Suleyman Demirel University Library

1 2 3 4 5 6 7 8
Speed
Power
Link/Act

FUNDAMENTALS OF COMPUTER NETWORKS IN MICROLEARNING STYLE

Zhamanov A.M.

УДК 004(075)

ББК 32.973 я73
Ж 26

Approved and recommended by the Academic Council of the University named after Suleyman Demirel, the protocol number 8, 2012

Утверждено и рекомендовано Ученым Советом Университета имени Сулеймана Демиреля, протокол №8, 2012

Reviewers: Doctor of Technical Sciences, Prof. **Niyazi A.**, Doctor of Technical Sciences, Prof. **Ashigaliyev D.**

Рецензенты: доктор технических наук, профессор **Ниязи А.**, доктор технических наук, профессор **Ашигалиев Д.**

Zhamanov Azamat Maratovich

Жаманов Азамат Маратович

Fundamentals of Computer Networks in microlearning style: textbook.
"Microlearning research center" under Suleyman Demirel University. – Almaty, 2012.-128 p.
Основы компьютерных сетей в стиле микрообучения: учебное пособие.
"Microlearning research center" при университете имени Сулеймана Демиреля. – Алматы, 2012. – 128 с.

ISBN 9965-792-58-5

The textbook describes the fundamentals of Computer Networks in microlearning style.
Textbook represents theoretical and practicable interest contains useful materials, illustrations and tables. Textbook is intended for students of IT engineers who study "Computer Networks" course in universities.

В учебном пособии описаны основы Компьютерных Сетей в стиле микрообучения.
Учебное пособие представляет теоретический и практический интерес, содержит полезные материалы, иллюстрации, таблицы. Учебное пособие предназначено для студентов ИТ инженерии ВУЗов, изучающих дисциплину «Компьютерные Сети»

ISBN 9965-792-58-5

Contents

Feedbacks

I hope that you'll get this book useful. This is my first book and that's why you can find some mistakes. If you have any comments regarding how I could improve the quality of book, you can contact me through email at zhamanov.azamat@gmail.com.

I greatly appreciate assistance

Motivator: Meirambek Zhaparov

Adviser: Meirambek Zhaparov

Book Designer: Almat Kurmashev

Proofreader: Alexander Temirov

Abstract

In modern world, people are always busy with their concerns. In addition to all this not an excessive amount of relevant information is processed by our brain every day. In this regard, it is difficult to find time for learning the required knowledge. For that reason I decided to write book in microlearning style, which will provide readers to get required information in short time, because of microlearning style gives ability to explain a lot of things without using much words which is separated into small parts.

In this book:

- Chapter 1 - **"Understanding the Computer Networks"** explains the structure of Computer Networks including Main Parts of Computer Networks, Types of Computer Networks, Explanation of Protocol and introduction to OSI and TCP/IP Layered Model
- Chapter 2 – **"Application Layer Protocol"** compares OSI model's Application, Presentation and Session Layers with TCP/IP model's Application layer. And also explains most important protocols in Application Layer.
- Chapter 3 – **"OSI Transport Layer"** explains main functionality of OSI Transport layer, provides information about most usable Transport Layer protocols: TCP and UDP. Compares TCP and UDP protocols.
- Chapter 4 – **"OSI Network Layer"** explains four basic processes of Network Layer, includes Encapsulation and Decapsulation processes. Provides information about Addressing.
- Chapter 5 – **"Addressing The Network – IPv4 and IPv6"** deeply explains structure of IPv4 and reviews IPv6.
- Chapter 6 – **"OSI Data Link Layer"** explains two Sub layers of Data Link layer, compares LLC and MAC Sub layers. Explains types of Media Access Mechanism.
- Chapter 7 – **"OSI Physical Layer"** provides information about physical connections in Computer Networks. Explains in details cables and connectors.

To get more information about microlearning see Appendix.

Preface

Nine years ago I studied in Aksay Kazakh – Turkish High School. At that time I had a big problem with the choice of university. I really did not know where to go and what to expect in future. My classmates were discussing universities day. And I made decision to follow my best friends wherever they go. Firstly they wanted to apply to Kaspian University, after what they changed their decision and went to applied to KazNU and ones more, they changed their plans and went to applied to German University, none of those universities met the criteria of my friends, since they were graduates of KTL school, and their expectations of university were too high. In the end, our choice fell on SDU by advice of our Adviser (abishka). At that time SDU was not so authoritative, for some people our choice was strange, but the main feature was education in English language.

After ENT we went to SDU with my mother, she agreed with my decision, because of respect and trust for Turkish teachers.

In the first year of my student's life I met a lot of good people who wanted to be my friends. We studied very hard, but at the same time we had to study much more.

Nevertheless we also had time to enjoy sdudent's live, if you are or if you've been sdudent you'll understand me. Picnics, Tea with friends and adviser, Maklube, Rivanie, Bicycle party, Ice Party, Football Tournament, LAN Party etc.

After first year we went to Turkey. It was my first trip abroad USSR. We had unforgettable trip.

My 2nd, 3rd and 4th years were also difficult to me. At 4th year of being sdudent I worked in Social Department of SDU with my friends: Almat and Adil. At that time our dean gave me chance to be an assistant of Mr. Nurlibayev, he was Cisco CCNA instructor, he was good teacher, but he was too busy. After I became an assistant, I felt a big responsibility on my shoulders. I had to study much more than I studied in student life.

Nevertheless during four years of being a teacher I met a lot of good people (sdudents). Now I am Certified Cisco CCNA instructor, I have two assistants and I am very happy.

I am married and I have a son, he is two years old and he goes to kindergarten with my colleague's son in one group. We go to kindergarten with my colleague and he always advises me to do something good. Finally with his motivation I have finished this book.

Acknowledgments

First and most important I would like to thank my wife, Zhulduz, my son Ibrahim, and my sister-in-law Zhazira. This book would not have been possible without their love, support, and understanding.

Thanks to my mother, father and my brother Kuandik. Special thanks to my colleague Mr. Meirambek Zhaparov, he gave me motivation many times to continue work on this book.

Thanks to dean of engineering faculty Mr. Humbet Aliyev. When I studied at 4th course he gave me a chance to be an assistant at Suleyman Demirel University, and starting from that point, my life has been changed. At the beginning of my career he had to tinker with my punctuality many times.

Thanks to my friends Assylbekov Berik, Akhmarov Ravil, Shavketov Eldar, Mels Begenov, Bekzat Lespayev, and Almat Kurmashev, they supported me during my school and university life.

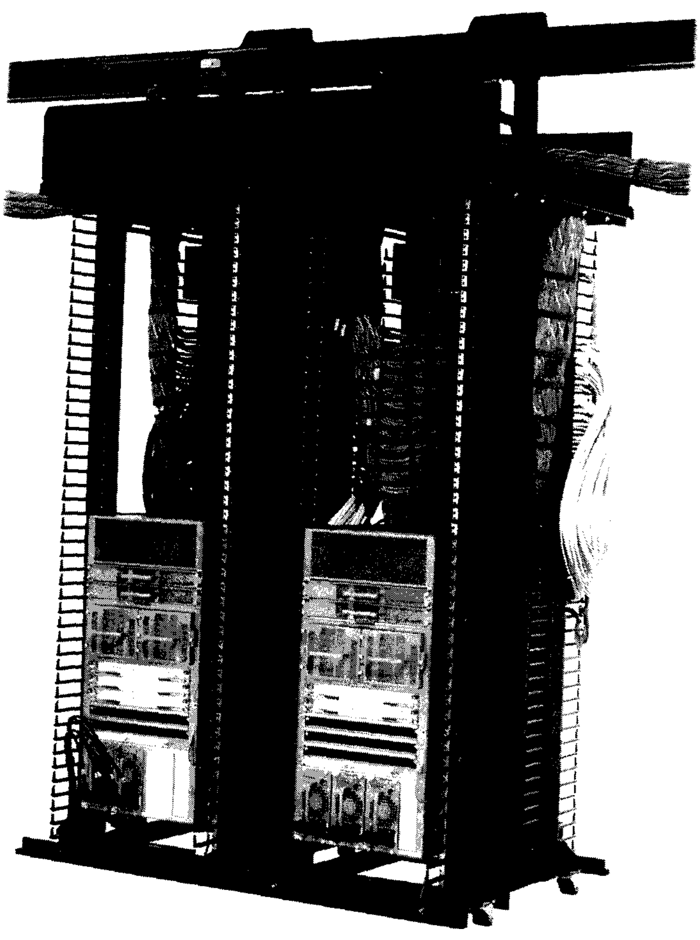
Thanks to my friends and colleagues Ardak Shalkarbayuli, Askar Satabaldiev, Abai Nusipbek, Andrey Bogdanchikov, Zhasdauren Duisebekov, Nurbek Saparkhozhayev, Cemil Tosik, Selim Guvercin, Konstantin Latuta, Rasim Suliyev, Bakhit Bakiyev, Omerbek Nurbavliyev, Ermek Nugmanov, Rasul Aitasov, Rasul Mashurov, Aset Onlasov.

Thanks to my students who supported me on writing this book.

Zhamanov Azamat

Chapter 1

Understanding the Computer Networks

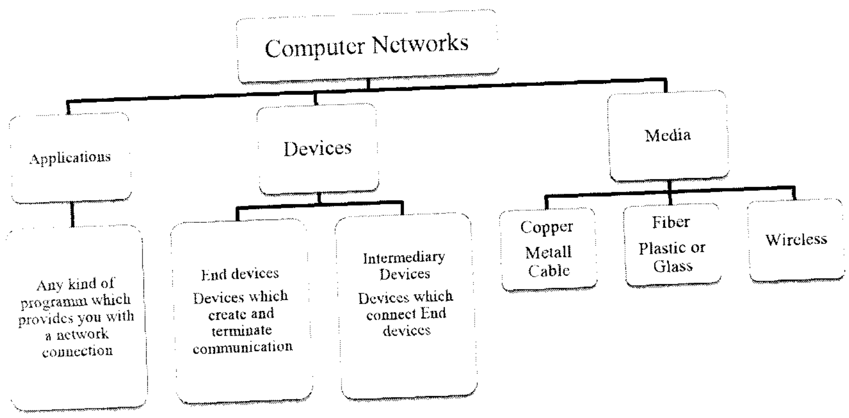


Main Parts of Computer Networks

Computer Networks consist of three main parts:

1. Applications
2. Devices
3. Media

Pic 1:1 shows structure of Computer Networks



Structure of Computer Networks

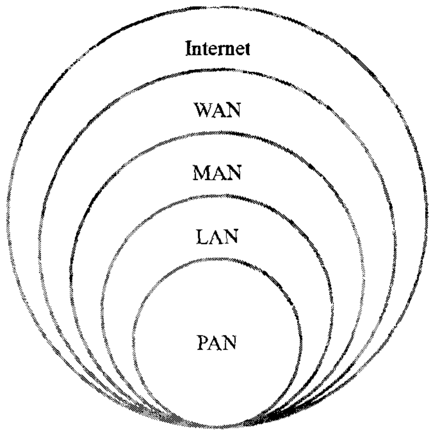
1. Application example: Skype, Gtalk, MSN Messenger etc.
2. Devices:
   - End device example: PC (computer), network printer, server etc.
   - Intermediary device example: Switch, router, hub
3. Media:
   - Copper media example: UTP, STP,
   - Fiber media example: Fiber cable
   - Wireless media example: Air

Now you know what Computer Networks consist of, so let us continue with the types of Computer Networks

Types of Computer Networks

1. **PAN** –Personal Area Network (the very close area, example: Bluetooth)
2. **LAN** – Local Area Network (Single geographical area, example: Enterprise network)
3. **MAN** – Metropolitan Area Network (Medium size geographical area, example: Disctrict connection)
4. **WAN** – Wide Area Network (Long distance connection, example: Interconnection between cities)
5. **Internet**- Global interconnection of LANs, MANs and WANs
6. **Intranet** – Private Interconnection between LANs, MANs and WANs.

Pic1:2 Shows type o Computer Networks



Pic 1: 2 Types of Computer Networks

Conversation rules (Protocols)

In making conversation people use some rules. Computers also use some rules in making communication. Let us discuss some basic human conversation rules:

1. Before starting conversation say "Hello" and before finishing it, say "good bye".
2. When you speak to someone, that person has to listen to you and vice-versa, when someone speaks to you, you have to listen.
3. Both of the people having a conversation, have to know a common language

In Computer Networks these rules are called **Protocols.**

Protocol – is a set of rules.

Standards of Computer Networks protocols are developed by IEEE (Institute of Electrical and Electronics Engineers) and IETF (Internet Engineering Task Force)

Let us describe some Network Protocols

Segmentation (division) of data rule

I think that one of the easiest ways of describing Network Protocols would be through some examples.

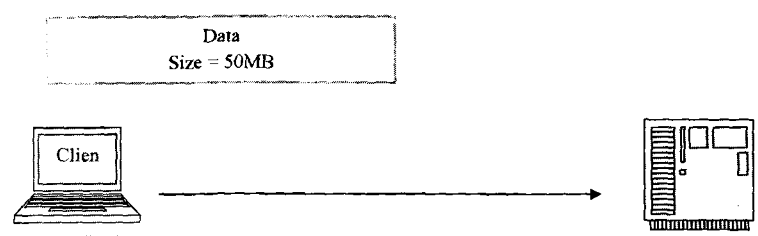
In this example user Client is going to send 50 MB of data to Server, but before doing that Client have to divide data into small parts. What for?

To answer this question let us describe problems which can occur during this transportation

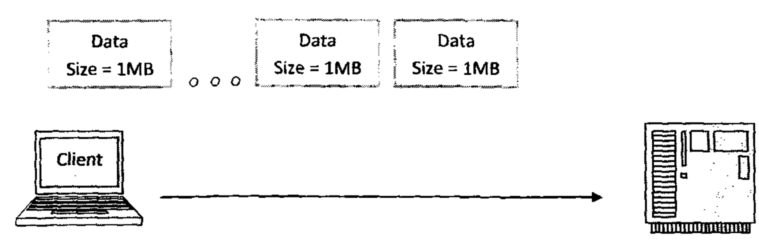
1. Media may be fully busy; it means that only one computer would be able to send or receive the data at the same time.
2. If during transportation some bits are lost, client will have to resend the whole 50 MB to server again.

Pic1:3 Represents sending data without segmentation

Pic 1:4 Represents sending data with segmentation



Pic 1:3 Sending Data without segmentation



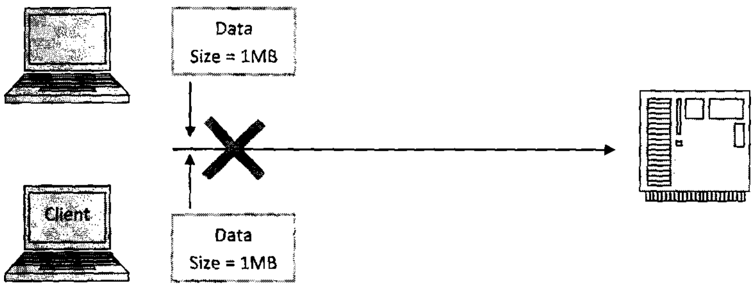
Sending Data after segmentation

Multiplexing

Next, what will happen if two or more PCs use the same media at the same time?

Answer: Collision will happen on the media. To improve the problem, Computer Networks have mechanism which is called **Multiplexing**.

Pic 1:5 shows how data segments can make collision in shared media.

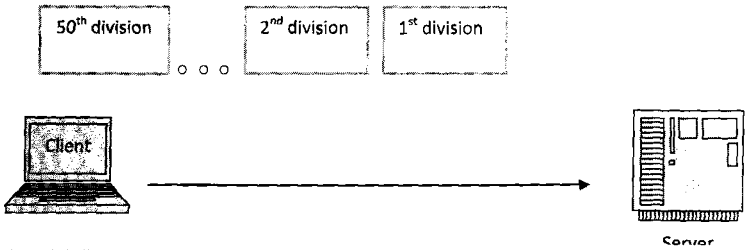


Pic 1: 5 Collision occurred in network

Labeling (giving sequence)

One more rule of communication in Computer Networks is **Labeling Process**.

Receiving device has to define a sequence of each part of information, because receiving device can receive them in random order due to different paths usage. After receiving them in wrong sequence, computer stores them in cash memory, improves the sequence and after that sends data to application. Pic 1:6 shows labeling process on transport layer.



Pic 1: 6 Labeling

*Alright friends, now you know some practical usage of Computer Networks rules (protocols), let us discuss Networking **Layered Model**.*

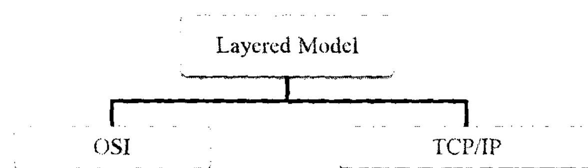
Networking Layered Model

One of the easiest ways to understand Computer Networks is to divide different types of protocols (rules) by their functionality and responsibilities.

Networking Layered Model

- Is the way of understanding the network structure
- No matter which model you use, you are speaking about the same network
- The model is not actual network

Currently we are using two models, they are: OSI (Open System Interconnections) and TCP/IP models. The first Layered model was TCP/IP model, which consists of four layers , whereas OSI consist of seven layers. Pic 1:7 Represents networking models

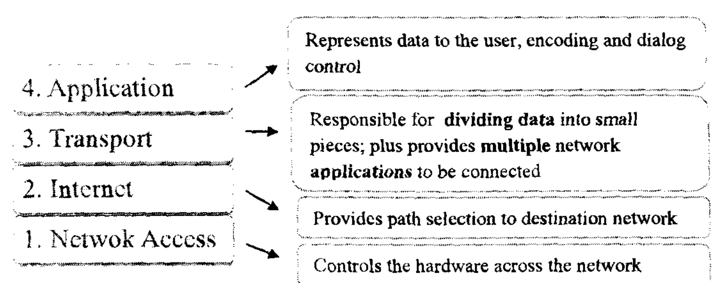


Pic 1:7 Types of Computer Networks

And again, no matter which Model you use, you are speaking about the same network

TCP/IP model – 4 layers

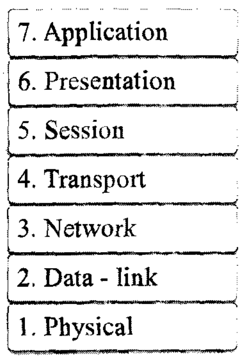
Each of the layers is responsible for different types of operations. Pic1:8 shows Layers of TCP/IP model.



Pic 1:8 Layers of TCP/IP networking model

OSI (Open System Interconnections) model – 7 layers

We are going to discuss OSI Model later in this chapter. Pic 1:9 shows Layers of OSI networking model.

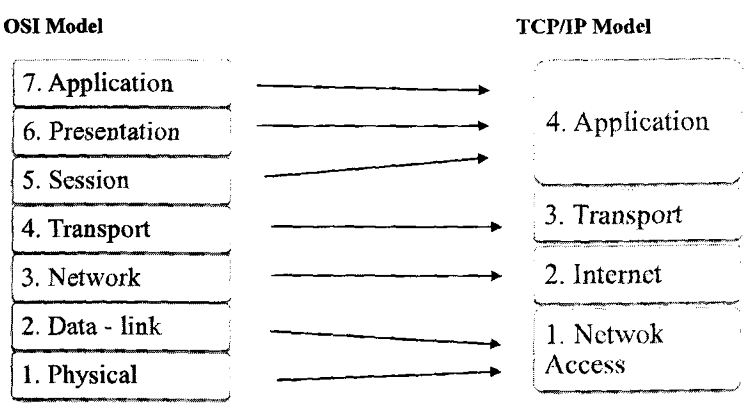


Pic 1: 9 Layers of OSI Networking model

Comparison of OSI and TCP/IP Models

In comparison of two OSI and TCP/IP models we can see that 7th Application, 6th Presentation and 5th Session Layers of OSI model are division of 4th Application layer of TCP/IP model.

4th Transport layer of OSI is equal to 3rd Transport of TCP/IP model, 3rd Network layer same as 2nd Internet layer of TCP/IP model. 2nd Data-Link and 1st Physical Layer are equal to functionality of 1st Network Access Layer of TCP/IP model. Pic 1:10 Shows comparison of OSI and TCP/IP Models.



Pic 1: 10 Comparison of OSI and TCP/IP networking models

Application layer of TCP Model and Application, Presentation and Session Layers of OSI Model

Application Layer (OSI) – The Application layer, Layer seven, is the top layer of both the OSI and TCP/IP models. It is the layer that provides the interface between the applications we use to communicate and the underlying network, over which our messages are transmitted. Application layer protocols are used to exchange data between programs running on the source and destination hosts. There are many Application layer protocols and new protocols are always being developed.

Also, name comes from the program, so it means that at this layer we can see programs which give as availability to make communication.

Example: Skype, Gtalk, MSN Messenger and MAgent.

Presentation Layer of OSI Model

As you know in computer system we have different types of files, example: mp3, PDF, GIF… And each of this file types must be encrypted and compressed in different ways. Presentation Layer is responsible for encryption and compression of different types of files before sending data and after receiving data.

Session Layer of OSI Model

As the name of the Session layer implies, functions at this layer create and maintain dialogs between source and destination applications. The Session layer handles the exchange of information to initiate dialogs, keeps them active, and restarts sessions that are disrupted or idle for a long period of time.

Transport Layer

Transport Layer is responsible for defining the application to which data has to be received and from which application data leaves the computer. Also Transport Layer makes management of data transportation.

Network Layer

Is responsible for finding out the network where or to which data has been sent.

Data-Link Layer

Responsible for Media Access Control, means that it controls how data inserted into the Media (cable).

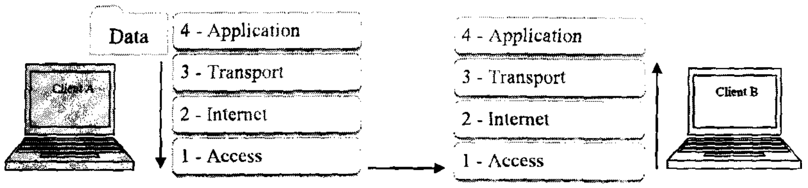
Physical Layer

Responsible for converting data into the electrical, optical and electromagnetic signals.

Now let us describe communication process with Networking Layered Model.

Communication Process

As the name of the Session layer implies, functions at this layer create and maintain dialogs between source and destination applications. The Session layer handles the exchange of information to initiate dialogs, keeps them active, and restarts sessions that are disrupted or idle for a long period of time. Pic 1:11 shows communication process in computer networks.



Pic 1: 11 Communication process

In this example "Client A" is going to send data to "Client B". A complete communication process includes these steps:

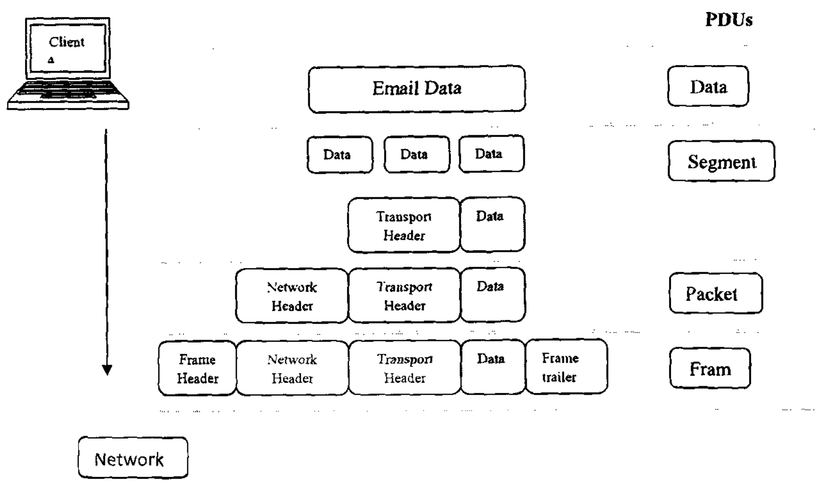
1. Creation of data at the application layer of the originating source end device
2. Segmentation and encapsulation of data as it passes down the protocol stack in the source end device
3. Generation of the data onto the media at the network access layer of the stack
4. Transportation of the data through the internetwork, which consists of media and any intermediary devices
5. Reception of the data at the network access layer of the destination end device
6. Decapsulation and reassembly of the data as it passes up the stack in the destination device
7. Passing this data to the destination application at the Application layer of the destination end device

Encapsulation

As application data is passed down the protocol stack on its way to be transmitted across the network media, various protocols add information to it at each level. This is commonly known as the encapsulation process.

Example of Communication Process.

"Client A" is going to make communication over the network. Pic 1:12 represents example of communicational process.



Pic 1: 13 Example of communication process

Protocol Data Unit

Protocol Data Unit (PDU) - The form that a piece of data takes at any layer is called a Protocol Data Unit (PDU).

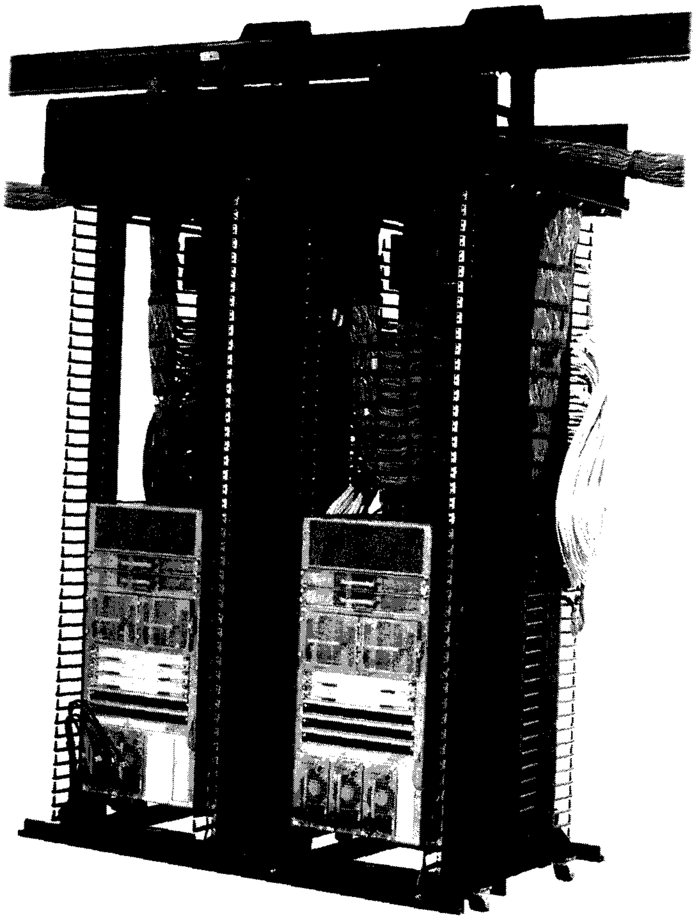
Here is the list of PDUs of TCP/IP layered model:

- Data - The general term for the PDU used at the Application layer
- Segment - Transport Layer PDU
- Packet - Internetwork Layer PDU
- Frame - Network Access Layer PDU
- Bits - A PDU used when physically transmitting data over the medium

Well, let us deeply describe all seven layers of OSI Networking Model, starting from the Application Layer.

Chapter 2

Application Layer Protocol's Functionality



Application Layer

Most of us experience the Internet through the World Wide Web, e-mail services, and file-sharing programs. These applications, and many others, provide the human interface to the underlying network, enabling us to send and receive information with relative ease. Typically the applications that we use are intuitive, meaning we can access and use them without knowing how they work. However, for network professionals, it is important to know how an application is able to format, transmit and interpret messages that are sent and received across the network.

In other words it is a program layer.

In application layer we have protocols like: HTTP, SMTP, POP, DHCP and DNS

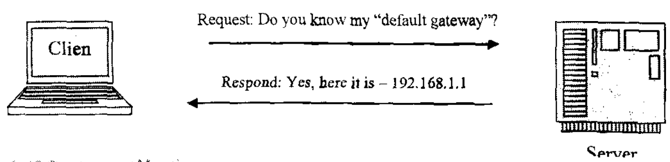
Like in human communication, Computer communication usually has two positions. 1st position: those who take service from someone, and 2nd position: those who provide service. Let us describe two models of communication in Computer Network.

The Client-Server Model

In this mode we can have many clients which are connected to one server. Single server can make service for many clients.

Client - device requesting the information is called a client.

Server - device responding to the request is called a server, also we can say that servers makes service for clients. Pic 1:13 shows intercommunication between Client and Server in Client-Server model



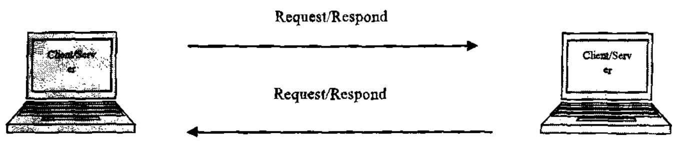
Pic. 1:13 Client-server Model

We can compare Client-Server model with front-desk worker. Usually they seat in front of the entrance door and every client firstly sees front-desk worker. It means that this worker is going to make service for many clients.

The Peer-to-Peer Model

In this kind of networking model every "Client" is a "Server" and every "Server" is a "Client".

Pic 1:14 shows communication process between clients in peer-to-peer model.

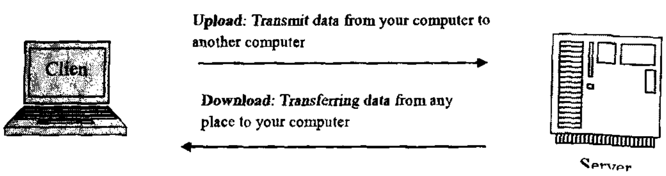


Pic 1: 14 Peer-to-Peer Model

*While people make communications they are listening and speaking, so we can say that when we are listening, we get information. When we are speaking we give information. When computer takes information it is called **Download**, when computer gives information, it is called **Upload**.*

Upload and Download

Pic 1:15 shows Upload and Download operations.

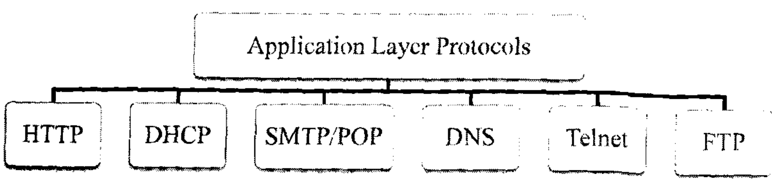


Pic 1: 15 Upload/Download

Let us describe some of the Application Layer Protocols.

Application Layer Protocols

Pic 1:16 shows Application Layer Protocols



Pic 1: 16 Application Layer Protocols

HTTP – Hypertext Transfer Protocol

Question: What is the meaning of the word "Hypertext"?

Hyper, Text?

Answer: All the texts and objects that are inside the browser are called Hypertext

Example of hypertext: In this picture you can see pictures, text and animation. All of it is called hypertext. Pic 1:17 shows example of hypertext.

Pic 1:17 Example of hypertext

HTTP Protocol is responsible for hypertext (web content) transportation.
When web client opens web browser and types in URL the address like www.sdu.edu.kz, the web browser makes request to web server: Get "**index.html**" from www.sdu.edu.kz. And after that web server makes respond to client.

DNS - Domain Name System

Each of us has a name and almost all of us have nicknames, for example: instead of "Berik" we can use "Bake", instead of "Serik" we can use "Seke".

Question: Why people use nickname?
Answer: Because nicknames are usually easier to remember.

Like in human life, in data networks, devices are labeled with numeric IP addresses (names), so that they can participate in sending and receiving messages over the network. However, most people have a hard time remembering this numeric address. Hence, domain names (nicknames) were created to convert the numeric address into a simple, recognizable name.

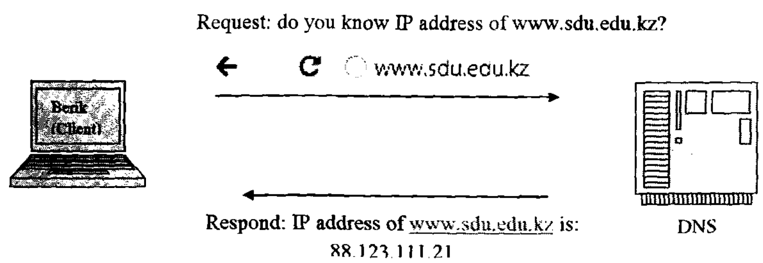
On the Internet these domain names, such as www.sdu.edu.kz (nickname), are much easier for people to remember than 88.123.111.21 (name), which is the actual numeric address for this server.

www.sdu.edu.kz – I can easily remember this name
88.99.11.12 – I can remember it, but not so easily

How DNS Works?

In this example Berik is trying to open www.sdu.edu.kz web site. He is typing the domain name of SDU: www.sdu.edu.kz in to the URL of the browser and pressing "Enter", but his computer doesn't know numerical IP address of www.sdu.edu.kz domain name. And without this IP address he can't open that page.

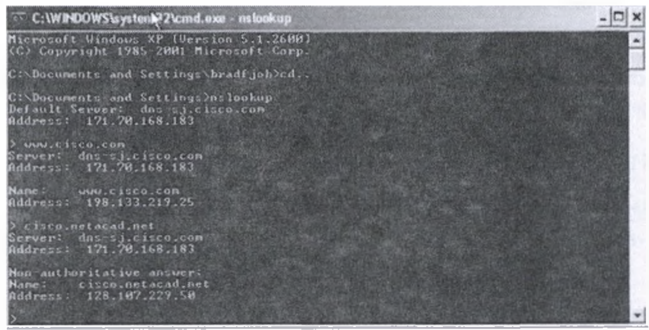
So Berik's computer has to learn the IP address of that domain, by sending request to DNS server. If server has got the IP address of that domain, it will send respond with it. After that Berik will be able to open that web page. Pic 1:18 shows DNS process.



Pic 1: 18 DNS in process

If you want to see the IP address of any domain name, open "CMD" application and type "nslookup" command, after what type domain name.

Pic 1:19 shows output of *nslookup* command in cmd.



Pic 1: 19 Output of *nslookup*

When a client makes a query, the server's "named" process first looks its own records to see if it can resolve the name. If it is unable to find out the name using its stored records, it contacts other servers in order to resolve the name.

The request may be passed along to a number of servers, which can take extra time and consume bandwidth. Once a match is found and returned to the original requesting server, the server temporarily stores the numbered address that matches the name in cache.

If that same name is requested again, the first server can return the address by using the value stored in its name cache. Caching reduces both the DNS query data network traffic and the workloads of servers higher up the hierarchy. The DNS Client service on Windows PCs optimizes the performance of DNS name resolution by storing previously resolved names in memory, as well.

The Domain Name System uses a hierarchical system to create a name database to provide name resolution. The hierarchy looks like an inverted tree with the root at the top and branches below.

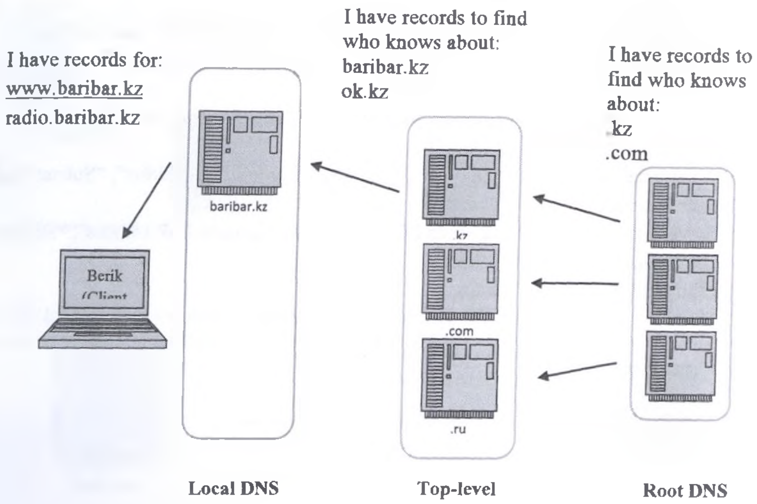
At the top of the hierarchy, the root servers maintain records about how to reach the top-level domain servers, which in turn have records that point to the secondary level domain servers and so on.

The different top-level domains represent either the type of organization or the country of origin. Examples of top-level domains are:

- .kz -Kazakhstan
- .com - a business or industry
- .org - a non-profit organization

After top-level domains are second-level domain names, and below them are other lower level domains.
Each domain name is a path down this inverted tree starting from the root.

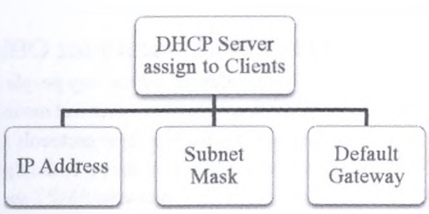
Pic 1:20 shows hierarchical view of DNS Servers.



Pic 1: 20 Hierarchical view of DNS Servers

DHCP – Dynamic Host Configuration Protocol

If a client wants to connect to a network he must have at least an "IP address", a "Subnet Mask" and a "Default Gateway" to be configured.
Without DHCP, users have to manually input configurations. Pic 1:21 shows what DHCP Server supports to client.



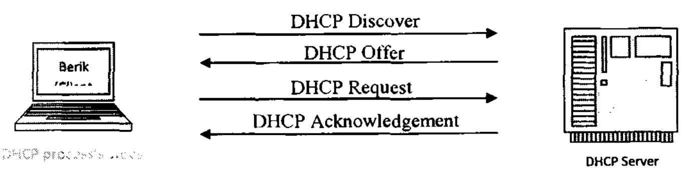
Pic 1: 21 DHCP Servers functionality

DHCP allows a host to obtain an IP address dynamically when it connects to the network. The DHCP server is contacted and an address requested. The DHCP server chooses an address from a configured range of addresses called a pool and assigns ("leases") it to the host for a set period.

To easily understand this protocol let us take a look for the DHCP four step process

Four Steps of DHCP Process

1st step: Client connects to a network without "IP address", "Subnet Mask" and "Default Gateway" but with DHCP client. After that, it starts to send DHCP Discovery (I am looking for DHCP server) packet to find out DHCP server.
2nd step: Server receives DHCP Discovery packets from client and sends offer (I am DHCP Client) to client.
3rd step: Client receives offer and sends DHCP Request (Give me "IP address", "Subnet Mask" and "Default Gateway").
4th step: Server receives request and sends DHCP Acknowledgement ("IP address", "Subnet Mask" and "Default Gateway") to client.
Pic 1: 22 shows DHCP process's steps.



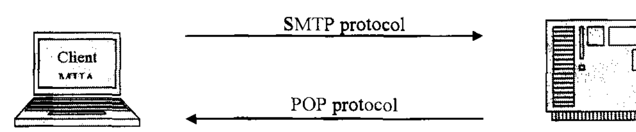
Pic 1: 22 DHCP process's steps

Telnet/SSH Protocols

Both of these protocols give you ability to a remote control of the computer. Example of application can be "putty". Difference between Telnet and SSH is in security, SSH (Secure Shell) is more securable, because it makes encryption all of the data. Telnet sends data in plain text (without encryption).

SMTP/POP – Simple Mail Transfer Protocol/Post Office Protocol

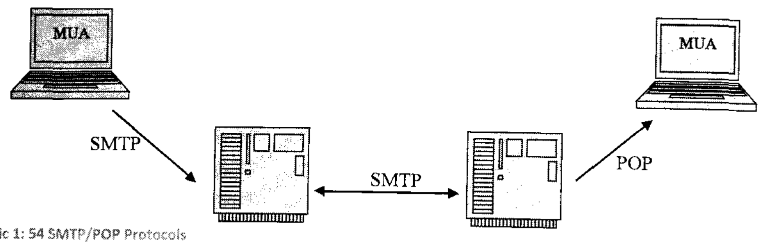
E-mail, the most popular network service, has revolutionized the way people communicate through its simplicity and speed. Yet to run on a computer or other end device, e-mail requires several applications and services. Two example Application layer protocols are Post Office Protocol (POP) and Simple Mail Transfer Protocol (SMTP), shown in the figure. As with HTTP, these protocols define client/server processes. Pic 1:23 Represents SMPT and POP protocols.



Pic 1: 23 SMTP/POP protocols

*Client is using Application which is called **MUA** - Mail User Agent*

Pic 1:24 represents SMTP and POP Protocols in use.

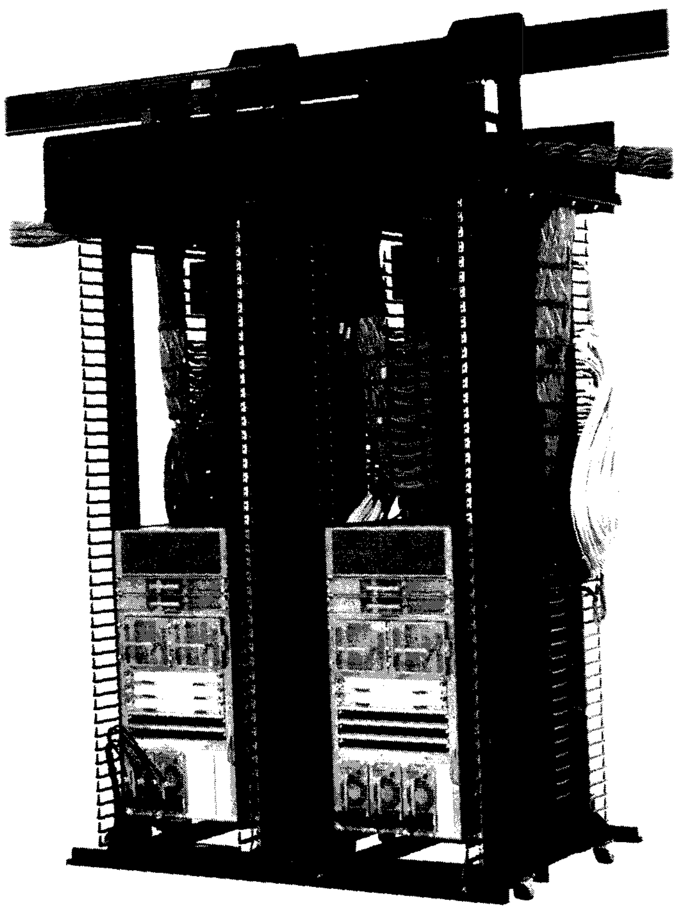


Pic 1: 54 SMTP/POP Protocols

Server that is resending message to another server use app. ***MTA***
Server that is resending message to recipient use app. ***MDA***

Chapter 3

OSI Transport Layer



Transport Layer

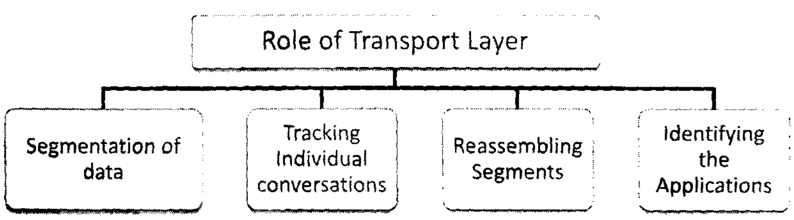
Data networks and the Internet support the human network by supplying seamless, reliable communication between people - both locally and around the globe. On a single device, people can use multiple services such as e-mail, the web, and instant messaging to send messages or retrieve information. Applications such as e-mail clients, web browsers, and instant messaging clients allow people to use computers and networks to send messages and find information.

Data from each of these applications is packaged, transported, and delivered to the appropriate server domain or application on the destination device. The processes described in the OSI Transport layer receive data from the Application layer and prepare it for addressing at the Network layer. The Transport layer is responsible for the overall end-to-end transfer of application data.

In this chapter, we examine the role of the Transport layer in encapsulating application data for use by the Network layer. The Transport layer also encompasses these functions:

- Enables multiple applications to communicate over the network at the same time on a single device
- Divides data into segments
- Ensures that, if required, all the data is received reliably and in order by the correct application

Pic 1:25 shows roles of Transport Layer in OSI networking model



Pic 1: 65 Roles of Transport Layer in OSI networking model

Segmentation of Data

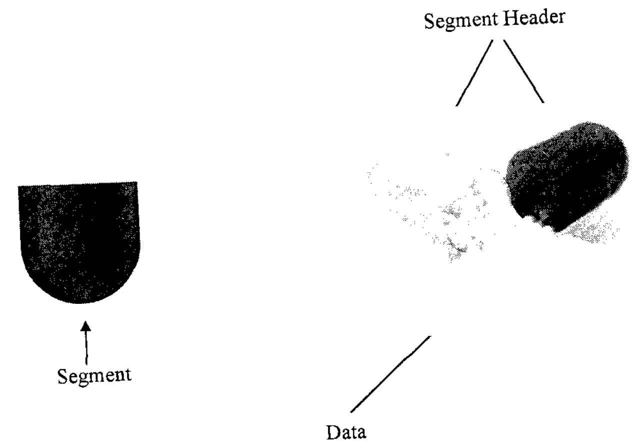
As each application creates a stream data to be sent to a remote application, this data has to be prepared to be sent across the media in manageable pieces. Transport Layer makes segmentation process for easier transportation, because if we send data in one stream, that data will fully load the media.

- The Transport layer protocols describe services that segment data from the Application layer.
- This includes the encapsulation, required for each piece of data.
- Each piece of application data requires headers to be added at the Transport layer to indicate to which communication it is associated.

*Firstly we have to understand meaning of word **Encapsulation**.*

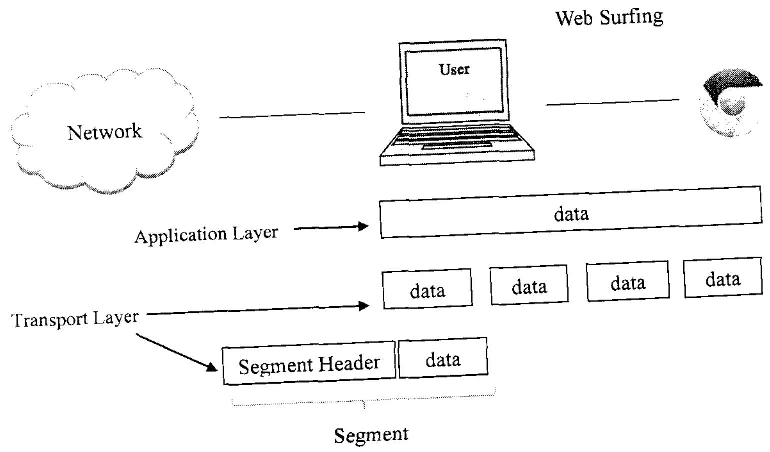
Encapsulation is the process of preparing data before placing into the media

Example of encapsulation in Transport Layer: Pic 1:26 shows Segment content and Header.



Pic 1: 26 Segment of Transport Layer

One more example of Encapsulation in Transport Layer: Pic 1:27 shows encapsulation process of Transport Layer.



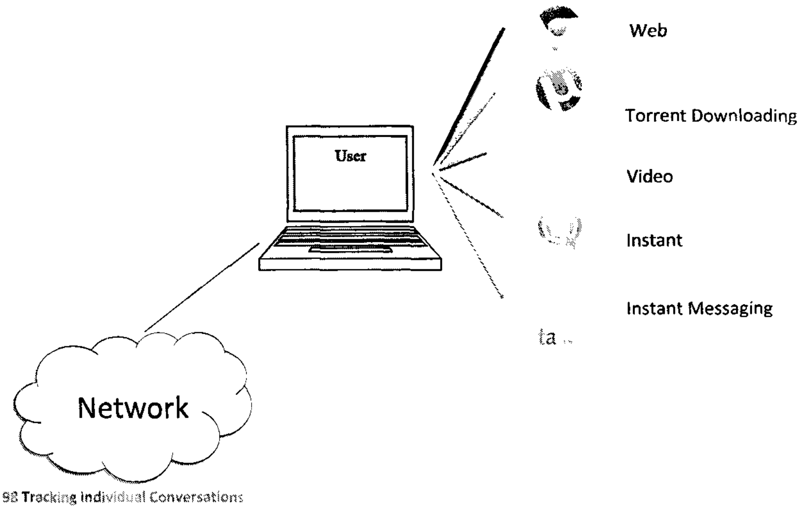
Pic 1: 27 Segmentation in Transport Layer

Tracking Individual Conversations

Transport Layer provides Multi-Connection by using "Ports".
Any host may have multiple applications that are communicating across the network. Each of these applications will be communicating with one or more applications on remote hosts. It is the responsibility of the Transport layer to maintain the multiple communication streams between these applications.

Let us take a look at the graphical example to easily understand how Transport Layer makes that.

Pic 1:28 shows tracking individual conversations in Transport Layer



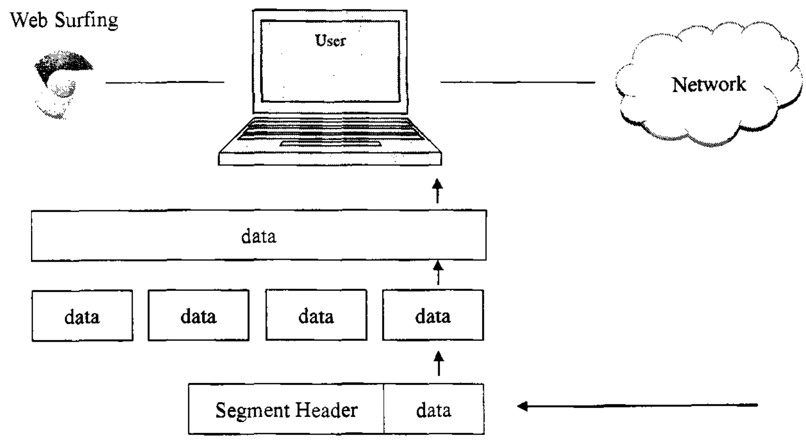
Pic 1: 98 Tracking Individual Conversations

In this graphic you see different types of application which are making communication over one media to the networks, in this example they are separated by differently coloured lines, but in real life separation is done by using ports.

Reassembling Segments

- At the receiving host, each piece of data may be directed to the appropriate application.
- Additionally, these individual pieces of data must also be reconstructed into a complete data stream that is useful to the Application layer.
- The protocols at the Transport layer describe how the Transport layer header information is used to reassemble the data pieces into streams to be passed to the Application layer.

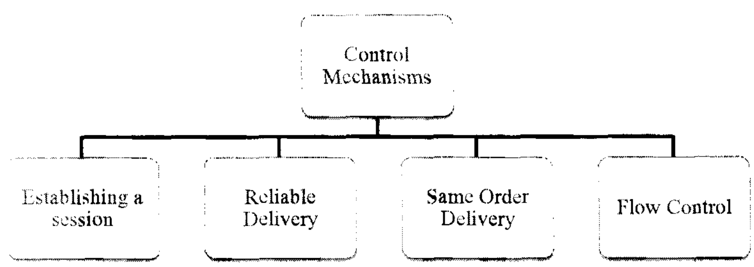
Example of Reassembling Segments: Pic 1:29 shows reassembling segments in process.



[illegible]ssembling segments in process

Controlling the Conversations

Pic 1:30 represents structure of control mechanisms in Transport Layer



Pic 1:30 Control Mechanisms of Transport Layer

Establishing a session

The Transport layer can provide this connection orientation by creating a sessions between the applications. These connections prepare the applications to communicate with each other before any data is transmitted. Within these sessions, the data for a communication between the two applications can be closely managed.

Reliable Delivery

For many reasons, it is possible for a piece of data to be corrupted, or lost completely, as it is transmitted over the network. The Transport layer can ensure that all pieces reach their destination by having the source device to retransmit any data that is lost.

Same Order Delivery

Because networks may provide multiple routes that can have different transmission times, data can arrive in the wrong order. By numbering and sequencing the segments, the Transport layer can ensure that these segments are reassembled into the proper order.

Flow Control Mechanism

Network hosts have limited resources, such as memory or bandwidth. When Transport layer is aware that these resources are overtaxed, some protocols can request that the sending application reduce the rate of data flow. This is done at the Transport layer by regulating the amount of data the source transmits as a group. Flow control can prevent the loss of segments on the network and avoid the need for retransmission.

Transport Layer Protocols

Computers use different types of Transport layers protocols for some reasons.

Question: What is the reason of using different Transport Layer Protocols?

To answer this question we have to list different types of Computer Networks Communications:

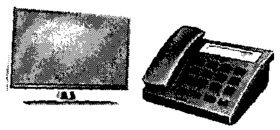
- Web Browsing
- File Sharing
- IP Telephony
- Video Streaming (Conference or online lessons)
- Working with e-mail

Question: For which of the above listed communications do we need reliable transportation and for which of them do we need to have high speed transportation?

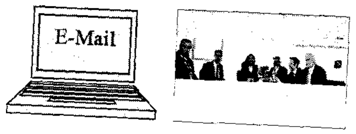
Answer: Web browsing, File sharing and work with e-mail need to have reliable transportation. IP telephony and Video Streaming need to have high speed transportation.

Comparison of needs for Transport Layer Protocols

Pic 1:31 Represents Comparison of Transport Layer Protocols' need



- P Telephony
- Video Streaming



- SMTP/POP
- HTTP

Required Protocol Properties

- Fast
- Low Overhead
- Doesn't require acknowledgements
- Doesn't resend lost data
- Delivers data as it arrives

7. Application
6. Presentation
5. Session
4. Transport
3. Network
2. Data - link
1. Physical

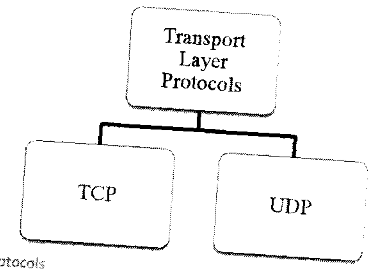
Required Protocol Properties

- Reliable
- Acknowledge data
- Resend lost data
- Delivers data in sent order

Pic : 31 Needs for different types of protocols in Transport Layer

Transport Layer Protocols

Pic 1:32 Represents two Transport Layer Protocols



Pic 1: 311 Transport Layer Protocols

TCP – Transmission Control Protocol

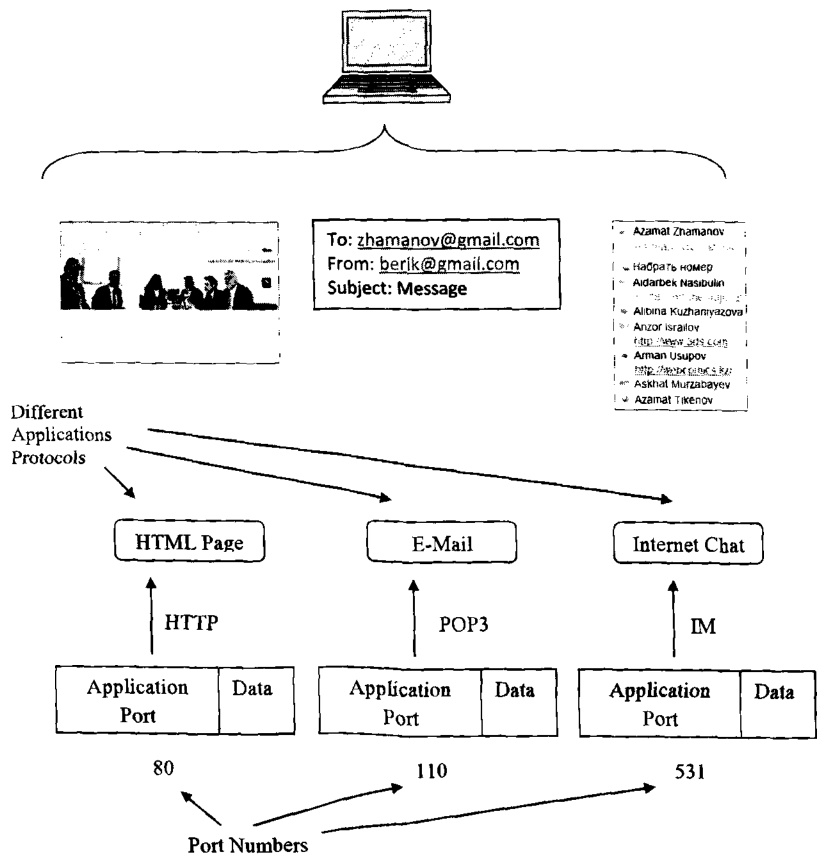
TCP is reliable protocol used in: Web browsing, E-mail and in File Transferring.

UDP – User Datagram Protocol

UDP is unreliable and fast protocol used in: Video Conference and IP Telephony.

Identifying Conversations

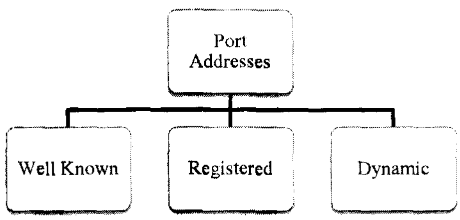
To identify different conversations, Transport Layer uses Port Addresses. Pic 1:33 shows process of identifying conversations in Transport Layer.



Pic 1: 33 Identifying Conversations in Transport Layer

Port Addresses

Pic 1:34 Shows structure of Port Addressing



Pic 1: 34 Port Addresses

Well Known Ports (Numbers 0 to 1023)

Are ports are served for services and applications.
They are commonly used for applications such as HTTP (web server) POP3/SMTP (e-mail server) and Telnet. Pic 1:35 Shows well known port's addresses usage.

Pic 1: 35 Well known ports

Registered Ports (Numbers 1024 to 49151)

Registered Ports are assigned to user processes or applications.

These processes are primarily individual applications that a user has chosen to install rather than common applications that would receive a Well Known Port.

When not used for a server resource, these ports may also be used dynamically selected by a client as its source port. Pic 1:36 Shows registered port's usage.

Pic 1: 36 Registered port's usage

Dynamic or Private Ports (Numbers 49152 to 65535)

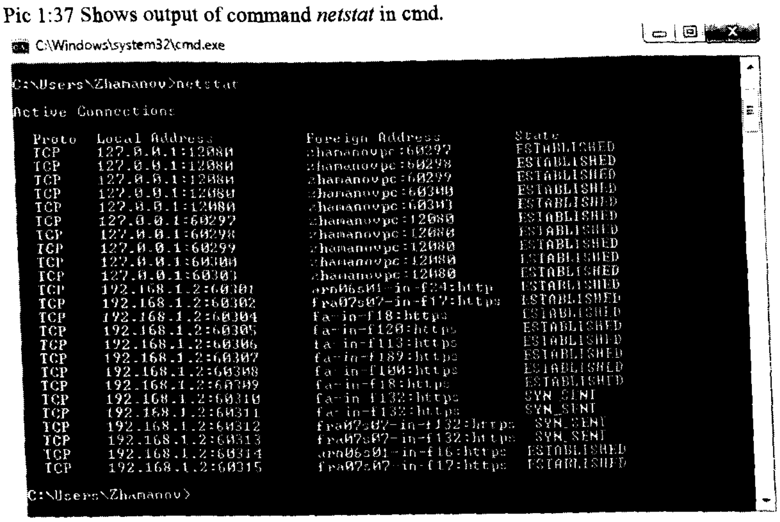
Also known as Ephemeral Ports, these are usually assigned dynamically to client applications when initiating a connection.

It is not very common for a client to connect to a service using a Dynamic or Private Port (although some peer-to-peer file sharing programs do).

NETSTAT is an important network utility that can be used to verify current connections

Example of Netstat command in cmd:

Pic 1:37 Shows output of command *netstat* in cmd.

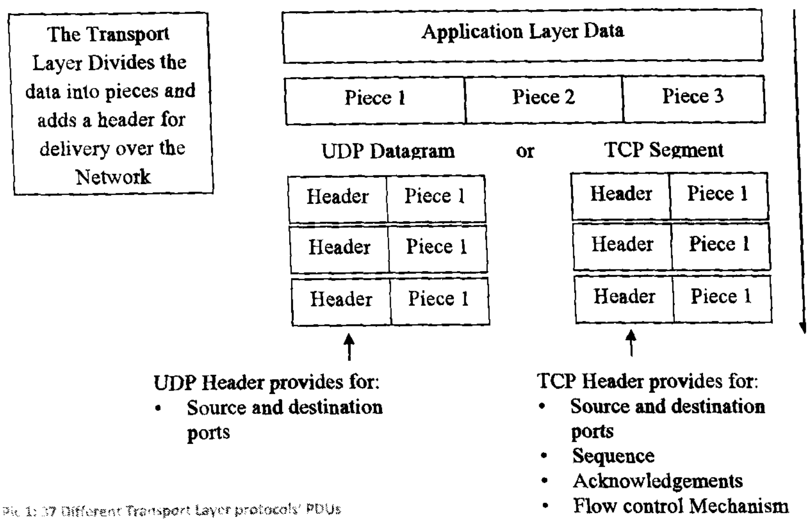


```
C:\Windows\system32\cmd.exe

C:\Users\Zhamanov>netstat

Active Connections

  Proto  Local Address          Foreign Address              State
  TCP    127.0.0.1:12080        zhamanovpc:60297             ESTABLISHED
  TCP    127.0.0.1:12080        zhamanovpc:60298             ESTABLISHED
  TCP    127.0.0.1:12080        zhamanovpc:60299             ESTABLISHED
  TCP    127.0.0.1:12080        zhamanovpc:60300             ESTABLISHED
  TCP    127.0.0.1:12080        zhamanovpc:60303             ESTABLISHED
  TCP    127.0.0.1:60297        zhamanovpc:12080             ESTABLISHED
  TCP    127.0.0.1:60298        zhamanovpc:12080             ESTABLISHED
  TCP    127.0.0.1:60299        zhamanovpc:12080             ESTABLISHED
  TCP    127.0.0.1:60300        zhamanovpc:12080             ESTABLISHED
  TCP    127.0.0.1:60303        zhamanovpc:12080             ESTABLISHED
  TCP    192.168.1.2:60301      arn06s01-in-f24:http         ESTABLISHED
  TCP    192.168.1.2:60302      fra07s07-in-f17:https        ESTABLISHED
  TCP    192.168.1.2:60304      fa-in-f18:https              ESTABLISHED
  TCP    192.168.1.2:60305      fa-in-f120:https             ESTABLISHED
  TCP    192.168.1.2:60306      fa-in-f113:https             ESTABLISHED
  TCP    192.168.1.2:60307      fa-in-f189:https             ESTABLISHED
  TCP    192.168.1.2:60308      fa-in-f100:https             ESTABLISHED
  TCP    192.168.1.2:60309      fa-in-f18:https              ESTABLISHED
  TCP    192.168.1.2:60310      fa-in-f132:https             SYN_SENT
  TCP    192.168.1.2:60311      fa-in-f132:https             SYN_SENT
  TCP    192.168.1.2:60312      fra07s07-in-f132:https       SYN_SENT
  TCP    192.168.1.2:60313      fra07s07-in-f132:https       SYN_SENT
  TCP    192.168.1.2:60314      arn06s01-in-f16:https        ESTABLISHED
  TCP    192.168.1.2:60315      fra07s07-in-f17:https        ESTABLISHED

C:\Users\Zhamanov>
```

Pic 1: 37 Output of *netstat* command in cmd

TCP and UDP Handle Segmentation Differently

Pic 1:38 Shows how different transport layer protocols work.



Pic 1: 37 Different Transport Layer protocols' PDUs

TCP Header

Table 1:1 Shows structure of TCP Header

Bit (0) Bit(15)	Bit(16) Bit(31)
Source Port(16)	Destination Port(16)
Sequence Number (32)	
Acknowledgement Number (32)	
Header Length(4) Reserved(6) Code Bits(6)	Window(16)
Checksum(16)	Urgent(16)
Options(0 or 32 if any)	
Application Layer Data (Variable size)	

Table 1:1 TCP Header

Source Port – Defines from which port data is transferred
Destination Port – Defines to which port data will be delivered
Sequence Number–Defines order of Segment
Acknowledgement Number – Defines next expected bit sequence
Header Length – Defines Header length in bytes
Reserved–Reserved
Code Bits–Used in session management and in the treatment of segments
Window – Window size defines number of bits before sending acknowledgement
Checksum – Used for error checking of Header and Data
Urgent – Used for defining that this Segment has to be sent urgently

UDP Header

Table 1:2 Shows structure of UDP Header

Bit (0) Bit(15)	Bit(16) Bit(31)
Source Port(16)	Destination Port(16)
Length(16)	Checksum(16)
Application Layer Data (Variable size)	

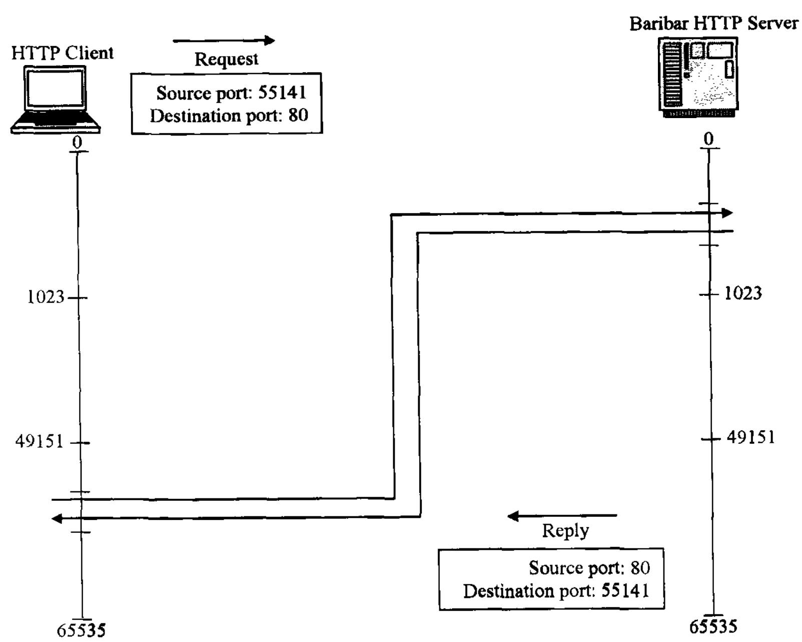
Table 1: 12 UDP Header

Source Port – Defines from which port data is transferred
Destination Port – Defines to which port data will be delivered
Length – Defines length of Datagram
Checksum – Specifies check
Application Layer Data - Data

TCP in Process

In this example Client wants to open home page of "www.baribar.kz" web server. For this purpose client has to send segment to port number 80, because 80s port is used by HTTP protocol only. Now we know the destination port number and we have to learn what will be source port number. Source port number is chosen randomly by computer from range of "Dynamic ports" or can also be chosen from "Registered port" number if they are not used by registered application.

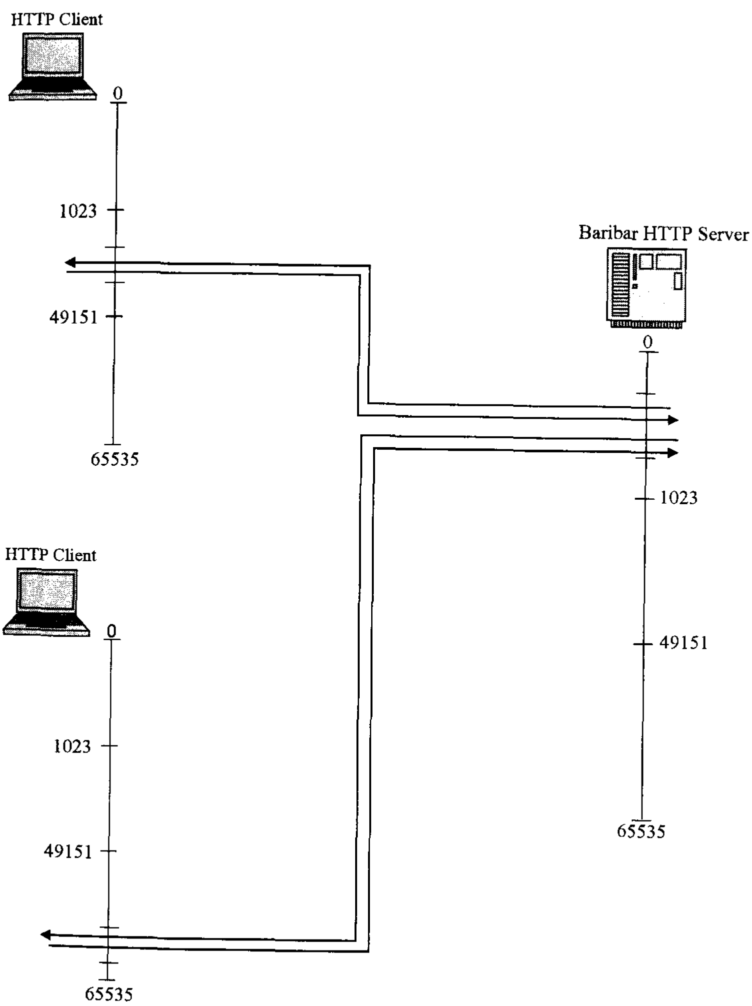
Pic 1:38 Shows TCP in process.



Pic 1: 38 TCP in process

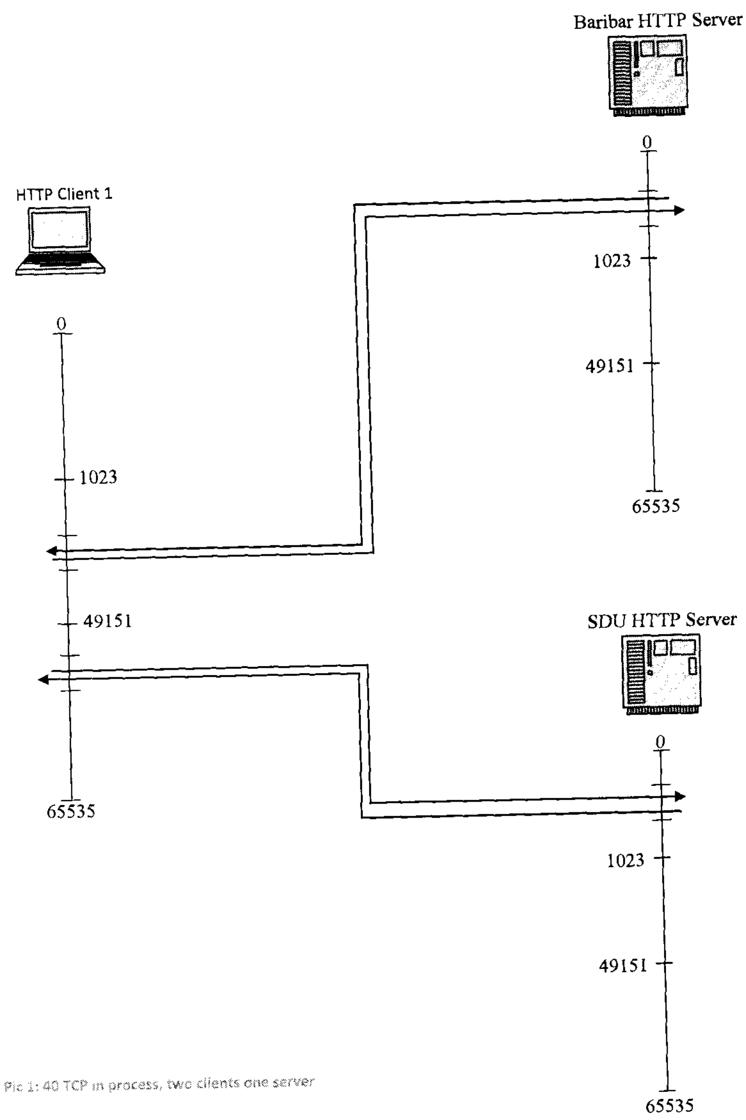
One more example of port usage:

Pic 1:39 Shows example of two clients that are making request to one server simultaneously.



Pic 1: 39 TCP in process, one server two clients

Pic 1:40 Shows example of communication single client to two web servers:



Pic 1: 40 TCP in process, two clients one server

TCP Connection Establishment and Termination

When we want to speak with friend, firstly we have to make establishment of our conversation by using handshake

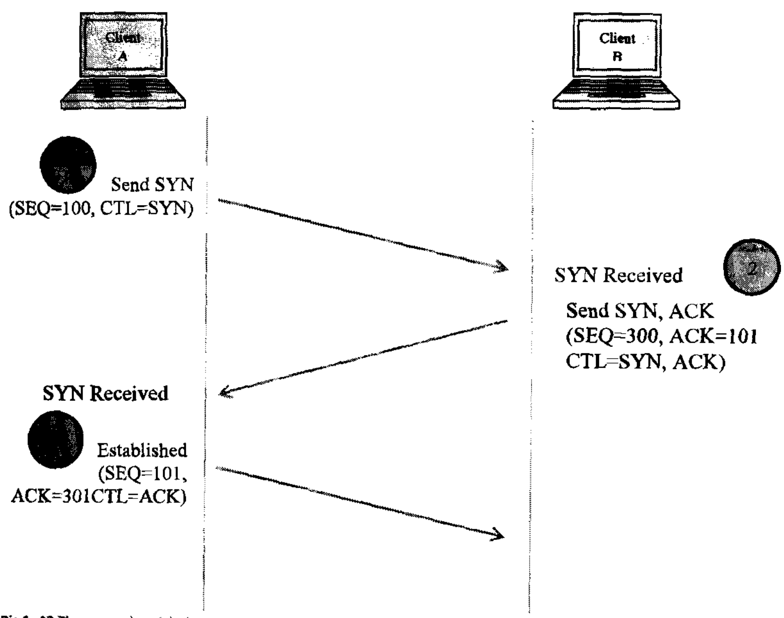
Pic 1: 41 Handshake representation

Pic 1:41 Represents handshake

TCP like people also makes establishment of connection by using handshake, but in three ways.

Three way handshake

Pic 1:42 Represents three way handshake in TCP protocol.



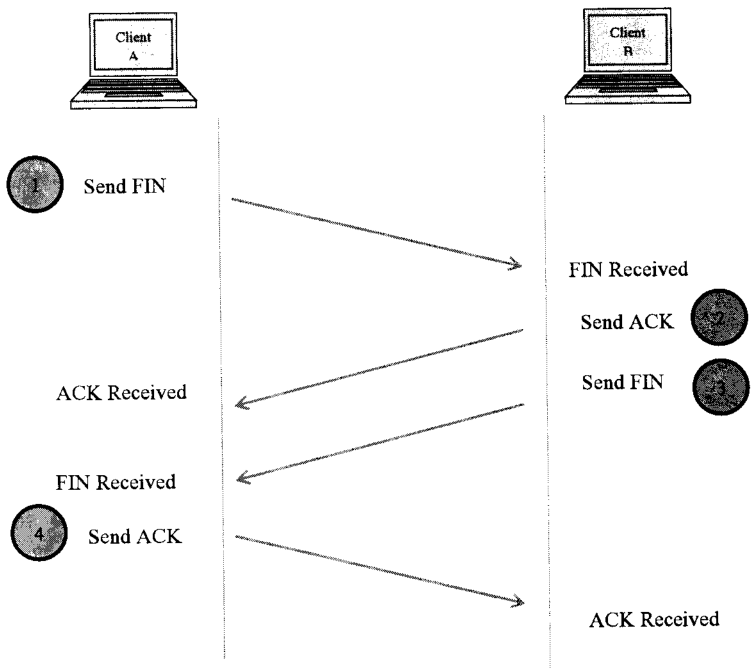
Pic 1: 42 Three way handshake

When people want to finish conversation they usually say "good-bye"

TCP like People also makes signal when it finishes a dialog

Session Termination (4 steps)

Pic 1:43 Shows termination of session in TCP protocol.

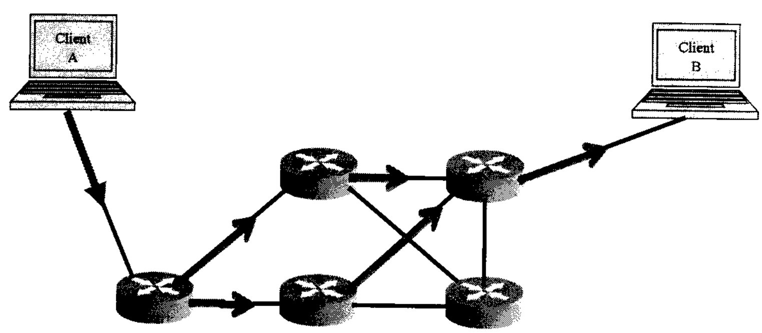


Pic 1:43 Session termination process

Re-ordering segments

Different segments may take different routes.

Pic 1:44 Shows re-ordering segments in process.



Segment 1	Segment 1	Segment 1
Segment 2	Segment 2	Segment 2
Segment 3	Segment 6	Segment 3
Segment 4	Segment 4	Segment 4
Segment 5	Segment 5	Segment 5
Segment 6	Segment 3	Segment 6

Segments traveling by different routes

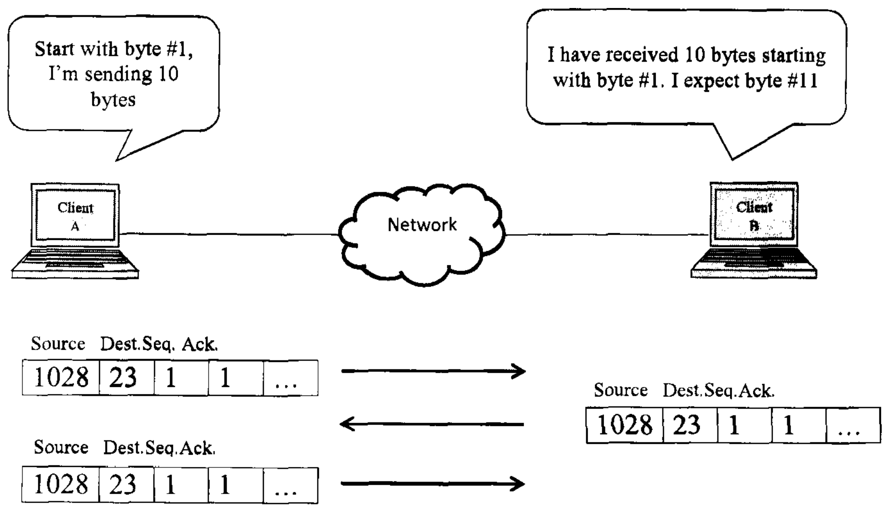
TCP re-orders the segments to original order

Pic 1: 44 Re-ordering segment in TCP protocol

Acknowledgements

Computers often sends acknowledgement to each other, to confirm that they have received data.

Pic 1:45 Shows Acknowledgment service of Transport Layer.



Pic 1: 45 Acknowledgement service of Transport Layer

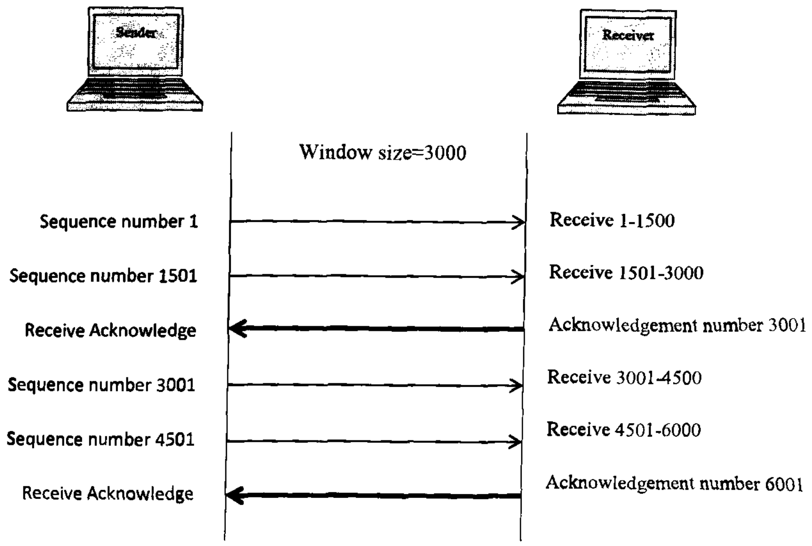
Flow Control Mechanism

Flow control assists the reliability of TCP transmission by adjusting the effective rate of data flow between the two services in the session. When the source is informed that the specified amount of data in the segments is received, it can continue to send more data for this session.

This Window Size field in the TCP header specifies the amount of data that can be transmitted before an acknowledgement must be received. The initial window size is determined during the session startup via the three-way handshake.

Example of Flow Control Mechanism:

Pic 1:46 Shows Flow control mechanism in process without collisions.

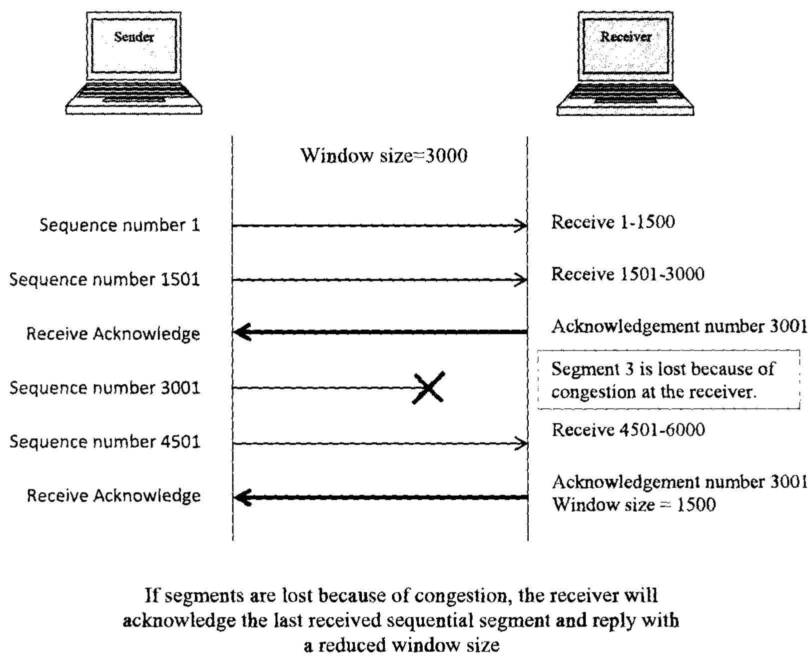


The **windows size** determines the number of bytes sent before an acknowledgement is expected
The **acknowledgement number** is the number of the next expected byte.

Pic 1: 46 Flow control mechanism without collisions

Example of Flow Control Mechanism with Problem:

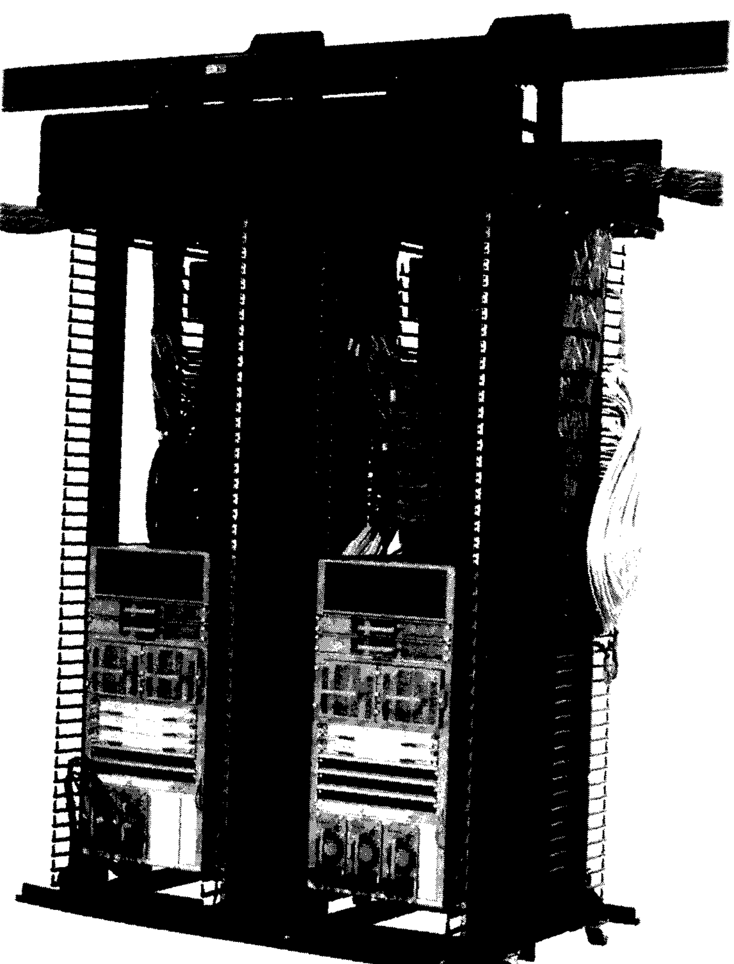
Pic 1:47 Shows Flow control mechanism in process with collisions.



Pic 1: 47 Flow control mechanism with collisions

Chapter 4

OSI Network Layer



Upon Completion of this chapter, you'll be able to:

- Identify the role of the Network layer as it describes communication from one end device to another end device.
- Examine the most common Network layer protocol, Internet Protocol (IP), and its features for providing connectionless and best-effort service.
- Understand the principles used to guide the division, or grouping, of devices into networks.
- Understand the hierarchical addressing of devices and how this allows communication between networks.
- Understand the fundamentals of routes, next-hop addresses, and packet forwarding to a destination network.

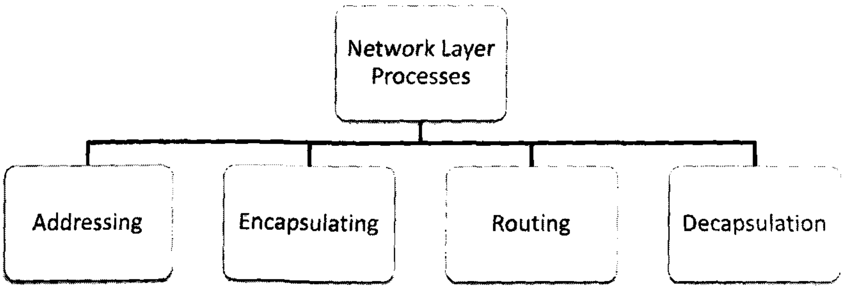
Introduction to OSI Network Layer

Transport Layer Provides connection between applications.
Network Layer Provides connection between Networks, by using IP addresses.

PDU of Network Layer is called Packet.

Four Basic Processes of Network Layer

Pic 1:48 Shows four basic processes of Network Layer



Pic 1: 48 Four basic processes of Network Layer

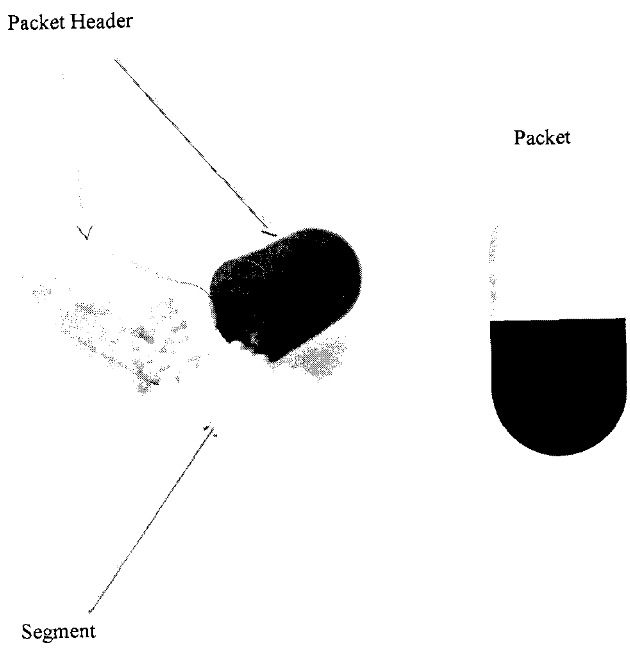
Addressing

First, the Network layer must provide a mechanism for addressing these end devices. If individual pieces of data are to be directed to an end device, that device must have a unique address. In an IPv4 network, when this address is added to a device, the device is then referred to as a host.

Encapsulation

Encapsulation is a process of preparing data before being transmitted to the media.

Pic 1:49 Shows encapsulation in Network Layer.



Pic 1: 49 Encapsulation in Network Layer

After the Network layer completes its encapsulation process, the packet is sent down to the Data Link layer to be prepared for transportation over the media.

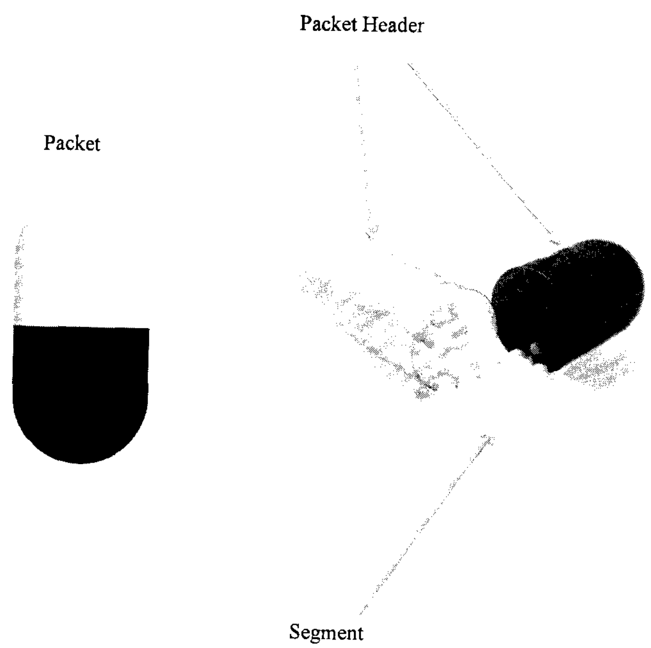
Routing

Giving path for destination network

Decapsulation

Preparing data for delivery to application layer

Pic 1:50 Shows Decapsulation process in Network Layer.

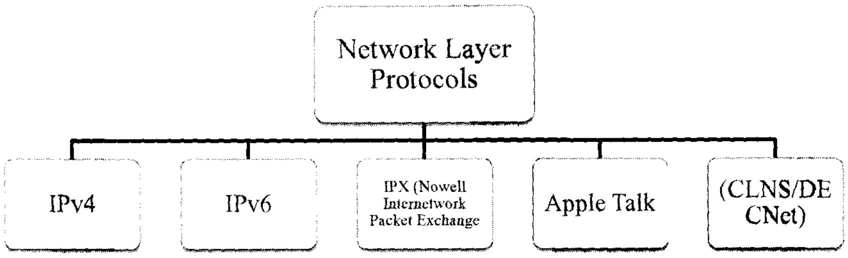


Pic 1: 50 Decapsulation in Network Layer

When data is received by network layer, network layer will delete unnecessary parts of packet called packet header and after what will deliver segment to the transport layer.

Network Layer Protocols

Pic 1:51 Shows different Network Layer protocols



Pic 1: 51 Network Layer Protocols

IPv4 – Internet Protocol Version 4

Is one of the famous Network Layer Protocols in modern computer network structure.

IPv6 – Internet Protocol Version 6

Soon is going to be one of the famous Network Layer Protocols.

IPX - Internetwork Packet Exchange

The IPX/SPXM protocol stack is supported by Novell's NetWare network operating system. Because of Netware's popularity through the late 1980s into the middle 1990s, IPX became a popular internetworking protocol. Novell derived IPX from Xerox Network Systems' IDP protocol.

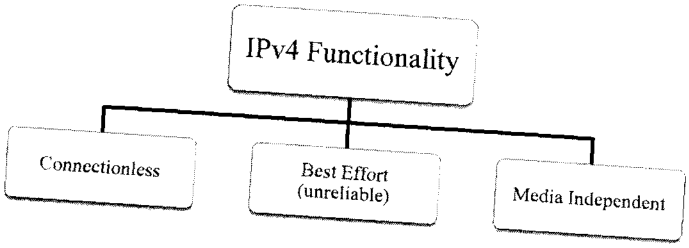
Apple Talk

Apple Talk is a proprietary suite of protocols developed by Apple Inc.

In this chapter we will describe in details IPv4 and review IPv6

IPv4 Four Basic Characteristics

Pic 1:52 shows IPv4 functionality.



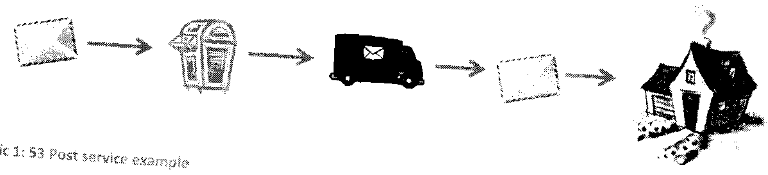
Pic 1: 52 IPv4 functionality

Connectionless

Connectionless means that IPv4 protocol doesn't create session before before packaging.

Example of Post office services:

Pic 1:53 Shows example of Post service.

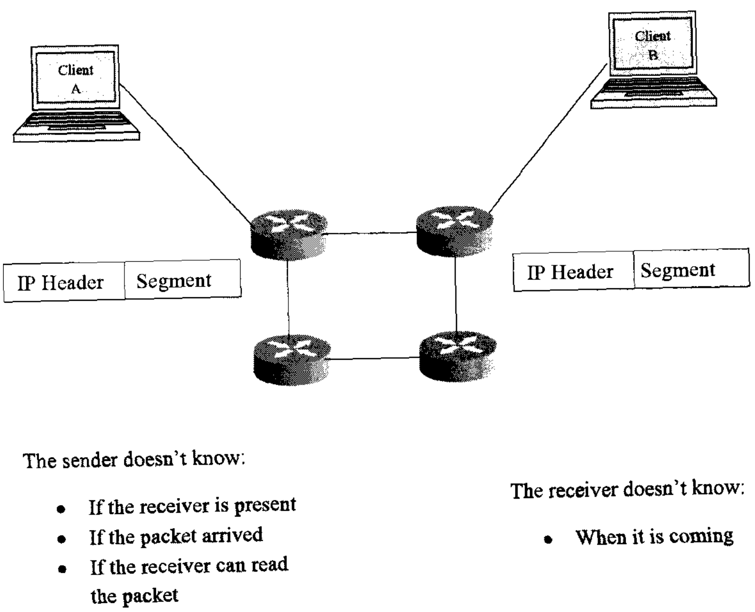


Pic 1: 53 Post service example

When we send message to someone, we are not sure, that at moment when postman delivers the message, the receiver will be at home.

Example of connectionless in computer networks:

Pic 1:54 Shows connectionless process in computer networks.

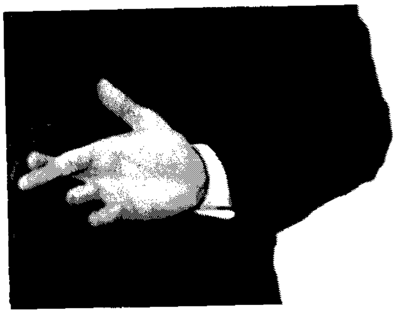


Pic 1: 54 Connectionless communication example

Best Effort

In other words ***Unreliable***

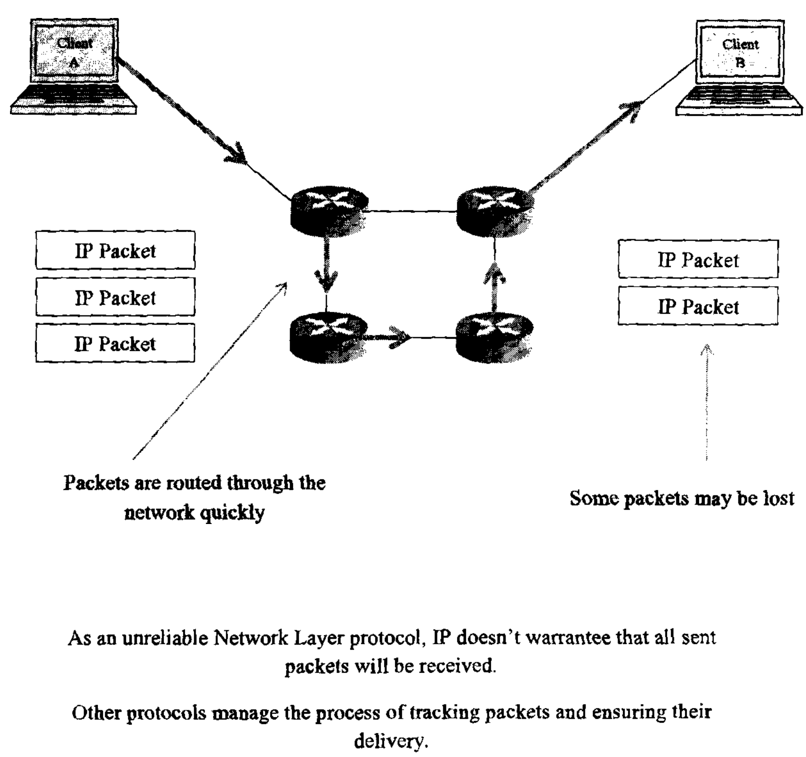
Pic 1:55 shows unreliable symbol



Pic 1: 55 symbol, that defining unreliability of person

Best effort example in computer networks:

Pic 1:56 Shows best effort example in computer networks.



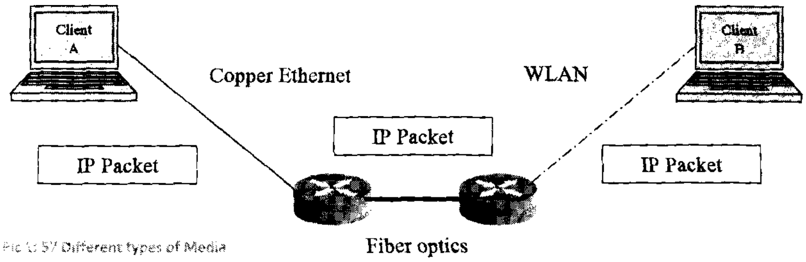
Pic 1: 56 Example of Best effort

Media Independence

In different types of media, IP Packet doesn't change structure, but data-link frame does.

Example of IP Packet in different media types:

Pic 1:57 Shows different types of media.



Pic 1:57 Different types of Media

Different types of media have different maximum amount of bytes for single packet that can be transferred through that media. Amount of maximum bytes for single packet is called **Maximum Transmission Unit – MTU**.

Table 1:1 shows different types of media.

MTU Table for popular media types:

Media type	MTU
802.3	1492 bytes
802.11	2272 bytes
802.5 Token ring	4464 bytes
FDDI	4500 bytes

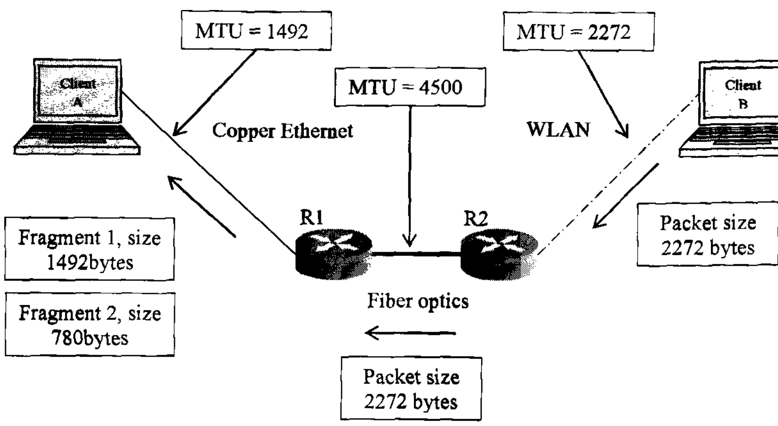
Table 1:1 Different types of media

If a packet switches between different medias with different MTU (from higher to lower), packet must be splitted into **Fragments**.

Process of splitting packets is called **Fragmentation**.

Example of fragmentation process:

Pic 1:58 **Shows fragmentation in process.**

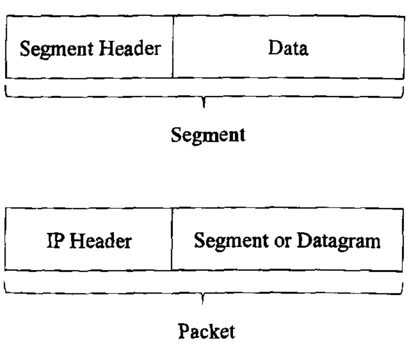


Pic 1: 58 Fragmentation in process

In this example, client B sends packet to client A. Router R2 receives packet and resends it through fiber optics media without fragmentation, because MTU of fiber optics is bigger than MTU of WLAN. R1 receives packet and makes fragmentation, because MTU of Copper Ethernet is smaller than MTU of Fiber optics. Client A will receive **two fragments** and will store them in cash memory, after what client A will combine two fragments into one packet.

Network Layer's PDU

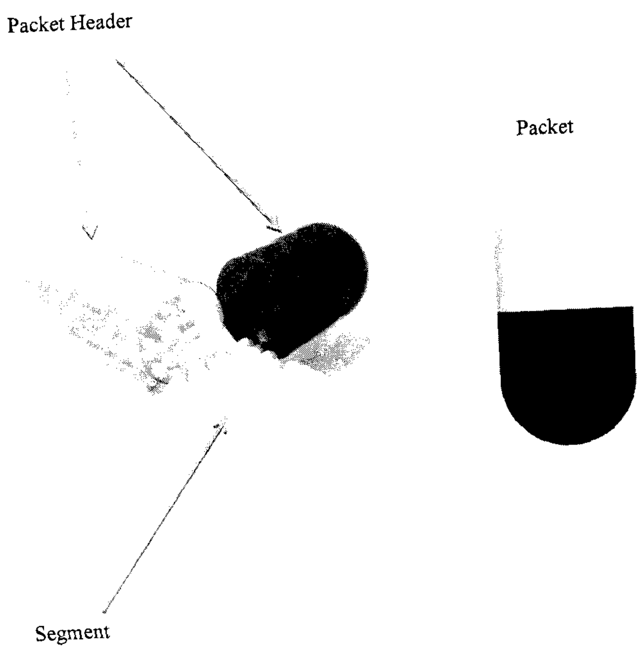
Network Layer's PDU is called **Packet**. Pic 1:59 Shows Network Layer's PDU.



Pic 1: 59 Network Layer's PDU

Another representation of Network Layer's PDU:

Pic 1:60 Shows example of Network Layer's PDU.



Pic 1: 60 Example of Network Layer's PDU

Packet Header in Details

Table 1:2 Shows Packet Headers in Details.

<table>
<tr><td colspan="2">Byte 1</td><td>Byte 2</td><td colspan="2">Byte 3</td><td colspan="2">Byte 4</td></tr>
<tr><td>Ver.</td><td>IHL</td><td>Type of Service</td><td colspan="4">Packet Length</td></tr>
<tr><td colspan="3">Identification</td><td>Flag</td><td colspan="3">Fragment Offset</td></tr>
<tr><td colspan="2">Time to Live</td><td>Protocol</td><td colspan="4">Header Checksum</td></tr>
<tr><td colspan="7">Source IP Address</td></tr>
<tr><td colspan="7">Destination IP Address</td></tr>
<tr><td colspan="6">Options</td><td>Padding</td></tr>
<tr><td colspan="7">Segment (Data)</td></tr>
</table>

Table 1:2 Packet Header in details

Ver.- Defines Version of Network Layer Protocol
IHL – Defines size of Packet Header, needed because packet size can be changed
Type of Service – Specifies Priority of Packet, used for QoS
Packet Length – Defines Packet Header + Data Length. Minimum size is 20 bytes = 20 bytes of Packet Header + 0 Bytes of Data. Maximum size of Packet is 65,535 bytes.
Identification – Uniquely identifies fragments of an original IP Packet
Flag – Flag consists of two sub-flags:

1. **MF** – More Fragment: 1bit
    a. If MF statement is 0, it means that this is last fragment of packet. If statement is 1, it means that there is one more fragment coming.
2. **DF** – Don't Fragment: 1bit
    a. If DF statement is 0, it means that packet can be fragmented. If statement is 1, it means fragment can't be fragmented

Fragment Offset – Sequence number of Fragment
Time to Live – Maximum Number of Hops that packet can do
Protocol – Defines upper layer protocols. Example: TCP or UDP
Header Checksum – Responsible for check header state at each hop
Source IP Address – Sender's IP Address
Destination IP Address – Receiver's IP Address
Options – Some options if exist

Example of Packet Header:
Table 1:3 Shows example of Packet Header

Byte 1		Byte 2	Byte 3	Byte 4
Ver=4	IHL=5	Type of Service	Packet Length = 472	
Identification=111			Flag=0	Fragment Offset=0
Time to Live=123		Protocol=6	Header Checksum	
192.168.1.1				
10.20.105.8				
Options				
Data				
Data				
Data				

Table 1:3 Example of Packet Header

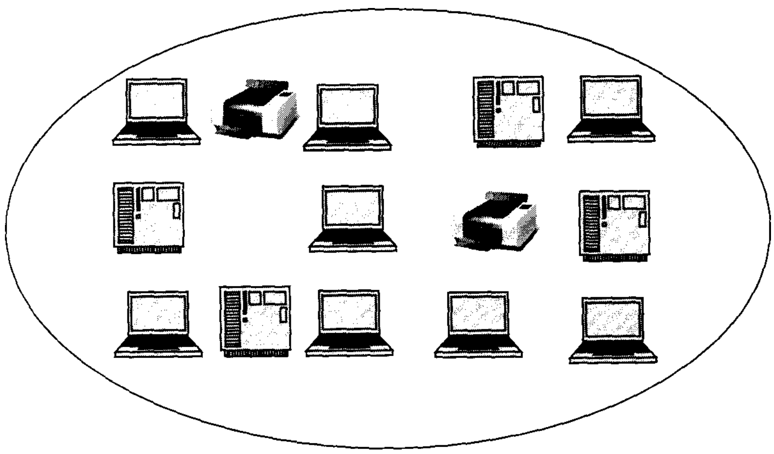
Dividing Network into Sub-networks

Question: Why do we need to divide networks into sub-networks?

Answer: Large networks are difficult to manage; Small networks are easy to Manage.

Large Network

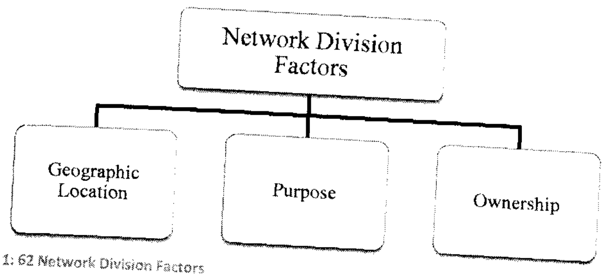
Pic 1:61 Represents Large network



Pic 1: 61 Large network

Network Division Factors

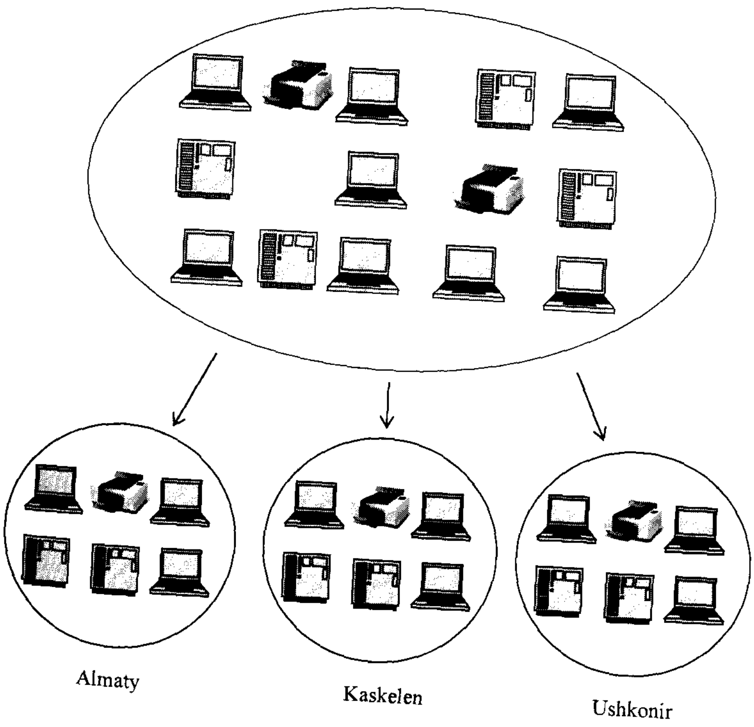
Pic 1:62 Shows network division factors



Pic 1: 62 Network Division Factors

Division by Geographical Location

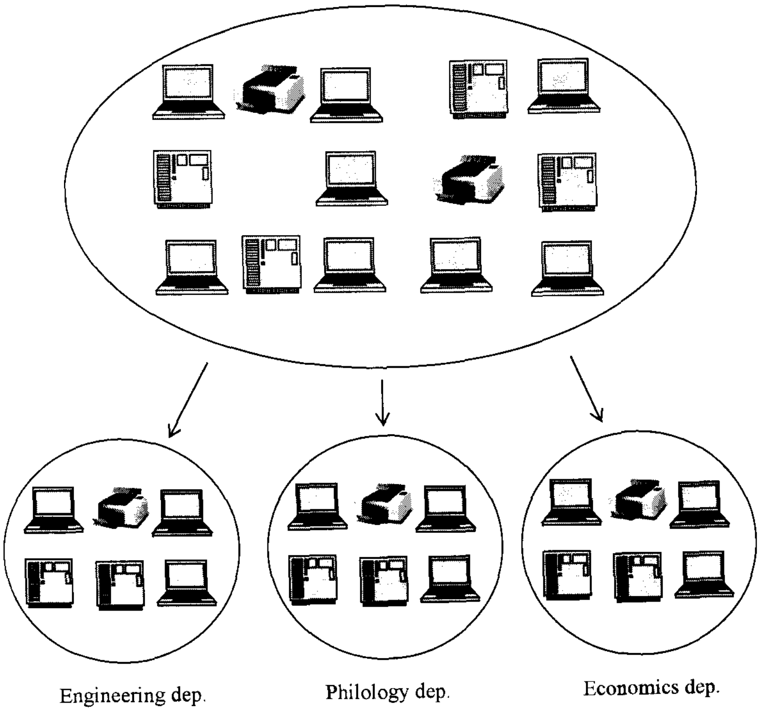
Pic 1:63 Shows division by Geographical Location



Pic 1: 63 Division by geographical location

Division by Purpose

Pic 1:64 Shows division by purpose

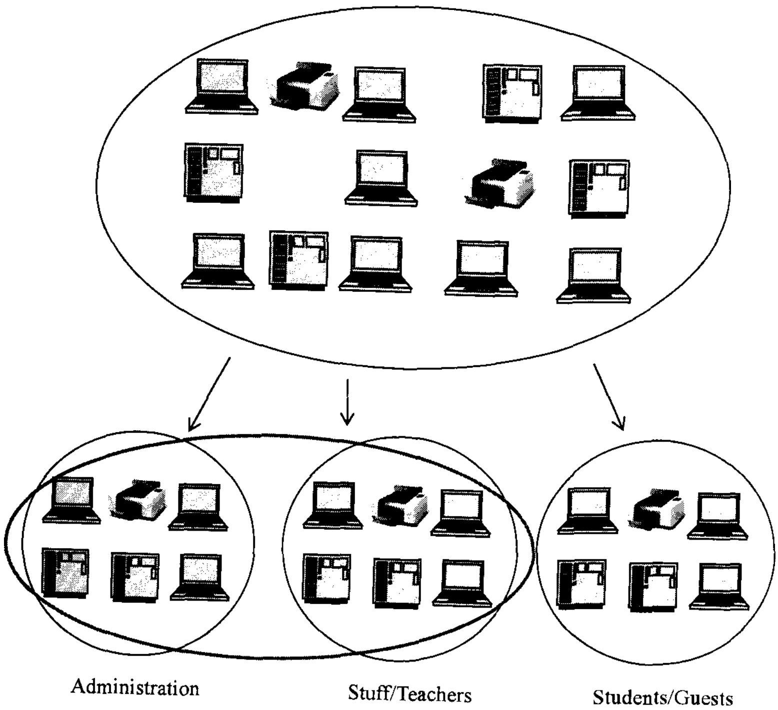


Pic 1: 64 Division by purpose

In division by purpose, computers of one department can be located in different places but they will be placed in one logical network.

Division by Ownership

Pic 1:65 Shows division by ownership.



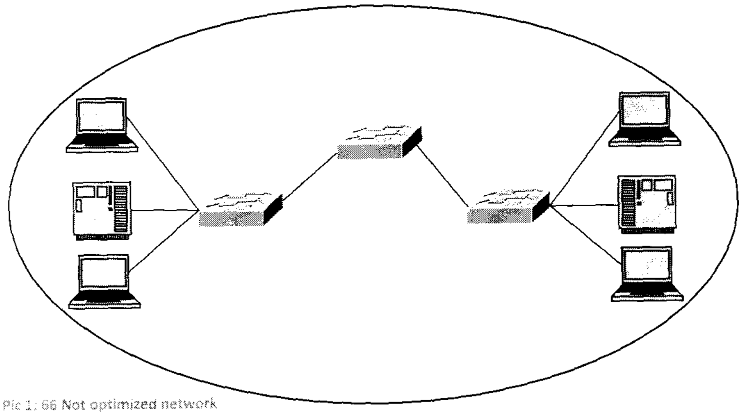
Pic 1: 65 Division by ownership

Division by ownership makes difference in rights between sub-networks. In this example Administration and Stuff/Teachers subdivisions have rights for unlimited internet, but Students/Guests subdivision has limitations.

Optimization of Network

Optimization of network - is changing structure of network topology to improve speed of connection. Pic 1:66 Shows not optimized network.

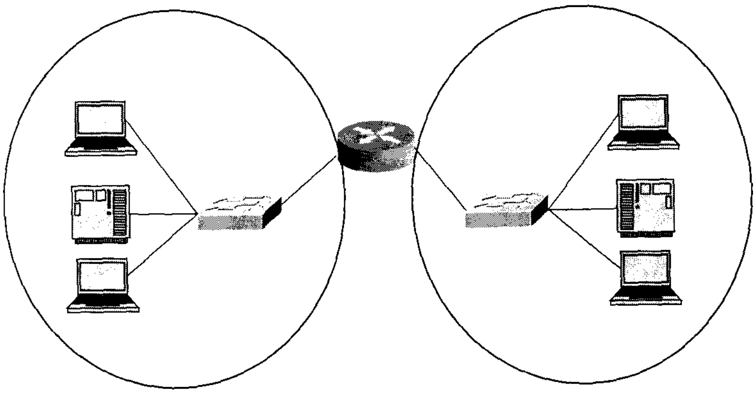
Example of not optimized network:



Pic 1: 66 Not optimized network

Example of optimized network:

Pic 1:67 Shows example of optimized network.



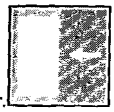
Pic 1: 67 Optimized network

In this example we have separated network into two sub-networks by using Layer 3 device (router). Each interface of router is making single broadcast domain.

Common Issues (problems) with large networks are:

- Performance degradation
- Security Issues
- Address Management

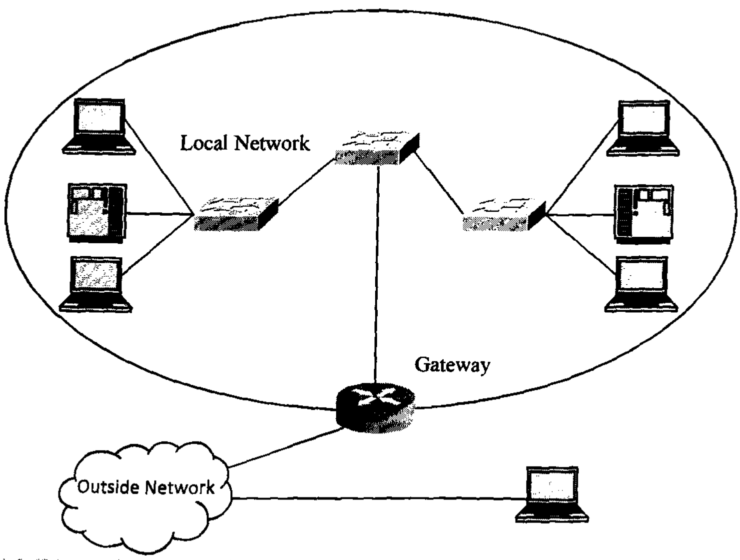
Question: If you want to leave the room, what do you have to do?

Answer: You have to go and find out the exit door. 

Question: When you want to send data outside the network what does your computer have to do?

*Answer: Computer has to find out a door, in computer networks terminology exit door is called **Gateway**.* Pic 1:68 Shows examle of Gateway.

Example of Gateway in Computer Networks:



Pic 1: 68 Gateway from the network

Hosts do not know where to deliver data to devices in a remote network – this is the role of the gateway.

Hierarchic Addressing

When we compose letter we have to write address of receiver like:

Letter to: Kazakhstan, Almaty, Kaskelen, SDU, Engineering Faculty, Zhamanov Azamat

By using this hierarchy postman can easily find out receiver. In computer networks addressing we also have hierarchy which consists of two portions: Network portion and Host portion. Pic 1:69 Shows hierarchical structure of IPv4 address.

Example of Computer Networks hierarchical addressing:

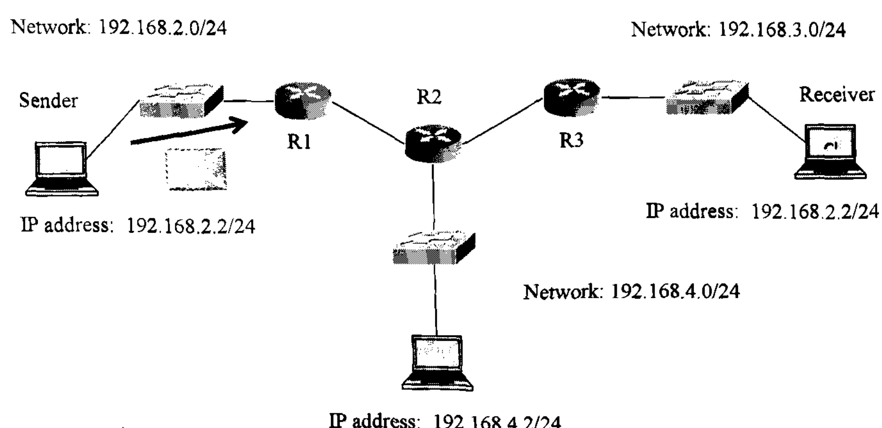
Network Portion			Host Portion
Network Address			Host Address
192	168	15	13

We will speak about IPv4 addressing later in details.

Pic 1: 69 Hierarchical structure of IPv4 address

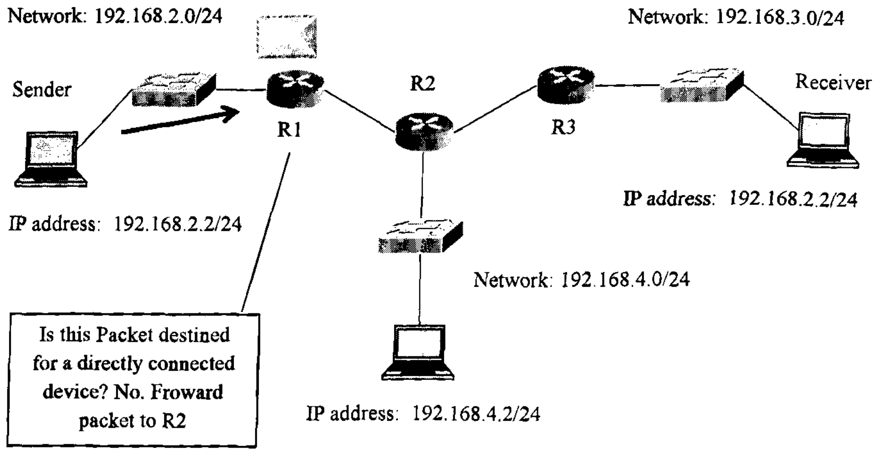
Routing IP packets in process

1st step: In first step Sender prepares packet with destination IP address of Receiver and sends it to local router. Pic 1:70 Shows 1st step of routing example.



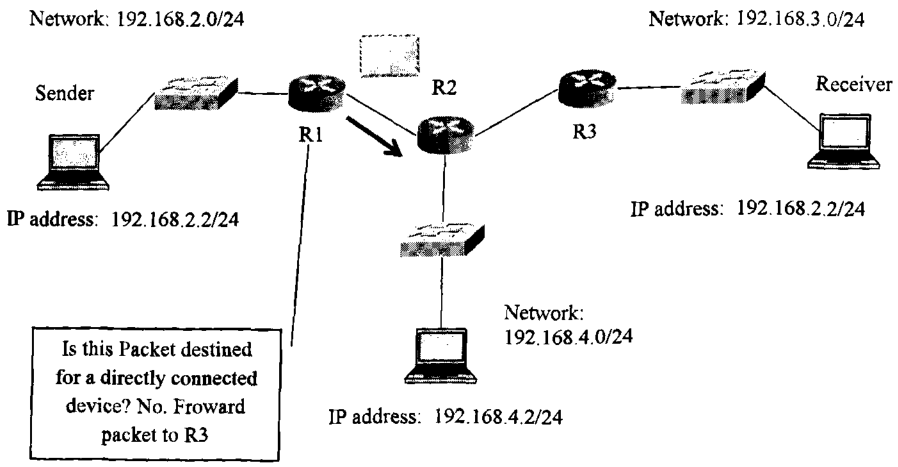
Pic 1: 70 1st step of Routing

2nd step: R1 receives packet and makes and thinks about destination network. *Pic 1:71* Shows 2nd step of routing.



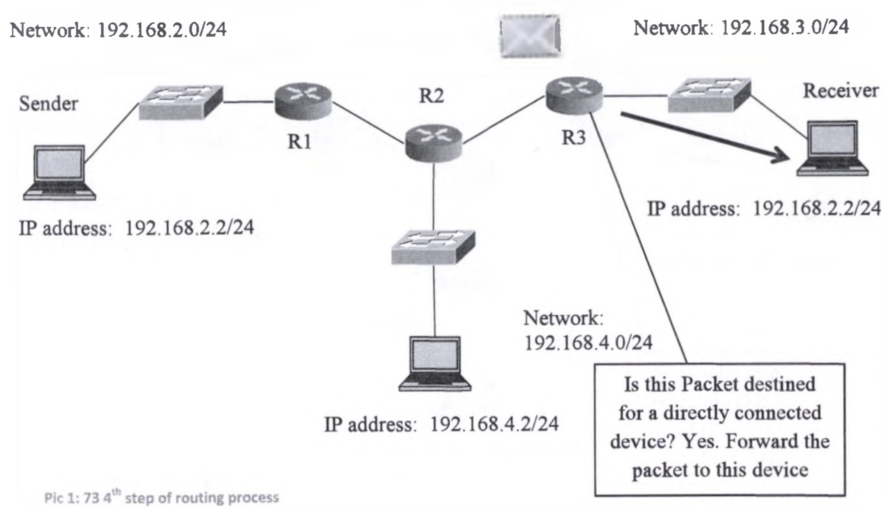
Pic 1: 71 2nd step of routing example

3rd step: R2 receives packet and makes and thinks about destination network. Pic 1:72 Shows 3rd step of Routing process.



Pic 1: 72 3rd step of routing process

4th step: R3 receives packet and makes and thinks about destination network. Pic 1: 73 Shows 4th step of routing process.



Pic 1: 73 4th step of routing process

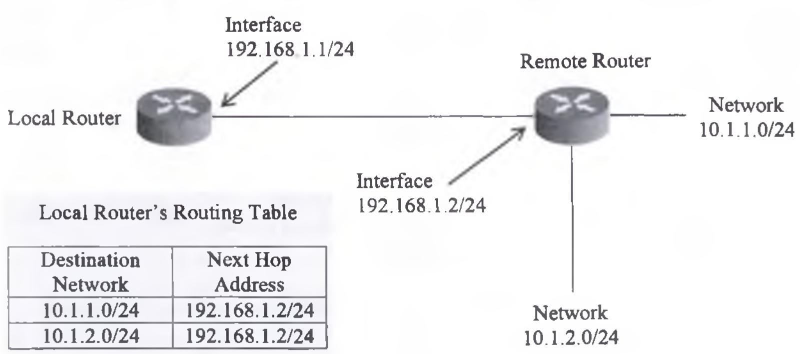
Best Path

Question: How do routers identify best path?

Answer: Routers use routing tables.

Pic 1:74 Shows how routers find best path.

Example of Routing table:



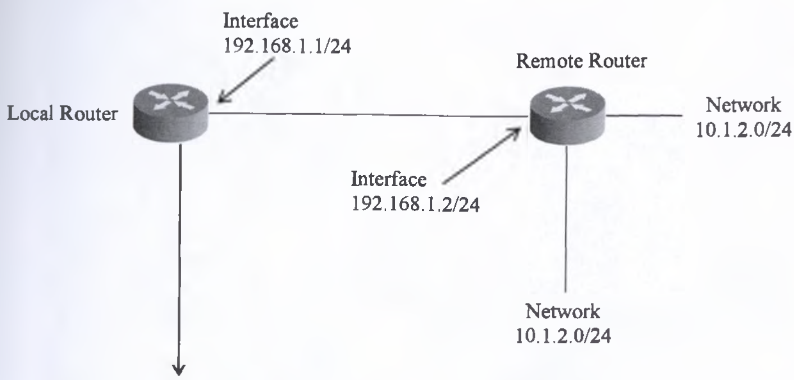
Local Router's Routing Table

Destination Network	Next Hop Address
10.1.1.0/24	192.168.1.2/24
10.1.2.0/24	192.168.1.2/24

Pic 1: 74 Routing table output

Example output from Cisco Router

Pic 1:75 Shows example of CLI output.




```
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/24 is subnetted, 2 subnets
S       10.1.1.0 [1/0] via 192.168.1.2
S       10.1.2.0 [1/0] via 192.168.1.2
C    192.168.1.0/24 is directly connected, Serial0/0/0
```

Pic 1: 75 CLI's routing table output

In Cisco IOS by using command **show ip route**, you can examine routing table.

In this example we have three rows in routing table:

- S 10.1.1.0/24 [1/0] via 192.168.1.2
- S 10.1.2.0/24 [1/0] via 192.168.1.2
- C 192.168.1.0/24 is directly connected

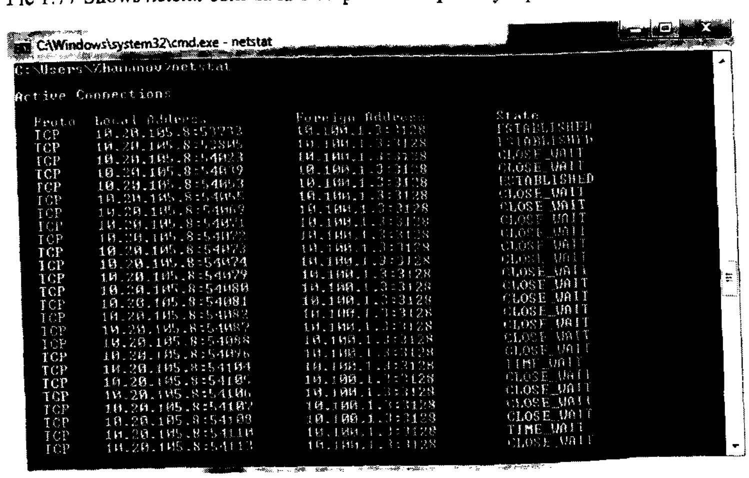
By using this record in routing table router makes decision where to send packet.

Useful Commands:

Pic 1:76 Shows *ipconfig/all* command's output- verifies TCP/IP stack configuration

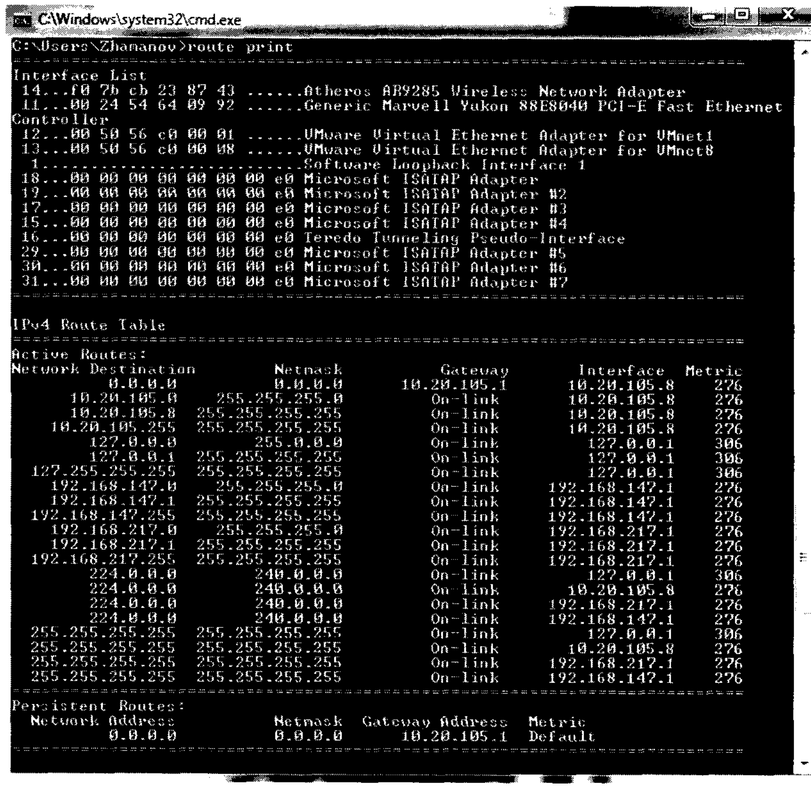
Pic 1: 76 *ipconfig/all* command's output

Pic 1:77 Shows *netstat* command's output - Transport layer protocol's connections



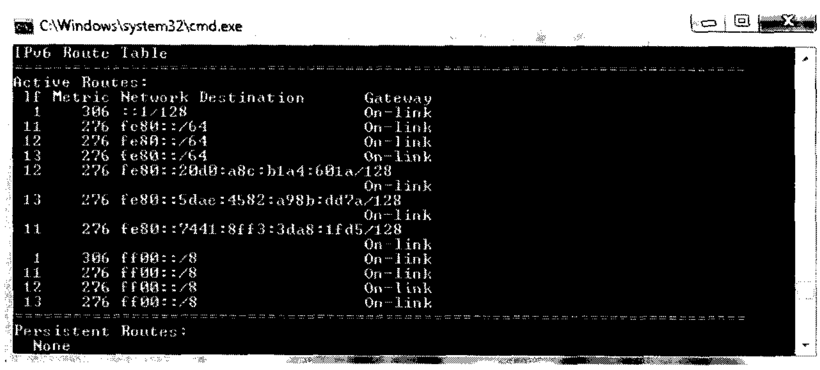
Pic 1: 77 *netstat* command's output

Pic 1:78 Shows *router print* command's output - routing table in computer



```
C:\Windows\system32\cmd.exe
C:\Users\Zhamanov>route print
===========================================================================
Interface List
 14...f0 7b cb 23 87 43 ......Atheros AR9285 Wireless Network Adapter
 11...00 24 54 64 09 92 ......Generic Marvell Yukon 88E8040 PCI-E Fast Ethernet
Controller
 12...00 50 56 c0 00 01 ......VMware Virtual Ethernet Adapter for VMnet1
 13...00 50 56 c0 00 08 ......VMware Virtual Ethernet Adapter for VMnet8
  1...........................Software Loopback Interface 1
 18...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter
 19...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #2
 17...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #3
 15...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #4
 16...00 00 00 00 00 00 00 e0 Teredo Tunneling Pseudo-Interface
 29...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #5
 30...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #6
 31...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #7
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      10.20.105.1     10.20.105.8    276
      10.20.105.0    255.255.255.0         On-link      10.20.105.8    276
      10.20.105.8  255.255.255.255         On-link      10.20.105.8    276
    10.20.105.255  255.255.255.255         On-link      10.20.105.8    276
        127.0.0.0        255.0.0.0         On-link        127.0.0.1    306
        127.0.0.1  255.255.255.255         On-link        127.0.0.1    306
  127.255.255.255  255.255.255.255         On-link        127.0.0.1    306
    192.168.147.0    255.255.255.0         On-link    192.168.147.1    276
    192.168.147.1  255.255.255.255         On-link    192.168.147.1    276
  192.168.147.255  255.255.255.255         On-link    192.168.147.1    276
    192.168.217.0    255.255.255.0         On-link    192.168.217.1    276
    192.168.217.1  255.255.255.255         On-link    192.168.217.1    276
  192.168.217.255  255.255.255.255         On-link    192.168.217.1    276
        224.0.0.0        240.0.0.0         On-link        127.0.0.1    306
        224.0.0.0        240.0.0.0         On-link      10.20.105.8    276
        224.0.0.0        240.0.0.0         On-link    192.168.217.1    276
        224.0.0.0        240.0.0.0         On-link    192.168.147.1    276
  255.255.255.255  255.255.255.255         On-link        127.0.0.1    306
  255.255.255.255  255.255.255.255         On-link      10.20.105.8    276
  255.255.255.255  255.255.255.255         On-link    192.168.217.1    276
  255.255.255.255  255.255.255.255         On-link    192.168.147.1    276
===========================================================================
Persistent Routes:
  Network Address          Netmask  Gateway Address  Metric
          0.0.0.0          0.0.0.0      10.20.105.1  Default
===========================================================================
```

Pic 1: 78 a) *route print* command's output

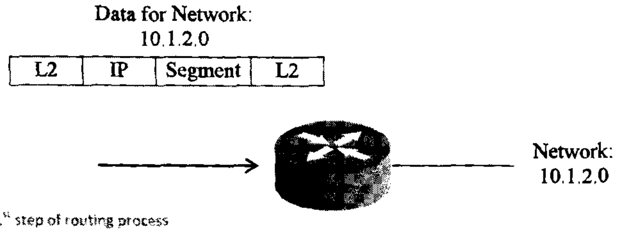


```
C:\Windows\system32\cmd.exe
IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
  1    306 ::1/128                  On-link
 11    276 fe80::/64                On-link
 12    276 fe80::/64                On-link
 13    276 fe80::/64                On-link
 12    276 fe80::20d0:a8c:b1a4:601a/128
                                    On-link
 13    276 fe80::5dae:4582:a98b:dd7a/128
                                    On-link
 11    276 fe80::7441:8ff3:3da8:1fd5/128
                                    On-link
  1    306 ff00::/8                 On-link
 11    276 ff00::/8                 On-link
 12    276 ff00::/8                 On-link
 13    276 ff00::/8                 On-link
===========================================================================
Persistent Routes:
  None
```

Pic 1: 78 b) *route print* command's output

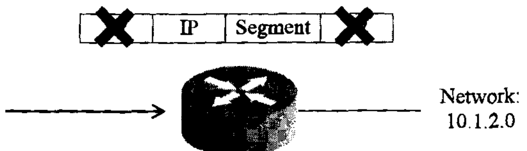
Routing Process in Details

1. Router receives OSI Layer 2's PDU called Frame. In graphic you can see L2s at the left and at the right sides, they define a frame (we will speak about L2 values later). Pic 1:79 Shows 1st step of routing process.



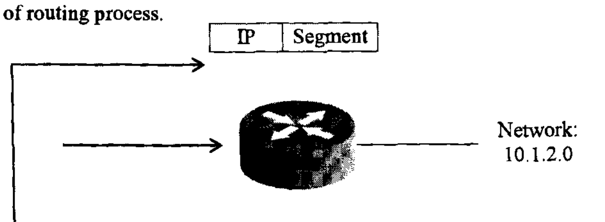
Pic 1: 79 1st step of routing process

2. After receiving a frame, router deletes unnecessary parts, because of router working on OSI Layer 3 (Network Layer). Pic 1:80 Shows 2nd step of routing process.



Pic 1: 80 2nd step of routing process

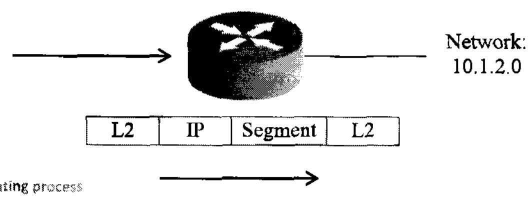
3. After Router examines IP header field to find out Network address. Pic 1:81 Shows 3rd step of routing process.




```
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/24 is subnetted, 1 subnets
C       10.1.2.0 is directly connected, FastEthernet0/1
C    192.168.1.0/24 is directly connected, Serial0/0/0
```

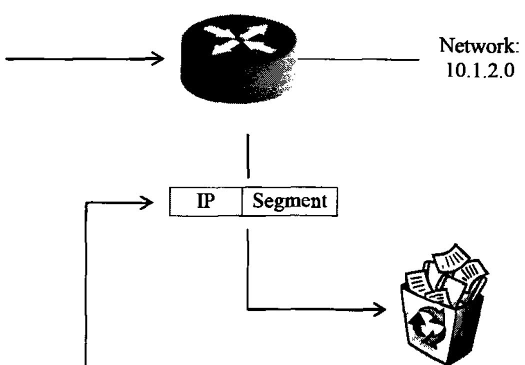
Pic 1: 81 3rd step of routing process

4. Router finds Network address in routing table, and makes encapsulation to OSI Layer 2 (frame). Pic 1:82 Shows 4th step of routing process.



Pic 1: 82 4th step of routing process

If router does not find out Destination Network address in routing table, packet will be discarded. Pic 1:83 Shows case when router did find destination network address in routing table.

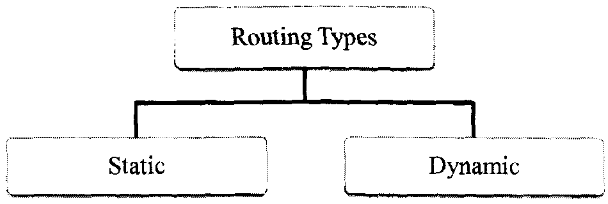



```
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/24 is subnetted, 1 subnets
C       10.1.1.0 is directly connected, FastEthernet0/0
C    192.168.1.0/24 is directly connected, Serial0/0/0
```

Pic 1: 83 Router discarding the packet

Routing Types

Pic 1:84 Shows routing types.

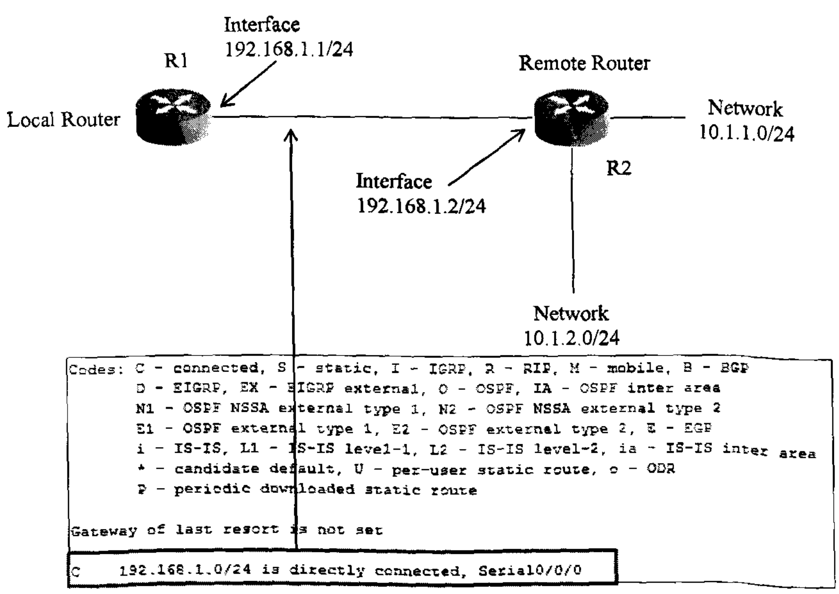


Pic 1: 84 Routing types

Static Routing

In static routing all networks which are not directly connected to the router have to be placed into the routing table **manually**.

Example of static routing: In this example, after configuring router's interfaces. Routers know **only directly connected networks. R1 knows network 192.168.1.0/24, R2 knows networks 192.168.1.0, 10.1.2.0 and 10.1.1.0. Pic 1:85 Shows Static routing example.**



Pic 1: 85 Static routing

We can give information to R1 about networks: 10.1.1.0/24 and 10.1.2.0/24 in two ways, or we may configure static route, or we may configure dynamic route. Pic 1:86 Shows example of static routing configuration of Cisco router

Example of static route configuration:

```
Router(config)#ip route 10.1.1.0 255.255.255.0 192.168.1.2
Router(config)#ip route 10.1.2.0 255.255.255.0 192.168.1.2
```

Pic 1: 86 Commands for static routing configuration

Pic 1:87 Shows examination of routing table.

After these commands have been entered, we can examine R1's routing table again:

```
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/24 is subnetted, 2 subnets
S       10.1.1.0 [1/0] via 192.168.1.2
S       10.1.2.0 [1/0] via 192.168.1.2
C    192.168.1.0/24 is directly connected, Serial0/0/0
```

Pic 1: 87 Shows output of routing table

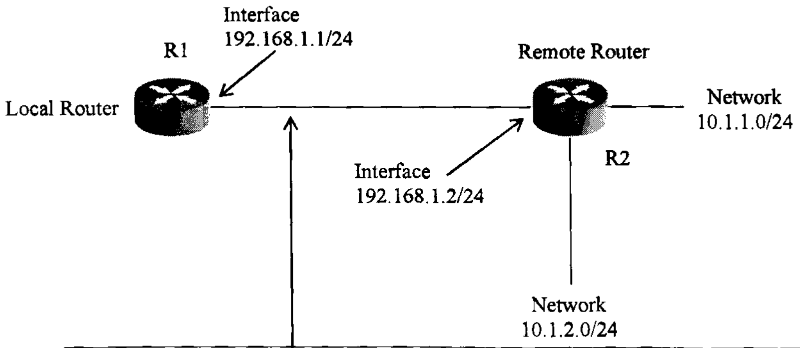
Now R1 knows about networks: 10.1.1.0/24 and 10.1.2.0/24.

Dynamic Routing

As we spoke before, all directly connected networks by default are going to be added into the routing table, all remote networks have to be included into the routing table manually by network administrator or by using dynamic routing protocols (set of rules which share routing information between routers, which are using same routing protocols).

Pic 1:88 **Shows example of Dynamic routing.**

Example of Dynamic Routing: **Same topology as in static routing and same situation, only directly connected network listed in routing table of R1.**




```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    192.168.1.0/24 is directly connected, Serial0/0/0
```

Pic 1: 88 Dynamic Routing

Pic 1:89 **and** Pic 1:90 **Shows Dynamic routing protocol configuration:**

- R1's **dynamic routing configuration:**

```
Router(config)#router ospf 1
Router(config-router)#network 192.168.1.0 0.0.0.255 area 0
```

Pic 1: 89 Dynamic Routing Configuration

- **R2's dynamic routing configuration:**

```
Router(config)#router ospf 1
Router(config-router)#ne
Router(config-router)#network 10.1.2.0 0.0.0.255 area 0
Router(config-router)#network 10.1.1.0 0.0.0.255 area 0
Router(config-router)#network 192.168.1.0 0.0.0.255 area 0
```

Pic 1: 90 Dynamic Routing Configuration

Pic 1:91 Shows Example of Dynamic routing output.

Examining routing table after dynamic routing configurations:

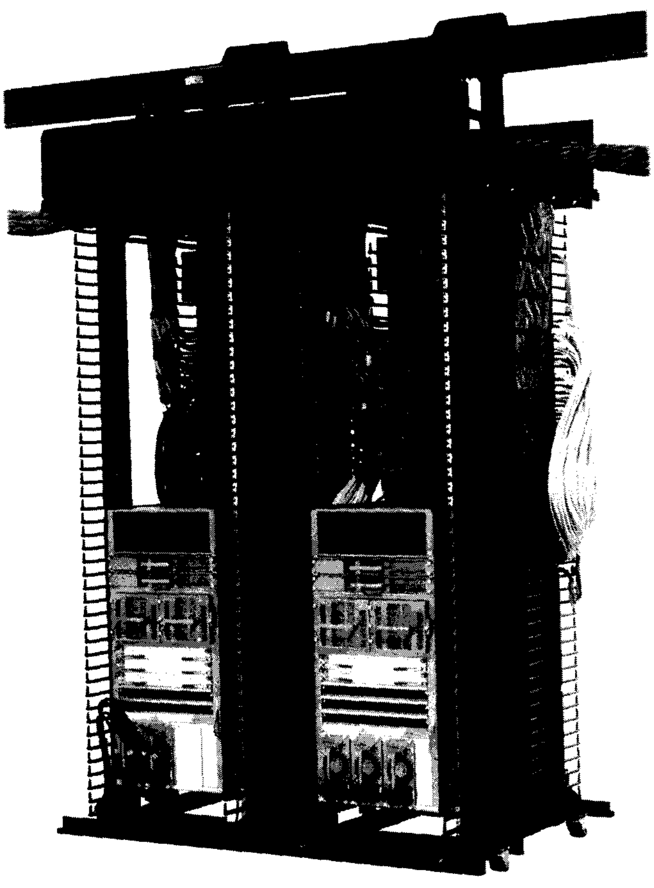
```
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/24 is subnetted, 2 subnets
O       10.1.1.0 [110/65] via 192.168.1.2, 00:05:31, Serial0/0/0
O       10.1.2.0 [110/65] via 192.168.1.2, 00:05:21, Serial0/0/0
C    192.168.1.0/24 is directly connected, Serial0/0/0
```

Pic 1: 91 Output of Dynamic routed routing table.

After dynamic routing protocols are configured, if any changes happen in the network, R1 will dynamically get the information from R2.

Chapter 5

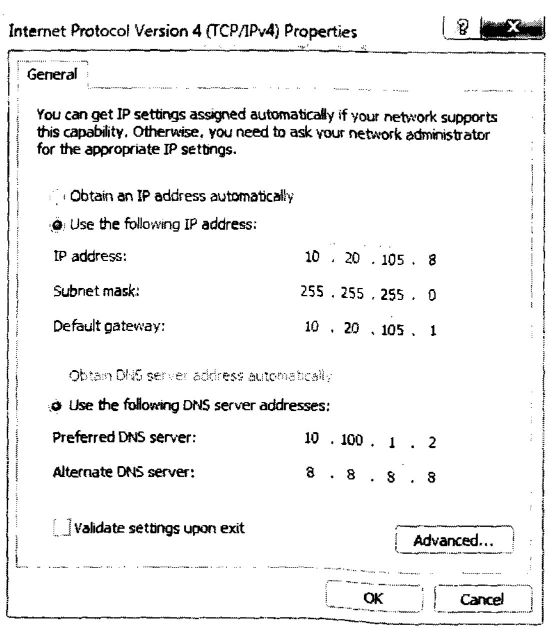
Addressing the Network – IPv4 and IPv6 (review)



In this chapter, you will learn to:

- **Explain the structure of IP addressing and demonstrate the ability to convert between 8-bit binary and decimal numbers.**
- **Given an IPv4 address, classify by type and describe how it is used in the network.**
- **Explain how addresses are assigned to networks by ISPs and within networks by administrators.**
- **Determine the network portion of the host address and explain the role of the subnet mask in dividing networks.**
- **Given IPv4 addressing information and design criteria, calculate the appropriate addressing components.**
- **Use common testing utilities to verify and test network connectivity and operational status of the IP protocol stack on a host.**

Pic 1:92 Represents IPv4 configuration on Windows 7 OS.



Pic 1: 92 IPv4 Configuration

IP Version 4 Characteristics

- Consists of 32 bits
- Divided into 4 octets
- Each octet consists of 8 bits (1byte)
- Represented in *decimal* form

Pic 1:93 Shows structure of IPv4 adress.
Example of IPv4 address:

1st octet 2nd octet 3rd octet 4th octet

192.168.1.21- > decimal representation

11000000.10101000.00000001.00010101 -> binary representation

Pic 1: 93 Structure of IPv4 address

We use decimal representation of IPv4, usually it is enough for us. But since we are engineers we have to know how to convert from binary to decimal and from decimal to binary, to make some operations.

Decimal vs Binary numeric systems

Decimal numeric system consists of 10 characters:

- 0
- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9

Binary numeric system consists of 2 characters:

- 0
- 1

People use Decimal numbers, computers can use only and only binary system, because computers operate by using electricity. By using electricity computers can understand that there is voltage on or voltage off. That's why computers use binary system, binary statement 0 means that voltage is off, binary statement 1 means that voltage is on.

By using binary numeric system we can make representation of decimal numeric system. And each representation of decimal or hexadecimal from binary will look like a predefined unique code.

Table 1:1 Shows representation of decimal numbers by using one bit:

Decimal	Binary
0	0
1	1

Table 1:1 One bit representation

Table 1:2 Shows representation of numbers by using two bits:

Decimal	Binary
0	00
1	01
2	10
3	11

Table 1:2 Two bits representations

Table 1:3 Shows representation with tree bits:

Decimal	Binary
0	000
1	001
2	010
3	011
4	100
5	101
6	110
7	111

Table 1:3 Three bits representations

As you see we have sequence, if we use 1 bit we can make representation of 2 decimal numbers, if 2 bits then 4 decimal numbers, if 3 bits then 8 decimal numbers. And if we take 4 bits, it means that we will have twice as bigger sequence of decimal numbers than if we take 3 bits.

Formula for identification of numbers of decimals which can be represented by binary numbers:

2^n, where ***n*** is quantity of bits.

Table 1:4 Shows number of combinations per different amount of bits.

Example table:

Number of bits	**Formula**	**Number combinations**
1	2^1	2
2	2^2	4
3	2^3	8
4	2^4	16
5	2^5	32
6	2^6	64
7	2^7	128
8	2^8	256
9	2^9	512
10	2^{10}	1024
11	2^{11}	2048
12	2^{12}	4096
13	2^{13}	8192
14	2^{14}	16384
15	2^{15}	32768
16	2^{16}	65536
17	2^{17}	131072
18	2^{18}	262144
19	2^{19}	524288
20	2^{20}	1048576

Table 1:4 Number of combinations from 1 to 20 bits

We can use three methods of conversion from decimal to binary:

1. Follow the sequence
2. Divide by 2 technique
3. Mapping

Follow the sequence

Just imagine that you have to convert decimal 5 to binary.

To make conversion we have to answer the question.

Question: How many bits do we need to have at least 5 combinations?

Answer: 3

Question: Why?

Answer: $2^3=8$, *if we take 2 bits, then* $2^2=4$ *it is not enough for us.*

Table 1:5 Shows 3 bits combinations.

Now we know that 3 bits will be enough for us, starting the sequence:

Decimal	Binary
0	000
1	001
2	010
3	011
4	100
5	101
6	110
7	111

Table 1:5 3 bits combinations

One more example of following the sequence technique: Find out binary representation of decimal 15. Table 1:6 Shows 4 bits combinations.

Question: How many bits do we need?

Answer: 4, $2^4=16$.

Let's start sequence:

Decimal	Binary
0	0000
1	0001
2	0010
3	0011
4	0100
5	0101
6	0110
7	0111
8	1000
9	1001
10	1010
11	1011
12	1100
13	1101
14	1110
15	1111

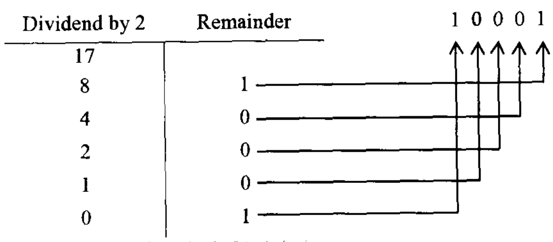
Table 1:6 4 bits combinations

Divide by 2 techniques

Divide by 2 techniques is very easy, all prerequisites which you need is just divide decimal numbers by 2.

Pic 1:94 Shows example of Divide by 2 techniques.

Example, decimal number 17 must be converted to binary:



Pic 1: 94 Example of Division by 2 techniquies

After division you have to place remainders in vice-versa sequence.

Answer is: 10001_2

We can check answer by using **follow the sequence** techniques. Table 1:7 Shows checking process.

Decimal	Binary
0	00000
1	00001
2	00010
3	00011
4	00100
5	00101
6	00110
7	00111
8	01000
9	01001
10	01010
11	01011
12	01100
13	01101
14	01110
15	01111
16	10000
17	10001

Table 1:7 Checking process

Later we will use other techniques to check results.

Mapping technique

Mapping is my favorite technique of conversion from decimal to binary and vice-versa.

Every bit starting from right side has position (value) which depends on exponent. Table 1:8 Represents values of each bit.

Exponent	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Position(value)	128	64	32	16	8	4	2	1

Table 1:8 Values of bits

Example of mapping technique of conversion from decimal to binary:
We have to find out binary representation of decimal 67.
Let's start mapping...
Firstly we have to define how many bits we need for conversion.
67 is less than 128, it means that we will place 0 to 8^{th} bit.
67 higher than 64, that's why we place 1 to 7^{th} bit.
Currently we have 64, which mean that we need to subtract 64 from 67: 67-64=3.
We need to add 3 to 64. Table 1:9 Shows example of converting decimal 67 to binary.

Exponent	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Position(value)	128	64	32	16	8	4	2	1
Result	0	1	0	0	0	0	1	1

Table 1:9 Example of converting from decimal to binary

And here is the result: $67_{10}=1000011_2$

Question: How to convert from binary to decimal by using mapping?

Answer: To answer for this question it will be useful to give an example.

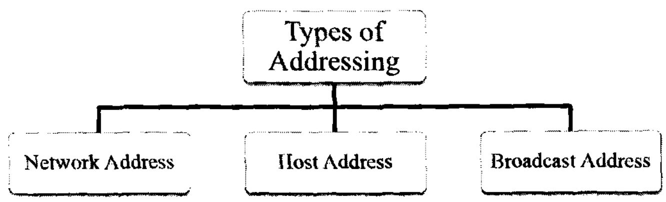
In this example we have to convert binary 1110010_2 into decimal: Table 1:10 Shows example of converting binary 1110010 into decimal.

Position(value)	64		32		16		8		4		2		1
Multiplication	*		*		*		*		*		*		*
Given binary stream	1		1		1		0		0		1		0
Result of Multiplication	64		32		16		0		0		2		0
Addition	64	+	32	+	16	+	0	+	0	+	2	+	0
Result = 114													

Table 1:10 Example of converting from binary to decimal

Types of IPv4 Addressing

Pic 1:95 Shows types of IPv4 Addresses.



Pic 1: 95 Types of IPv4 Addresses

Network Address

The address by which we refer to the network. Network address is the same as a Group Name in university.

Example of Group Names (Network Addresses):

- En4a03
- En4b03
- En4a04
- En4b04
- En4c04

Host Address

Host Address defines host in the network, like name of student defines unique person inside the group.

Example of usernames (Host Addresses)

- 4a03 - Aytekov Danur
- 4a03 - Abzhanov Nurbek
- 4a03 - Alahunova Kaminur
- 4a03 - Arzmetov Zarif
- 4a03 - Ahet Abilhayir
- 4a03 - Ahinbekova Akerke
- 4a03 - Mukashev Serik
- 4a03 - Muhammed Bagdji

Broadcast Address

A special address used to send data to all hosts in the network, example of broadcast in group: *En4a03-All.*

Prefix and Subnet Mask

Prefix defines numbers of bits which belong to Network Address starting from the left side of IPv4 address.
Subnet Mask defines Prefix

Example of IPv4 Address with prefix:

192.168.1.2/24 – decimal representation, /24 is prefix which defines length of network address from the left side. It means that 192.168.1.0 is network address.

Computers make AND operation of binary IPv4 address and subnet mask,

IPv4 ∩ Subnet Mask

Table 1:11 Shows AND operation.

Review of AND operation:

A	B	$A \cap B$
0	0	0
0	1	0
1	0	0
1	1	1

Table 1:11 AND operation

11000000.10101000.00000001.00000010 - binary representation of IPv4

AND

11111111.11111111.11111111.00000000 – subnet mask of prefix /24

=

11000000.10101000.00000001.00000010 – Network Address (binary)

192.168.1.0 – Network Address (decimal)

Example of finding out the Network Address, Range of usable addresses and Broadcast Address:

Given: **192.168.111.112/21**

1st step: Conversion of IPv4 from decimal to binary

11000000.10101000.11011111.11100000 – Given IPv4 address in binary system

2nd step: Finding Subnet mask from given prefix /21

11111111.11111111.11111000.00000000 – **Subnet Mask**

3rd step:ANDing **IPv4 with Subnet Mask**

11000000.10101000.11011111.11100000
AND
11111111.11111111.11111000.00000000
=
11000000.10101000.11011*000.00000000* – Network Address

First usable address will be next combination of Host portion in IPv4 address.

Finding first usable address: **11000000.10101000.11011***000.00000001*

Last usable address is before the last combination of Host portion Range.

Finding Last usable address: **11000000.10101000.11011***111.11111110*

Network Address	192.168.216.0
First Usable Address	192.168.216.1
Last Usable Address	192.168.223.254
Broadcast Address	192.168.223.255

Table 1:12 Result of task

Table 1:12 Shows result of Task.

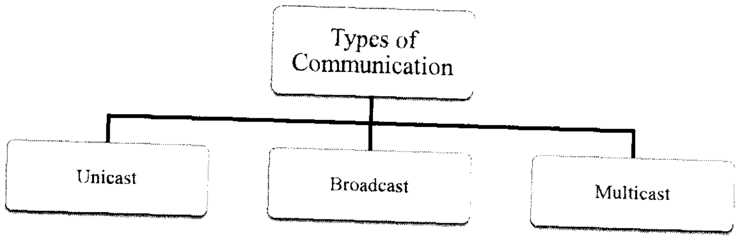
Network Address and Broadcast Addresses cannot be assigned to host, that is why in every network we have by two addresses, which are busy and cannot be assigned to hosts.

And if we want to calculate the number of hosts that could be placed into the network we have to take a look at the subnet mask. If the subnet mask is /24, to identify the number of bits belonging to host portion we have to make subtraction of 32 (IPv4 Address consists of 32 bits) – 24 (prefix, number of bits from the left side which are responsible for the network address). Then you'll have 8, by using 8 bits we can have $2^8 = 256$ combinations. We have to consider that in every network 2 combinations are not usable by hosts (Network address and Broadcast addresses). It means that we need to subtract: $2^8-2=254$

In previous example prefix was 21, it means that 11 bits belong to host portion. And we can insert into the network $2^{11}-2= 2046$ hosts.
Next time you can use the formula: 2^n-2 = Number of Usable Hosts in the network.
Where ***n*** is the number of bits belonging to host portion of IPv4 address.

Types of Communication with IPv4

Pic 1:96 Shows types of Communication with IPv4.

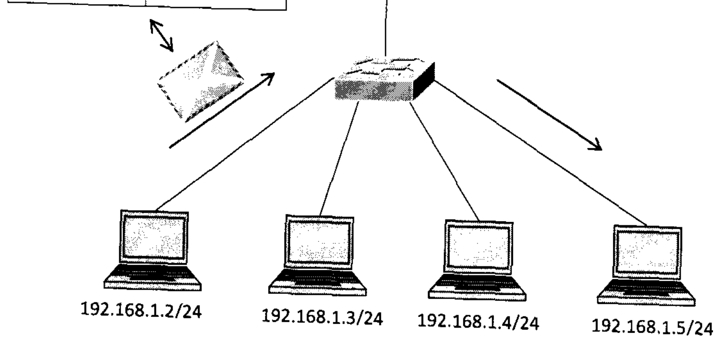


Pic 1:96 Types of Communication with IPv4

Unicast

Pic 1:97 Shows process of sending a packet from one host to an individual host.

Source IP address	192.168.1.2
Destination IP address	192.168.1.5



Pic 1: 97 Process of unicast communication

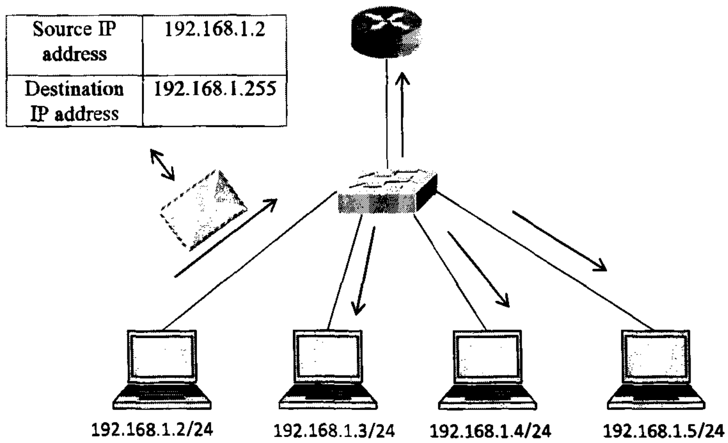
Broadcast

Broadcast – is the process of sending a packet from one host to the rest of the hosts within the network. Broadcast address is last combination of host range in IP address.

Broadcast usage:

- Mapping upper layer addresses to lower layer addresses
- Requesting an address
- Exchanging routing information by routing protocols

Pic 1:98 Shows Broadcast communication in process.



Pic 1: 98 Process of broadcast communication

Broadcast issues:

- Broadcast requests make too much noise noise in a network, and network speed is extremely decreased on networks where a lot of broadcasts exist.
- Security risk exists, because information is sent to every host in the network. It means that someone can read that data and use secret information.

Multicast

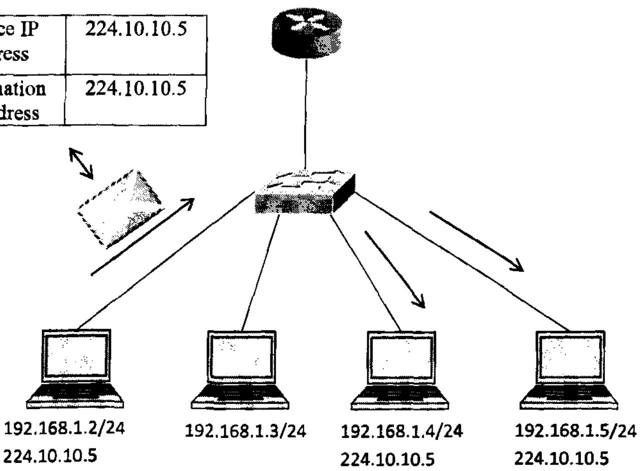
Multicast – is the process of sending packets from one host to many hosts. In multicast communication computers who are inside multicast group use special multicast address to share data between many but not all hosts in the network.

Multicast usage:

- Video and audio distribution
- Routing information exchange by routing protocols
- Distribution of software
- News feeds

Pic 1:99 Shows Multicast communication in process.

Source IP address	224.10.10.5
Destination IP address	224.10.10.5



Pic 1: 99 Process of Multicast communication

Reserved IPv4 Addresses Range

Table 1:13 Shows IPv4 Addresses Range

Type of Address	Usage	Reserved	RFC
Host Addresses	Used for IPv4 hosts	0.0.0.0 – 223.255.255.255	790
Multicast Addresses	Used for multicast groups on a local network	224.0.0.0 – 239.255.255.255	1700
Experimental Addresses	Used for research or experimental Cannot currently be used for hosts in IPv4 networks	240.0.0.0 – 255.255.255.255	1700 3330

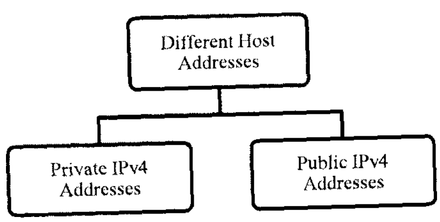
Table 1:13 IPv4 Addresses Range

IPv4 totally consists of $2^{32} = 4.294.967.296$ combinations. Only range of 0.0.0.0 – 223.255.255.255 IP addresses can be assigned to hosts. Soon IPv4 addresses will not be enough for our society that is why we already have next generation of IP address, IPv6 which consists of 2^{128} combinations.

RFC – Request For Comments is used for description of any protocols. If for example you want to know information about Host Address of IPv4 you can read document RFC 790.

Host Addresses for Different Purposes

Pic 1:100 Shows Private and Public addresses



Pic 1:100 Private and Public IPv4 Addresses

Host addresses are separated into two parts: Private and Public.

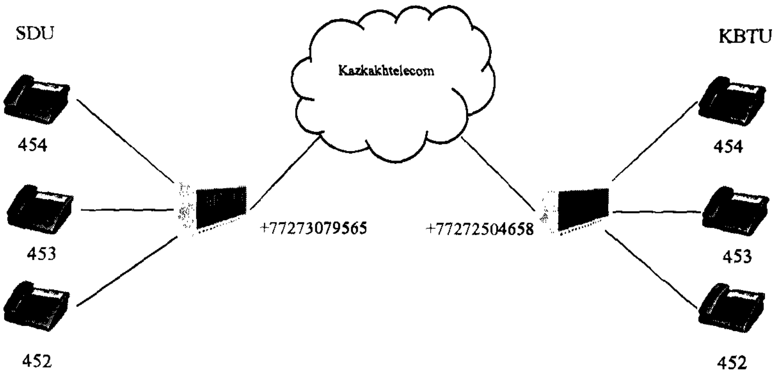
Public IPv4

Public IPv4 addresses can be used only in Global Connection (Internet).

Question: Why do we need to have Private and Public IPv4 host addresses?

Answer: We need to have them, because range of IPv4 host addresses range is limited. Every host has to have unique IPv4 address. If one company has 200 hosts it means that we need to assign 200 unique global IPv4 addresses. But if we use Private and Public IPv4 addresses, it will be enough to use 1 global unique IPv4 address and 200 local IPv4 addresses.

Pic 1:101 Shows Private and Public telephone numbers:



Pic 1: 101 Private and Public telephone numbers.

In this example we have different public phone numbers of universities, but private (local) phone numbers can be the same. If you will call from SDU to KBTU full phone number will be: +77272504658#454, if you will call from KBTU to SDU full phone number will be: +77273079565#454. Conversion from Public and Private phone numbers is done by PBX (Мини АТС).

Same situation happens with Computer Networks

Private IPv4

Private IPv4 can be used only and only in Private (Local) Networks.

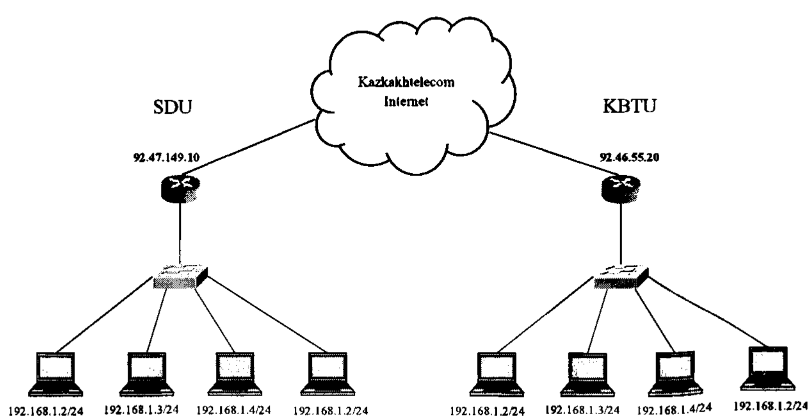
Table 1:14 Shows range of Private IPv4 Addresses.

Private IPv4 Range:

10.0.0.0	10.255.255.255
172.16.0.0	172.31.255.255
192.168.0.0	192.168.255.255

Table 1: 14 Private range of IPv4 addresses

Pic 1:102 Shows Private and Public IPv4 addresses:



Pic 1: 102 Private and Public IPv4 addresses

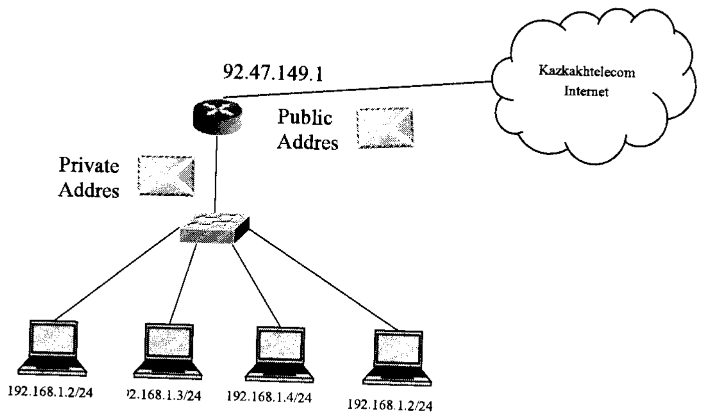
In this example we have different public IPv4 of universities, but private (local) IPv4 can be the same. If you contact from SDU to KBTU full IPv4 address will be: 92.46.55.20#192.168.1.4. If you contact from KBTU to SDU full IPv4 address will be: 92.47.49.10#192.168.1.4

Conversion between Private and Public IPv4 addresses is done by NAT, which can be placed in router.

NAT- Network Address Translation

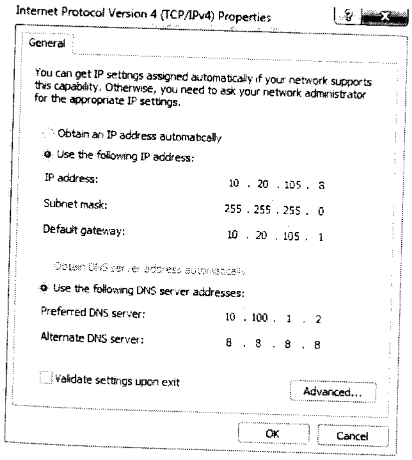
NAT Mechanism is responsible for Translation of Public to Private IP Addresses

Pic 1:103 Shows example of NAT:



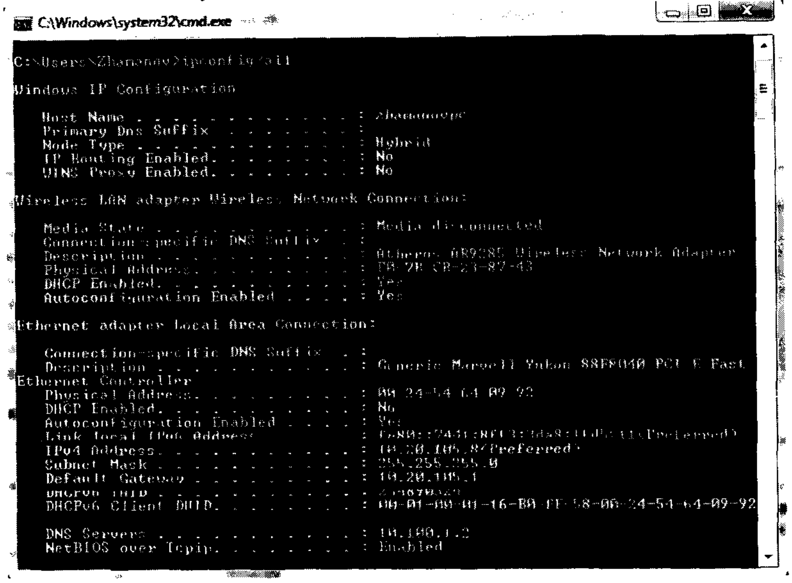
Pic 1: 103 NAT example

Pic 1:104 Shows example of addressing end device:



Pic 1: 104 Example of IPv4 addressing

You also can examine your TCP/IP stack configuration by using command **ipconfig/all** in CMD:



Pic 1: 105 *ipconfig/all* command's output in cmd

Pic 1:105 shows output of *ipconfig/all* command.

Question: Who assigns Public (Global) IP addresses?

Answer: IANA – Internet Assigned Numbers Authority.

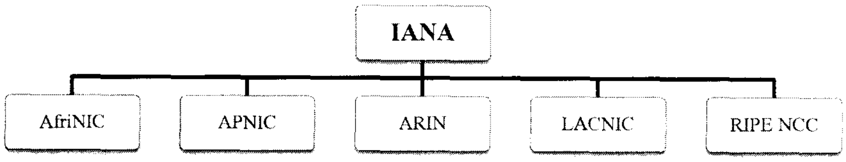
IANA – Internet Assigned Numbers Authority (www.iana.net)

IANA is the master holder of the IP addresses.
The IP multicast addresses and the IPv6 addresses are obtained directly from IANA.

Until the mid-1990s, all IPv4 address space was managed directly by the IANA.
Nowadays IANA separated responsibilities to five Regional Internet Registries (RIRs)

IANA and RIRs

Pic 1:106 Shows RIRs of IANA



Pic 1: 106 RIRs

AfriNIC

- African Network Information Centre
- http://www.afrinic.net

APNIC

- Asia Pacific Network Information Centre
- http://www.apnic.net

ARIN

- American Registry for Internet Numbers
- http://www.arin.net

LACNIC

- Regional Latin-American and Caribbean IP Address Registry) - Latin America and some Caribbean Islands
- http://www.lacnic.net

RIPE NCC

- (Reseaux IP Europeans) - Europe, the Middle East, and Central Asia
- http://www.ripe.net

RIRs on Map

Pic 1:107 shows geographical locations of RIRs.

Pic 1: 107 Geographical locations of RIRs

Subnetting the Network

In this section we will have some practice with division of networks and assigning the IPv4 addresses.

Example: Given Network IPv4 address 192.168.1.0/24

11000000.10101000.00000001.**00000000**–Network address

11000000.10101000.00000001.**00000001** –First usable address

11000000.10101000.00000001.**00000010** –Second usable address

.

.

.

11000000.10101000.00000001.**11111110**–Last usable address

11000000.10101000.00000001.**11111111** –Broadcast address

In this network, since 8 bits can be used in host address, we can insert 254 hosts and it is only one network.

If we want to extend number of networks, we have to take one more bit for network address portion.

192.168.1.0/25

*11000000.10101000.00000001.0*0000000

Table 1:15 Shows Example of dividing network into two parts.

Subnet	Network address	Host range	Broadcast address
0	192.168.1.0/25	192.168.1.1 - 192.168.1.26	192.168.1.127
1	192.168.1.128/25	192.168.1.129 - 192.168.1.254	192.168.1.255

Table 1:15 Example of division network into two sub-networks

We took one bit from host portion; it means that we have two more combinations for network addresses:

- *11000000.10101000.00000001.0*0000000
- *11000000.10101000.00000001.1*0000000

But host address range is decreased: 2^7-2=126

If we take two bits from host portion, we will have 4 sub-networks with 2^6-2=62 addresses in each sub-network. Table 1:16 Shows example of division network into four sub-networks.

Subnet	Network address	Host range	Broadcast address
0	192.168.1.0/26	192.168.1.1 - 192.168.1.62	192.168.1.63
1	192.168.1.64/26	192.168.1.65 - 192.168.1.126	192.168.1.127
2	192.168.1.128/26	192.168.1.129 – 192.168.1.190	192.168.1.191
3	192.168.1.192/26	192.168.1.193 – 192.168.1.254	192.168.1.255

Table 1:16 Example of division network into four sub-networks

If we take 3 bits from host portion, then we will have 8 sub-networks: Table 1:17 Shows example of division network into eight sub-networks.

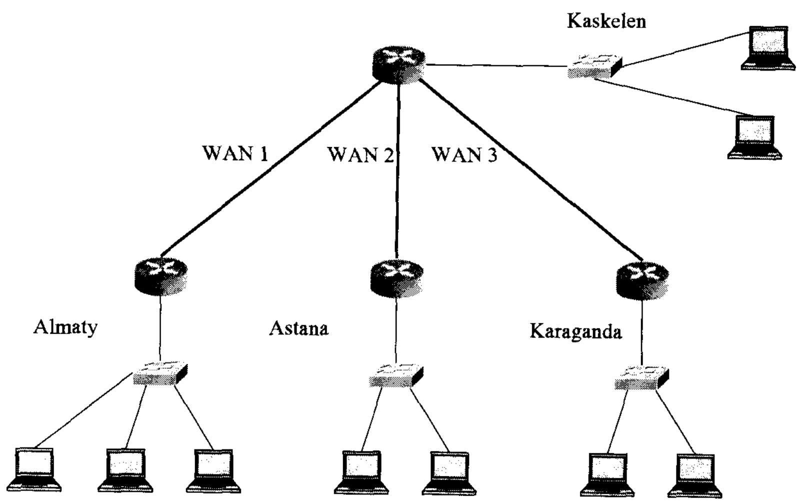
Subnet	Network address	Host range	Broadcast address
0	192.168.1.0/27	192.168.1.1 - 192.168.1.30	192.168.1.31
1	192.168.1.32/27	192.168.1.33 - 192.168.1.62	192.168.1.63
2	192.168.1.64/27	192.168.1.65 - 192.168.1.94	192.168.1.95
3	192.168.1.96/27	192.168.1.97 - 192.168.1.126	192.168.1.127
4	192.168.1.128/27	192.168.1.129 - 192.168.1.158	192.168.1.159
5	192.168.1.160/27	192.168.1.161 - 192.168.1.190	192.168.1.191
6	192.168.1.192/27	192.168.1.193 - 192.168.1.222	192.168.1.223
7	192.168.1.224/27	192.168.1.225 - 192.168.1.254	192.168.1.255

Table 1:17 Example of division network into eight sub-networks

Pic 1:108 Shows example of addressing branch offices with IPv4 addresses:

Our task is to assign IP addresses for branch offices with optimal subnet mask not to waste addresses. Start with address 192.168.1.0

Branch office	Host numbers
Almaty	58
Astana	26
Karaganda	10
Kaskelen	10
WAN Links	2 hosts at each



Pic 1: 108 Example of Addressing task

Advice: Start from branch office with higher number of computers.

Almaty Branch office has to be configured with 58 host's addresses, we need to find out optimal subnet mask (prefix).

Table 1: 18 Shows example of solving problems.

It is good practice to use table of bits to solve such kind of problems:

Exponent	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Position(value)	128	64	32	16	8	4	2	1

Table 1:18 Solving problems

By using mapping technique we can define that only 6 bits of last octet are necessary for us to have 58 hosts, it means that prefix will be 32-6=**26**. Table 1.19 Shows solved result for Almaty branch office.

Almaty Branch office	
Network Address	192.168.1.0/26
First Usable Address	192.168.1.1/26
Last Usable Address	192.168.1.62/26
Broadcast Address	192.168.1.63./26

Table 1: 19 Almaty branch office

Now we need to give configuration of IPv4 addresses of Astana Branch office.

Let us find out the prefix of Astana office, which needs only 26 host addresses.

Looking at previous mapping table we can easily define that last 5 bits, it means that prefix is equal to 32-5=**27**. Table 1:20 Shows solved result for Astana branch office.

Astana Branch office	
Network Address	192.168.1.64/27
First Usable Address	192.168.1.65/27
Last Usable Address	192.168.1.94/27
Broadcast Address	192.168.1.95./27

Table 1: 20 Astana branch office

Next office is Karaganda with 10 hosts. Table 1:21 Shows solved result for Karaganda branch office.

Prefix will be **28**

Karaganda Branch office	
Network Address	192.168.1.96/28
First Usable Address	192.168.1.97/28
Last Usable Address	192.168.1.110/28
Broadcast Address	192.168.1.111./28

Table 1: 21 Karaganda branch office

Last office is Kaskelen also with 10 hosts and we will use same prefix **28.** Table 1:22 Shows solved result for Kaskelen branch office.

Kaskelen Branch office	
Network Address	192.168.1.112/28
First Usable Address	192.168.1.113/28
Last Usable Address	192.168.1.126/28
Broadcast Address	192.168.1.127./28

Table 1: 22 Kaskelen branch office

And now we need to give addressing for WAN links which need only 2 addresses each.

Prefix will be 30, because only two last bits will be in host portion site and we will have 2^2-2=2 usable addresses. Table 1:23, 1:24 and 1:25 Shows solved result for WANs.

WAN 1	
Network Address	192.168.1.128/28
First Usable Address	192.168.1.129/28
Last Usable Address	192.168.1.130/28
Broadcast Address	192.168.1.131./28

Table 1: 23 WAN 1

WAN 2	
Network Address	192.168.1.132/28
First Usable Address	192.168.1.133/28
Last Usable Address	192.168.1.134/28
Broadcast Address	192.168.1.135./28

Table 1: 24 WAN 2

WAN 3	
Network Address	192.168.1.136/28
First Usable Address	192.168.1.137/28
Last Usable Address	192.168.1.138/28
Broadcast Address	192.168.1.139./28

Table 1: 25 WAN 3

Overview of IPv6

Question: What is the main reason of using IPv6?

Answer: Extended range of IP addresses.

IPv6 Characteristics

- Consists of 128 bits
- Divided into 8 octets
- Represented in hexadecimal numeric system

It means that we can have 2^{128} unique IPv6 addresses, it will be enough for our planet and not only.

Let us review Hexadecimal numeric system. Hexadecimal numeric system consist of 16 combinations:

- 0
- 1
- 2
- 3
- 4

- 5
- 6
- 7
- 8
- 9
- A
- B
- C
- D
- E
- F

To make binary representation of hexadecimal we need to use 4 bits. Table 1:26 Shows binary view of hexadecimal numbers.

Hexadecimal	Binary
0	0000
1	0001
2	0010
3	0011
4	0100
5	0101
6	0110
7	0111
8	1000
9	1001
A	1010
B	1011
C	1100
D	1101
E	1110
F	1111

Example of IPv6 address:

fe80:0000:0000:0000:0202:b3ff:fe1e:8329

It can be abbreviated as:

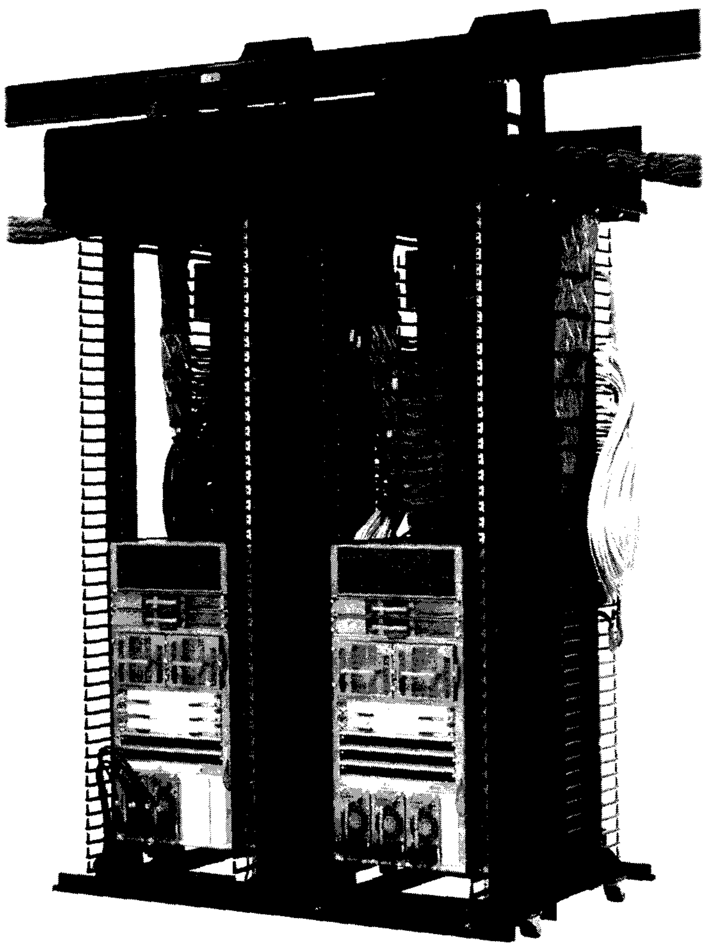
fe80:0:0:0:202:b3ff:fe1e:8329

And finally can be represented like:

fe80::202:b3ff:fe1e:8329

Chapter 6

OSI Data Link Layer

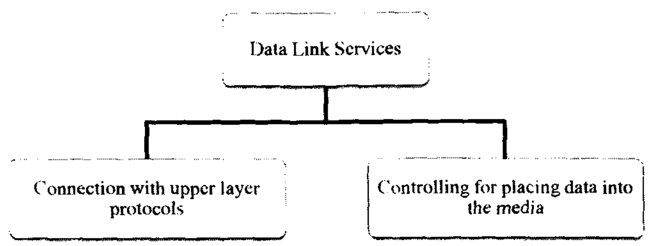


Upon completion of this chapter, you will be able to:

- Explain the role of Data Link layer protocols in data transmission.
- Describe how the Data Link layer prepares data for transmission on network media.
- Describe the different types of media access control methods.
- Identify several common logical network topologies and describe how the logical topology determines the media access control method for that network.
- Explain the purpose of encapsulating packets into frames to facilitate media access.
- Describe the Layer 2 frame structure and identify generic fields.
- Explain the role of key frame header and trailer fields, including addressing, QoS, type of protocol, and Frame Check Sequence.

Data Link Layer performs two basic services:

Pic 1:109 Shows Data Link Services.



Pic 1:109 Data Link Services

Connection with upper layer protocols

Allows the upper layers to access the media using techniques such as framing

Controlling for placing data into the media

Controls how data is placed onto the media and is received from the media using techniques such as media access control and error detection

Data Link Layer's PDU – Frame

As you know, on different layers of OSI Networking Model, data has different name, in Application, Presentation and Session layer data is called data. In OSI Transport Layer it is called Segment or Datagram depending on which protocol you're working with. In Network Layer it is called Packet and in Data Link Layer it is called **Frame.**

Structure of Frame:

Frame Header	Packet	Frame Trailer

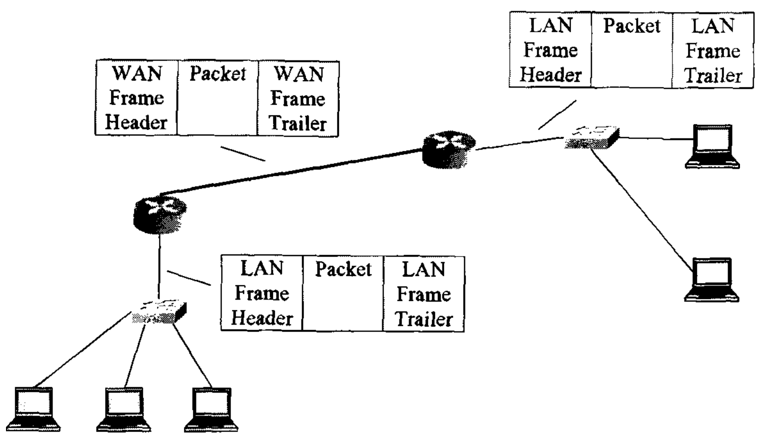
Frame Header consists of:

- Frame Start –Unique combination of bits which identifies start of the frame
- Addressing – Source and Destination MAC addresses (Physical Addresses)
- Type – Type of Upper Layer protocol
- Quality of Service – Priority value between frames

Frame Trailer consists of:

- Error Detection –FCS Error check mechanism
- Frame Stop – Unique combination of bits which identifies end of frame

In different types of media Frames are different, but packet doesn't change structure. Pic 1:110 Shows how Data Link Layer uses different structure of Frames in different media.

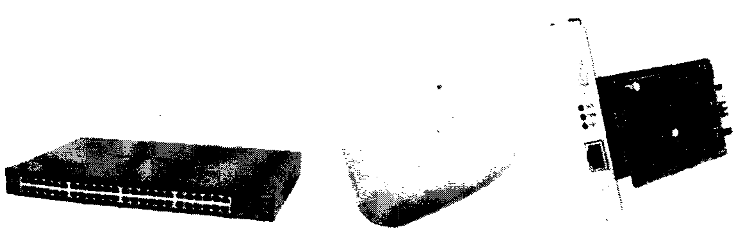


Pic 1:110 Different frames in different media

Data Link is called OSI Layer 2. Devices which are work with Layer 2:

- Switch
- Wireless Access Point (AP)
- Network Interface Card (NIC)

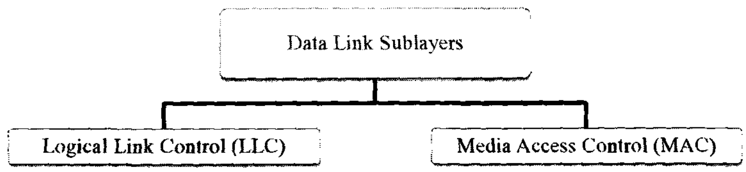
Pic 1:111 Shows physical devices of Data Link Layer.



Pic 1:111 Physical Devices of Data Link Layer

Data Link Layer consists of two Sub Layers

Pic 1:112 Shows Data Link Sublayers



Pic 1:112 Physical Devices of Data Link Layer

LLC

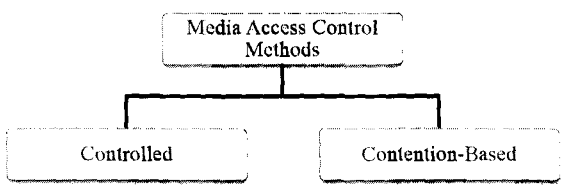
Logical Link Control (LLC) places information in the frame that identifies which Network layer protocol is being used for the frame. This information allows multiple Layer 3 protocols, such as IP and IPX, to utilize the same network interface and media.

Media Access Control

Media Access Control (MAC) provides Data Link layer addressing and delimiting of data according to the physical signaling requirements of the medium and the type of Data Link layer protocol in use.

Two Basic Media Access Control Mechanism

Pic 1:113 Shows Media Access Control Methods.



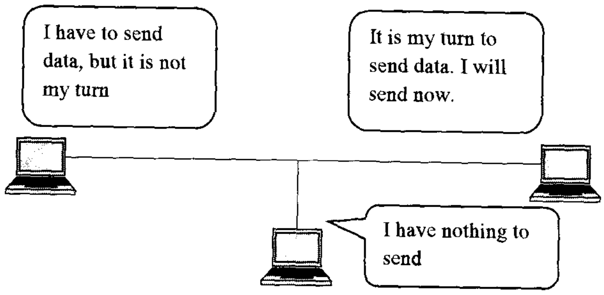
Pic 1:113 Media Access Control Methods

Controlled

When using the controlled access method, network devices take turns, in sequence, to access the medium.

This method is also known as scheduled access or deterministic.

Pic 1:114 Represents Controlled Access Method

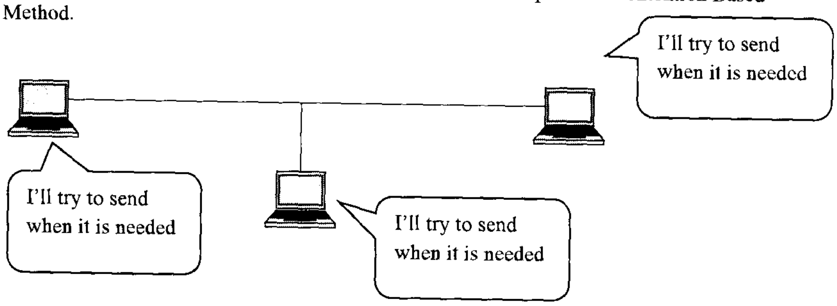


Method	Characteristics	Example
Controlled Access	• Only one station transmits at a time • Devices wishing to transmit must wait their turn • No Collisions • Some deterministic network use token passing	• Token Ring • FDDI

Pic 1:114 Controlled Access Method

Contention-Based

Also referred to as non-deterministic, contention-based methods allow any device to try to access the medium whenever it has data to send. Pic 1:115 Represents Contention Based Method.



Method	Characteristics	Example
Contention Based Access	• Stations can try to transmit at any time • Collision Exists • Mechanism That resolve problems: • CSMA/CD for Ethernet • CMSA/CA for Wireless connection	• Token Ring • FDDI

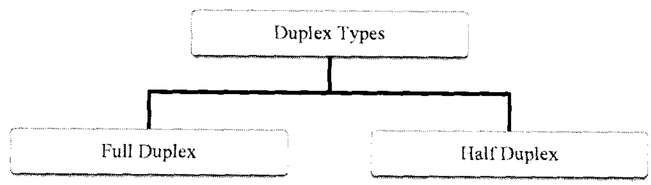
Pic 1:115 Contention Based Access Method

Full Duplex vs. Half Duplex

Question: What does duplex mean?

Answer: ***Duplex*** *commonly means double or twofold.*

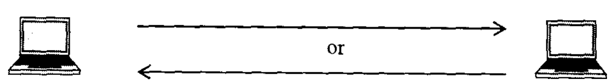
Example of Duplex usage: Duplex Printing, double sided printing Pic 1:116 Shows duplexes.



Pic 1:115 Duplexes

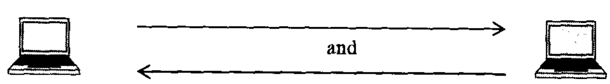
Half Duplex

In half duplex connection data can be sent or received. Data cannot be sent and received at the same time. Pic 1:117 Shows Half Duplex. Pic 1:118 Shows Full Duplex.



Pic 1:117 Half Duplex

Full Duplex



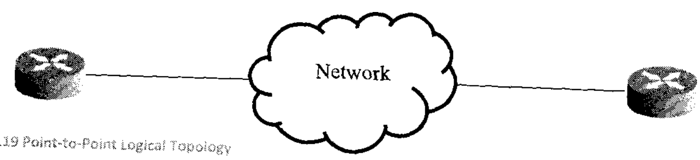
Pic 1:118 Full Duplex

Logical vs. Physical Topologies

Logical Topology

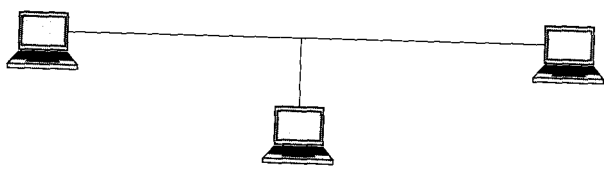
This arrangement consists of virtual connections between the nodes of a network independent of their physical layout. Pic 1:119 Shows Point-to-Point Logical Topology. Pic 1:120 Shows Multi-Access Logical Topology. Pic 1:121 Shows Ring Logical Topology.

Point – to- Point Logical Topology



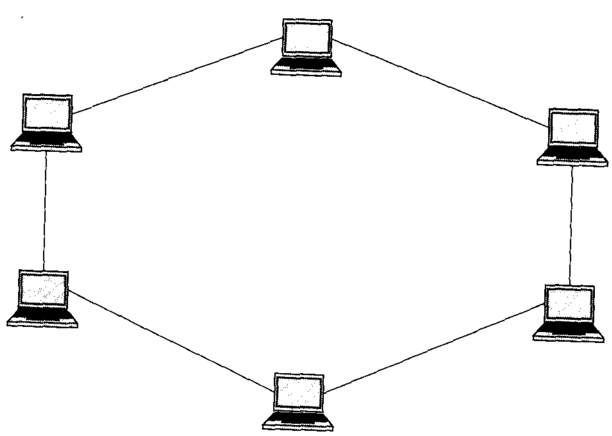
Pic 1:119 Point-to-Point Logical Topology

Multi-Access Logical Topology



Pic 1:120 Multi-Access Logical Topology

Ring Logical Topology



Pic 1:121 Ring Logical Topology

Physical Topology

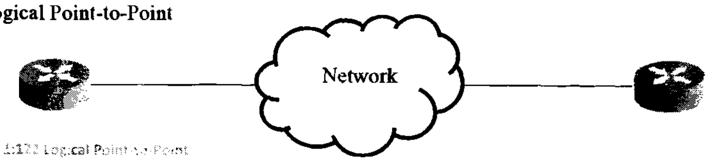
The physical topology is an arrangement of the nodes and the physical connections between them.

The representation of how the media is used to interconnect the devices is the physical topology. These will be covered in later chapters of this course.

Comparison of Logical and Physical Topologies:

Pic 1:122 Shows Logical Point-to-Point topology. Pic 1:123 Shows Physical Point-to-Point topology.

Logical Point-to-Point



Pic 1:122 Logical Point-to-Point

Physical Point-to-Point

Pic 1:123 Physical Point-to-Point

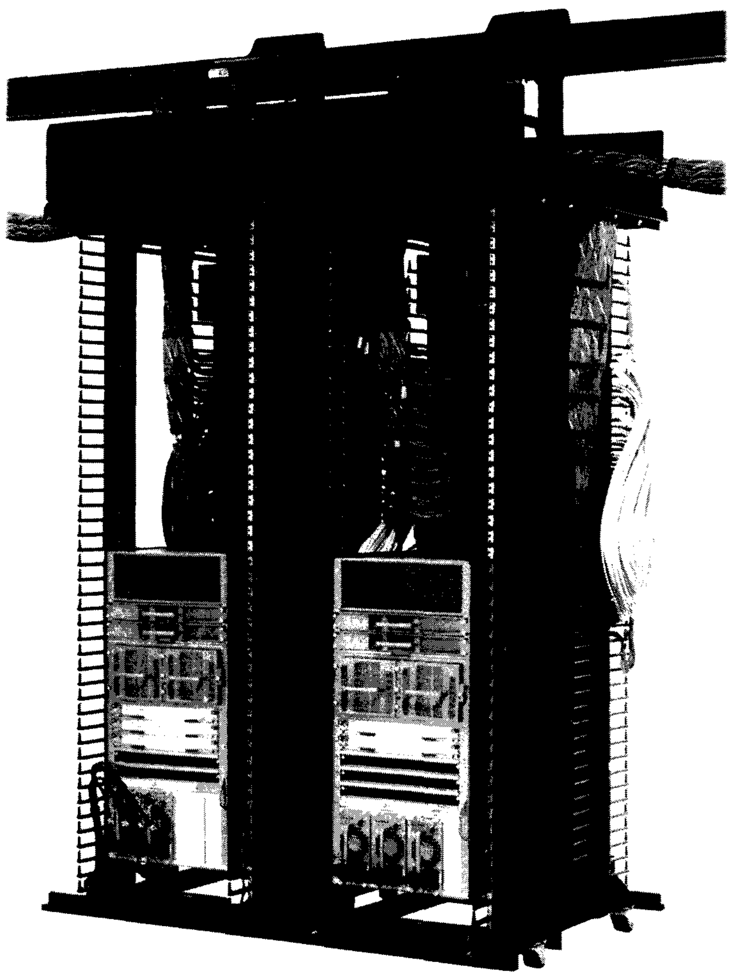
MAC Address Structure

- MAC Address consist of 48 bits, it is 2^{48} or 281 474 976 710 656 addresses.
- Is divided into two parts
  - OUI , Organizationally Unique Identifier, 24 bits
  - Rest 24 bits are belong to identify the device in the organization
- Stored in ROM (Read Only Memory)
- By estimation of IEEE this range is enough till 2100 year.

Example: 01:23:45:67:89:ab

Chapter 7

OSI Physical Layer



In this chapter, you will learn to:

- Explain the role of Physical layer protocols and services in supporting communication across data networks.
- Describe the purpose of Physical layer signaling and encoding as they are used in networks.
- Describe the role of signals used to represent bits as a frame is transported across the local media.
- Identify the basic characteristics of copper, fiber, and wireless network media.
- Describe common uses of copper, fiber, and wireless network media.

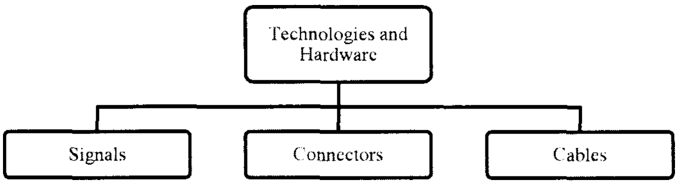
OSI Physical Layer Elements

- The physical media and associated connectors
- A representation of bits on the media
- Encoding of data and control of information
- Transmitter and receiver circuitry on the network devices

Main Purpose of OSI Physical Layer
The purpose of the Physical layer is to create the electrical, optical, or microwave signal that represents the bits in each frame.

Physical Layer Technologies and Hardware

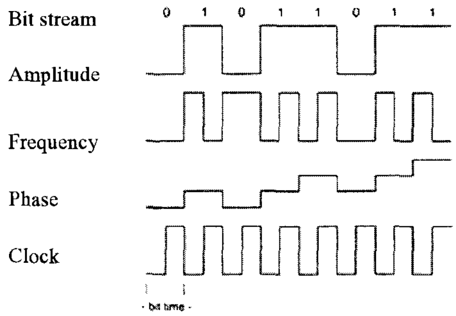
Pic 1:124 Shows Technologies and Hardware.



Pic 1:124 Technologies and Hardware

Signaling

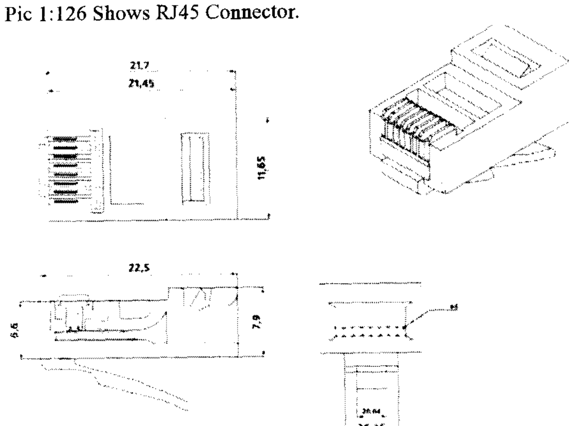
Pic 1:125 Shows Different signaling



Pic 1:125 Signaling types

Connectors

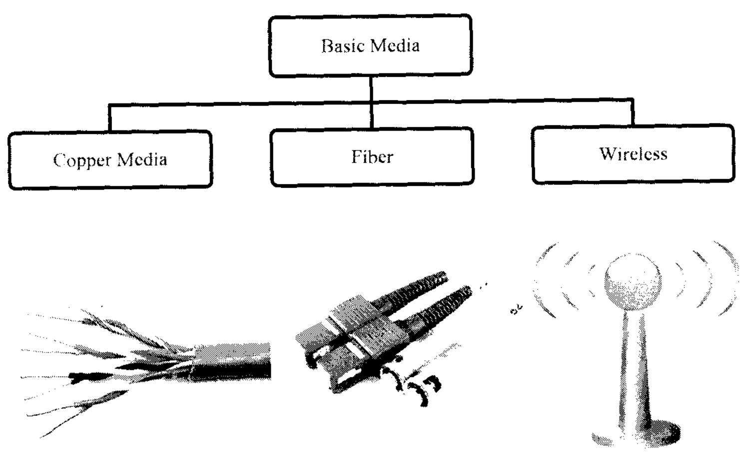
Pic 1:126 Shows RJ45 Connector.



Pic 1:126 RJ45 Connector

Cable - Three Basic Forms of Media

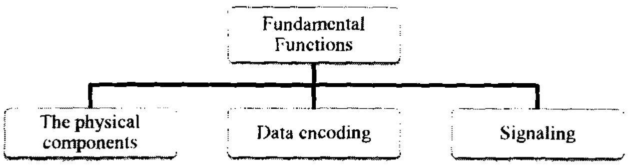
Pic 1:127 Shows Basic Media



Pic 1:127 Basic Media

Three Fundamental Functions of Physical Layer

Pic 1:128 Shows Fundamental Functions of Physical Layer.



Pic 1:128 Fundamental Functions

The Physical Components

The physical elements are the electronic hardware devices, media and connectors that transmit and carry the signals to represent the bits.

Data Encoding

Encoding is a method of converting a stream of data bits into a predefined code.

Codes are groupings of bits used to provide a predictable pattern that can be recognized by both the sender and the receiver.

Using predictable patterns helps to distinguish data bits from control bits and provide better media error detection.

Benefits of Data Encoding:

- Reducing bit level error
- Limiting the effective energy transmitted into the media
- Helping to distinguish data bits from control bits
- Better media error detection

Example of Data Encoding: In Ethernet technology with Bandwidth of 10MB/s , technique used for encoding is called 4B/5B. Table 1:1 Shows 4B/5B encoding technique.

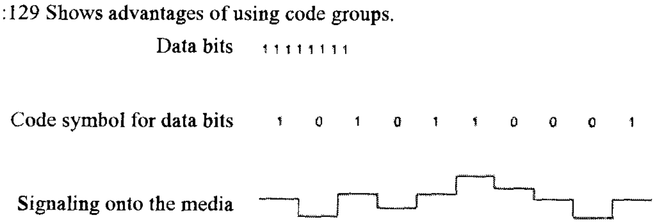
0000	11110
0001	01001
0010	10100
0011	10101
0100	01010
0101	01011
0110	01110
0111	01111
1000	10010

1001	10011
1010	10110
1011	10111
1100	11010
1101	11011
1110	1110
1111	11101
idle	11111
Start of stream	11000
Start of stream	10001
End of stream	01101
End of stream	00111
Transmit error	00111
Invalid	00000
Invalid	00001
Invalid	00010
Invalid	00011
Invalid	00100
Invalid	00101
Invalid	00110
Invalid	01000
Invalid	10000
Invalid	11001

Table 1:1 4B/5B Encoding

Advantages of using code groups include:

Pic 1:129 Shows advantages of using code groups.



Pic 1:129 Advantages of code groups.

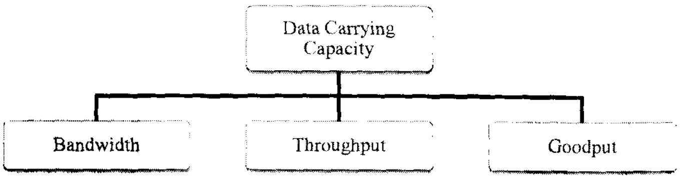
Signaling

The Physical layer must generate the electrical, optical, or wireless signals that represent the "1" and "0" on the media.

The method of representing the bits is called the signaling method.

Data Carrying Capacity

Pic 1:130 Shows Data Carrying Capacity.



Pic 1:130 Data Carrying Capacity

Bandwidth

The capacity of a medium to carry data is described as the raw data bandwidth of the media.

Bandwidth is typically measured in kilobits per second (kbps) or megabits per second (Mbps)

Bandwidth is theoretical speed which cannot be gained ever, because we always have latency on the network. Table 1:2 Shows different measurement units of Bandwidth.

Unit of Bandwidth	Abbreviation	Equivalence
Bits per second	bps	1bps = fundamental unit of bandwidth
Kbits per second	kbps	1kbps = 10^3bps
Megabits per second	Mbps	1Mbps = 10^6bps
Gigabits per second	Gbps	1Gbps = 10^9bps
Terabits per second	Tbps	1Tbps = 10^{12}bps

Table 1:2 Measurements of Bandwidth

Throughput

Throughput = Bandwidth – Device's delays

In transmitting data over the network, data is retransmitted many times by devices like switches, hubs and routers. While they process data, we have delays.

Goodput

Goodput = Throughput – Protocol Overhead

As you know we have many steps of encapsulation (preparing data to transmission over the network). All the encapsulation process takes time for process of division of data into small pieces of data which are called segments or datagrams etc.

In other words Goodput is Real Network Speed.

There can be situation that you have LAN's bandwidth = 100 Mbps, Throughput can be 50 Mbps and Goodput can be 30 Mbps, depending on network structure and load on network.

Ethernet Media

Table 1:3 Shows Ethernet media types

	10BASE-T	100BASE-TX	1000BASE-T	1000BASE-SX	10GBASE-ZR
Media	EIA/TIA Category 3,4,5 UTP-four pair	EIA/TIA Category 5 UTP – two pair	EIA/TIA Category 5 (or greater) UTP, four pair	50/62.5 microns Multimode fiber	9 m single mode fiber
Maximum Segment Length	100 m	100 m		Up to 550m	Up to 80 km
Topology	Star	Star		Star	star

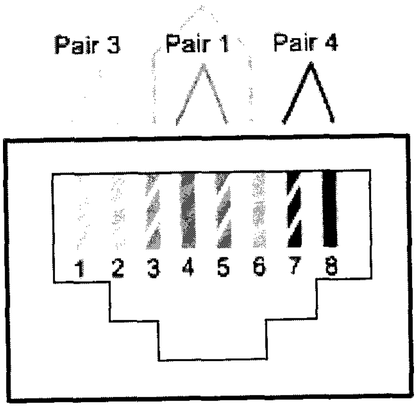
Table 1:3 Ethernet Media Types

UTP and STP cables

Two very popular cables. Used in Ethernet connection. Using RJ45 connectors. Makes connection between hosts, switches, IP Phones, printers and routers.

Usually consist of 8 or 4 small, different colored cables.
Pic 1:131 Shows T568A and T568B UTP Cable connection standards.
Connects to RJ45 connector by two combinations of cables:

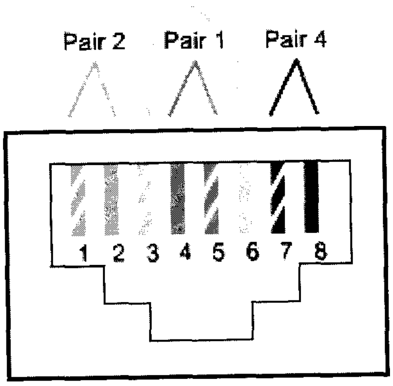
1. T568A



T568A

1st pin: White Green
2nd pin: Green
3rd pin: White Orange
4th pin: Blue
5th pin: White Blue
6th pin: Orange
7th pin: White Brown
8th pin: Brows

2. T568B



T568B

1st pin: White Orange
2nd pin: Orange
3rd pin: White Green
4th pin: Blue
5th pin: White Blue
6th pin: Green
7th pin: White Brown
8th pin: Brows

Pic 1:131 T568A and T568B

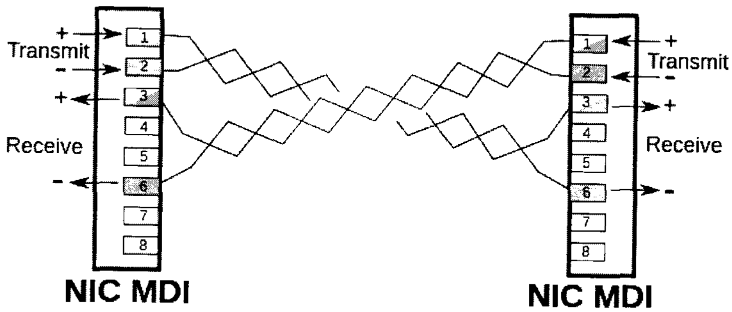
UTP and STP have two connection types:

1. Straight – Through – On both sides of cable connection with RJ45 Connector by using T568A or T568B.
   Example of usage: If speed of connection is not bigger than 100Mb/s, this cable connection type will be used in:

- PC-Switch (and vice versa)
- Switch-Router (and vice versa)
- PC-Hub (and vice versa)

2. Crossover – From one side of cable connection with RJ45 by T568A from the other side T568B.
   Example of usage: If speed of connection is not bigger than 100Mb/s, this cable connection type will be used in:
   - PC-PC (and vice versa)
   - PC-Router (and vice versa)
   - Switch-Switch

Pic 1:132 Shows Crossover Cable Structure.



Pic 1:132 Crossover Cable structure

Summary

Data networks are systems of end devices, intermediary devices, and the media connecting the devices, which provide the platform for the human network.

These devices, and the services that operate on them, can interconnect in a global and user-transparent way because they comply with rules and protocols.

The use of layered models as abstractions means that the operations of network systems can be analyzed and developed to cater the needs of future communication services.

The most widely-used networking models are OSI and TCP/IP. Associating the protocols that set the rules of data communications with the different layers is useful in determining which devices and services are applied at specific points as data passes across LANs and WANs.

As it passes down the stack, data is segmented into pieces and encapsulated with addresses and other labels. The process is reversed as the pieces are decapsulated and passed up the destination protocol stack.

Applying models allows various individuals, companies, and trade associations to analyze current networks and plan the networks of the future.

The Application layer is responsible for directly accessing the underlying processes that manage and deliver communication to the human network. This layer serves as the source and destination of communications across data networks.

The Application layer applications, protocols, and services enable users to interact with the data network in a way that is meaningful and effective.

Applications are computer programs with which the user interacts and which initiate the data transfer process at the user's request.

Services are background programs that provide the connection between the Application layer and the lower layers of the networking model.

Protocols provide a structure of agreed-upon rules and processes that ensure services running on one particular device can send and receive data from a range of different network devices.

Delivery of data over the network can be requested from a server by a client, or between devices that operate in a peer-to-peer arrangement, where the client/server relationship is established according to which device is the source and destination at that time. Messages are exchanged between the Application layer services at each end device in accordance with the protocol specifications to establish and use these relationships.

Glossary

Bandwidth - the rated throughput capacity of a given network media or protocol. The amount of data that can be transmitted in a fixed amount of time.

Backbone - A high-speed link joining together several networks.

Bit – A unit of information having just two possible values, as either of the binary digits 0 or 1.

Byte - a series of consecutive binary digits that are operated upon as a unit. There are 8 bits in a byte.

Category 5 (cat 5) cable -A type of twisted pair network wiring in which there is a certain number of twists per foot. It is the most commonly used network cabling.

Coaxial Cable - A type of cable consisting of two insulating layers and two conductors most commonly used in older networks.

Collision - An attempt by two devices to transmit over the network at the same time usually resulting in the data being lost.

DNS (Domain Name System) - an internet service that translates domain names into IP addresses. For example www.google.com translates to 66.102.7.99.

Dynamic DNS - A method of keeping a domain name linked to a changing IP address using a pool of available IP addresses so you can use applications that require a static IP address.

Domain - A group of computers and devices on a network that are administered as a unit.

DHCP (Dynamic Host Configuration Protocol) - A TCP/IP protocol that dynamically assigns an IP address to a computer. Dynamic addressing simplifies network administration because the software keeps track of IP addresses rather than requiring a network administrator to do so.

Ethernet - Ethernet is the most widely installed local area network technology. It was developed during the late 1970s through a partnership of DEC, Intel, and Xerox.

Fiber Optic - A cable technology that uses glass (or plastic) threads (fibers) to transmit data. It is a very fast technology

Gateway - A device on a network that serves as an entrance to another network and routes traffic

Hardware (MAC) address - A unique address associated with a particular network device

Hub - A common connection point for computers and devices in a network that takes an incoming signal and repeats it on all other ports

Internet - Term used to refer to the world's largest internetwork, connecting thousands of networks worldwide. Also known as the world wide web (www)

IP address - a 32-bit address assigned to hosts using the TCP/IP protocol. Each computer/device on the public internet has a unique IP address. An example of an IP address is 192.168.1.

LAN (Local Area Network) – computer/data network which is confined in a limited geographical area.

MAC Address (Media Access Control) - A unique identifier attached to most forms of networking equipment. It is burned into the device and cannot be changed

Megabit - A measure of data transmission speed - 1 million bits per second or approximately 125,000 characters per second

Megabyte - A unit of measure for memory or hard disk storage capacity. 1024 megabytes – 1 gigabyte.

Network - A group of computers and devices that can communicate with each other and share resources.

Network Interface Card (NIC) - A hardware device inside a computer or other network device that enables communication with a network.

Packet - The unit of data sent across a network. Data is broken up into packets for sending over a packet switching network.

PING (Packet Internet Groper) - A command used to test connectivity to a device over a TCP/IP network.

Protocol - Rules determining the format and transmission of data over a network

RJ-45 - Standard connectors used for unshielded twisted-pair cable. Most commonly used with Cat5 network cabling.

Route - A path through an internetwork.

Router - A device that routes/forwards data across a networks.

Server - A computer that handles requests for data, email, files, and other network services from other computers (clients)
Subnet - A portion of a network that shares a common address component but is on a different segment than the rest of the network.
TI Line - A high speed dedicated data line that supports a transmission rate of 1.544 Mbps
TCP/IP - Transmission Control Protocol/Internet Protocol. A suite of protocols used as the basis of the nation's internetwork (Internet). It can also be used on internal networks.

UNC (Universal Naming Convention) Path - A UNC provides a naming convention for identifying network resources. UNC names consist of three parts, a server name, a share name, and an optional file path.

WAN (wide area network) - A network linking together networks located in other geographic areas.

Appendix

Microlearning has evolved because of the need to stress less on new technologies and more on individual learning needs. It mostly happens in an informal learning. Microlearning tools should reflect, not determine the pedagogy of a course. How technology is used is more important than which technology is used.

Microlearning is a learning strategy which is associated with 3 common approaches: short time, mobile learning and cloud computing.

There are many stages of microlearning starting from the simplest one to more complex elements. The point is that complex elements include simpler ones and in order to understand the whole issue, one has to learn from the basics. For example, one wants to learn how cheeseburger is prepared. From the first sight everything seems to be mixed up and looks very messy. But differentiating its components gives exact understanding that cheese, meat, salad, tomato and onions rings are used to prepare that delicious meal. Dividing the complex task into small chunks helps to accomplish it much more quickly.

One of the most important issues in microlearning is that it makes some transition from traditional models of learning to micro environment and shows the significance of micro dimensions in the process of learning.

As a practical part, microlearning mostly deals with digital media environment, which is already a daily reality for gaining knowledge nowadays.

1.1. Definitions

Microlearning is a learning activity that deals with small chunks of information within micro unit time. In this case, the whole tasks are subdivided into consecutive subtasks and form a "chain" of micro activities.

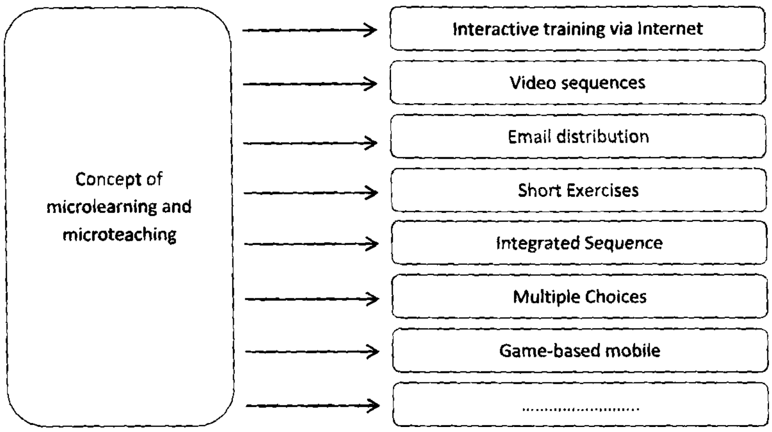
Microlearning is a term that can be used to describe the way more and more people are actually doing informal learning and gaining knowledge in microcontent, micromedia or multitasking environments, especially those that become increasingly based on web and mobile technologies. In this wider sense, the borders between microlearning and the complementary concept of microknowledge are blurring.

Microlearning deals with relatively small learning units and short-term learning activities. The "**microlearning**" refers to micro-perspectives in the context of learning, education and training

1.2 Anytime-Anywhere Access to Learning Resources

Microlearning is considered to be a learning method which is not dependent on time and place.

In other words, "just in time open learning" and "on the spot learning". Therefore, microlearning material should be built as short as possible and information has to be mobile. Since people share different lifestyles and learner's daily activities may take place in different space locations and moments of time, microlearning is definitely the most suitable form of anytime-anywhere learning.



Pic 1:133 Concept of microlearning and microteaching

The concepts of microlearning and microteaching

There are many ways to send information to a target learner. Since technology is rapidly developing, a lot of tools can be useful to operate with data. For microlearning, several specifications have to take place: Computer Assisted Learning Environment is a major field from which a lot of Web-based applications derive. Microlearning is extracted from eLearning and therefore, from web-based applications there is a need to deepen into eLearning. Nowadays, users and targer learners are connected in a global network. This make it easier for anytime/anywhere access to eLearning tools.

Computer Assisted Learning Enviroments

Web-based applications

eLearning

Microlearning

Pic 1:134 Location of Microlearning

1.3 Learning Theories for Microlearning

All the learning environments have something in common. They reflect a general cultural theory as a common understanding of knowledge absorption. Microlearning makes no exception to that, but can also be informed by a range of more recent learning approaches, projects and studies, that have focused on investigating the characteristics of adult learning during lifelong activities.

The informal learning stresses on specific parts of overall information, rather than on complete body of knowledge. This approach helps learner to focus on particular task and it supports decision making or the acquisition of a certain skill. Mobile and web technologies support microlearning

Microlearning is considered as a lifelong activity which has to enable:
- The creation of tiny connections between past and future experiences
- Conversation between the world around and mobile learning tool
- The control of learning strategy

2. Characterization of microlearning

Microlearning can be characterized as follows:

- Microlearning processes often derive from interaction with microcontent, which takes place either in designed (media) settings (eLearning) or in emergent microcontent structures like weblog postings or social bookmark managers on the World Wide Web

- Microlearning can be an assumption about the time needed to solve a learning task, for example answering a question, memorizing an information item, or finding a needed resource .Learning processes that have been called "microlearning" can cover a span from few seconds (e.g. in mobile learning) up to 15 minutes or more. There is some relation to the term microteaching, which is an established practice in teacher education.

- Microlearning can also be understood as a process of subsequent, "short" learning activities, i.e. learning through interaction with microcontent objects in small timeframes. In this case, the design, selection, feedback and pacing of repeated or otherwise 'chained' microlearning tasks comes into view.

- In a wider sense, microlearning is a term that can be used to describe the way more and more people are actually doing informal learning and gaining knowledge in microcontent, micromedia or multitasking environments (microcosm), especially those that become increasingly based on Web 2.0 and wireless web technologies. In this wider sense, the borders between microlearning and the complementary concept of microknowledge are blurring.

3. Dimensions of microlearning

The following dimensions can be used to describe or design micro learning activities:

- **Time**: relatively short effort, operating expense, degree of time consumption, measurable time, subjective time, etc.

- **Content**: small or very small units, narrow topics, rather simplex issues, etc.

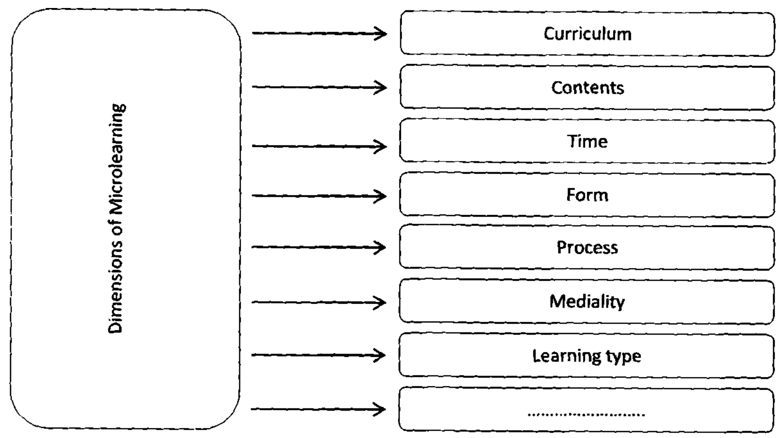
- **Curriculum**: small part of curricular setting, parts of modules, elements of informal learning, etc.

- **Form**: fragments, facets, episodes, "knowledge nuggets", skill elements, etc.

- **Process**: separate, concomitant or actual, situated or integrated activities, iterative method, attention management, awareness (getting into or being in a process), etc.

- **Mediality**: print media, electronic media, mono-media vs. multi-media, (inter-)mediated forms, etc.

- **Learning type**: repetitive, activist, reflective, pragmatist, conceptionalist, constructivist, connectivist, behaviourist; also: action learning, classroom learning, corporate learning, etc.



Pic 1:135 Dimensions of Microlearning

4. Requirements of Microlearning

At the following, a list of requirements for technologies and contents for microlearning are given:

1. **Highly transferable** and **unobstrusive** of the learner's activities, so that learners can easily download and upload the didactic materials they have been provided from one device to another

2. **Easily available and user-friendly**, enabling anytime-anywhere access to it, supported by the use of mobile phones, PDAs or other wireless communication devices connected also by Local Area Networks (LANs).

3. **Persistent,** meaning that the learning environment including all the modifications operated on it by a learner in a lifetime, should be independent from its physical MICROLEARNING instantiation on a certain device, thus easily accessible at any time through the specific technology at hand.

4. **Useful,** especially through enhancing the different activities contributing to the achievement of the learning goal(s).

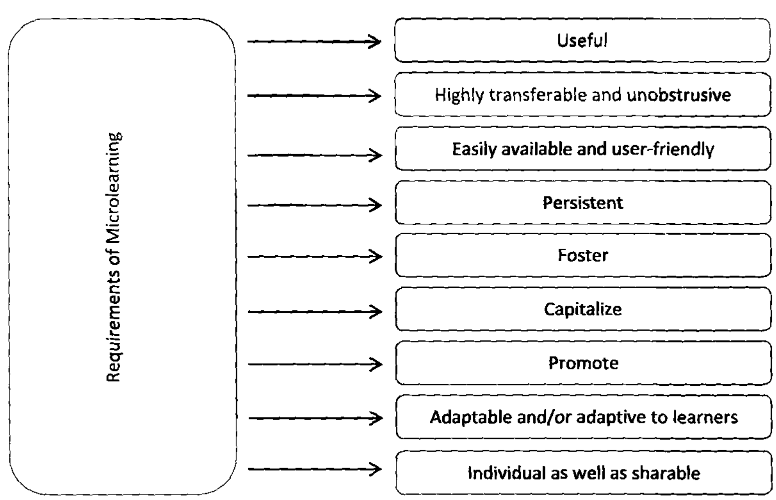
5. **Individual as well as sharable**, so that they adequately support individual learning activities but also enable learners to get or provide support from/to peers, tutors or other experts by the use of communication technology.

6. **Adaptable and/or adaptive to learners'** needs, so that different interaction styles can be selected by learners according to their preferences or skills or automatically suggested by the system according to specific learner profiles or models developed during lifetime interactions with the microlearning environment.

7. **promote** the acquisition of basic skills such as flexibility and adaptability in learners, making them aware of the very rapid and changing nature of knowledge in everyday environments,

8. **foster** the development of creativity skills, as well as problem solving and managing competences,

9. **capitalize** on learners communication abilities as a way of supporting the social production and reconstruction of knowledge during learning and working activities and try to improve them by providing learners ways of analyzing their own communication styles as recurrently practiced in the field.



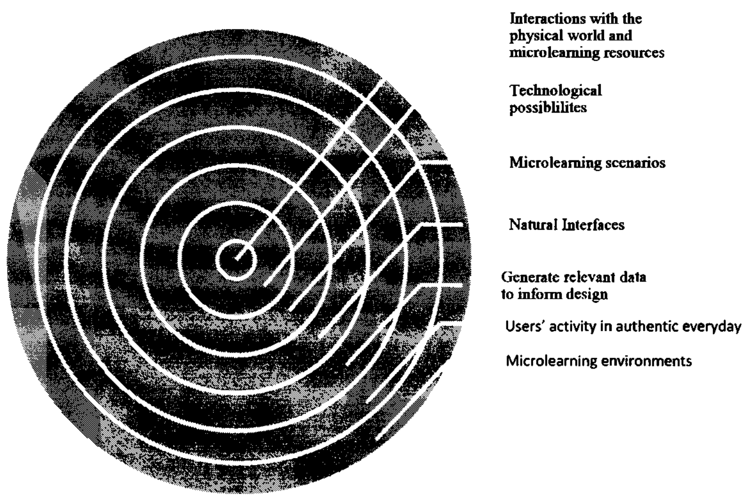
Pic 1:136 Requirements of Microlearning

5. **Design and Evaluation Approaches** MICROLEARNING

The following factors are to specify for the design and evaluation approach of Microlearning.

- microlearning environments

- users' activities in authentic everyday
- generate relevant data to inform design
- effective combinations of microcontent with natural interfaces
- microlearning scenarios
- technological possibilities
- and interactions with the physical world and with microlearning resources



Pic 1:137 Design and Evaluation Approach Microlearning

6. Examples of microlearning activities

- reading a paragraph of text, email or sms
- listening to an informational (short) podcast or an educational video-clip
- viewing a flashcard
- memorizing a word, vocabulary, definition or formula
- sorting a set of (microcontent) items by (chrono)logical order
- selecting an answer to a question

- answering questions in quizzes
- playful learning with micro-games
- composing a haiku or a short poem

7. Microlearning applications (examples)

Some examples of Microlearning activities are given in the following:

- Screensavers which prompt the user to solve small series of simple tasks after a certain amount of inactivity
- Quizzes with multiple choice options on cell phones by use of sms or mobile applications (java midlets, symbian)
- Word of the day as daily RSS-feed or email

Flashcard-software for memorizing content through spaced repetition

Recourses

1. Google – http://www.google.kz/
2. Wikipedia – http://www.wikipedia.org/
3. Cisco Inc. – http://www.cisco.com/web/learning/netacad/index.html
4. Elsevier - http://www.journals.elsevier.com/computer-networks/
5. About com- http://compnetworking.about.com/
6. Bulletin - http://www.networkingboards.com/
7. Tech Forums - http://www.tech-forums.net/pc/f44/?s2=
8. Networks Builders - http://www.network-builders.com/
9. My blog – zhamanov.blog.com

Approved and recommended by the Academic Council of the University named after Suleyman Demirel

SULEYMAN DEMIREL UNIVERSITY

1/1 Abylaikhan St., Kaskelen, Almaty,
Kazakhstan, 040900
Tel.: +7 727 307 95 65
Fax.: +7 727 307 95 58
sdu.edu.kz / info@sdu.edu.kz