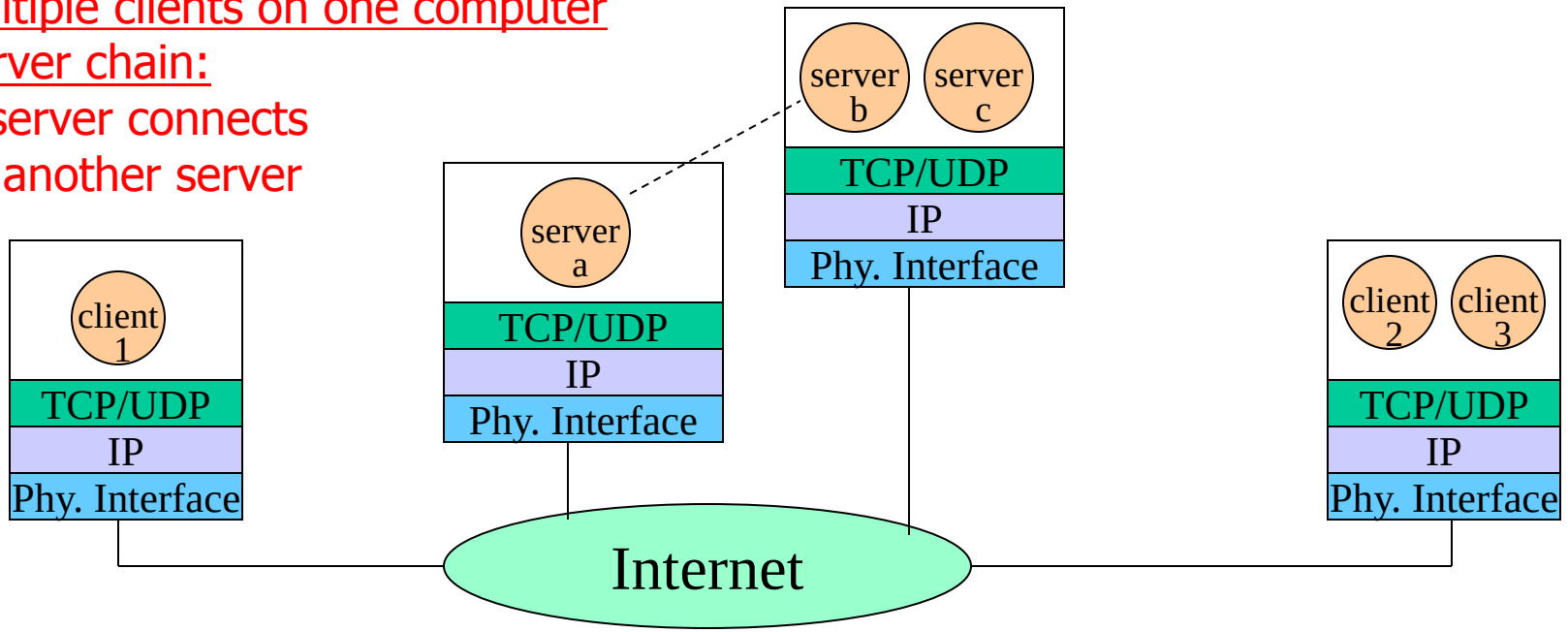
DNS, DHCP, SNMP & Network Security

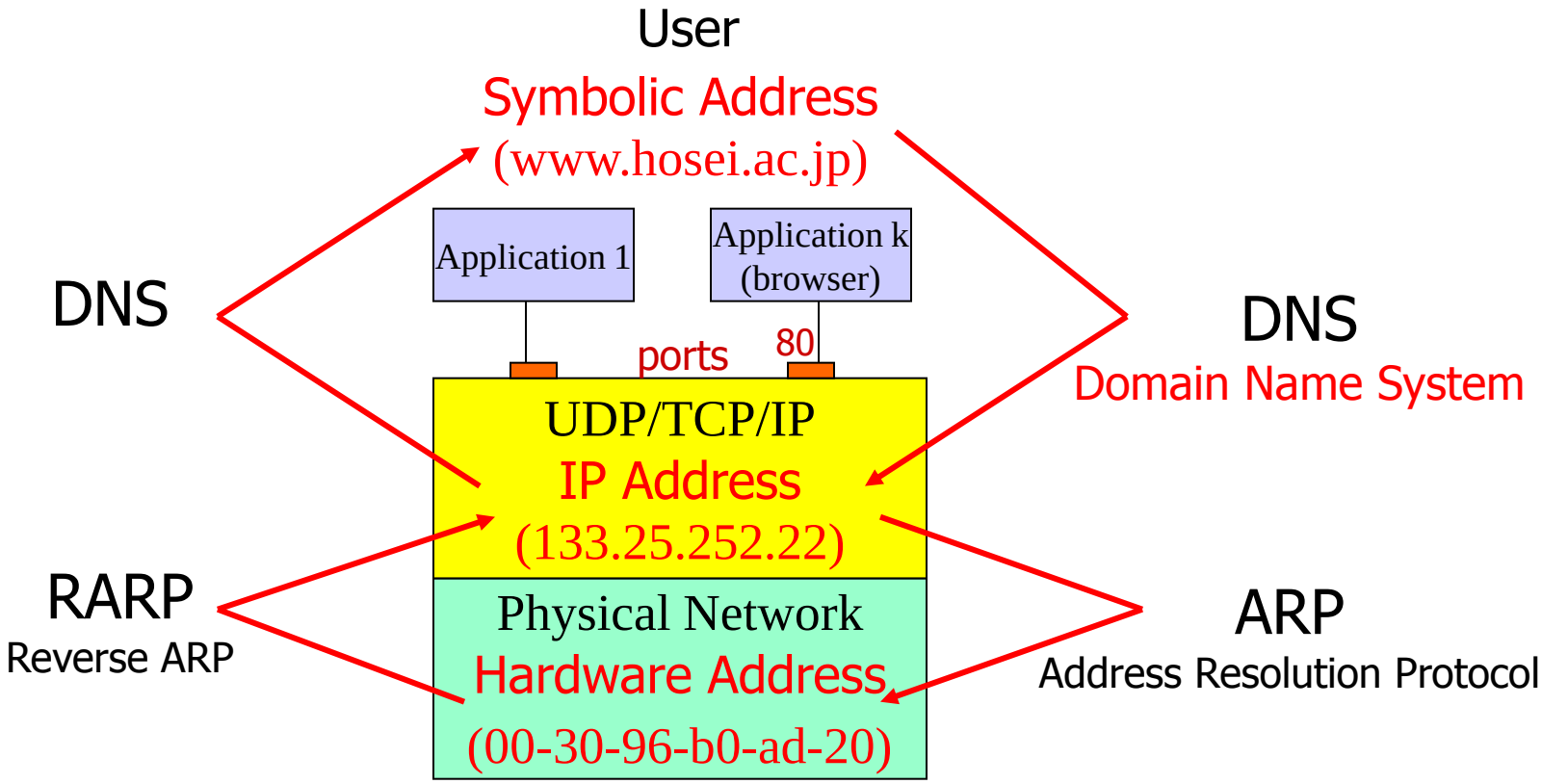
- Server–Client Model
- DNS Hierarchy and Syntax
- DNS Server Architecture and IP Address Resolution
- DHCP (Dynamic Host Configuration Protocol)
- NAT (Network Address Translation)
- Network Management Software and Model
- SNMP (Simple Network Management Protocol)
  - MIB Object Identifier and Data Representation
  - SNMP Operations and Message Format
- Network Security
  - Network Attack and Security Policy
  - Data Encryption Standards
  - Packet Filter and Internet Firewall

Server-Client Model

- Server
  - A program in a remote or local machine
  - Executed first and passively waits connection from clients
  - Accepts request from client and reply to the client
- Client
  - A program in a local machine
  - Executed later and actively initiates connection to server
  - Sends request to server and accepts reply from server
- Multiple servers on one computer
- Multiple clients on one computer
- Server chain:
  a server connects
  to another server



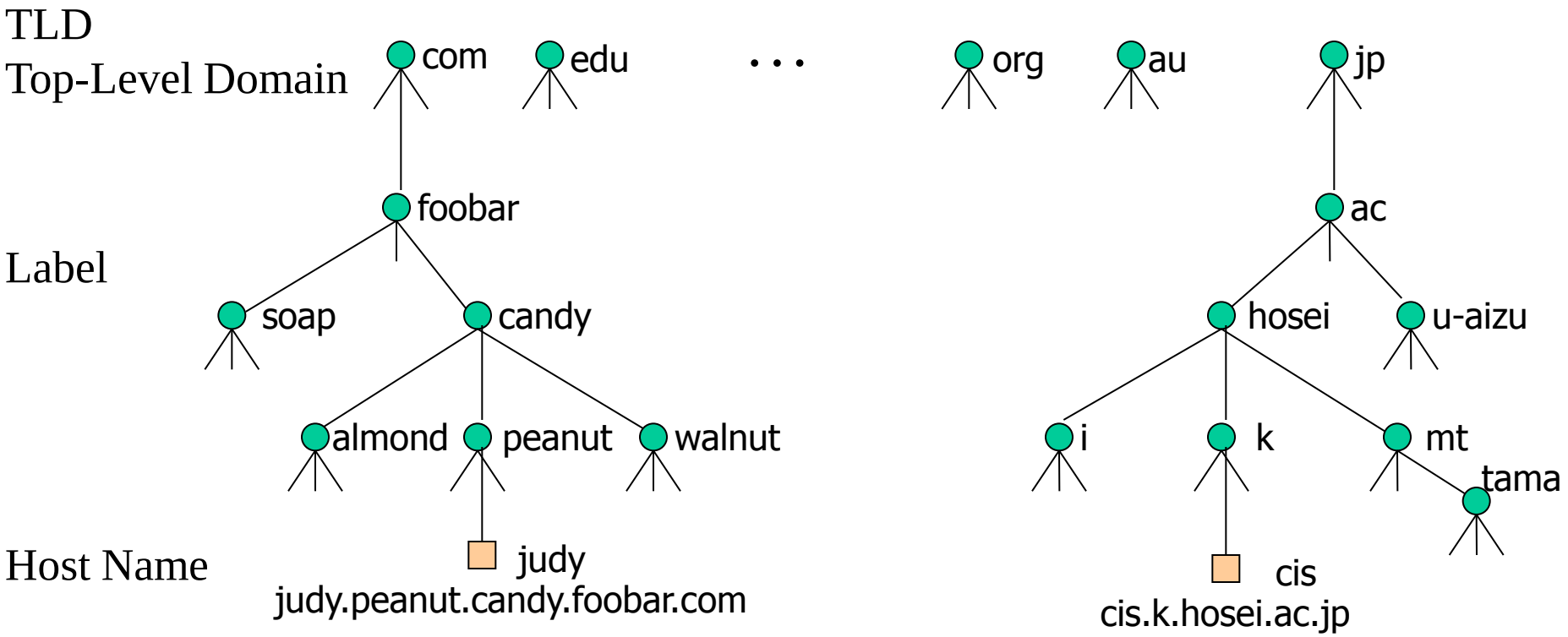
Address Resolution



- Hardware address used in physical network
- IP address used in the Internet
- Symbolic address (domain name) used in application or by users
- Address resolution - translation between different address schemes
- ARP/RARP: translation between IP address and hardware address
- DNS: translation between symbolic address (domain name) and IP address

Video: DHCP Introduction

DNS Hierarchy and Syntax

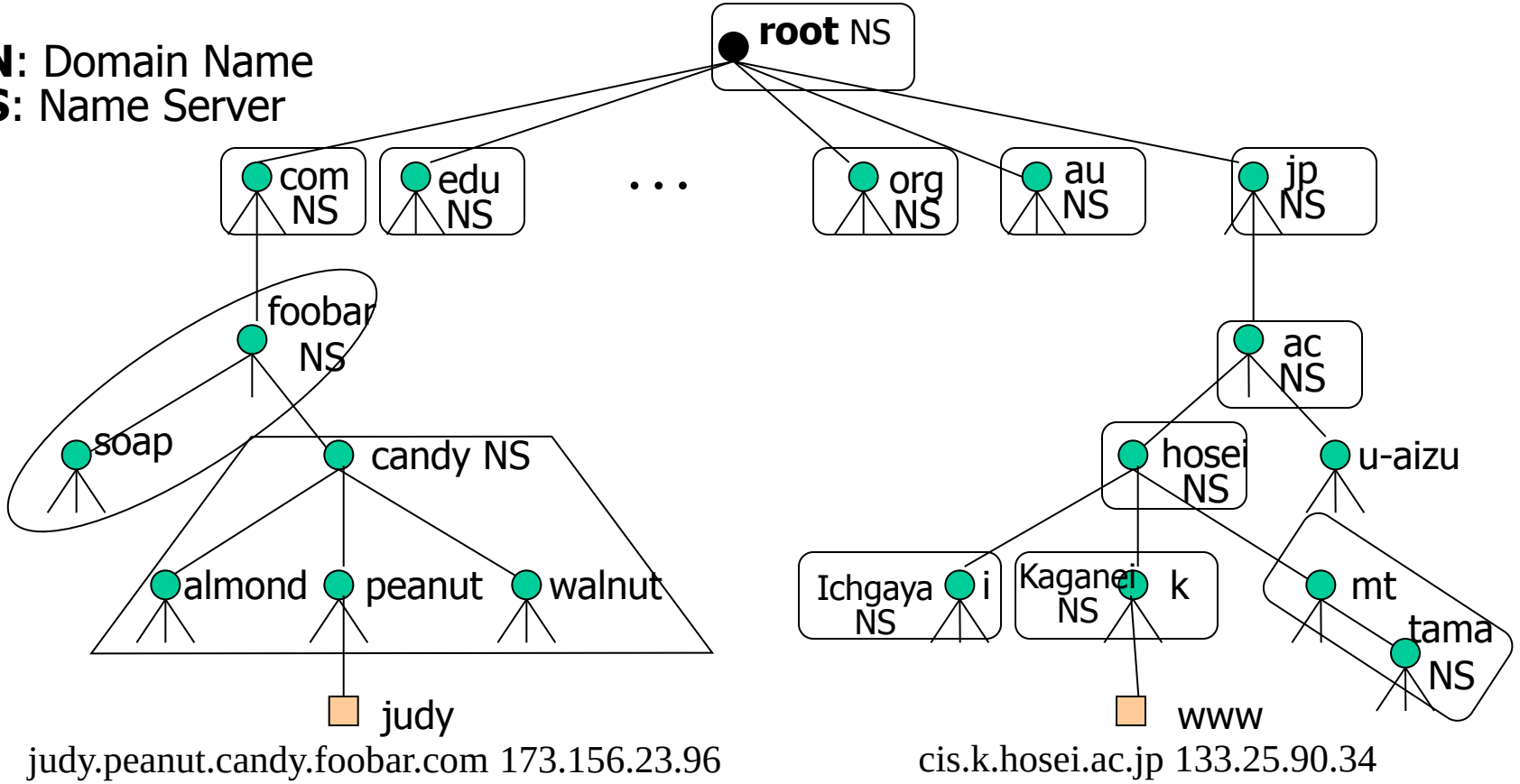


- Each organization registers its unique name like foobar, hosei and so on, with central authority under one TLD such as com, edu, org, au, jp, …
- Name subdivision, level, label and host name are controlled locally by organization

http://en.wikipedia.org/wiki/Domain_Name_System

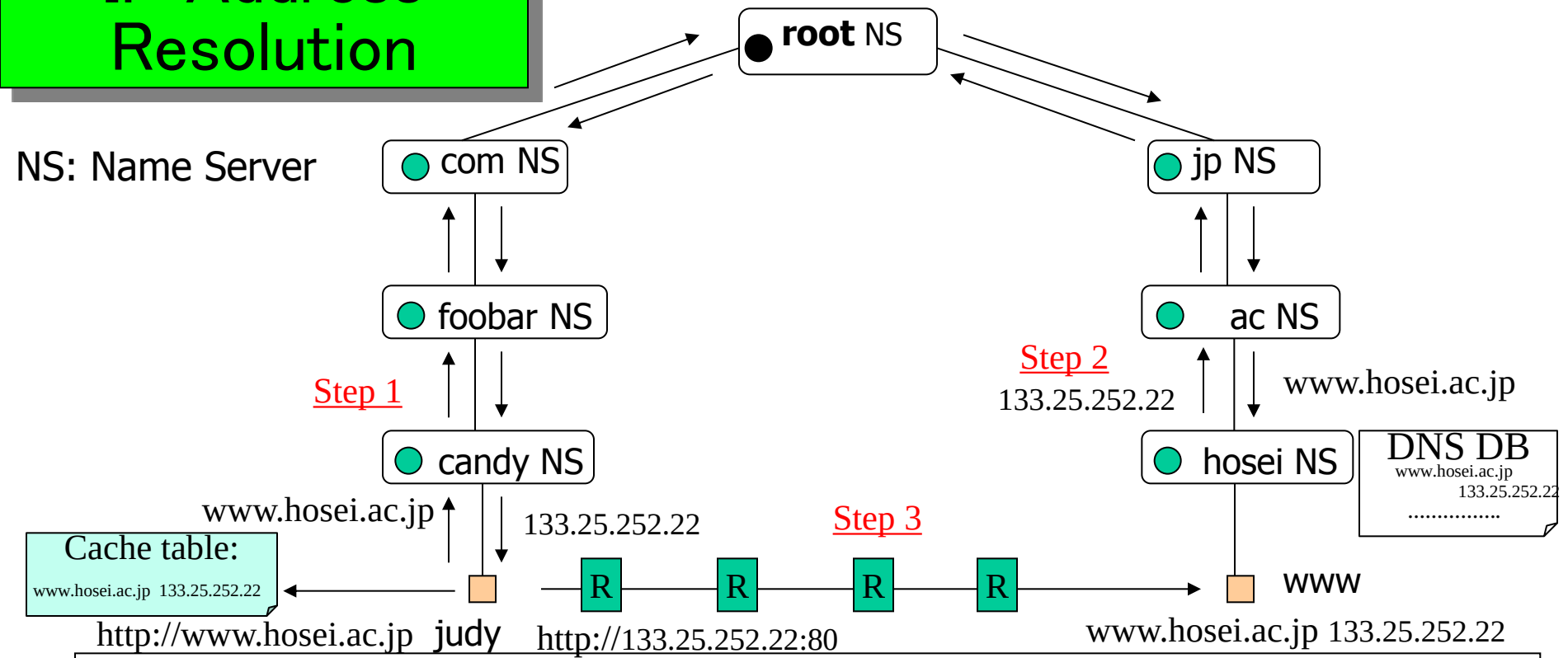
DNS Server Hierarchy

DN: Domain Name
NS: Name Server



- Root NS is needed to interconnect different TLD
- Choosing DNS server architecture
  - Small organizations can use a single name server
  - Large organizations often use multiple name servers according to division/location
- Each NS keeps a table of DN-IPAddr pairs of local hosts and knows up/low NS

IP Address Resolution



- DNS request is forwarded to root server, which points at next server to use
- Eventually, authoritative server is located and IP address is returned
- DNS server hierarchy traversal is called *iterative resolution*
- Servers and hosts use *caching* to reduce the number of DNS requests
- Each domain may keep many NS copies to speedup address resolution
  more than 13 root servers distributed all around the world
- DNS Types: A, NS, MX (Mail Exchange), SOA (Start OF Authority), CNAME (Canonical Name)
- nslookup utility: >domain_name or IP address, >set querytype=NS, A, …

An Animation at http://www.youtube.com/watch?v=2ZUxoi7YNgs

Computer Booting and Configuration

- Booting or Bootstrapping
  - Software system/network initialization process when computer turned on
- Protocol software needs specific information for operation
- Software employs *parameters* for operation on a specific hardware and network
- Configuration

  Process of supplying parameters to protocol software
  - IP address - depends on network, must be unique on network
  - Default router address - where to send packets aimed at remote network
  - Subnet mask - to specify if subnet addressing is used and what the subnet is
  - DNS server address - for DNS queries
  - Other Server addresses – printer

  Static (no change) and dynamic (change each time) parameters

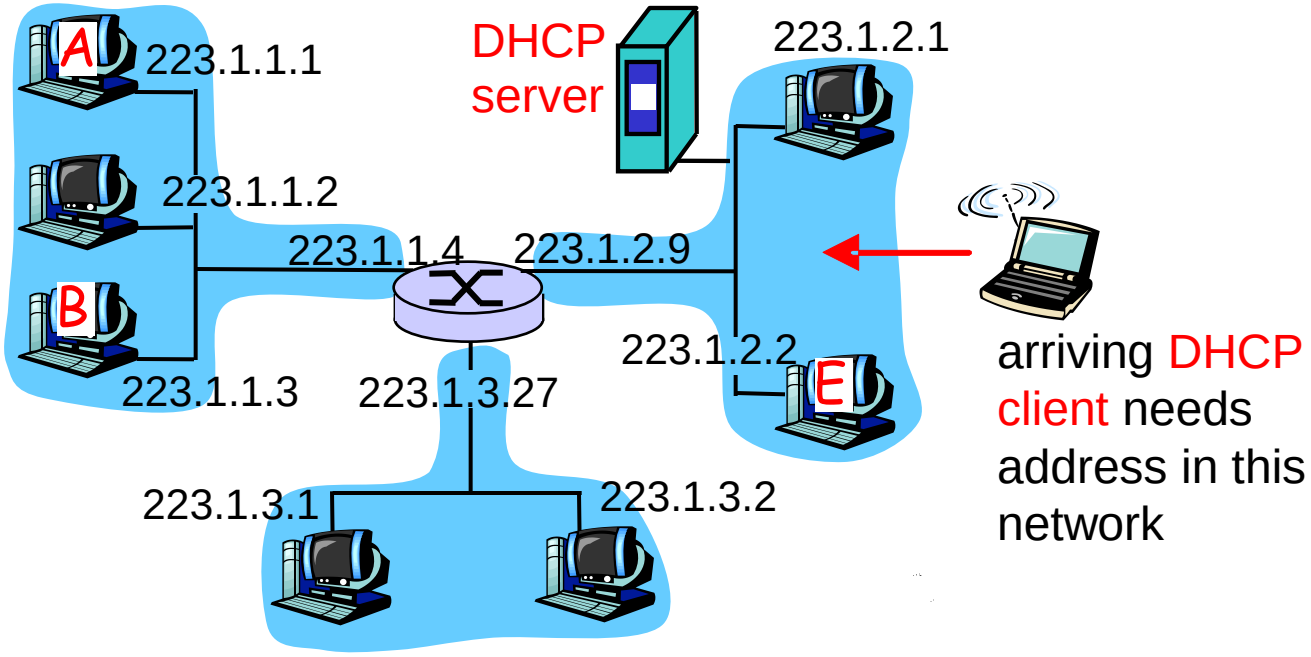
Manual configuration
- sets and saves parameters in local disk

Automated configuration
- Gets parameters from another computer connected the same network
- Previous technique is BOOTP (Bootstrap Protocol)
- Current technique is DHCP (Dynamic Host Configuration Protocol)
- Uses UDP for parameter transfer. How to transfer when unknowing parameters?

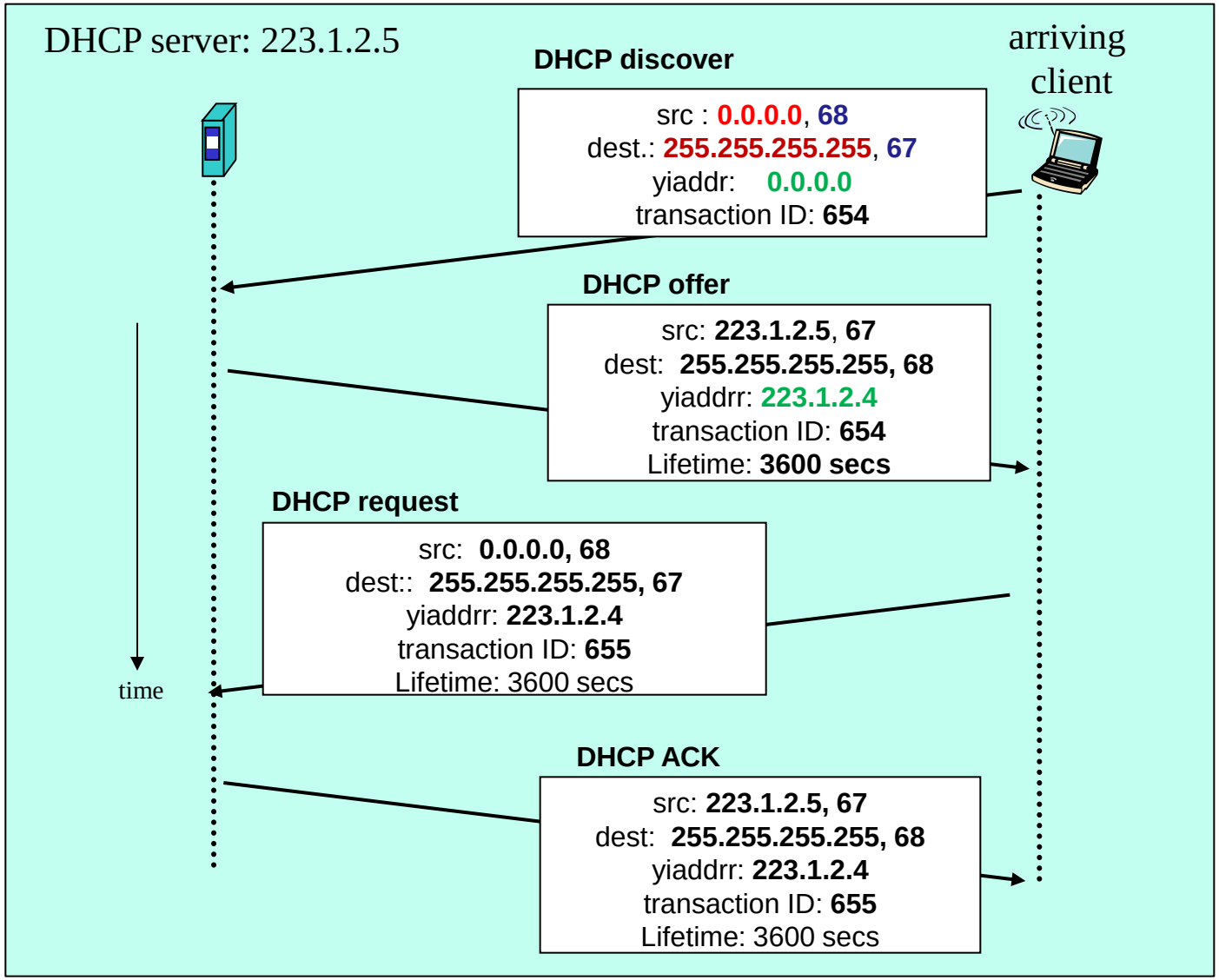
DHCP: Dynamic Host Configuration Protocol

Goal: allow host to *dynamically* obtain its IP address from network server when each of us brings a laptop and want to use it in W103

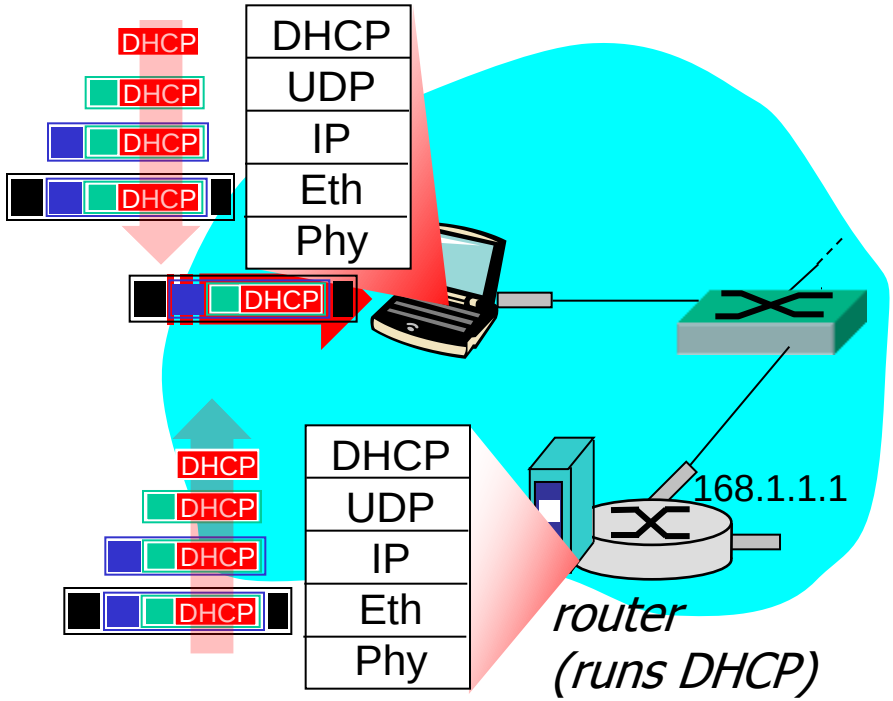
- Can renew its lease on address in use
- Allows reuse of addresses (only hold address while connected an "on")
- Support for mobile users who want to join network (more shortly)



DHCP Messages for Getting IP Address

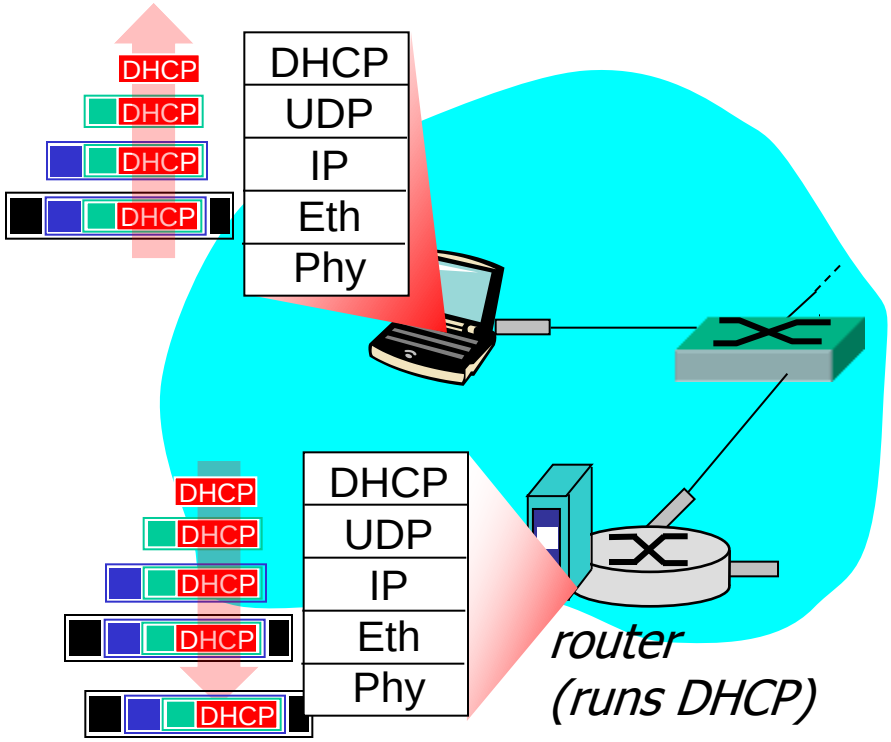


DHCP Messaging Example



- connecting laptop needs its IP address, addr of first-hop router, addr of DNS server: use DHCP
- DHCP request message encapsulated in UDP, encapsulated in IP, encapsulated in 802.1 Ethernet
- Ethernet frame broadcast (dest: FFFFFFFFFFFF) on LAN, received at router running DHCP server
- Ethernet demux'ed to IP demux'ed, UDP demux'ed to DHCP

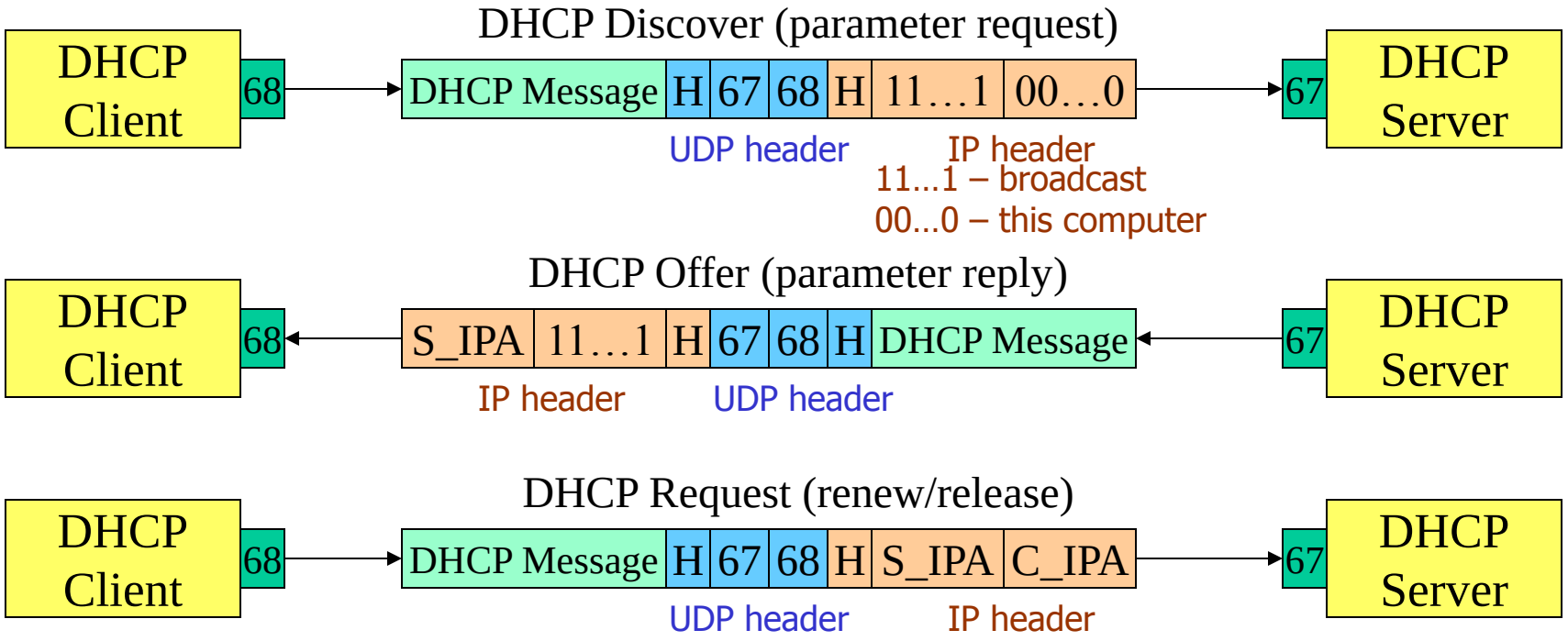
DHCP Messaging Example



- DCP server formulates DHCP ACK containing client's IP address, IP address of first-hop router for client, name & IP address of DNS server
- encapsulation of DHCP server, frame forwarded to client, demux'ing up to DHCP at client
- client now knows its IP address, name and IP address of DSN server, IP address of its first-hop router

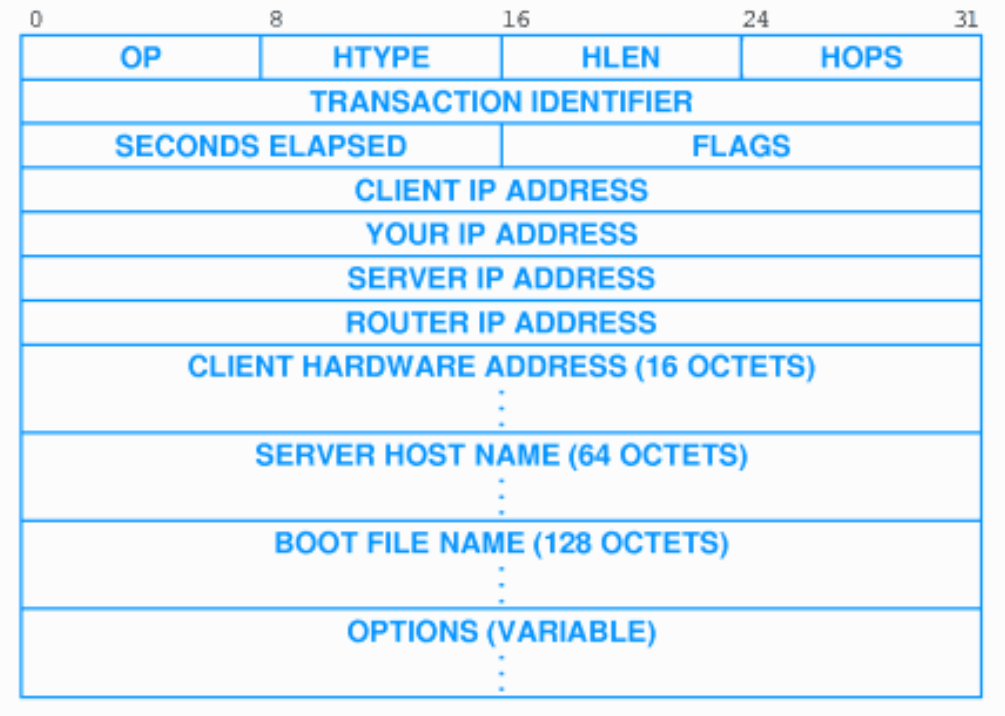
DHCP Server And Client

DHCP client in booting computer communicates with DHCP server



- Efficient use of IP Addresses
  Suppose host leaves subnet? Address no longer in use; server should reassign !
- Address is assigned with a *lease (1 hour default)*
  - Client cannot use the assigned address after lease expires without renew request
  - Client can automatically ask for *extension* prior to expiration (50% lease time)
- Host can get IP address using DHCP, but cannot get domain name → D-DHCP

DHCP Message Format



- Operation code: 1-request; 2-reply,
- Hardware type: physical network, 1-Ethernet
- Hardware length: length of physical address, 6-Ethernet
- Hop count: the maximum number of hops the packet can travel
- Transaction ID: set by client and used to match a reply
- Client IP address: set 0 by client in the beginning
- Your IP address: client IP address filled by server
- Server IP address: filled by server
- Router/gateway IP address: filled by server
- Client hardware address: supplied by client
- Server name (optional 64-byte field): string
- Boot file name (optional 128-byte field): full path of the booting file. The client can use this path to retrieve booting information via TFTP
- Options: subnet mask, DNS server, printer server, lease time, etc.

http://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol

Video: How DHCP works?

NAT – Network Address Translation

Problem:

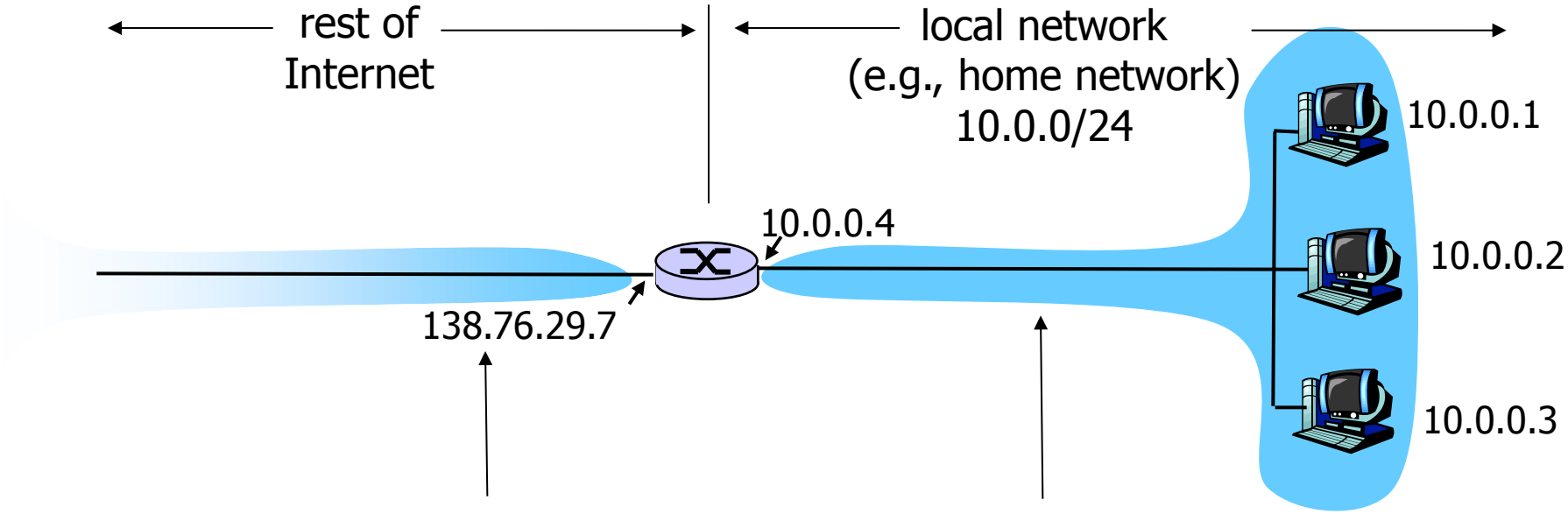
- In your home you have several computers, laptops, mobile phones, networked game-boys, X-Boxes, tablets, even a networked refrigerator.
- What if you have only one IP address from an ISP?

Solution → NAT (Network Address Translation)

- Use the single IP address from ISP for all devices
- Can get and change addresses of devices in local network
- Can change ISP without changing addresses of local devices
- Local devices not explicitly addressable, visible by outside world

https://en.wikipedia.org/wiki/Network_address_translation

NAT Working Mechanism



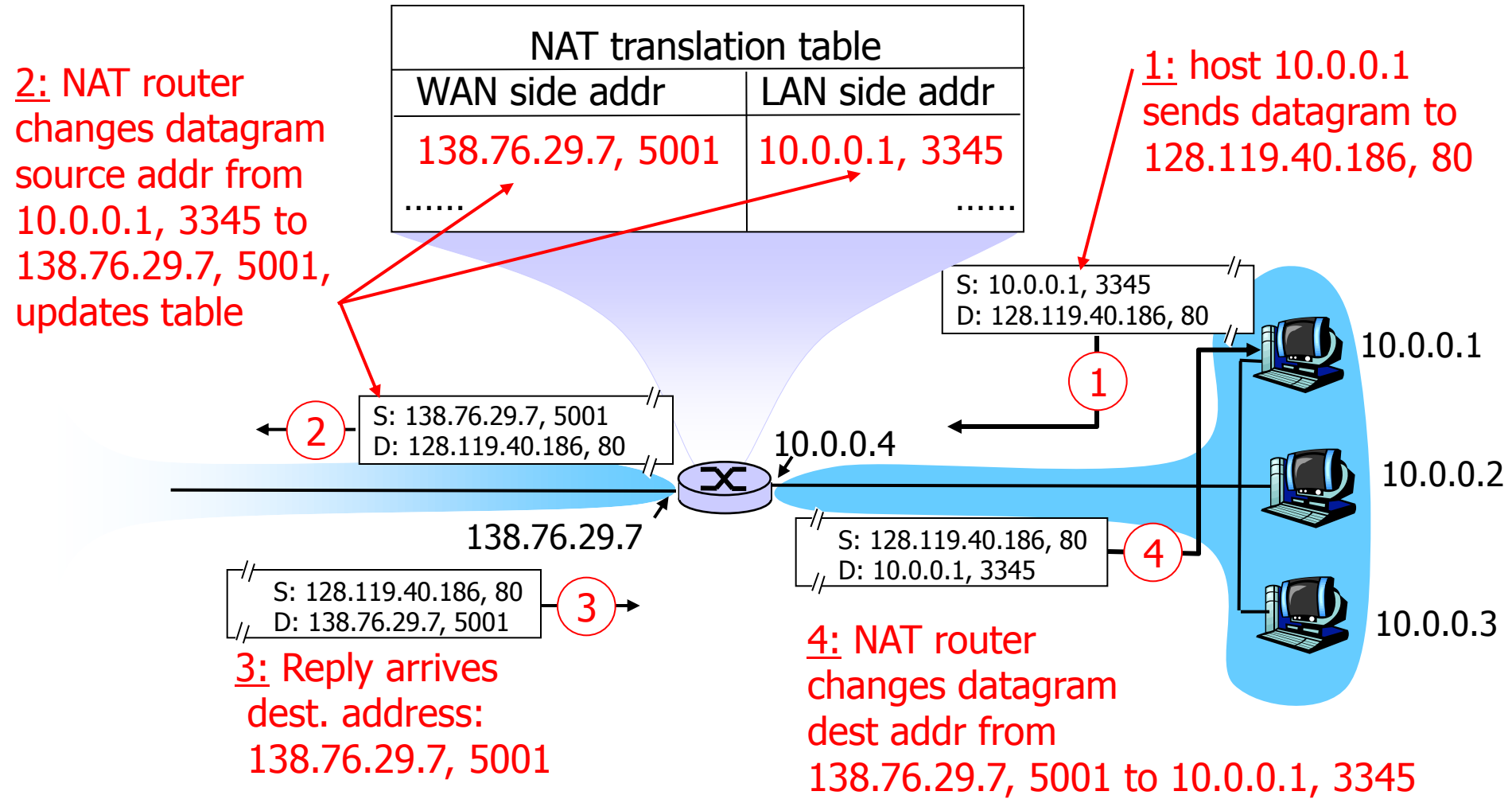
All datagrams *leaving* local network have same single source NAT IP address: 138.76.29.7, different source *port* numbers

(NAT often called a router does not look like a "router" but as a *single* device)

Datagrams with source or destination in this network have 10.0.0/24 address for source, destination (as usual)

(devices get their IP from a DHCP server running within the router!)

NAT Working Details



Network Management

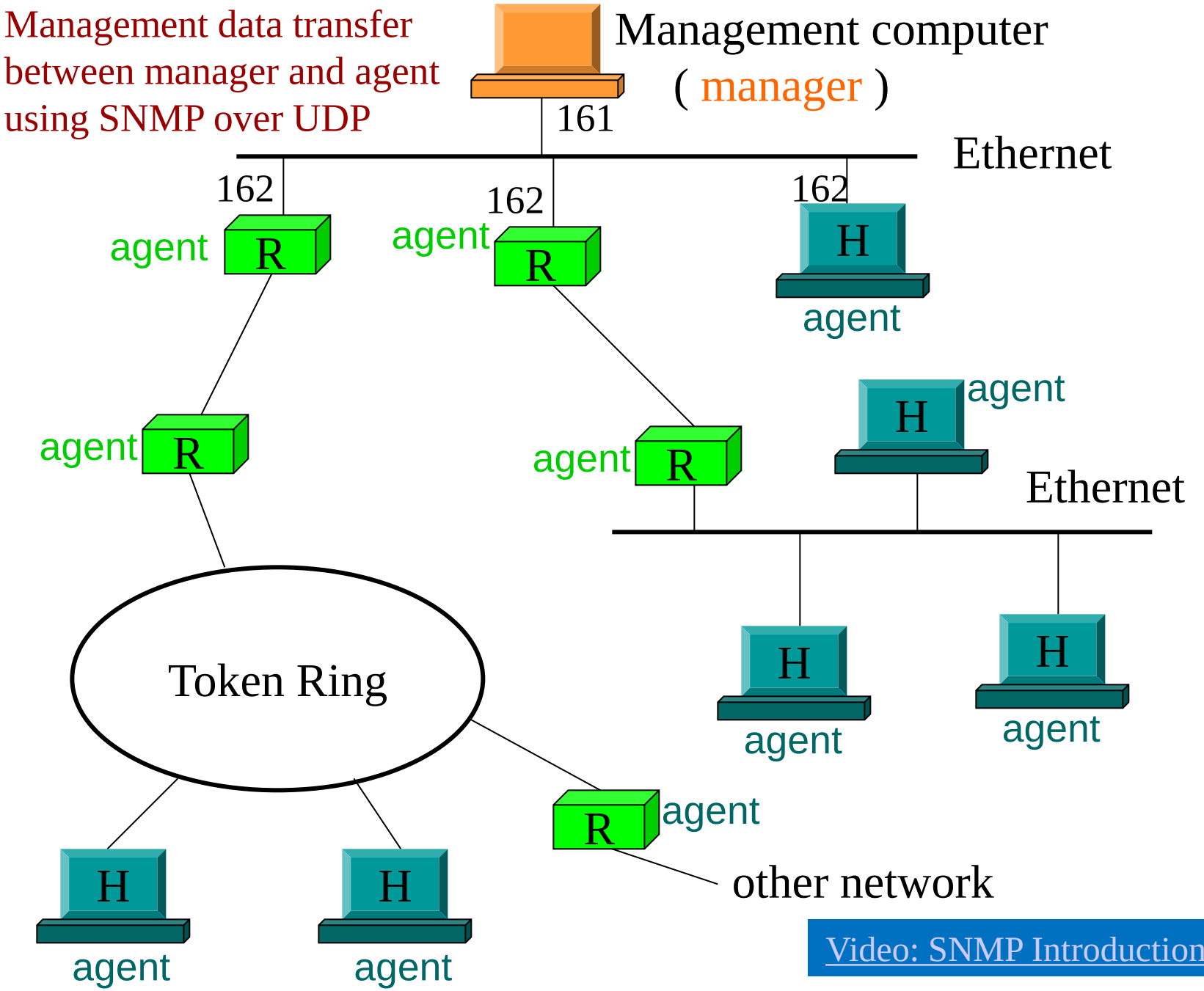
- Responsibility of network administrator: monitor/control network hardware/software
  - Designs and implements efficient and robust network infrastructure
  - Identifies and corrects hardware/software problems as they arise
- Network management work is hard because networks are heterogeneous and large
- Types of network problems
  - Catastrophic
    - * Fiber broken by backhoe
    - * LAN switch loses power
    - * Invalid route in router
    - * *Easier* to diagnose
  - Intermittent or partial
    - * NIC sends frames with bit errors occasionally
    - * Router has one invalid entry
    - * *Harder* to diagnose
- Some intermittent of partial failures may not be evident to user
    - * Hardware may drop frames with data errors
    - * Network protocols may recover from lost packet
    - * However, network performance decreases !!

Network Management Software, Model and SNMP

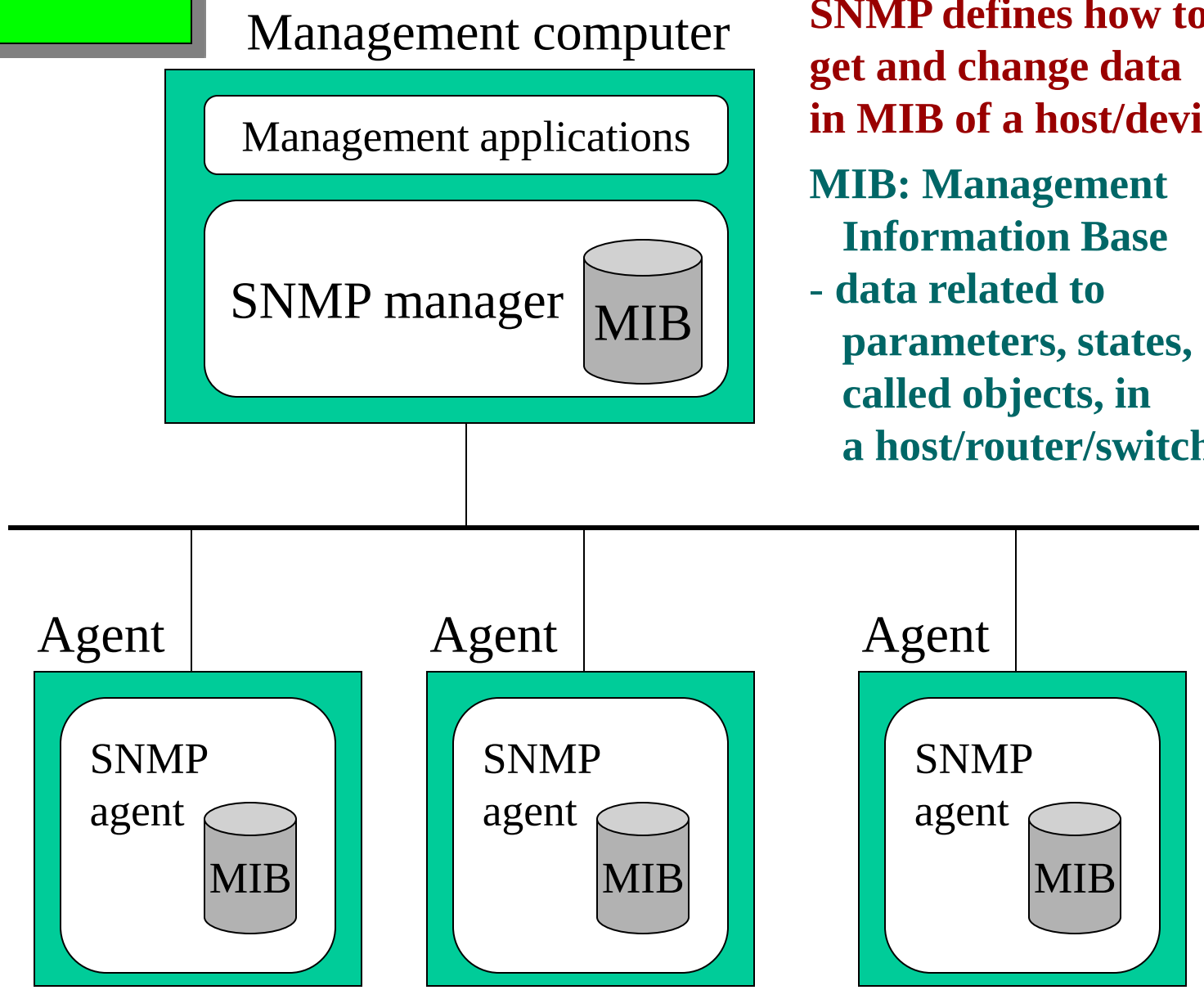
- Network management software
  - Monitor operation and performance of network devices
    * hosts, routers, switches, bridges, …
  - Control operations through rebooting, changing routing table entries

- Network management model
  - Network management does *not* have an internet or transport layer protocol
  - Defines application layer protocol using TCP/IP transport layer protocol
  - Based on client-server model; names changes
    * *Manager* == client; run by network administrator
    * *Agent* == server; runs on managed device
  - Manager composes requests for agent;
  - agent composes response and returns to manager

- SNMP (Simple Network Management Protocol)
  - TCP/IP network management standard
  - Defines all communications between manager and agent
    * Message formats
    * Interpretation of messages
    * Data representations


Management data transfer between manager and agent using SNMP over UDP
Management computer
(manager)
161
Ethernet
162
agent
R
162
agent
R
162
H
agent
agent
R
agent
R
H
agent
Ethernet
Token Ring
H
agent
H
agent
R
agent
other network
H
agent
H
agent
Video: SNMP Introduction

SNMP & MIB

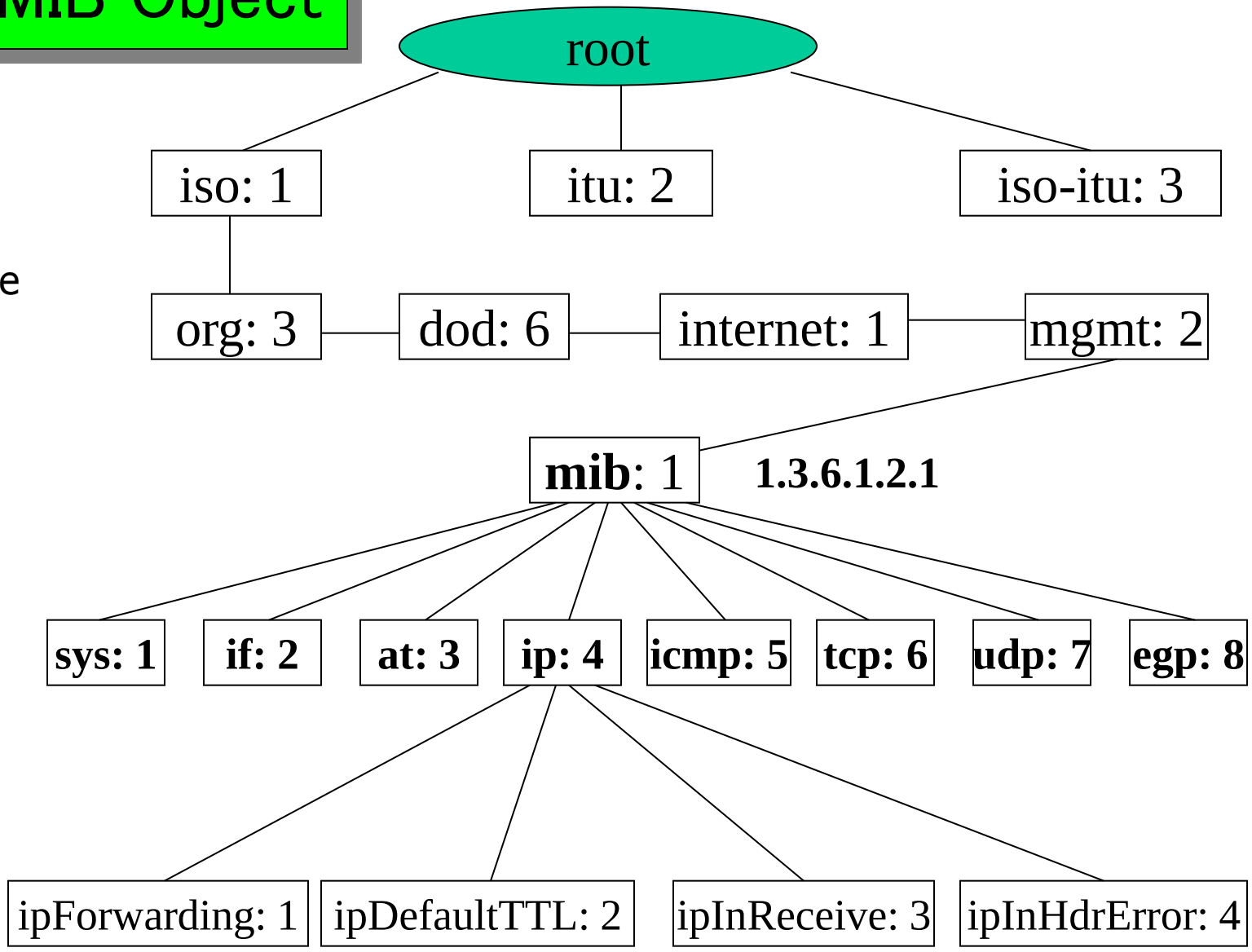


SNMP defines how to get and change data in MIB of a host/device

MIB: Management Information Base
- data related to parameters, states, called objects, in a host/router/switch

Identify MIB Object

Hierarchical
ASN.1
Name scheme



1.3.6.1.2.1.4.3
identifier of object ipInReceive

SNMP Data Representation

- SNMP uses *Abstract Syntax Notation.1* (ASN.1)
  - Platform-independent data representation standard; Strongly-typed
  - Can accommodate arbitrary data types

- General format: type length value
  - type: 02→integer, 04→ string, 05→object, 40→IP address

- Example 1 - integer 14 (integer length is fixed to 4 bytes)
  00000010 00000100 00000000 00000000 000000000 00001110
  or in hexadecimal: 02 04 00 00 00 0D
- Example 2 - string "HI"
  00000100 00000010 01001000 01001001
  or in hexadecimal: 04 02 48 4A
- Example 3 – Object Identifier 1.3.6.1 (iso.org.dod.internet)
  00000101 00000100 00000001 00000011 000000110 00000001
  or in hexadecimal: 05 04 01 03 06 01
- Example 4 – IP Address 131.21.14.8
  01000000 00000100 10000011 00010101 000001110 00001000
  or in hexadecimal: 40 04 83 15 0D 08

SNMP Operations and Message Format

- *GetRequest* (fetch) retrieves value of object in device MIB
- *GetResponse* (answer) sends requested value of object to manager
- *SetRequest* (store) stores new values into object in device MIB
- *Get-next* retrieves *next* object (for scanning)

- SNMP message format

Version	Community	Req. ID	Err Status	Err Index	Variables

- Version. 1-SNMPv1, 2-SNMPv2
- Community. password, or "public" if no password
- Request ID. match a request to a response
- Error status. no-error/error type in response by an agent
- Error index. tell manager which variable caused error
- Variables. reply manager's request from agent

https://en.wikipedia.org/wiki/Simple_Network_Management_Protocol

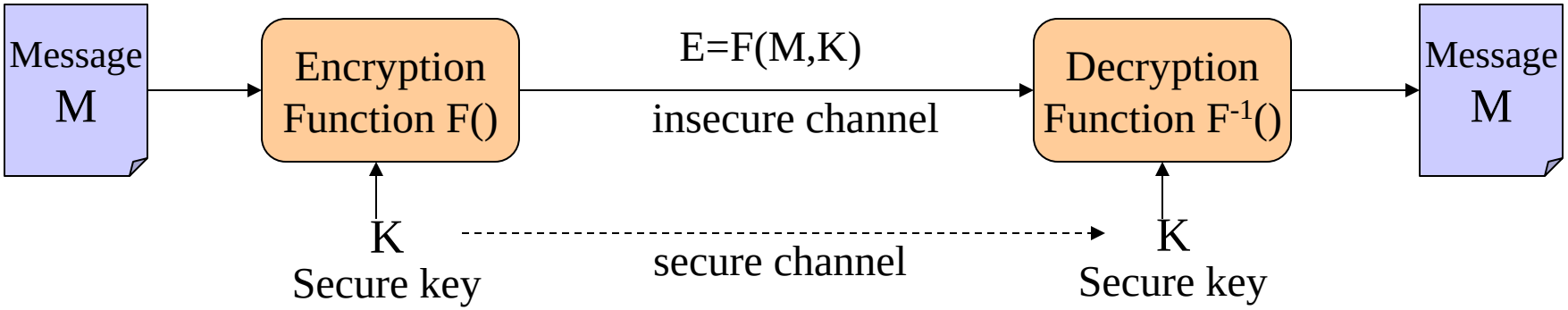
Network Security

- The Internet is open, Routers forward packets - from *any source*
  - Somebody can get the packets transmitted for others (passive attack)
  - Somebody can send in packets from outside (active attack)

- Security Policy should consider
  - Computer systems, LANs, interconnection devices, ...
  - Data stored on servers
  - Messages traversing LANs
  - Internal or external access
  - Read/write versus read-only access
  - Network software application software security holes

- Aspects of Security
  - System/network security
  - Data/information security
    - ➢Data accessibility - contents accessible
    - ➢Data integrity - contents remain unchanged
    - ➢Data confidentiality - contents not revealed

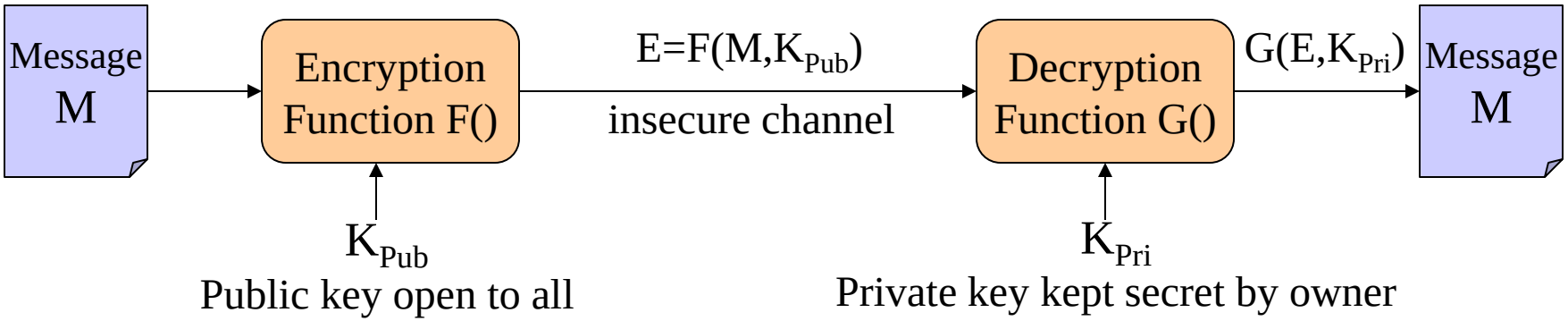
Secure Key Encryption



Encryption Standards

- DES (Data Encryption Standard)
  - designed originally by IBM, and adopted by the US government in 1977 and by ANSI in1981
  - 64-bit block (encryption unit) and 56-bit key
  - not recommended use after 1998 because it can be broken
- Triple-DES
  - three keys and three executions of DES
- IDEA (International Data Encryption Algorithm) - 128-bit block/key
- AES (Advanced Encryption Standard) - 128-bit block/key

Public Key Encryption



RSA (Rivest, Shamir, Adleman, 1978)

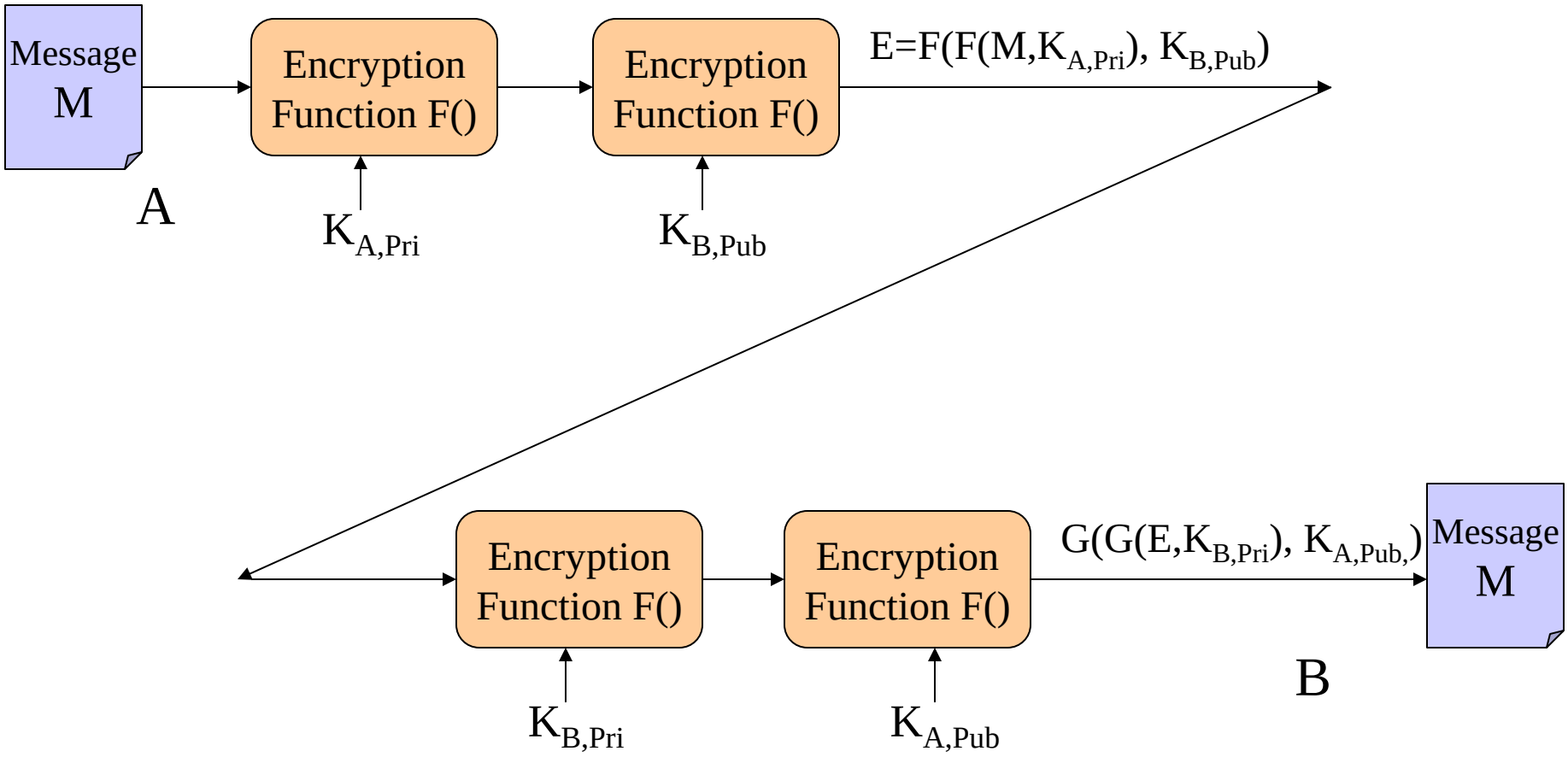
- Key Generation
  - Select p, q which are primes
  - Calculate n=pxq, and t(n)=(p-1)x(q-1)
  - Select integer e satisfied gcd(t(n), e)=1 and e<t(n)
  - Calculate d satisfied exd=1 mod t(n)
  - Public key: KU={e, n}
  - Private key: KR={d, n}
- Encryption
  - Plaintext: M < n
  - Ciphertext: $C = M^e \pmod n$
- Decryption
  - $M = C^d \pmod n$

- Hard to factor n into 2 primes p and q
- RSA key size: 128 to 300 decimal digitals
  i.e., 425 to 1024 bits
- RSA needs more computations than DES much slower than DES

- Example
  - Given M=19
  - Select two prime numbers p=7 and q=17
  - Calculate n=7x17=119, and t(n)=6x16=96
  - Select e=5
  - Determine d=77 since 5x77=385=4x96+1
  - Ciphertext $C=19^5 \pmod{119}=66$
  - Decryption $66^{77} \pmod{119}=19$

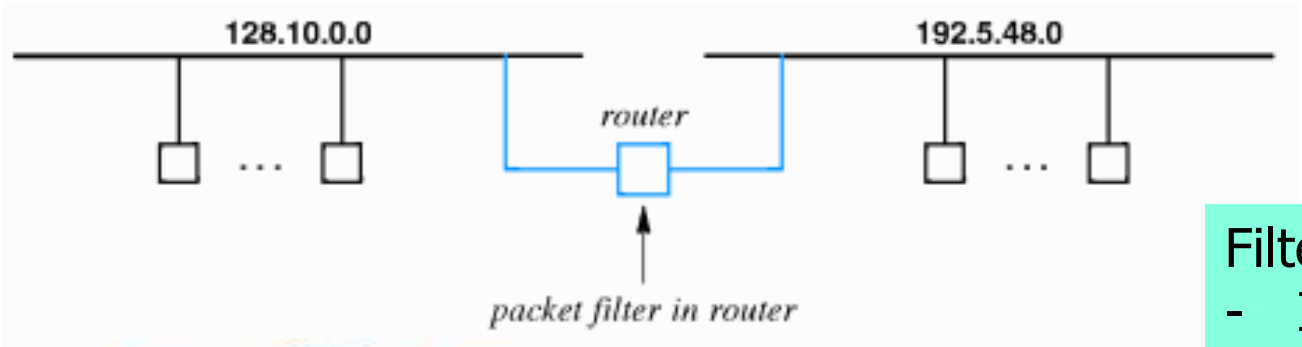
Authentication and Confidence in Digital Signature

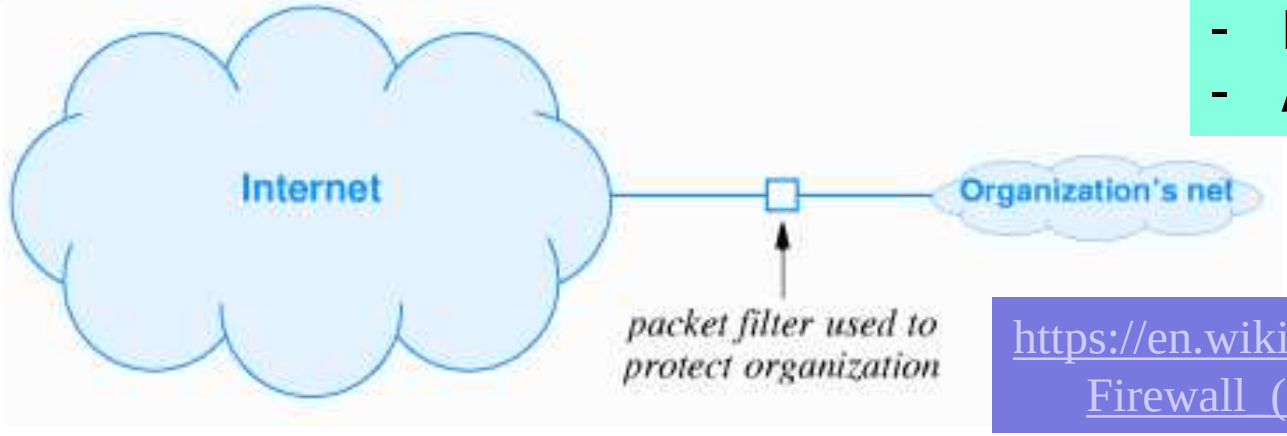
- Digital signature guarantees that message is authenticated from certain person
- Only sender (A) who is owner of private key could have generated original message
- Only recipient (B) can decrypt the message for further guarantee of confidence



Packet Filter and Internet Firewall

- Packet filter: configuring routers to drop certain packets according to IP address
- Suppose 192.5.48.0 is test network and 128.10.0.0 has controlling workstations
  - Install filter to allow packets only from 192.5.48.0 to 128.10.0.0
  - Keeps potentially bad packets away from remainder of Internet
- Packet filter at edge of intranet can disallow unauthorized packets
- Called firewall that restricts external packets to just a few internal hosts





Filter based on
- IP address
- Port number
- Application

https://en.wikipedia.org/wiki/Firewall_(computing)

Exercise 12

1. Using nslookup utility to get IP address of www.k.hosei.ac.jp. Find out how many name servers in domain k, hosei, ac and jp, respectively.

2. A host can dynamically get an IP address by means of exchanging information with a DHCP server using TCP/IP protocols. However, the host has no IP address before getting the IP address. How does the host communicate with DHCO server when having no IP address? Furthermore, the host can only hold the issued IP address with finite lease time such as one hour. Why? What method in DHCP is used to renew the release to hold the IP address more than one hour?

3. Data of parameters and states called objects of a host/router is stored in MIB (management information database). Each object in MIB has a unique identifier represented in hierarchical ASN.1 name scheme. Explain the meaning of ipForwarding object of a router, and give its identifier.

4. SNMP uses ASN.1 to represent data of an object. Give the SNMP representations of string data "SNMP" and IP address "133.25.252.22" in hexadecimal format, respectively.

5. Explain why the digital signature method shown in the lecture note can guarantee both authentication and confidence.