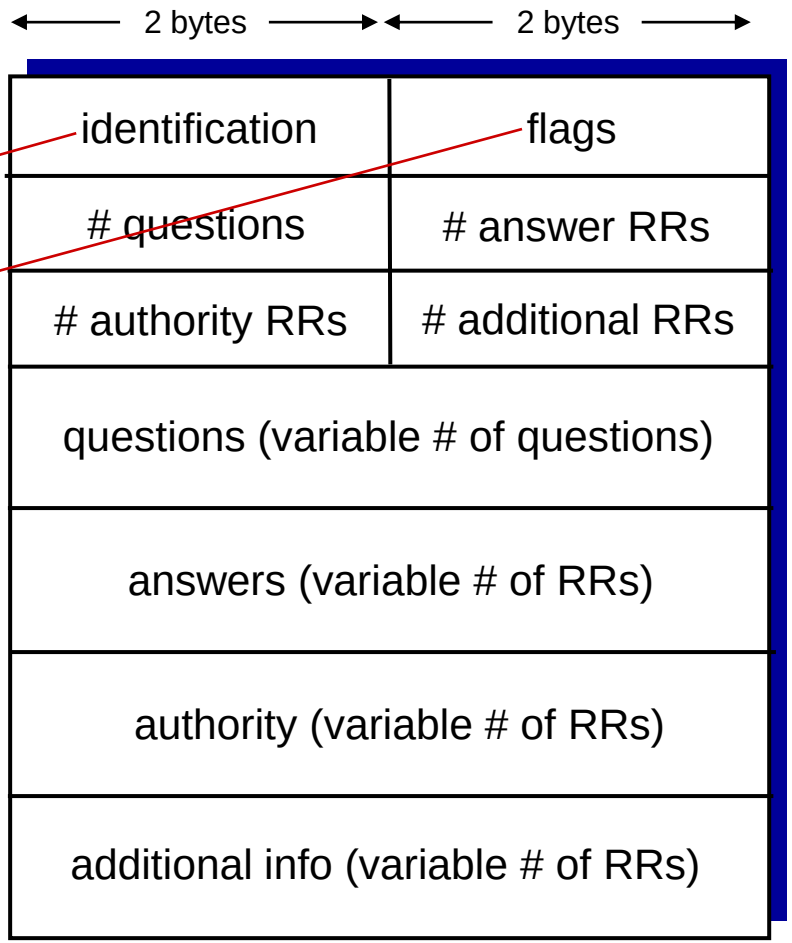
- **`value`** is name of mailserver associated with **`name`**

DNS protocol, messages

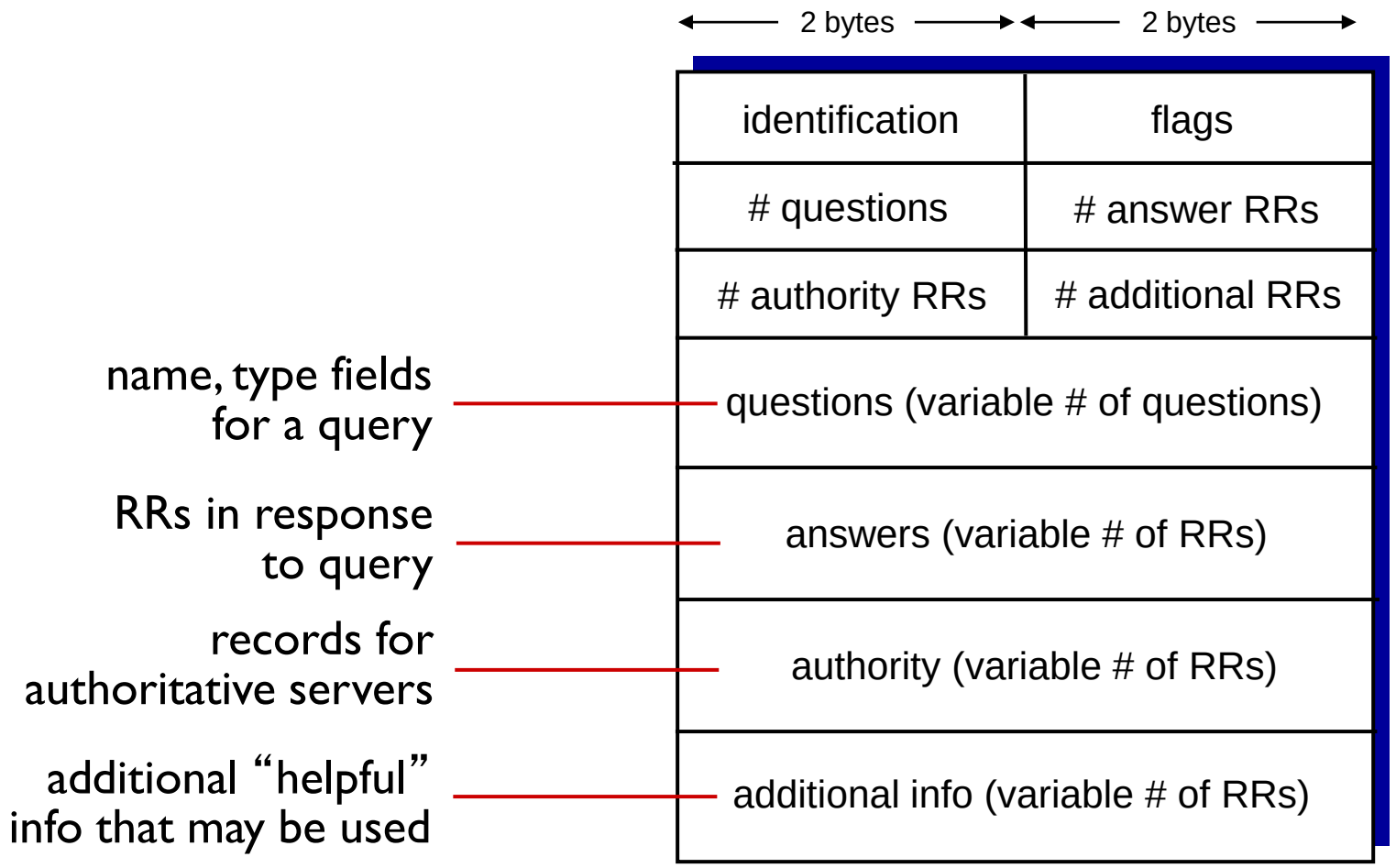
- *query* and *reply* messages, both with same *message format*

message header

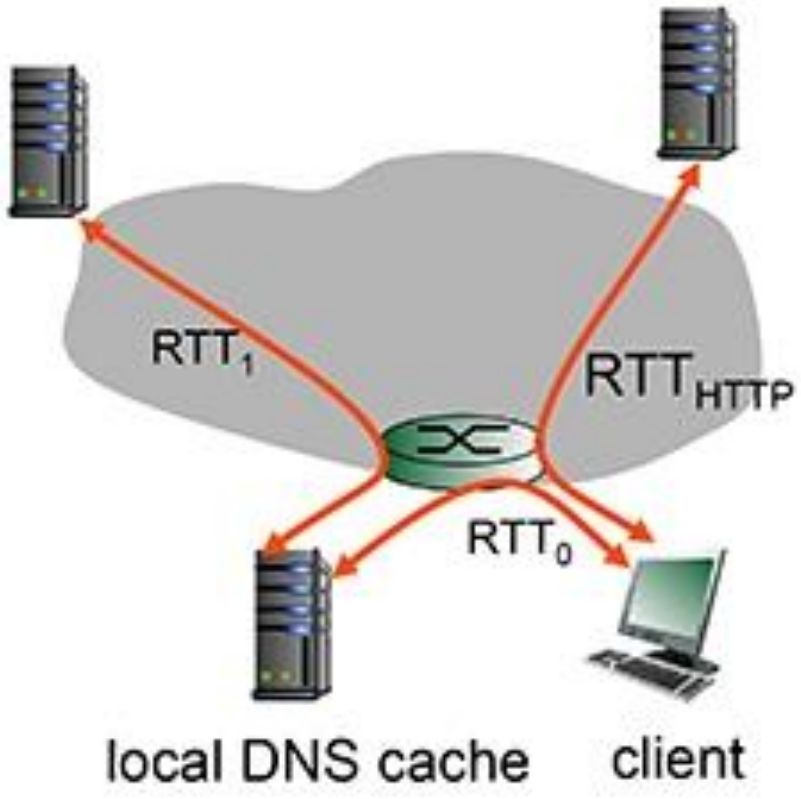
- identification: 16 bit # for query, reply to query uses same #
- flags:
  - query or reply
  - recursion desired
  - recursion available
  - reply is authoritative



DNS protocol, messages



Question



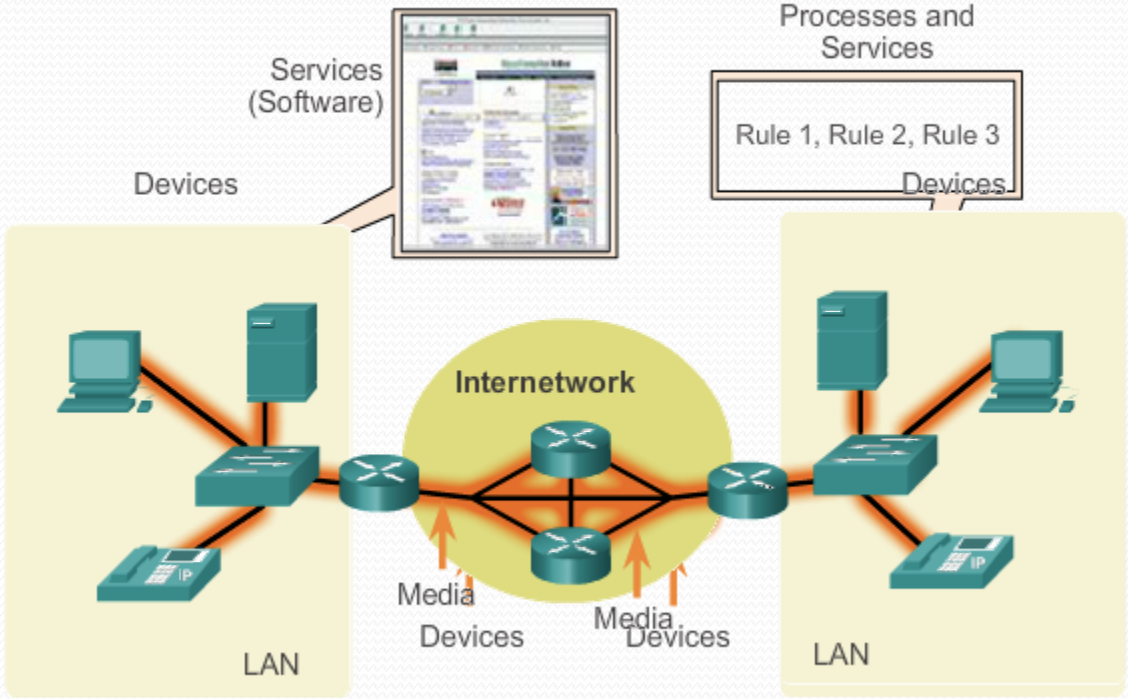
- You click on a link to obtain a web page. To obtain the IP address of the server, two DNS servers are visited. Given that RTT_0=1ms; RTT_1 = 16ms; RTT_{HTTP}=23ms. How long does it take from when the client clicks on the link until the client receives the object?

Part 2: Network Configurations based on Cisco Devices

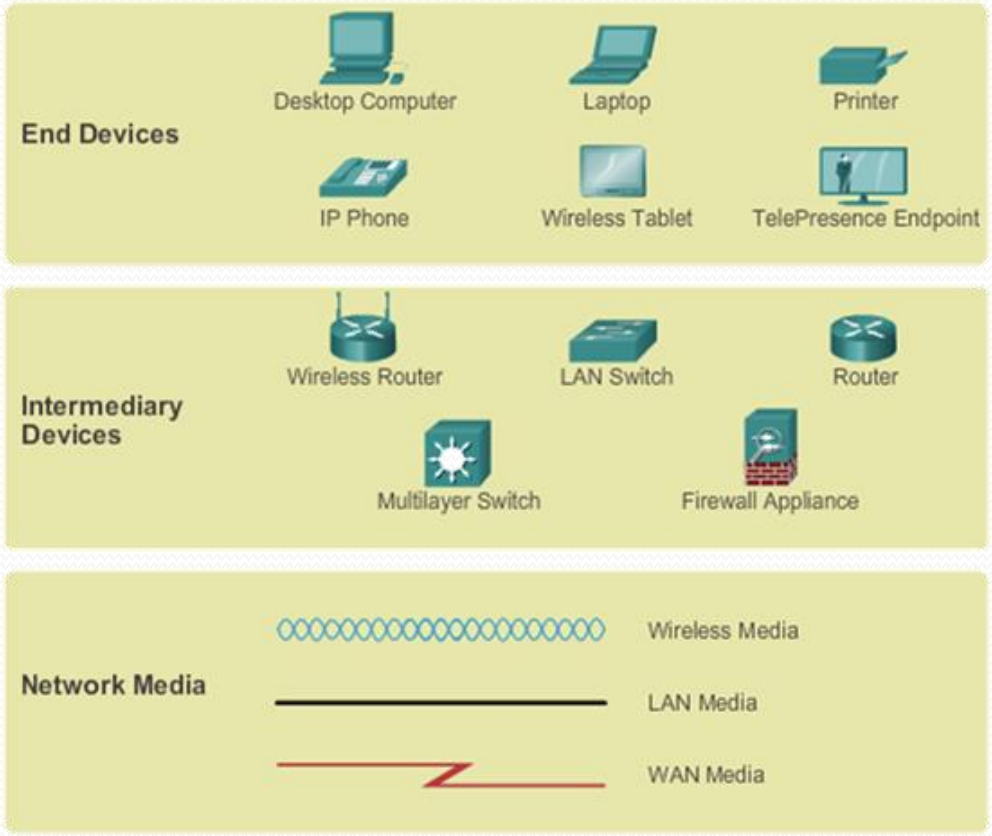
Network Configurations

- Some Network Background (CCNA1 Chapter 1)
  - Network Components
  - Network Topology
  - LANs and WANs
  - internet and the Internet
- Basic Switch and End Devices Configuration (Chapter 2)
  - Cisco IOS
  - IOS configuration
  - Addressing

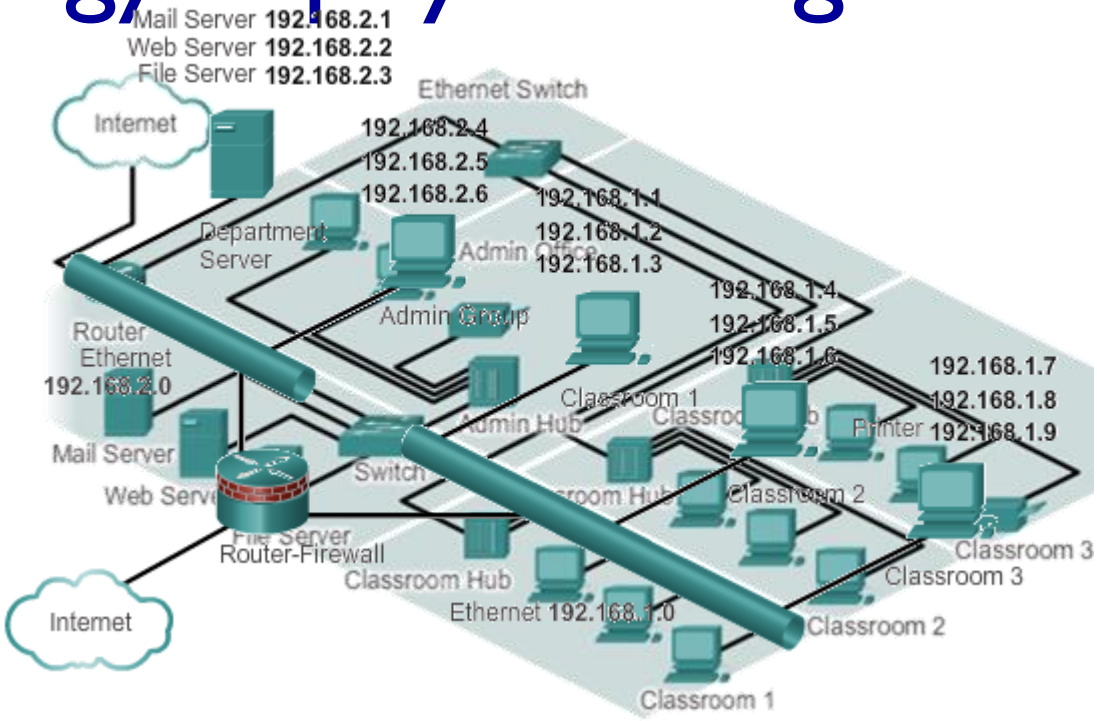
Network components



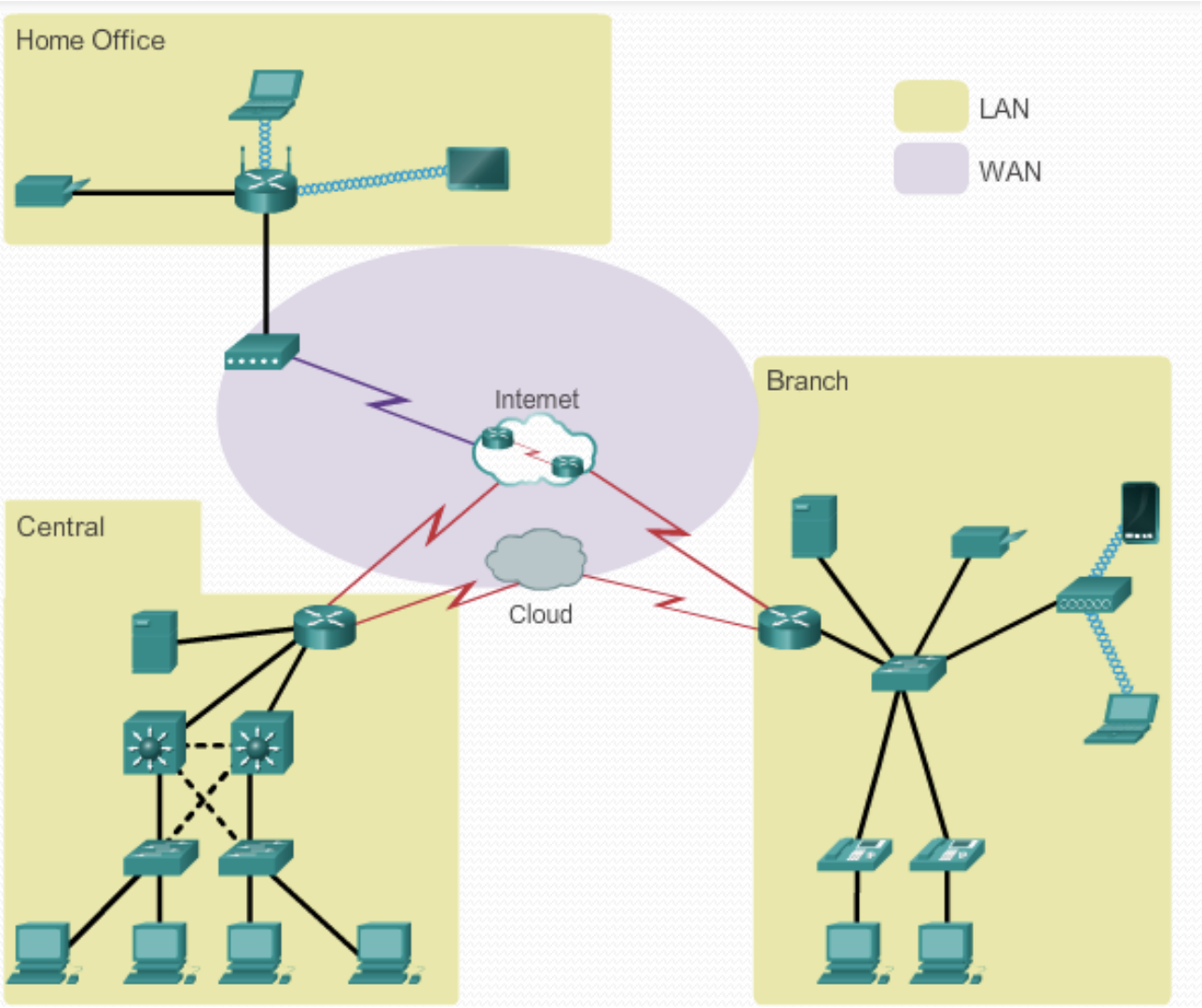
Network components



Topology - physical/logical



LANs and WANs



internet and the Internet

- internet – a collection of interconnected networks, providing a range of communication services
- (the) Internet – the largest internet in place, spanning over the entire globe
- a worldwide collection of interconnected networks (internetworks or internet for short), cooperating with each other to exchange information using common standards

Cisco IOS

- Provides devices with network services
  - Basic routing and switching functions
  - Reliable and secure access to resources
  - Network scalability
- Typically accessed through a Command Line Interface (CLI)
- IOS (Internetworking Operating System) – single file (few MB in size)
  - stored in the semi-permanent memory – flash
  - Content maintained when rebooted
  - May be erased
- IOS - loaded into RAM at each reboot

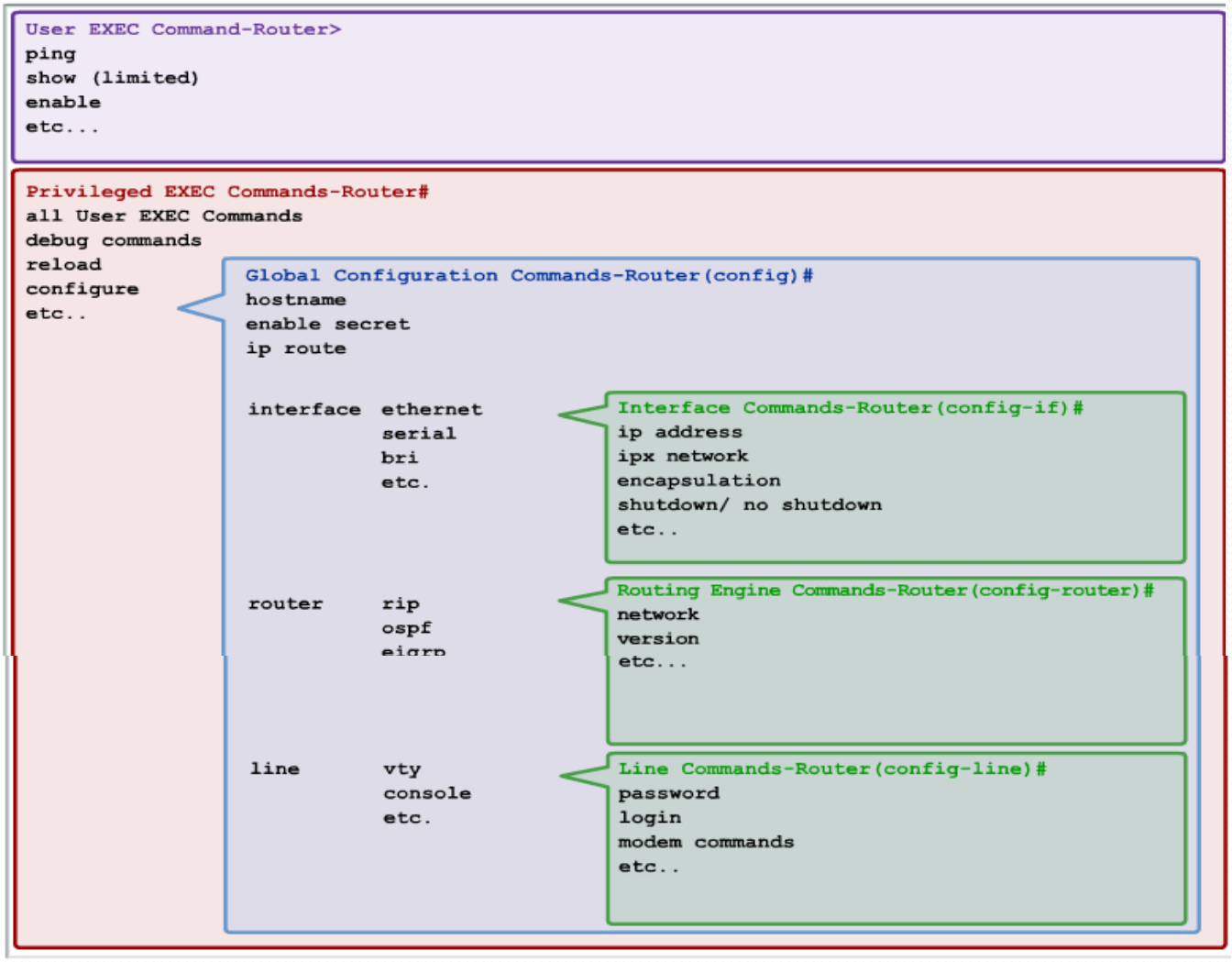
IOS functions

- Providing network security
- IP addressing of virtual and physical interfaces
- Enabling interface-specific configurations to optimize connectivity of the respective media
- Routing
- Enabling quality of service (QoS) technologies
- Supporting network management technologies

Accessing IOS

- Console (CTY line)
  - Using a low speed serial connection
  - initial configuration, disaster recovery, troubleshooting, password recovery
  - Physical security – may not require a password to connect
- Telnet or SSH (VTY line)
  - Require active networking services
  - Avoid telnet – no encryption, password in clear
- AUX port
  - Used via a telephone connection
  - Can be used locally, similar to CTY
  - Used only when CTY fails

IOS modes


User EXEC Command-Router>
ping
show (limited)
enable
etc...
Privileged EXEC Commands-Router#
all User EXEC Commands
debug commands
reload
configure
etc..
Global Configuration Commands-Router(config)#
hostname
enable secret
ip route
interface ethernet
serial
bri
etc.
Interface Commands-Router(config-if)#
ip address
ipx network
encapsulation
shutdown/ no shutdown
etc..
router rip
ospf
eigrp
Routing Engine Commands-Router(config-router)#
network
version
etc...
line vty
console
etc.
Line Commands-Router(config-line)#
password
login
modem commands
etc..

IOS primary modes

User EXEC Mode

Limited examination of router. Remote access.

```
Switch>
Router>
```

Global Configuration Mode

Global configuration commands.

```
Switch(config)#
Router(config)#
```

Privileged EXEC Mode

Detailed examination of router, Debugging and testing. File manipulation. Remote access.

```
Switch#
Router#
```

Other Configuration Modes

Specific service or interface configurations.

```
Switch(config-)#
Router(config-)#
```

Navigating configuration modes

```
Router con0 is now available.

Press RETURN to get started.

User Access Verification
Password:
Router>
Router>enable
Password:
Router#
Router#disable
Router>
Router>exit
```

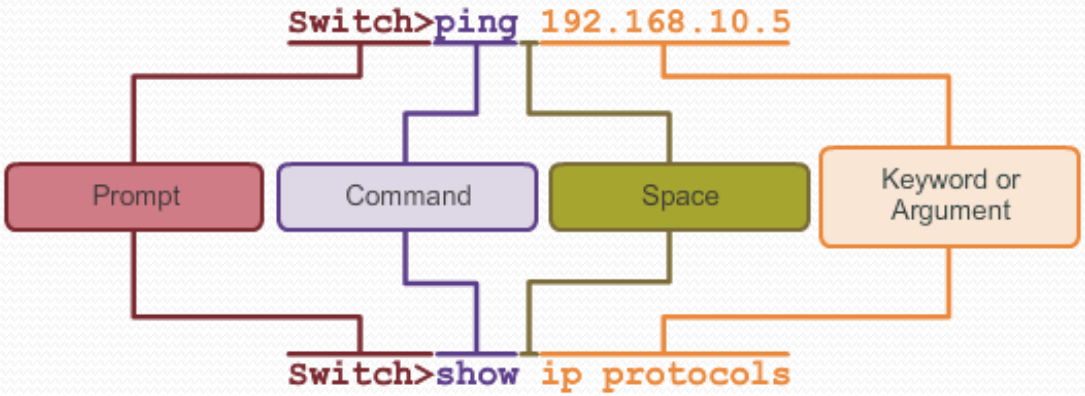
User EXEC Mode Prompt

Privileged EXEC Mode Prompt

User EXEC Mode Prompt

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.
End with CNTL/Z.
Switch(config)#interface vlan 1
Switch(config-if)#exit
Switch(config)#exit
Switch#
```

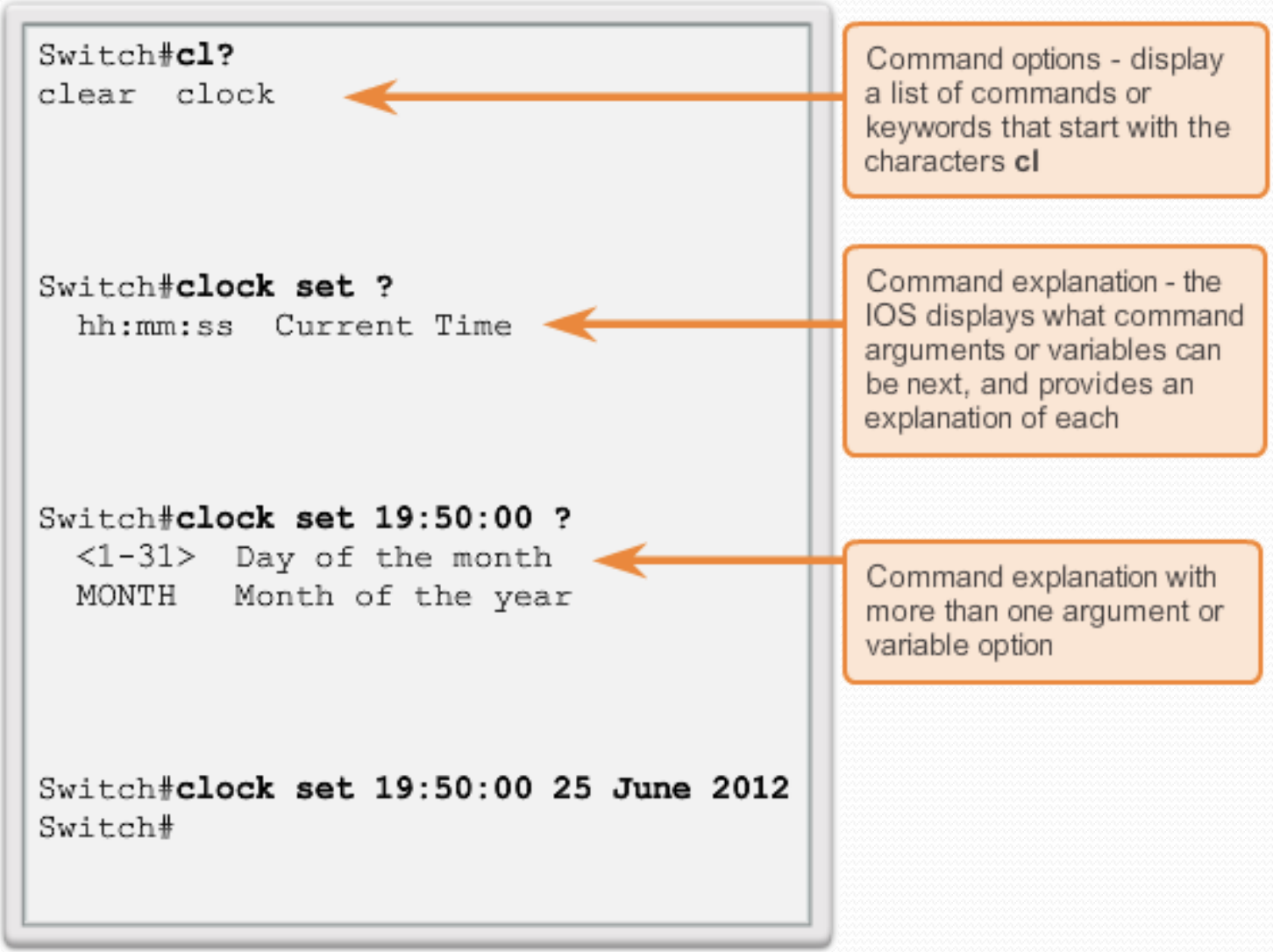
IOS commands



When describing the use of commands, we generally use these conventions.

Convention	Description
boldface	Boldface text indicates commands and keywords that you enter literally as shown.
italics	Italic text indicates arguments for which you supply values.
[x]	Square brackets indicate an optional element (keyword or argument).
{x}	Braces indicate a required element (keyword or argument).
[x {y | z}]	Braces and vertical lines within square brackets indicate a required choice within an optional element.

Context-sensitive help



Command syntax help

```
Switch#>clock set
% Incomplete command.
Switch#clock set 19:50:00
% Incomplete command.
```

The IOS returns a help message indicating that required keywords or arguments were left off the end of the command.

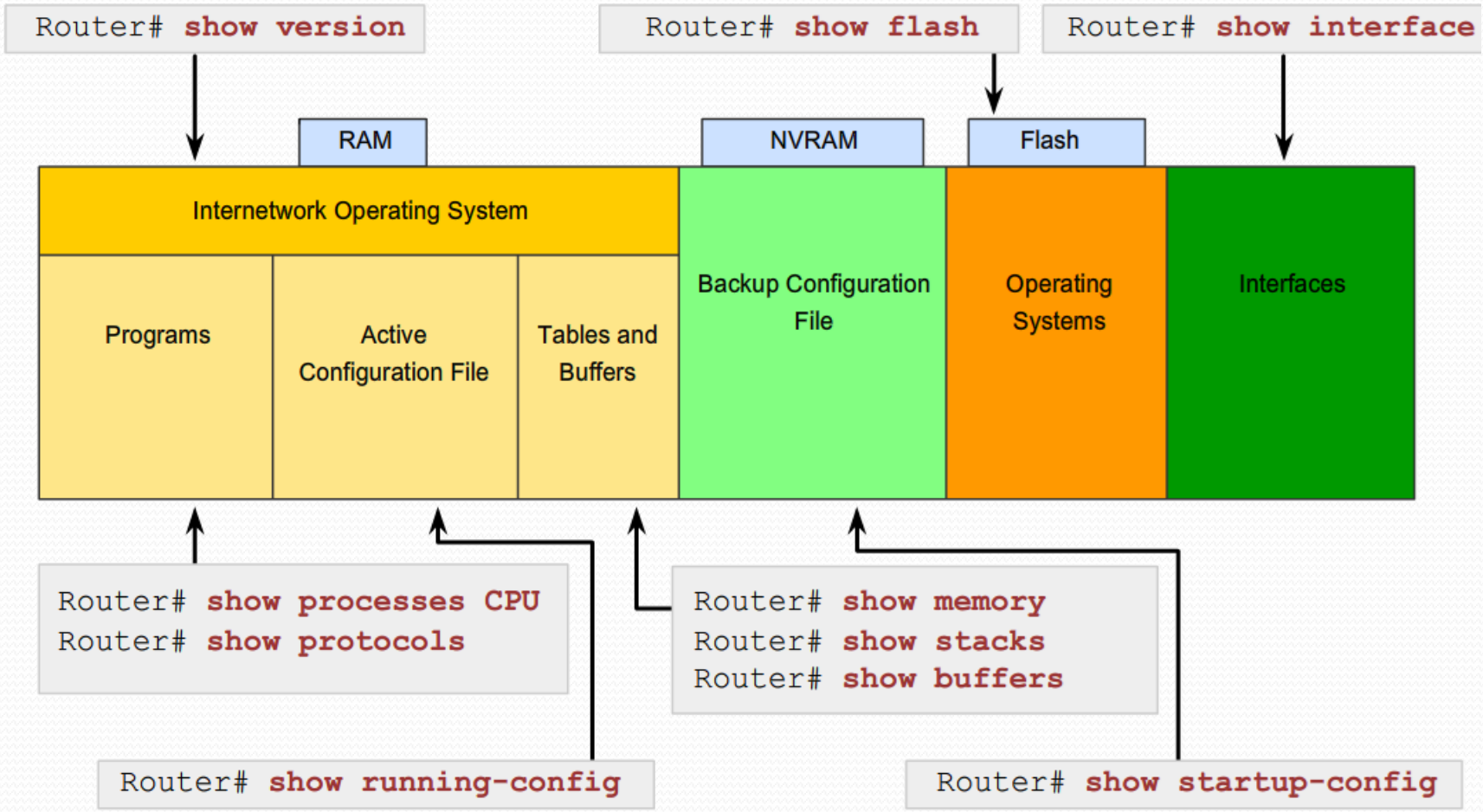
```
Switch#c
% Ambiguous command:'c'
```

The IOS returns a help message to indicate that there were not enough characters entered for the command interpreter to recognize the command.

```
Switch#clock set 19:50:00 25 6
                           ^
% Invalid input detected at '^'
marker.
```

The IOS returns a **"^"** to indicate where the command interpreter can not decipher the command.

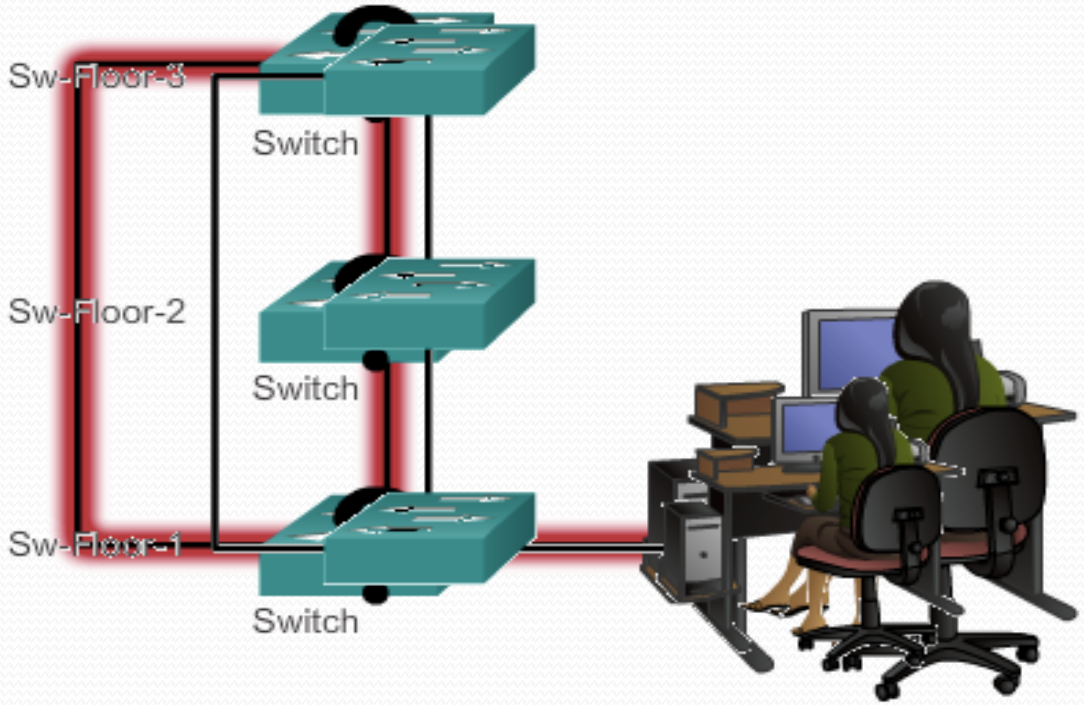
IOS examination commands



Getting basic

- Hostnames
- Limiting access
- Saving configurations

Hostnames



Configure the switch hostname to be 'Sw-Floor-1'.

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# hostname Sw-Floor-1
Sw-Floor-1(config)#
```

You successfully configured the switch hostname.

Passwords

- Console password - console connection

```
Switch(config)#line console 0
Switch(config-line)#password password
Switch(config-line)#login
```

- Enable password - privileged EXEC mode

```
Router(config)#enable password password
```

- Enable secret - privileged EXEC mode (encrypted)

```
Router(config)#enable secret password
```

- VTY password – telnet access

```
Router(config)#line vty 0 4
Router(config-line)#password password
Router(config-line)#login
```

- Service password-encryption
  - Encrypt the password stored in the config file

```
Router(config)#service password-encryption
```

MOTD banner


Sw1-Floor-1(config)#banner motd # This is a secure system. Authorized Access ONLY!!! #
This configuration results in this message of the day banner.
Delimiting characters are not included in the message.
Sw1-Floor-1 con0 is now available
Press RETURN to get started.
This is a secure system. Authorized Access ONLY!!!
User Access Verification
password:
Sw1-Floor-1>enable
Password:
Sw1-Floor-1#

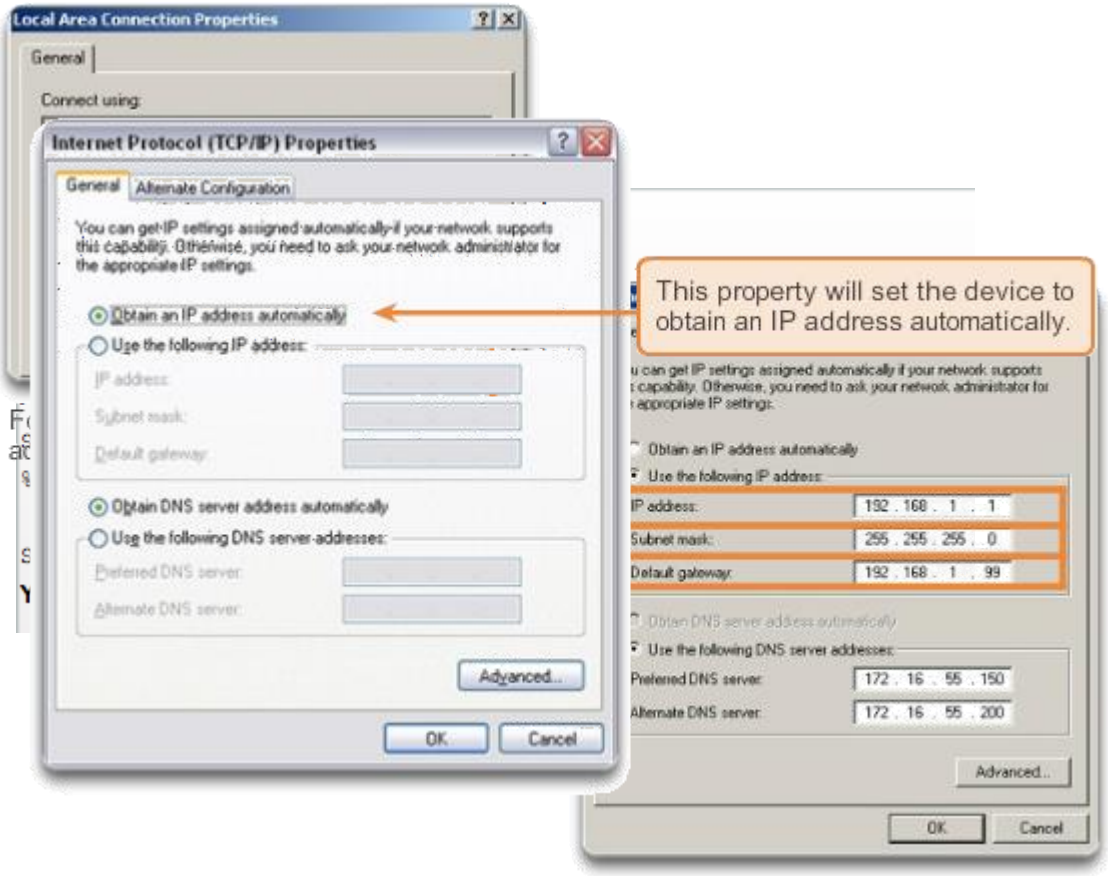
Managing configuration files

```
copy running-config startup-config
copy running-config tftp
erase startup-config
```

- Copy-paste using the terminal

  ```
  show running-config
  copy-paste
  ```

Addressing a device



Configuring router interfaces

- Ethernet

```
Router(config)#interface FastEthernet 0/0
Router(config-if)#ip address ip_address netmask
Router(config-if)#no shutdown
```

- Serial

```
Router(config)#interface Serial 0/0/0
Router(config-if)#ip address ip_address netmask
Router(config-if)#clock rate 56000
Router(config-if)#no shutdown
```

Testing configuration

- Ping loopback, local, remote interfaces
- Traceroute remote interfaces

Enter the command to verify the interface configuration on S1.

```
S1# show ip interface brief
Interface          IP-Address      OK?  Method  Status      Protocol
FastEthernet0/1    unassigned      YES  manual  up          up
FastEthernet0/2    unassigned      YES  manual  up          up
<output omitted>
Vlan1              192.168.10.2    YES  manual  up          up
```

You are now on S2. Enter the command to verify the interface configuration on S2.

```
S2# show ip interface brief
Interface          IP-Address      OK?  Method  Status      Protocol
FastEthernet0/1    unassigned      YES  manual  up          up
FastEthernet0/2    unassigned      YES  manual  up          up
<output omitted>
Vlan1              192.168.10.3    YES  manual  up          up
```

You successfully verified the interface assignment on S1 and S2.

Configure SVI

- Switch Virtual Interface – used for accessing the switch for configuration

```
Switch#configure terminal
Switch(config)#interface vlan 1
Switch(config-if)#ip address 192.168.1.10 255.255.255.0
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config)#ip default-gateway 192.168.1.1
```

Labs

- 2.9.1 – Basic switch and end device configuration – Packet tracer
  - Login onto www.netacad.com
  - Download packet tracer - https://www.netacad.com/portal/resources/packet-tracer