The Hong Kong Polytechnic University
Industrial Centre

Knowledge Update Course for Secondary Computer Teachers

Internetworking

By
Edward Cheung
email: icec@polyu.edu.hk

15 July, 2003.

Agenda

- Internetworking & universal services
- Protocols for Internetworking
  - ISO 7-Layer Reference Model
  - TCP/IP Layering Model
- Internet Protocol
  - IP address: scheme, hierarchy and classes
  - Computing the class of an IP address
  - Special IP addresses
  - IP address and routing table entries
- Transmission Control Protocol
  - Packet loss and retransmission, 3 way handshake
- Domain Name System

The Motivation for Internetworking

Network Technology:

- LAN technologies are designed to provide high speed communication across short distances.
- WAN technologies are designed to provide communication across large areas.

A large organization with diverse networking requirements needs multiple physical networks.

If the organization chooses the type network that is best for each task, the organization will have several types of networks.

No single networking technology is best for all needs.

Universal Service

The concept of universal service was introduced by AT&T's Theodore Vail for AT&T telephone service. Now it means telecommunication services. A communication system that supplies universal service allow arbitrary pairs of computer to communicate.

Universal service is desirable because it increase individual productivity and a user does not need to change computer systems when changing tasks – all information is available to all computers. Although universal service is highly desirable, incompatibilities among network hardware and physical prevent an organization from building a bridged network that include arbitrary technologies

For more information:- http://www.benton.org/

Protocols for Internetworking

- TCP/IP is most widely used for internetworking.
- TCP/IP was the first set of protocols developed for use in an internet.
- Work on TCP/IP began in the 1970s.
- By the mid-1980s the ***National Science Foundation*** and other U.S. government agencies were funding development of TCP/IP and a large internet that was used to test the protocols

Internetworking

Internetworking, the scheme uses both hardware and software:

- Hardware systems are used to interconnect a set of physical networks.
- Software on all the attached computers then provides universal service.
- The resulting system of connected physical networks is best known as the Internet. An internet is not restricted in size.

- Two styles of internetworking are common:
  - Connection-oriented concatenated virtual circuit model
  - Connectionless-oriented datagram model

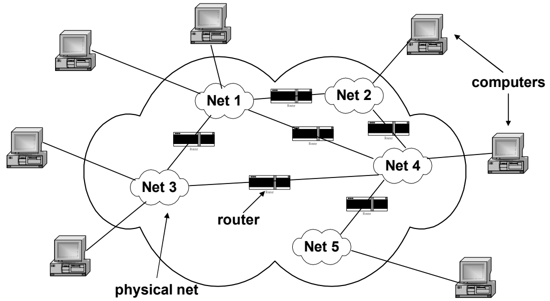
Physical Network Connection with Routers

The basic hardware component used to connect heterogeneous networks is a **router**.

Router

- A special purpose computer dedicated to the task of interconnecting networks.
- A router has a conventional processor and memory as well as a separate I/O interface for each network to which it connects.

Physical Network Connection with Routers



The underlying physical structure in which a computer attaches to one physical network, and routers interconnect the networks.

The Need for Protocols

Basic communication:

- Hardware consists of mechanisms that can transfer bits from one point to another.
- Software handles most low-level communication details and problems, making it possible for applications to communicate easily.

Protocol is applied to computer communication as well:

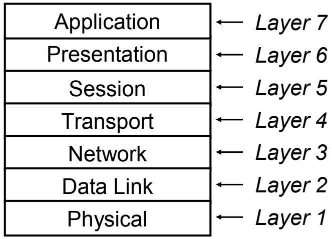
- A set of rules that specify the format of messages and the appropriate actions required for each message is known as a network protocol

ISO 7-Layer Reference Model

***International Organization for Standardization* (ISO)**

- **7-layer Reference Model.**

A layering model is a tool to help protocol designers construct a suite of protocols that solves all communication problems.



Application ← *Layer 7*

Presentation ← *Layer 6*

Session ← *Layer 5*

Transport ← *Layer 4*

Network ← *Layer 3*

Data Link ← *Layer 2*

Physical ← *Layer 1*

ISO 7-Layer Reference Model

Layering models provide a simple explanation of the relationships among the complex hardware and protocol components of a network.

Application (Layer 7):

- Interface between network and application software.
- Example: Telnet, HTTP, WWW browsers

Presentation (Layer 6):

- Provides a variety of coding and conversion functions that are applied to application level data.
- Such as encryption.
- Example: JPEG, MPEG, MIDI, ASCII

ISO 7-Layer Reference Model

Session (Layer 5):

- Responsible for establishing and maintaining end-to-end bi-directional flows between endpoints.
- Includes managing transaction flows.
- Example: RPC, SQL, NetBios Names, AppleTalk.

Transport (Layer 4):

- Provides delivery of the data and error correction prior to retransmit.
- Example: TCP, UDP, SPX

ISO 7-Layer Reference Model

Network (Layer 3):

- Provides logical addressing so that routers can perform route determination.
- Example: IP, IPX

Data Link (Layer 2):

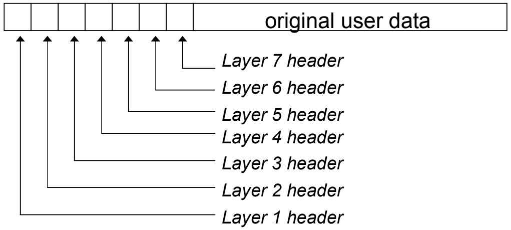
- Converting bits into bytes into frames and with error detection and error recovery.
- Example: 802.3/802.2, HDLC

Physical (Layer 1):

- Moving of bits between devices
- Puts the actual data onto the wire
- Example: EIA/TIA-232, V.35

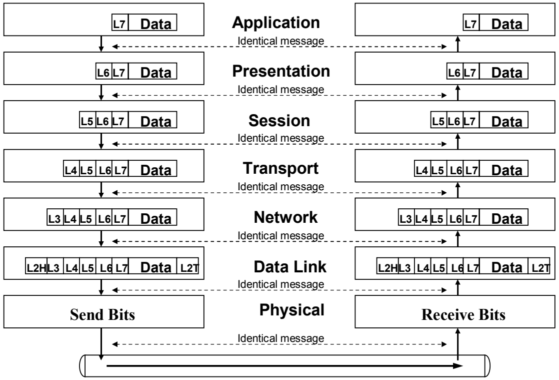
Multiple, Nested Headers

Each layer places additional information in a header before sending data to a lower layer. Thus, a frame traveling across a network contains a series of nested headers as Figure shown.



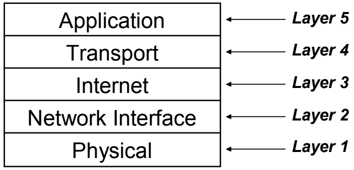
The nested protocol headers that appear in a frame as the frame travels across a network.

Interaction between ISO Layer



TCP/IP Layering Model

The ***TCP/IP layering model****,* which is also called the ***Internet Layering Model*** or the ***Internet Reference Model****,* contains five layers as Figure illustrates.



TCP/IP Layering Model

The purpose of each layer

Layer 1: Physical

Layer I corresponds to basic network hardware just as Layer I in the IS0 7-layer reference model.

Layer 2: Network Interface

Layer 2 protocols specify how to organize data into frames and how a computer transmits frames over a network, similar to Layer 2 protocols in the IS0 reference model.

TCP/IP Layering Model

Layer 1: Physical

Layer 3 protocols specify the format of packets sent across an internet as well as the mechanisms used to forward packets from a computer through one or more routers to a final destination.

Layer 4: Transport

Layer 4 protocols, like layer 4 in the IS0 model, specify how to ensure reliable transfer.

Layer 5: Application

Layer 5 corresponds to layers 6 and 7 in the IS0 model. Each Layer 5 protocol specifies how one application uses an internet.

TCP/IP Data Encapsulation

A five-step encapsulation process, the following list provides the details and explanation.

Step 1: Application (Layer 5)

- **Create the data** – This simply means that the application has data to send

Step 2: Transport (Layer 4):

- **Package the data for transport** – The transport layer (TCP or UTP) crates the transport header and places the data behind it.

TCP/IP Data Encapsulation

Step 3: Internet (Layer 3):

- **Add the destination and source network layer address to the data** – The network layer creates the network header, which includes the network layer address, and places the data behind it.

Step 4: Network Interface (Layer 2):

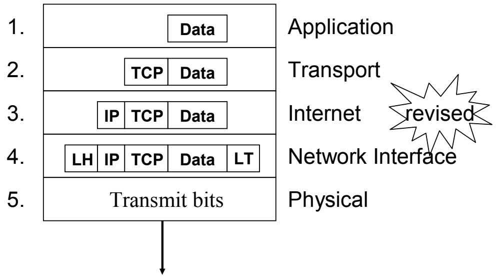
- **Add the destination and source data link layer address to the data** – The data link layer creates the data link header, places the data behind it, and places the data link trailer at the end .

Step 5: Physical (Layer 1):

- **Transmit the bits** – The physical layer encodes a signal onto the medium to transmit the frame.

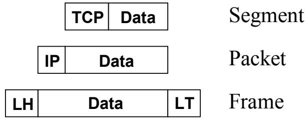
TCP/IP Data Encapsulation

Five Steps of Data Encapsulation – TCP/IP



TCP/IP Data Encapsulation

Figure illustrates the construction of ***frames, packets*** and ***segment*** and the different layers' perspectives on what is considered to be **data.**



Internet Protocol & IP Addressing Scheme

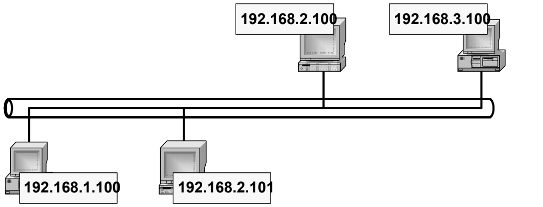
In the TCP/IP protocol stack, addressing is specified by the ***Internet Protocol (IP)***.

The IP standard specifies that each host is assigned a ***unique 32-bit number*** known as the host's ***Internet Protocol address,*** which is often abbreviated ***IP address,*** or ***Internet address.***

Each packet sent across an internet contains the 32-bit IP address of the sender (source) as well as the intended recipient (destination).

Internet Protocol & IP Addressing Scheme

- The IP address identifies a computer's location on the network
  - An IP address consists of a set of four numbers, each of which can range from 0 to 255.



IP Address Hierarchy

All 32 bits being treated as the ***network address***, and the other part is designated as either the ***subnet and host*** or ***node address***

The ***network address*** uniquely identifies each network. Every machine on the same network shares that network address as part its IP Address.

The ***node address*** (uniquely identifies) is assigned to each machine on a network.

For Example: IP address 172.16.53. 46

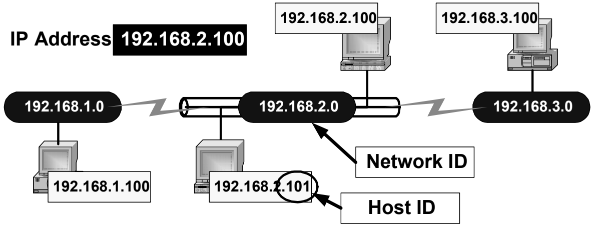
- 172.16 is the network address, and
- 53. 46 is the node address

IP Address Hierarchy

IP Address	**172**	**16**	**53**	**46**
Network ID	**172**	**16**	**0**	**0**
Host ID	**0**	**0**	**53**	**46**

IP Address Hierarchy

- Network ID and Host ID



IP Address Classes

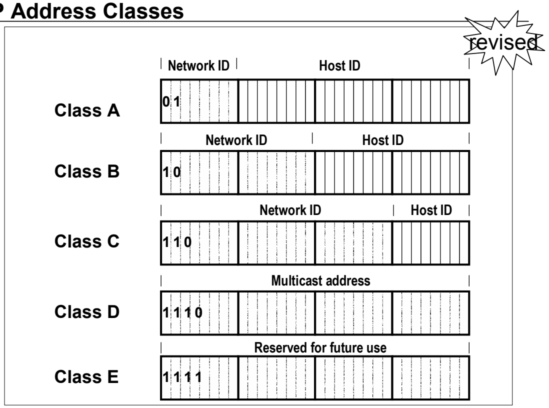
The original scheme, which is known as IP addressing, divides the IP address space into three primary *classes,* where each class has a different size of ***network address*** and ***node address.***

Classes *A,* B, and **C** are called the primary classes because they are used for host addresses.

Class D is used for multicasting, which allows delivery to a set of computers.

Class E is used for research

IP Address Classes



revised

Class A: 0 1 | Network ID | Host ID

Class B: 1 0 | Network ID | Host ID

Class C: 1 1 0 | Network ID | Host ID

Class D: 1 1 1 0 | Multicast address

Class E: 1 1 1 1 | Reserved for future use

Network Address Range

Address schemes define the difference between a Class A, Class B and Class C

Network Address Range: **Class A**

Class A address must be between 0 and 127

- **00000000 = 0**
- **01111111 = 127**

First Octet Range: **1 to 126**

Valid Network Numbers: **1.0.0.0 to 126.0.0.0**

Reserved IP: **127.0.0.1** (loopback)

Network Address Range

Network Address Range: **Class B**

Class A address must be between 128 and 191

- **00000000 = 128**
- **01111111 = 191**

First Octet Range: **128 to 191**

Valid Network Numbers: **128.1.0.0 to 191.254.0.0**

Reserved IP: **191.255.0.0** and **192.0.0.0**

Network Address Range

Network Address Range: **Class C**

Class A address must be between 192 and 223

- **11000000 = 192**
- **11011111 = 223**

First Octet Range: **192 to 223**

Valid Network Numbers: **192.0.1.0 to 223.255.254.0**

Reserved IP: **223.255.255.0**

Network Address Range

Class	No. of networks	No. of hosts per network	Range of Network Ids (First Octet)	Description
A	**126**	**16,777,214**	**1 ~ 126**	**Very Large number of hosts**
B	**16,384**	**65,534**	**128 ~ 191**	**Large size network**
C	**2,097,152**	**254**	**192~223**	**LANs**
D	**Not available**	**Not available**	**Not available**	**Multicasting**
E	**Not available**	**Not available**	**Not available**	**Reserved**

Subnet Masks

- Subnetting allows a single classful network ID to be divided into smaller network IDs.
- Using these multiple smaller network IDs, the single network can be segmented into subnets, each with a different network ID, also known as a subnet ID.
- To divide a network ID, you use a **subnet mask**.
- For example, 255.255.0.0 is a valid subnet mask, whereas 255.0.255.0 is not. The subnet mask 255.255.0.0 identifies the network ID as the first two numbers in the IP address.

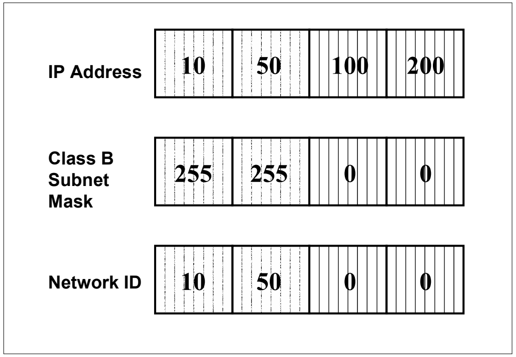
Subnet Masks

- A subnet mask is a screen that differentiates the network ID from a host ID in an IP address
- A subnet mask consists of a set of four numbers, similar to an IP address. These numbers can range in value from 0 to 255.

Table shown the default subnet masks for Classes A, B and C

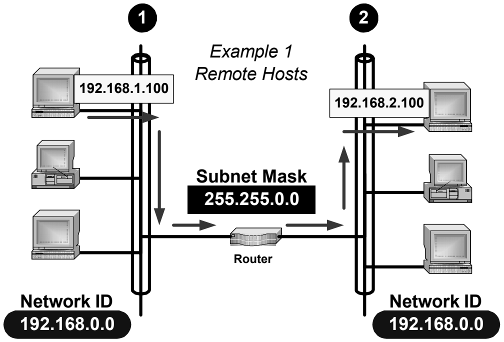
IP address class	IP address	Default Subnet mask	Network ID	Host ID
A	***w . x . y . z***	**255.0.0.0**	***w . 0 . 0 . 0***	***x.y.z***
B	***w . x . y . z***	**255.255.0.0**	***w . x . 0 . 0***	***y.z***
C	***w . x . y . z***	**255.255.255.0**	***w . x . y . 0***	***z***

Subnet Masks



IP Address	10	50	100	200
Class B Subnet Mask	255	255	0	0
Network ID	10	50	0	0

Router



1

2

Example 1
Remote Hosts

192.168.1.100

192.168.2.100

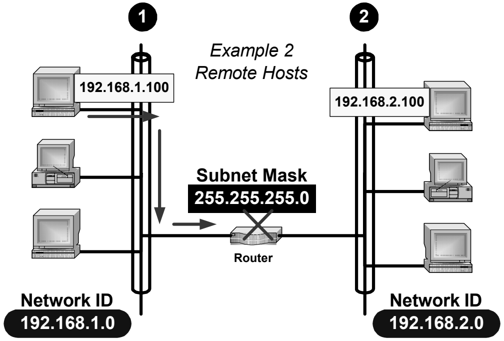
Subnet Mask
255.255.0.0

Router

Network ID
192.168.0.0

Network ID
192.168.0.0

Subnet Masks



1

2

Example 2
Remote Hosts

192.168.1.100

192.168.2.100

Subnet Mask
255.255.255.0

Router

Network ID
192.168.1.0

Network ID
192.168.2.0

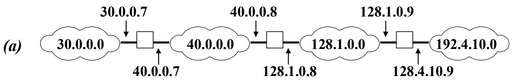
IP Address and Routing Table Entries

An IP routing table is more complex.

- First, the ***Destination*** field in each entry contains the network prefix of the destination network.
- Second, an additional field in each entry contains ***an address mask*** that specifies which bits of the destination correspond to the network prefix.
- Third, an IP address is used when the ***Next Hop*** field denotes a router.

IP Address and Routing Table Entries

(a)



(b)

Destination	Mask	Next Hop
30.0.0.0	255.0.0.0	40.0.0.7
40.0.0.0	255.0.0.0	deliver direct
128.1.0.0	255.255.0.0	deliver direct
192.4.10.0	255.255.255.0	128.1.0.9

(a) An internet of four networks and three routers with an IP address assigned to each router interface

(b) the routing table found in the center router. Each entry in the table lists a destination, a mask, and the next hop used to reach the destination.

IP Address and Routing Table Entries

The first two networks in Figure, each have a ***class A network*** , the third network has a ***class B network*** , and the fourth network has a ***class C network*** .

Each router has been assigned two IP addresses, one for each interface.

For example, the router that connects net 30.0.0.0/8 to net 40.0.0.0/8 has been assigned addresses 30.0.0.7 and 40.0.0.7.

Although the same host suffix has been assigned to both interfaces on the router, IP does not require uniformity - a network administrator is free to assign different values to each interface.

Special IP Address

- 0.0.0.0 means this host
  - Only use for booting
- 255.255.255.255 means broadcast to all hosts
- 0+host address means to address a host on this network
  - Need to known the class of the network
- Network addr + all “1” means broadcast on a distance network
- 127.xx.yy.zz means addresses for loop back test, the packets are not put out onto the wire. The packets are processed locally and treated as incoming packets.

Private Network

- IANA has reserved 3 blocks of IP address space for private networks:-

  10.0.0.0 – 10.255.255.255
  172.16.0.0 – 172.31.255.255
  192.168.0.0 – 192.168.255.255
  - The first block is a single class A network number. The second block is a set of 16 contiguous class B network numbers and the last block is a set of 255 contiguous class C network numbers.
- No registration is required for using these addresses but routers in the network or from the ISPs will block the packet and shown as routing error if source IP is private.
- A gateway or network address translation (NAT) device is needed for private LAN to communicate with outside.

CIDR

Classless Inter-Domain Routing (CIDR) is a new addressing scheme for the Internet which allows for more efficient allocation of IP addresses than the old Class A, B, and C address scheme.

With a new network being connected to the Internet at astonishing speed, the Internet was faced with two critical problems:

- Running out of IP addresses
- Running out of capacity in the global routing tables

Running Out of IP Addresses

There is a maximum number of networks and hosts that can be assigned unique addresses using the Internet's 32-bit long addresses.

Traditionally, the Internet assigned "classes" of addresses: Class A, Class B and Class C were the most common.

Each address had two parts: one part to identify a unique network and the second part to identify a unique host in that network.

Running Out of IP Addresses

Class	Network Bits	Hosts Bits	Decimal Address Range
A	8 bits	24 bits	1- 126
B	16 bits	16 bits	126 - 191
C	24 bits	8 bits	192 - 223

- Because Internet addresses were generally only assigned in these three sizes, there was a lot of wasted addresses.
- For example, if you needed 100 addresses you would be assigned the smallest address (Class C), but that still meant 154 unused addresses.
- The overall result was that while the Internet was running out of unassigned addresses, only 3% of the assigned addresses were actually being used.
- CIDR was developed to be a much more efficient method of assigning addresses.

Restructuring IP Address Assignments

Classless Inter-Domain Routing (CIDR) is a replacement for the old process of assigning Class A, B and C addresses with a generalized network "prefix".

Instead of being limited to network identifiers (or "prefixes") of 8, 16 or 24 bits, CIDR currently uses prefixes anywhere from 13 to 27 bits.

Thus, blocks of addresses can be assigned to networks as small as 32 hosts or to those with over 500,000 hosts. This allows for address assignments that much more closely fit an organization's specific needs.

Restructuring IP Address Assignments

A CIDR address includes the standard 32-bit IP address and also information on how many bits are used for the network prefix.

For example, in the CIDR address 206.13.01.48/25, the "/25" indicates the first 25 bits are used to identify the unique network leaving the remaining bits to identify the specific host.

CIDR Block Prefix	Equivalent Class C	Host Addresses
27	1/8th of a Class C	32 hosts
26	1/4th of a Class C	64 hosts
20	16 Class C	4,096 hosts
14	1,024 Class C	262,144 hosts
13	2,048 Class C	524,288 hosts

Restructuring IP Address Assignments

A CIDR address includes the standard 32-bit IP address and also information on how many bits are used for the network prefix.

For example, in the CIDR address 206.13.01.48/25, the "/25" indicates the first 25 bits are used to identify the unique network leaving the remaining bits to identify the specific host.

User Impacts

The Internet is currently a mixture of both "CIDR-ized" addresses and old Class A, B and C addresses.

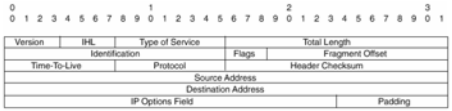
Almost all new routers support CIDR and the Internet authorities strongly encourage all users to implement the CIDR addressing scheme.

The conversion to the CIDR addressing scheme and route aggregation has two major user impacts:

- Justifying IP Address Assignments
- Where To Get Address Assignments

IP Header

- Version – version 4 = 0100
- IHL – Length of header (min. 5x32bit words)= 0101
- ToS = 000 for routine normal traffic, 001 for priority, etc.
- Total Length = max. 2^{16} -1=65,535 bytes (min. 576 bytes)
- Identification – identifies fragments for reassembly
- Flags – allow fragment/don't fragment/more fragment/less….
- TTL – lifetime of packet in seconds, hop counter in practice.
- Protocol Number – 8 bits, e.g. TCP, UDP, ICMP, OSPF, etc.
- Header Checksum verifies the header only
- Options are variable length and pad for 32 bit boundary.



Example - Protocol Analysis Ethernet

- Record #4 (From Hub To Node) Captured on 01.23.96 at 22:52:27.021406799 Length = 269
- Runtime Frame# 4
- ------------ ETHER Header ------------
- ETHER: Destination: Cisco-01-FE-1D (00-00-0C-01-FE-1D)
- ETHER: Source: HP-25-42-CD (08-00-09-25-42-CD)
- ETHER: Protocol: IP
- ETHER: FCS: ADF83D1F

Example - Protocol Analysis IP

```
•   ------------  IP Header  ------------
•   IP: Version = 4
•   IP: Header length = 20
•   IP: Type of service = 0
•   IP:     000. .... Precedence = Routine(0)
•   IP:     ...0 .... Delay = Normal (0)
•   IP:     .... 0... Throughput = Normal (0)
•   IP:     .... .0.. Reliability = Normal (0)
•   IP: Packet length = 251
•   IP: Id = 2332
•   IP: Fragmentation Info = 0x0000
•   IP:     .0.. ....  .... .... Don't Fragment Bit = FALSE
•   IP:     ..0. ....  .... .... More Fragments Bit = FALSE
•   IP:     ...0 0000  0000 0000 Fragment offset = 0
•   IP: Time to live = 64
•   IP: Protocol = TCP (6)
•   IP: Header checksum = 0766
•   IP: Source address = 15.17.161.31
•   IP: Destination address = 15.42.144.11
```

Example - Protocol Analysis HTTP

```
•   ------------  HTTP Header  ------------
•   HTTP: Full Request
•   HTTP: Method= GET
•   HTTP: Request-URI= http://www-cco.col.hp.com/
•   HTTP: HTTP-version= HTTP/1.0
•   HTTP: Referer= http://www-cco.col.hp.com/
•   HTTP: User-Agent= Mozilla/1.0N (Windows)
•   HTTP: Pragma= no-cache
•   HTTP: Accept= */*
•   HTTP: Accept= image/gif
•   HTTP: Accept= image/x-xbitmap
•   HTTP: Accept= image/jpeg
```

Transmission Control Protocol

The application relies on the underlying computer system to ensure reliable transfer.

The system guarantees that data will not be lost, duplicated, or delivered out of order.

*Transmission Con*trol Protocol *(TCP)* provides reliable transport service (no data duplication or loss).

Applications interact with a transport service to send and receive data in the TCP/IP suite.

Transmission Control Protocol

TCP has six major features:

- *Connection Orientation.*
  - An application must first request a connection to a destination, and then use the connection to transfer data.
- *Point-To-Point Communication.*
  - Each TCP connection has exactly two endpoints.
- *Complete Reliability.*
  - Data sent across a connection will be delivered exactly as sent, with no data missing or out of order.

Transmission Control Protocol

- *Full Duplex Communication.*
  - *Data to flow in either direction, and allows either application program to send data at any time.*
- *Reliable Connection Startup.*
  - *Two applications create a connection, both must agree to the new connection.*
- *Graceful Connection Shutdown.*
  - *An application program can open a connection, send arbitrary amounts of data, and then request that the connection be shut down.*

Packet Loss and Retransmission

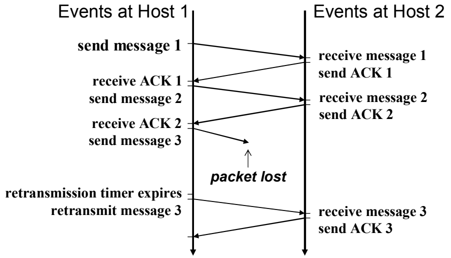
TCP uses a variety of techniques to handle parts of the problem. One of the most important techniques is ***retransmission***.

When TCP sends data, the sender compensates for packet loss by implementing a retransmission scheme.

When TCP receives data, it sends an ***acknowledgement*** back to the sender.

Whenever it sends data, TCP starts a timer. If the timer expires before an acknowledgement arrives, the sender retransmits the data.

Packet Loss and Retransmission



Events at Host 1

Events at Host 2

send message 1

receive message 1
send ACK 1

receive ACK 1
send message 2

receive message 2
send ACK 2

receive ACK 2
send message 3

packet lost

retransmission timer expires
retransmit message 3

receive message 3
send ACK 3

Items on the left correspond to events in a computer sending data, items on the right correspond to events in a computer receiving data, and time goes down the figure. The sender retransmits lost data.

Packet Loss and Retransmission

Acknowledgement form a computer on a local area network are expected to arrive within a few milliseconds.

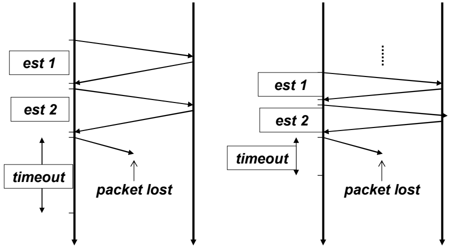
Waiting too long for such an acknowledgement leaves the network idle and does not maximize throughput.

Bursts of datagrams can cause congestion, which causes transmission delays.

The delay required for data to reach a destination and an acknowledgement to return depends on traffic in the internet as well as the distance to the destination.

Comparison of Retransmission Times

Adaptive retransmission can help TCP maximize throughput on each connection, consider a case of packet loss on two connections that have different round-trip delays.



Comparison of Retransmission Times

TCP optimizes throughput by using a round-trip estimate to compute a retransmission timer.

TCP set the retransmission timeout to be slightly longer than the mean round-trip delays.

- If the delay is large, TCP uses a large retransmission timeout.
- If the delay is small, TCP uses a small timeout.

The goal is to wait long enough to determine that a packet was lost, without waiting longer than necessary.

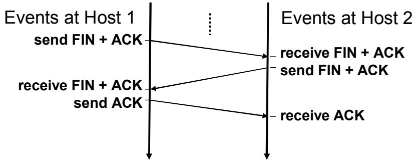
Three-Way Handshake

To guarantee that connections are established or terminated reliably, TCP uses a ***3-way handshake*** in which three messages are exchanged.

Scientists have proved that a 3-way exchange is necessary and sufficient to ensure unambiguous agreement despite packet loss, duplication, and delay.

TCP uses the term ***synchronization segment*** *(SYN segment)* to describe messages in a 3-way handshake used to create a connection, and the term ***FIN segment*** (short for fin*ish)* to describe messages in a 3-way handshake used to close a connection.

Three-Way Handshake



The 3-way handshake used to close a connection.

Acknowledgements sent in each direction are used to guarantee that all data has arrived before the connection is terminated.

Three-Way Handshake

TCP retransmits lost SYN or FIN segments. The handshake guarantees that TCP will not open or close a connection until both ends have interacted.

Part of the 3-way handshake used to create a connection requires each end to generate a random 32-bit sequence number.

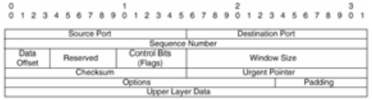
If an application attempts to establish a new TCP connection after a computer reboots, TCP chooses a new random number.

Because each new connection receives a new random sequence, a pair of application program scan use TCP to communicate, close the connection, and then establish a new connection without interference from duplicate or delayed packets.

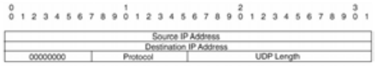
TCP Header

- Fixed format 20 bytes header plus 20 bytes options.
- All connection starts with ISN=0
- Data offset indicates where the data begins. (header length)
- 6 Control flags URG / ACK / PSH / RST / SYN / FIN

TCP header



Pseudoheader included in the TCP checksum



Example - Protocol Analysis TCP

- ------------ TCP Header ------------
- TCP: Source port = 2119
- TCP: Destination port = 8088
- TCP: Sequence number = 233590786
- TCP: Ack number = 4544001
- TCP: Data offset = 20
- TCP: Flags = 0x18
- TCP: ..0. .... URGENT Flag = FALSE
- TCP: ...1 .... ACK Flag = TRUE
- TCP: .... 1... PUSH Flag = TRUE
- TCP: .... .0.. RST Flag = FALSE
- TCP: .... ..0. SYN Flag = FALSE
- TCP: ....0 FIN Flag = FALSE
- TCP: Window = 1024
- TCP: Checksum = 5FB5
- TCP: Urgent pointer = 00000000

Domain

A ***domain*** is simply a subtree of the domain name space. The domain name of a domain is the same as the domain name of the node at the very top of the domain. So for example, the top of the ***polyu.edu*** domain is a node named ***polyu.edu***.

Every node in the tree must have a unique domain name, but the same label can be used at different points in the tree. The top-level domains are divided into three areas:

1. arpa is a special domain used for address-to-name mapping.
2. The seven 3-character domain names (organizational domains).
3. The 2-character domains are based on the country codes. These are called the country (the geographical) domains.

Domain Name System (DNS)

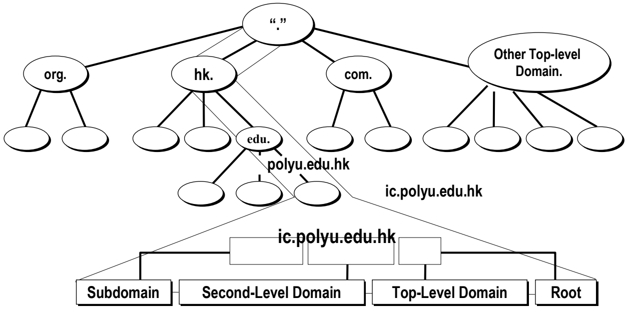
The ***domain name system*** uses a hierarchical naming scheme known as domain names, which is similar to the tree structure of a Unix file system.

The root of the DNS tree is a special node with a null label.

The name of each node (except root) has to be up to 63 characters.

The domain name of any node in the tree is the list of labels, starting at that node, working up to the root, using a period ("dot") to separate the labels

Domain Name System (DNS)



Domain

The domain name system does specify values for the most significant segment, which is called the top-level of the DNS. The table in Figure lists the top-level domains:

Domain Name	Assigned To
com	Commerical organizations
edu	Educational institutions
gov	Government institutions
mil	Military groups
net	Major network support centers
org	Organizations other than those above
int	International organizations

Domain Name (1)

- Domain name is a unique alphanumerical name that is mapped to an unique IP address. Domain name can be used to identify a host in the Internet instead of using IP addresses which is more difficult to memorize.
- e.g. www.ic.polyu.hk ↔ 158.132.155.107
  www.info.gov.hk ↔ 202.128.227.99
- Generic Top Level Domain Names (gTLDs)
  .com - commercial entities
  .org - non-profit making organizations
  .edu - academic institutions
  .net - network providers
  .gov - government

Domain Name (2)

- Country Code Top Level Domain (ccTLDs)
  - For example, .hk, .ca, .cn, .tw, .jp, .uk, .to,
  - http://www.iana.org/cctld/cctld-whois.htm
- Global Administration
  - Internet Assigned Numbers Authority (IANA)
- In Hong Kong
  - Hong Kong Domain Name Registration Co. Ltd.
  - http://www.hkdnr.net.hk/
- In China
  - China Internet Network Information Center
  - http://www.cnnic.net.cn/

Domain Name (3)

Infrastructure Domain

- Address and Routing Parameter Area domain (.arpa)

Currently 3 domains

- in-addr.arpa
  - Name servers for IPv4
- ip6.arpa
  - Name servers for IPv6
- e164.arpa
  - Name servers for ENUM
  - A method to enter ITU-T E.164 telephone numbering format into Internet – RFC2916

Name Server and Zone

The programs that store information about the domain name space are called *name servers*.

Name servers generally have complete information about some part of the domain name space (a *zone*), which they load from a file or from another name server.

The name server is then said to have *authority* for that zone. Name servers can be authoritative for multiple zones, too.

The difference between a zone and a domain is important, but subtle. All top-level domains, and many domains at the second level and lower, such as ***polyu.edu,*** are broken into smaller, more manageable units by delegation.

Subdomain

A ***subdomain***, also called a child domain, is a DNS domain that is located directly beneath another domain in the DNS hierarchical structure.

A simple way of deciding whether a domain is a subdomain of another domain is to compare their domain names.

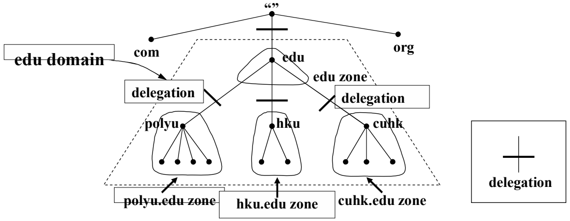
A subdomain's domain name ends with the domain name of its parent domain.

For example, ic.polyu.edu.hk. is a ***subdomain*** of the polyu.edu.hk. ***domain***

Name Server and Zone

The ***edu*** domain, shown in Figure, is divided into many zones, including the ***polyu.edu*** zone, the ***hku.edu*** zone, and the ***cuhk.edu*** zone.

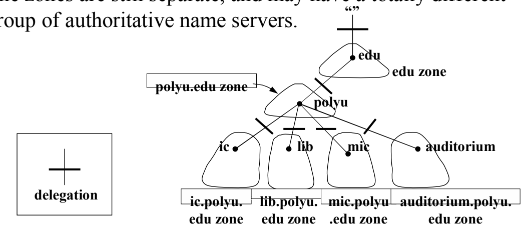
At the top of the domain, there's also an ***edu*** zone. It's natural that the folks who run ***edu*** would break up the ***edu*** domain.



Name Server and Zone

The ***polyu.edu*** subdomain is, in turn, broken up into multiple zones by delegation, as shown in Figure. There are delegated subdomains called ***ic***, ***lib***, ***auditorium***, and more. Each of these subdomains is delegated to a set of name servers.

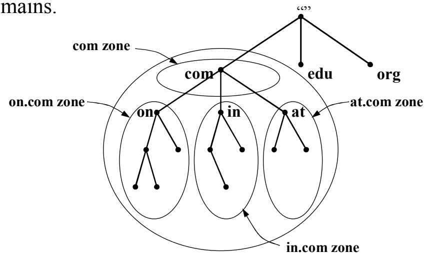
The zones are still separate, and may have a totally different group of authoritative name servers.



Name Server and Zone

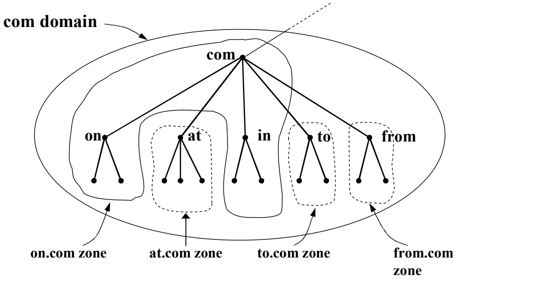
A zone and a domain may share the same domain name but contain different nodes.

In particular, the zone doesn't contain any nodes in delegated subdomains.



Name Server and Zone

If a subdomain of the domain isn't delegated away, however, the zone contains the domain names and data in the subdomain.



DDNS

Allows remote users to gain full access to your corporate intranet and Exchange worldwide with a dynamic I.P.

The DDNS service, an IP Registry provides a public central database where information such as email addresses, hostnames, IPs etc. can be stored and retrieved.

This solves the problems if your DNS server uses an IP associated with dynamic IPs.

DDNS

Without DDNS, we always tell the users to use the IP to access the internal server. It is inconvenient for the users if this IP is dynamic.

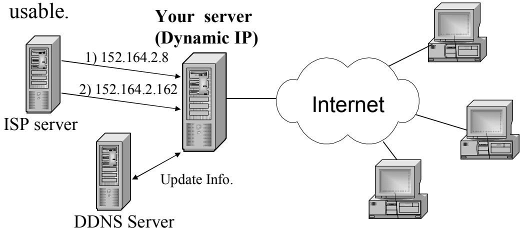
With DDNS supported, you apply a DNS name (e.g., www.tug.com) for your server (e.g., Web server) from a DDNS server.

The outside users can always access the web server using the www.tuv.com regardless of the IP.

DDNS

When the ISP assigns the a new IP, the application program inform the DDNS server the change of this IP so that the server can update its IP-to-DNS entry.

Once the IP-to-DNS table in the DDNS server is updated, the DNS name for your web server (i.e., www.tuv.com) is still usable.


Your server
(Dynamic IP)
1) 152.164.2.8
2) 152.164.2.162
ISP server
Internet
Update Info.
DDNS Server