BSc in Telecommunications Engineering

TEL3214

Computer Communication Networks

Lecture 02
Internetworking Models

Eng Diarmuid O'Briain, CEng, CISSP

Department of Electrical and Computer Engineering,
College of Engineering, Design, Art and Technology,
Makerere University

Table of Contents

Illustration Index

1. Internetworking Models

1.1 OSI 7 layer Model

The OSI, or Open System Interconnection, model defines a networking framework for implementing protocols in seven layers. Control is passed from one layer to the next, starting at the application layer in one station, and proceeding to the bottom layer, over the channel to the next station and back up the hierarchy.

OSI Layer		
7	Application	File, Print, database & Application services
6	Presentation	Data encryption, compression & translation services
5	Session	Dialogue control
4	Transport	End to End connection
3	Network	Routing
2	Data Link	Framing, Bridging, Switching
1	Physical	Physical network topology

Illustration 1: OSI 7 Layer Model

1.1.1 Application

This layer supports application and end-user processes. Communication partners are identified, quality of service is identified, user authentication and privacy are considered, and any constraints on data syntax are identified. Everything at this layer is application-specific. This layer provides application services for file transfers, e-mail, and other network software services. Telnet and File Transfer Protocol (FTP) are applications that exist entirely in the application level. Tiered application architectures are part of this layer.

1.1.2 Presentation

This layer provides independence from differences in data representation (e.g., encryption) by translating from application to network format, and vice versa. The presentation layer works to transform data into the form that the application layer can accept. This layer formats and encrypts data to be sent across a network, providing freedom from compatibility problems. It is sometimes called the syntax layer. Examples at this layer include Tagged Image File Format (TIFF), Joint Photographic Experts Group (JPEG), Moving Pictures Experts Group (MPEG), Musical Instrument Digital Interface (MIDI).

1.1.3 Session

This layer establishes, manages and terminates connections between applications. The session layer sets up, coordinates, and terminates conversations, exchanges, and dialogues between the applications at each end. It deals with session and connection coordination. Session Layer protocols include Structured Query Language (SQL), Remote Procedure Call (RPC), Unix X-Windows.

1.1.4 Transport

This layer provides transparent transfer of data between end systems, or hosts, and is responsible for end-to-end error recovery and flow control. It ensures complete data transfer. In IP this function is achieved using a connection oriented mechanism called Transmission Control Protocol (TCP) or a non connection oriented protocol called User Datagram Protocol (UDP).

1.1.5 Network

This layer provides switching and routing technologies, creating logical paths, known as virtual circuits, for transmitting data from node to node. Routing and forwarding are functions of this layer, as well as addressing, internetworking, error handling, congestion control and packet sequencing. This layer has two basic packet types;

1.1.5.1 Data Packets

Used to transport data through the internetwork.

1.1.5.2 Route Update Packets

Used to update neighbouring routers of new routing information i.e. Open Shortest Path First (OSPF), Enhanced Interior Gateway Routing Protocol (EIGRP) and Routing Internet Protocol (RIP). These route updates take the form of;

Address – Network or Host route is about.

Interface – The Router Interface associated with this network or host.

Metric – The distance to the network or host expressed as a hop count or bandwidth, delay, interface type etc.

1.1.6 Data Link

At this layer, data packets are encoded and decoded into bits. It furnishes transmission protocol knowledge, handles errors in the physical layer, flow control and frame synchronisation. The data link layer is divided into two sub-layers: The Media Access Control (MAC) layer (802.3) and the Logical Link Control (LLC) layer (802.2). The MAC sub-layer controls how a host on the network gains access to the data and permission to transmit it. The LLC layer controls frame synchronisation, flow control and error checking. This layer is managed by Bridge and Switching devices. Bridges are devices which manage the interconnection of Physical segments using a mainly software function whereas Switches (sometimes called Layer 2 Switches) handle the bridging function using hardware Application Specific Integrated Circuits (ASICs) and such switching is often termed wire speed switching.

1.1.7 Physical

This layer conveys the bit stream, electrical impulse, light or radio signal through the network at the electrical and mechanical level. It provides the hardware means of sending and receiving data on a carrier, including defining cables, cards and the physical aspects. Ethernet, Fast Ethernet, RS232, and Frame Relay are protocols with physical layer components. Typically we associate hubs with this layer.

1.2 Peer Level

This diagram demonstrates the communication at each level. Peer relationships exist from hop to hop across the network.

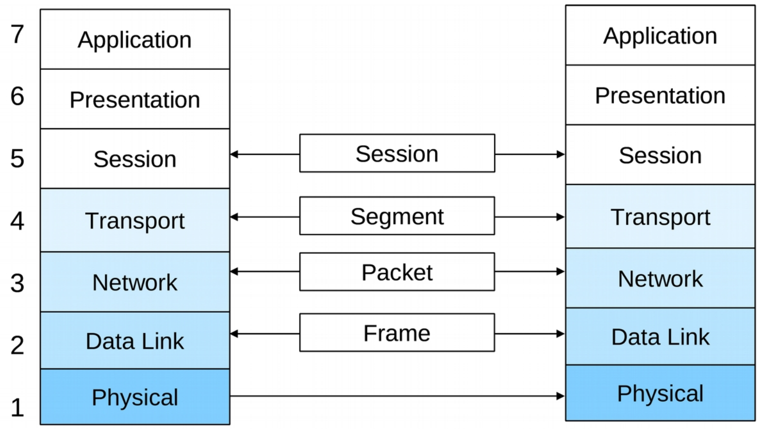

Illustration 2: Peer relationships

1.3 Protocol Mapping

Layer	Name	TCP/IP	SS 7	OSI	UMTS
7	Application	HTTP, RIP, SMTP, SMPP, SNMP, FTP, Telnet, NFS, NTP, RTP	ISUP, INAP, MAP, TUP, TCAP	FTAM, X.400, X.500, DAP	
6	Presentation	MIME, XDR, SSL, TLS		ISO 8823, X.226	
5	Session			ISO 8327, X.225	
4	Transport	TCP, UDP, SCTP		TP0, TP1, TP2, TP3, TP4	
3	Network	IP, ICMP, IPsec, ARP, BGP, OSPF	MTP-3, SCCP	X.25, CLNP	RRC
2	Data Link	Ethernet, 802.2, 802.3, 802.5, 802.11, 802.14, 802.16, PPP, HDLC	MTP-2	X.25 (LAP-B)	MAC
1	Physical	RS-232, V.35, V.34, E1, T1, 10BASE-T, 100BASE-TX, 802.11, 802.15, 802.16, DSL, DOCSIS	MTP-1	X.25, EIA/TIA-232, EIA/TIA-449, EIA-530, G.703	PHY

Illustration 3: Protocol mapping

2. TCP/IP and DoD Model

The Internet protocol suite is the set of protocols that implement the protocol stack on which the Internet runs. It is sometimes called the TCP/IP protocol suite after two of the many protocols that make up the suite: the Transmission Control Protocol (TCP) and the Internet Protocol (IP).

The Internet Protocol suite can be described by analogy with the OSI model, which describes the layers of a protocol stack, not all of which correspond well with Internet practice. In a protocol stack, each layer solves a set of problems involving the transmission of data. Higher layers are logically closer to the user and deal with more abstract data, relying on lower layers to translate data into forms that can eventually be physically manipulated.

The Internet model was designed as the solution to a practical engineering problem. The OSI model, on the other hand, was a more theoretical approach, and was built by committee. Therefore, the OSI model is easier to understand, but the TCP/IP model is more practical. It is helpful to have an understanding of the OSI model before learning TCP/IP, as the same principles apply, but are easier to understand in the OSI model.

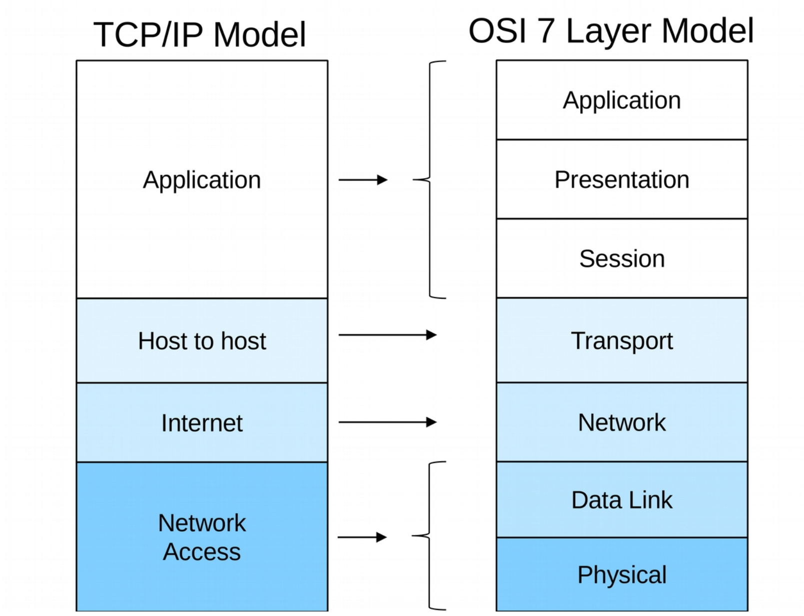

Illustration 4: Mapping TCP/IP to the OSI 7 Layer model

2.1 DoD Four-Layer Model

The DoD Four-Layer Model was developed in the 1970s for the DARPA Internetwork Project that eventually grew into the Internet.

The four layers in the DoD model:

The **Network Access Layer** is responsible for delivering data over the particular hardware media in use. Different protocols are selected from this layer, depending on the type of physical network.

The **Internet Layer** is responsible for delivering data across a series of different physical networks that interconnect a source and destination machine. Routing protocols are most closely associated with this layer, as is the IP Protocol, the Internet's fundamental protocol.

The **Host-to-Host Layer** handles connection rendezvous, flow control, retransmission of lost data, and other generic data flow management. The mutually exclusive TCP and UDP protocols are this layer's most important members.

The **Process Layer** contains protocols that implement user-level functions, such as mail delivery, file transfer and remote login.

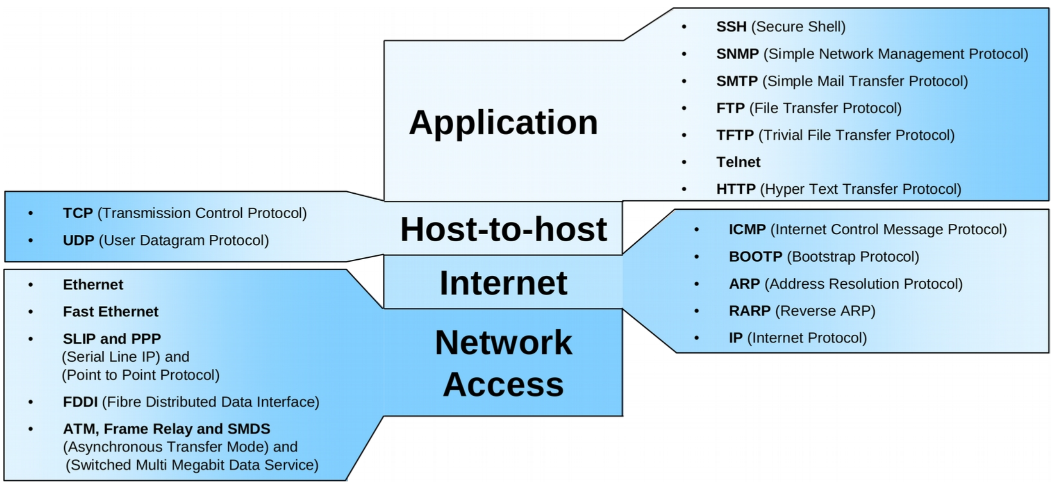

Illustration 5: TCP/IP

3. Domain Name System

The Domain Name System (DNS) is an essential part of the Internet. It is the standard by which Internet connected devices translate user-friendly domain names like "www.netlabsug.org" into an IP address like 2012:7f6::1 or 72.163.4.161.

3.1 Root nameservers

The top hierarchy of DNS are root name servers delegated by the Internet Corporation for Assigned Names and Numbers (ICANN) to a number of companies and organisations to ensure resiliance. Examples of such organisations are Verisign, University of Southern California, Internet Systems Consortium (ISC) and Réseaux IP Européens (RIPE). Each of these organisations manage a distributed set of servers right across the world and are collectively called the root zone. These root servers contain the global list of IP Addresses for the name servers of each of the Top Level Domains (TLD).

3.2 Top Level Domains

The Internet is organised into a hierarchy of domains, administered by the respective registrars and domain name holders. The TLDs in the root zone are:

- generic TLDs (gTLD): .com, .net, .int, .edu, .gov, .mil and .org
- country code TLDs (ccTLD): two-letter codes for each country, .ie for Ireland or .ug for Uganda.

3.2.1 Internationalised Domain Names

In 2009, ICANN decided to implement a new class of TLD called Internationalised Domain Names (IDN), assignable to countries and independent regions, similar to the rules for ccTLDs. However, the domain names may be any desirable string of characters, symbols, or glyphs in the language-specific, non-Latin alphabet or script of the applicant's language, within certain guidelines to assure sufficient visual uniqueness.

For example Egypt, Saudi Arabia and the United Arab Emirates were the first three countries to use Arabic characters in the last portion of their Internet domain names, such as dot-eg (Egypt), dot-sa (Saudi Arabia) or dot-ae (United Arab Emirates). They are called country code top-level domains or ccTLDs. An example is the IDN ccTLD for Saudi Arabia (.السعودية).

3.2.2 Expansion of gTLDs

In 2012 it was decided by iCANN to expand the gTLD set to allow a registry to register any word or set of characters. This however has come under some criticism from many trade associations and large companies claiming it can confuse user and spreads Internet searches across a slew of new TLDs. Example of these are

.academy .rugby .club .cash .christmas .mom .dog

3.3 Nameservers

A nameserver is a server that stores the DNS records, such as IPv4 address records (A) or IPv6 address Quad-A records (AAAA), name server records (NS), mail exchanger records (MX), canonical name (alias) records (CNAME) and pointer records (PTR) that resolve IP address to a domain/hostname (reverse of A and AAAA).

3.3.1 Authoritative Name Server

An authoritative nameserver holds the actual DNS records for a particular domain.

3.3.2 Recursive Name Server

A recursive nameserver or recursive resolver is a DNS server that queries an authoritative nameserver to resolve a domain to an address. Actually when a request is made of a recursive nameserver it first checks to see if it has an existing cached entry with a valid Time-To-Live (TTL). If it has it responds with that, otherwise it starts the recursive process of going through the authoritative DNS hierarchy.

3.4 Query example

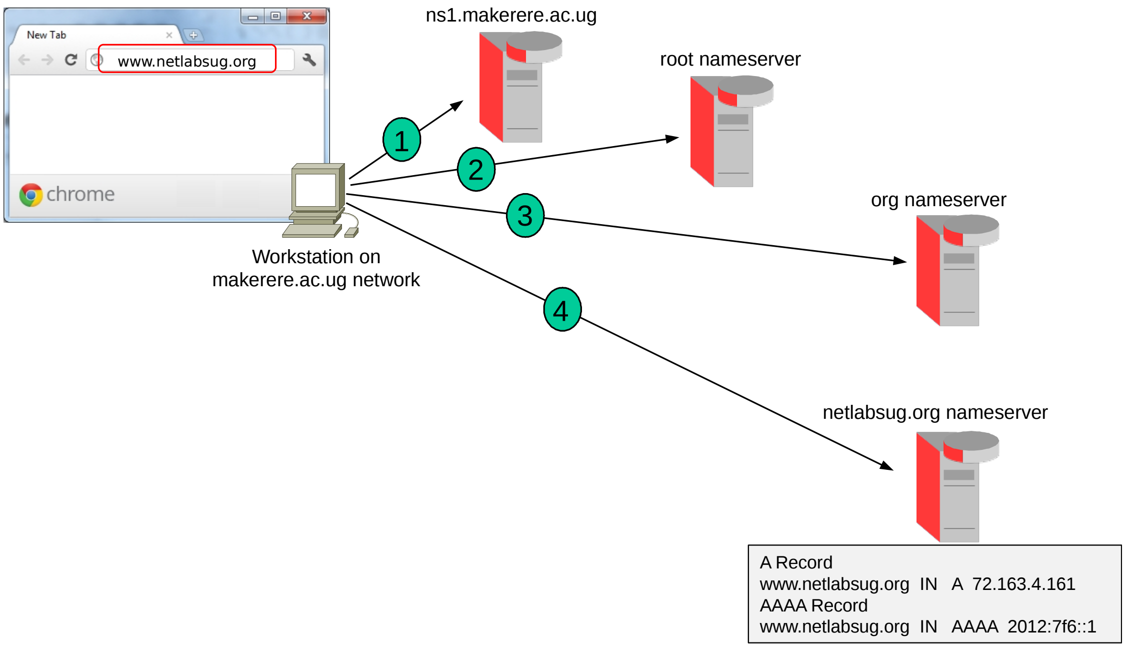

Illustration 6: DNS Query

Illustration 6 Is an example where a workstation on the makerere.ac.ug network makes a DNS query of the nameserver *ns1.makerere.ac.ug* for the domain *www.netlabsug.org*.

As the requested host is not in the domain *ns1.makerere.ac.ug* then the nameserver acts in a recursive mode, checking if it has a cached entry. Assuming it doesn't have a cached entry, it will therefore direct the query to the TLD for the requested domain within the root zone. The query then reaches out to the the nearest root server which returns an IP address for the .org nameserver. A request to this IP address is responded to with the IP address of the *netlabsug.org* nameserver which is authoritative for the domain *netlabsug.org*. It looks up its database and gets the A and AAAA records for the host *www*. This is then returned to the requesting workstation so a resolution of domain name to IP address can be made.