Computer Hardware & Networking& Server Configurations (H7E3 04)

UNIT 05: Network devices and protocols

JAVA INSTITUTE for Advanced Technology

INNOVATIONS FOR THE KNOWLEDGE SOCIETY

Lecturer: Thilina Rajakaruna

BEng(SEng), SCQF Level 7(EQF 5)(SEng), SCQF Level 8(EQF 5)(SEng), PgDip(Edu)

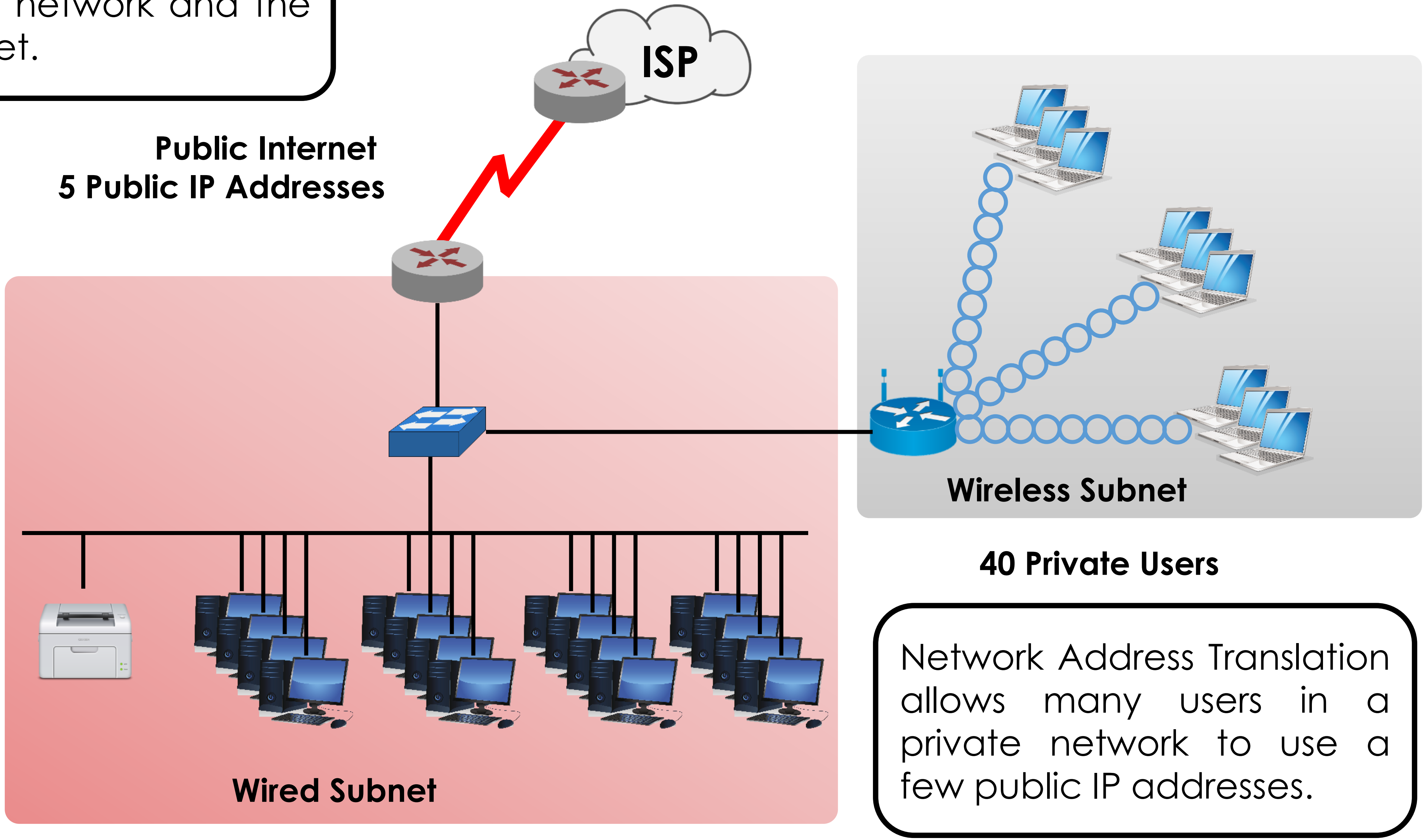
Network Address Translation (NAT)

- Routers are required to route between subnets on an internal network, regardless of whether the IP address range is public or private. However, if the address range is private, private networks cannot be routed across the public Internet. Therefore, how do host devices using a private addressing scheme communicate across the Internet? Network Address Translation (NAT) must be enabled on the device connecting the private network to the ISP network.

- NAT allows a large group of private users to access the Internet by sharing one or more public IP addresses. Address translation is similar to how a telephone system works in a company. As a company adds employees, at some point, they no longer run a public phone line directly to each employee desk. Instead, they use a system that allows the company to assign each employee an extension number. The company can do this because not all employees use the phone at the same time. Using private extension numbers enables the company to purchase a smaller number of external phone lines from the phone company.

- NAT works similarly to a company phone system. Saving registered IP addresses is one of the main reasons that NAT was developed. NAT can also provide security to PCs, servers, and networking devices by withholding their actual IP host addresses from direct Internet access.

NAT required between the local private network and the public internet.



40 Private Users

Network Address Translation allows many users in a private network to use a few public IP addresses.

- The main advantages of NAT are that IP addresses can be re-used and many hosts on a single LAN can share globally unique IP addresses. NAT operates transparently and helps shield users of a private network against access from the public domain.
- In addition, NAT hides private IP addresses from public networks. The advantage to this is that NAT operates much like an access control list, not allowing outside users to access internal devices. The disadvantage is that additional configurations are required to allow access from legitimate, external users.

- Another disadvantage is that NAT has an impact on some applications that have IP addresses in their message payload, because these IP addresses must also be translated. This translation increases load on the router and hinders network performance.

Advantage of NAT	Disadvantage of NAT
• Public IP address Sharing	• Incompatibility With Certain applications
• Transparent to end users	• Hinders legitimate Remote Access
• Improved Security	• Performance Reduction Caused by Increased Router Processing.
• LAN Expandability or Scalability	
• Local Control Including ISP Connectivity	

IP address

Short for **Internet Protocol address**, an **IP** or **IP address** is a number used to indicate the location of a computer or other device on a network using TCP/IP. These addresses are similar to those of your house; they allow data to reach the appropriate destination on a network and the Internet.

IPv4

IPv4

Types of IPv4 addresses can be categorized into five classes namely: Class A, Class B, Class C, Class D and Class E. Class A, B and C are commonly used for devices to connect to the internet. Each class provides a range of IP addresses and the following are the classes:

IP address (IPv4)

Must be 4 decimals

0-255 →

0.0.0.0 – 255.255.255.255

32 bits / 4 bytes

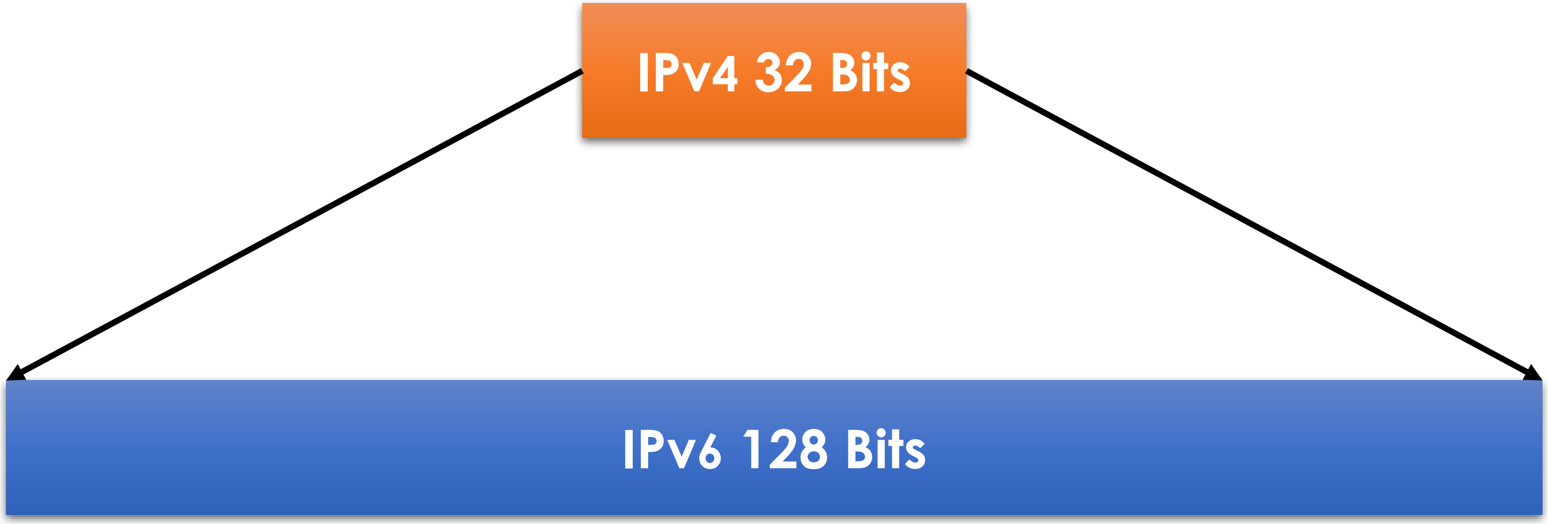
separate with ‘.’

IPv6

CONTRASTING IPv4 AND IPv6 ADDRESSING

- The IPv4 address space provides approximately 4.3 billion addresses. Of that address space, approximately 3.7 billion addresses are actually assignable. The other addresses are reserved for special purposes such as multicast, private address space, loopback testing, and research. There are few IPv4 address ranges available for assignment. Some ISPs are beginning to pass out IPv6 address assignments.

- An IPv6 address is a 128-bit binary value, which can be displayed as 32 hexadecimal digits. It provides 3.4 X 10^38 IP addresses.



IPv4

- 32 Bits or 4 Bytes Long
- 4,200,000,000 Possible addressable Nodes.

IPv6

- 128 Bits or 16 Bytes: 4 times the Bits of IPv4
- 340,284,366,920,938,463,374,607,432,768,211,456 Possible Addressable Nodes.

IPv6 offers powerful enhancements to IPv4. The enhancements include:

- Mobility and security
- Simpler header
- Address formatting

Mobility and Security

- Mobility enables people with mobile network devices to move around in networks. Mobile IP is an IETF standard that is available for both IPv4 and IPv6. This standard enables mobile devices to move without breaks in established network connections. IPv4 does not support this kind of mobility. Mobility is an IPv6 feature.

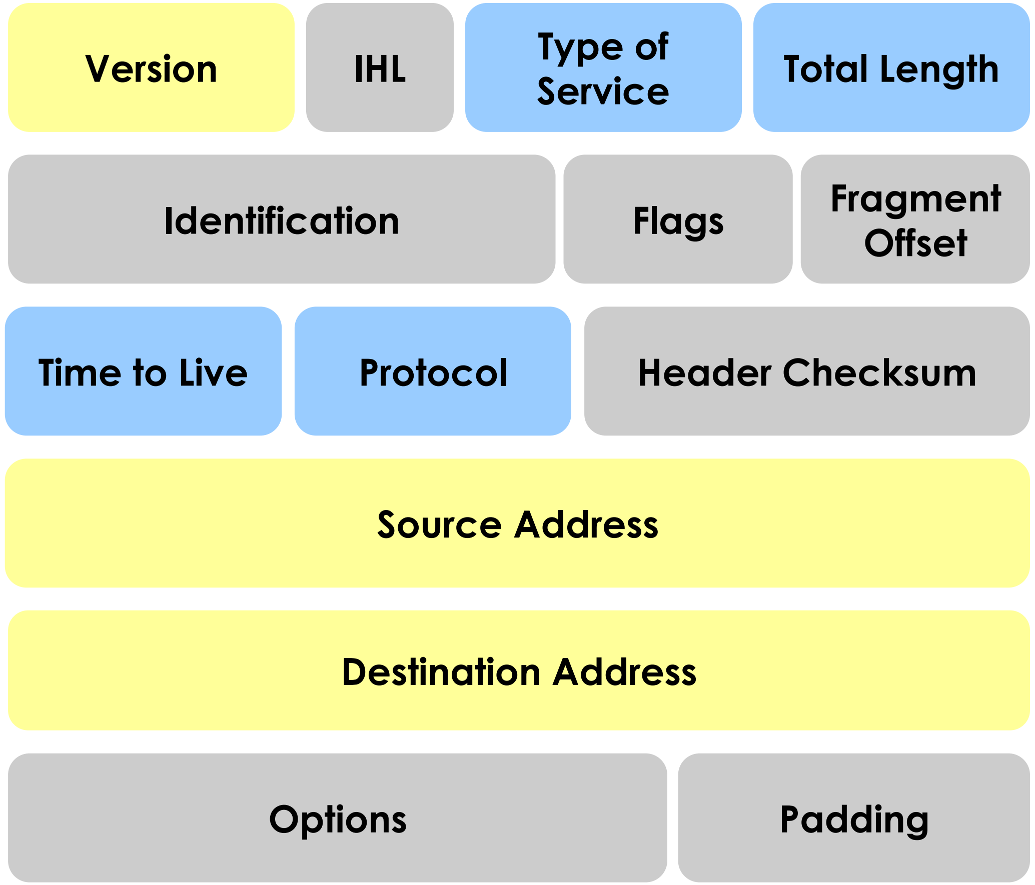
- IPSec is the IETF standard for IP network security. It is available for both IPv4 and IPv6. The IP network security functions are essentially identical in both environments. IPSec is more tightly integrated in IPv6 and can be enabled on every IPv6 node.

Simpler Header

- The header used for IPv6 increases routing efficiency by reducing the number of entries in the routing tables.

- No broadcasts are associated with IPv6. With IPv4, the broadcasts created generate a high level of traffic within the network. This traffic creates an event known as a broadcast storm and the entire network ceases to function. IPv6 replaces broadcasts with multicasts and anycasts.

IPv4 Header



Version | IHL | Type of Service | Total Length

Identification | Flags | Fragment Offset

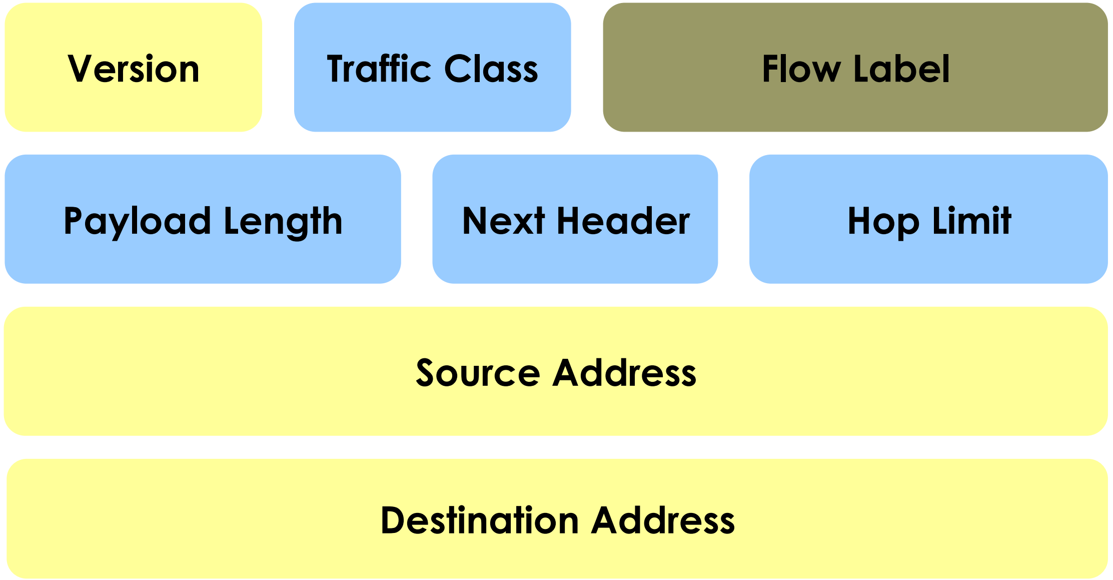
Time to Live | Protocol | Header Checksum

Source Address

Destination Address

Options | Padding

IPv6 Header



Version | Traffic Class | Flow Label

Payload Length | Next Header | Hop Limit

Source Address

Destination Address

Legend

🟨 Field names retained from IPv4 to IPv6.

⬜ Fields not retained in IPv6.

🟦 Name & Position changed in IPv6.

🟩 New Field in IPv6.

Address Formatting

- Colons separate entries in a series of eight 16-bit hexadecimal fields that represent IPv6 addresses. The hexadecimal digits A, B, C, D, E, and F represented in IPv6 addresses are not case-sensitive.

- Unlike IPv4, the IPv6 address string format is not fixed. The following guidelines are used for IPv6 address string notations:

- The leading 0s in a field are optional: 09C0 equals 9C0 and 0000 equals 0.

- One or more groups of 0s can be omitted and replaced with "::". Only one "::" is allowed in an address.

- An unspecified address is written as "::" because it contains only 0s.

- Using the "::" notation greatly reduces the size of most addresses. For example, FF01:0:0:0:0:0:0:1 becomes FF01::1. This formatting is in contrast to the 32-bit dotted decimal notation of IPv4. The primary type of IPv6 address is called unicast.

IPv6 Address Representation

Format :

- X:X:X:X:X:X:X:X Where X is a 16-bit Hexadecimal Field Case-insensitive for hexadecimal A, B, C, D, E and F
- Leading Zeros in a field are optional
- Successive fields of zeros can be represented as :: only once per address.

Examples :

- 2031:0000:130F:0000:0000:09c0:876A:130B
  - Can be Represented as 2031:0:130f::9c0:876a:130b
  - Cannot be represented as 2031::130f::9c0::876a::130b
- FF01:0:0:0:0:0:0:1 → FF01::1
- 0:0:0:0:0:0:0:1 → ::1
- 0:0:0:0:0:0:0:0 → ::

IP address (IPv6)

8 hexadecimal numbers

0000-FFFF

Separate by colon (:)

128 bits / 16 bytes

OSI AND TCP IP REFERANCE MODEL

7 Layers OSI Model

OSI Model
(Open Systems Interconnection Model)

History

- Rapid growth of computer networks caused compatibility problems

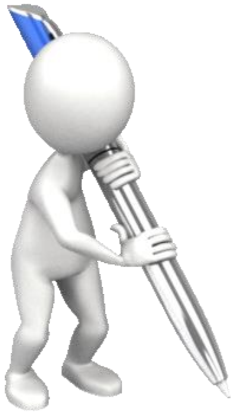
- ISO recognized the problem and released the OSI model in 1984

- OSI stands for Open Systems Interconnection and consists of 7 Layers

- The use of layers is designed to reduce complexity and make standardization easier

Mnemonics

07). Application	Away
06). Presentation	Pizza
05). Session	Salami
04). Transport	Throw
03). Network	Not
02). Data Link	Do
01). Physical	Please



7 Layers of the OSI Model

Layer	Example
07). Application	HTTP, FTP, SMTP
06). Presentation	ASCII, MPGE, BCD
05). Session	BOOTP, NetBIOS, DHCP, DNS
04). Transport	TCP, UDP, SPX
03). Network	IP, IPX, ICMP
02). Data Link	Ethernet, Token Ring, Frame Relay
01). Physical	Bits, Interfaces, Hubs

Flat Addressing

- Flat addressing schemes do not provide anything other than a unique identifier. They provide no real information about where the object being addressed resides.

- Example:

  SSN# (may provide insight to where the person was born, but not to where they are now)

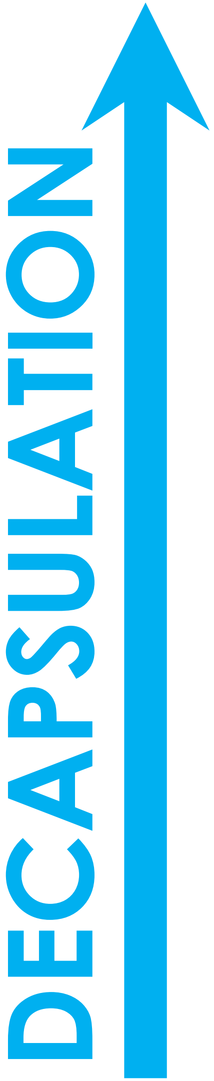
Hierarchical Addressing

- Hierarchical addressing schemes provide layers or a hierarchy to the address that provide information about where the addressed object exists within the hierarchy.

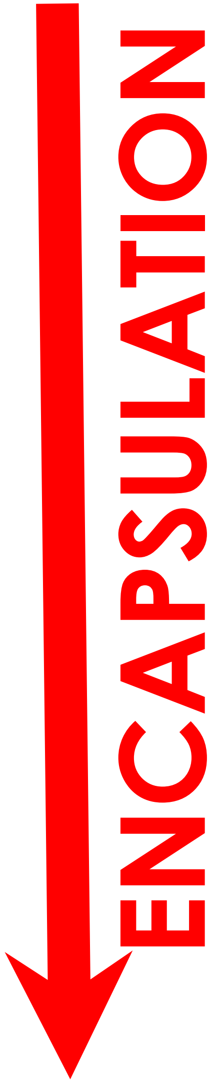
- Example:

  phone numbers (area code, local prefix, and four digit number unique to that area code/prefix combination).

Protocol Data Units and the OSI Model



Layer	Protocol Data Unit Name
07). Application	Data
06). Presentation	Data
05). Session	Data
04). Transport	Segment / Datagram
03). Network	Packet
02). Data Link	Frame
01). Physical	Bit



Layer 1: The Physical Layer

- Defines physical medium and interfaces
- Determines how bits are represented
- Controls transmission rate & bit synchronization
- Controls transmission mode: simplex, half-duplex, & full duplex
- Protocol Data Units : Bits
- Devices: hubs, cables, connectors, etc…

Layer 2: The Data Link Layer

- Protocol Data Units : Frames
- Keeps Link alive & provides connection for upper layer protocols
- Based on physical (flat) address space
- Physical addresses are fixed and don’t change when the node is moved
- Medium/media access control

Layer 3: The Network Layer

- Protocol Data Units : Packet
- End to end delivery of packets
- Creates logical paths
- Path determination (routing)
- Hides the lower layers making things hardware independent

- Uses logical hierarchical addresses
- Logical hierarchical addresses do change when a node is moved to a new subnet
- Devices: routers, firewalls

Layer 4: The Transport Layer

- Protocol Data Units : Segment
- Service Point Address (more often called a port) used to track multiple sessions between the same systems. SPA’s are used to allow a node to offer more than one service (i.e. it could offer both mail and web services)

- This layer is why you have to specify TCP or UDP when dealing with TCP/IP
- Connection oriented sessions require the sender to first request a connection, the receiver to acknowledge the connection, and that they negotiate how much data can be sent/received before its reception is acknowledged

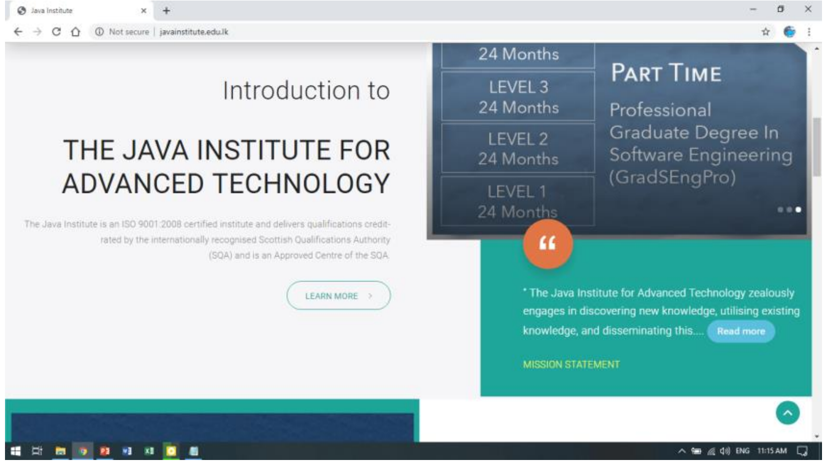
- Uses acknowledgements & retransmission for error correction
- Example: TCP (used by things like telnet, http)

Transport Layer Protocols

- The two protocols that operate at the transport layer are **Transport Control Protocol (TCP)** and **User Datagram Protocol (UDP)**
  - TCP is considered reliable, because it ensures that all of the data arrives at the destination.
  - UDP does not provide for any reliability.

TCP - Transport Control Protocol

SMPT / POP(E-Mail)



Introduction to

THE JAVA INSTITUTE FOR ADVANCED TECHNOLOGY

The Java Institute is an ISO 9001:2008 certified institute and delivers qualifications credit-rated by the internationally recognised Scottish Qualifications Authority (SQA) and is an Approved Centre of the SQA.

24 Months

LEVEL 3
24 Months

LEVEL 2
24 Months

LEVEL 1
24 Months

PART TIME

Professional Graduate Degree In Software Engineering (GradSEngPro)

" The Java Institute for Advanced Technology zealously engages in discovering new knowledge, utilising existing knowledge, and disseminating this....

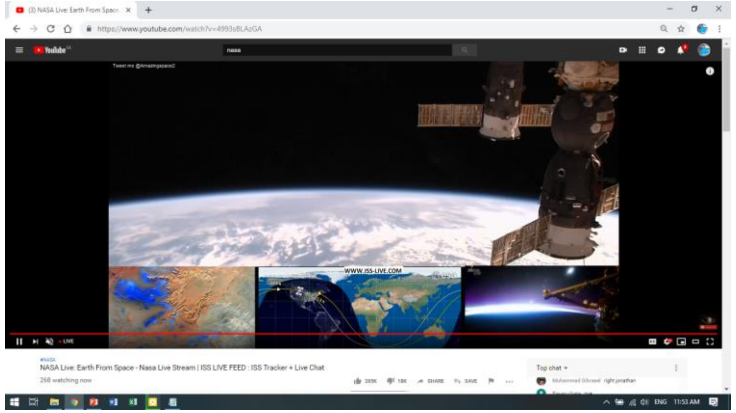
HTTP

Required Protocol Properties :

- ➢ Reliable
- ➢ Acknowledge data
- ➢ Resends Lost Data
- ➢ Delivers Data in Sequenced Order.

UDP - User Datagram Protocol

IP Telephone



(3) NASA Live: Earth From Space
https://www.youtube.com/watch?v=4993sBLAzGA
YouTube
nasa
Tweet me @Amazingspace2
WWW.ISS-LIVE.COM
LIVE
#NASA
NASA Live: Earth From Space - Nasa Live Stream | ISS LIVE FEED : ISS Tracker + Live Chat
268 watching now
285K
18K
SHARE
SAVE
Top chat
ENG
11:53 AM

Streaming Live Video

Required Protocol Properties :

- Fast
- Low Overhead
- Does not Require Acknowledgments
- Does not Resend Lost Data
- Delivers Data as it Arrives

Transport Layer Protocols

- TCP and UDP use a source and destination port number to keep track of application conversations.

- The destination port number is associated with the destination application on the remote device.

- The source port number is dynamically generated by the sending device.

Layer 5: The Session Layer

- Protocol Data Units : Data (from here on up)
- Sometimes called the dialog controller, this layer establishes, maintains, and terminates sessions between applications
- Sets duplex between applications
- Defines checkpoints for acknowledgements during sessions between applications

- Provides atomization – Multiple connections can be treated as one virtual session. If one fails or is terminated, all should be terminated.
- Identifies raw data as either application data or session control information
- Uses fields provided by layers 3 & 4 to track dialogs between applications / services

- Provides translations for naming services
- Ex: RPC, X-Windows, LDAP, NFS

Layer 6: The Presentation Layer

- Protocol Data Units : Data (from here on up)
- Data formatting, translation, encryption, and compression
- Ex: ASCII, BCD, Unicode

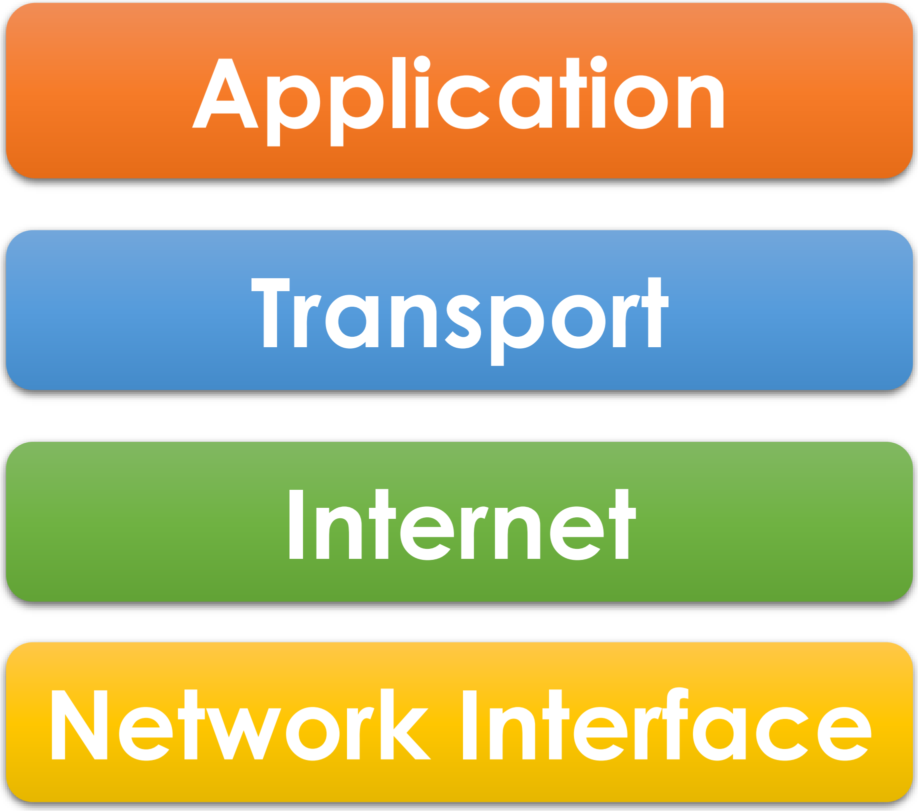
Layer 7: The Application Layer

- Protocol Data Units : Data (from here on up)
- Provides communication services to applications
- Ex: HTTP, FTP, SMTP,DNS,DHCP,POP3

TCP IP MODEL

- Much older than OSI model
- Consists of 4 layers instead of 7
- TCP/IP model can be mapped to the OSI model

TCP / IP



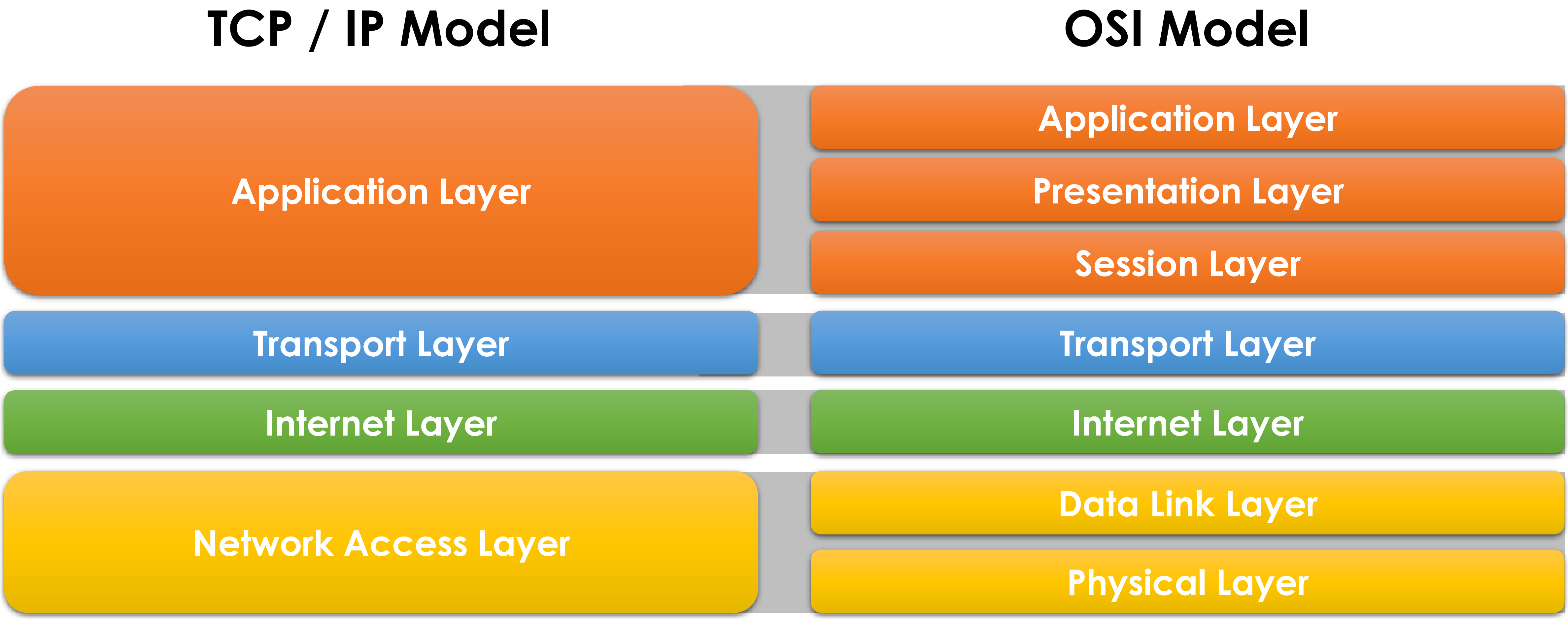
Application

Transport

Internet

Network Interface

TCP IP vs. OSI

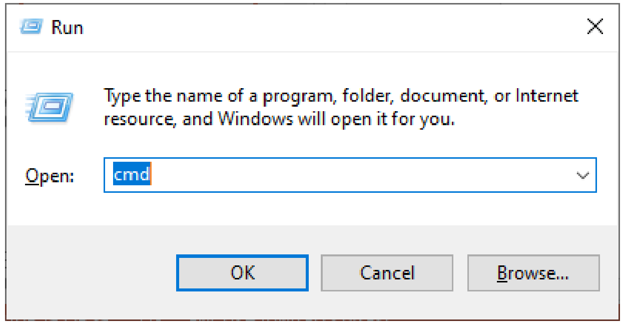


TCP / IP Model	OSI Model
Application Layer	Application Layer
	Presentation Layer
	Session Layer
Transport Layer	Transport Layer
Internet Layer	Internet Layer
Network Access Layer	Data Link Layer
	Physical Layer

Network Tools

Access Command Prompt Codes

The best command prompt trick is how easy it is to access it. On Windows XP, Vista, Windows 7 or Windows 8 just press and hold the **Windows Key + R** on your keyboard. The other way to access the DOS Command prompt is to simply go to your **Windows Start menu**, Then go to **Run**. When the little box pops up you type in **cmd**. Once the Black Command Prompt pops up you can type any of these commands in and have some fun



Run

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: cmd

IPCONFIG Command

ipconfig

Is used to find out your current TCP/IP settings. With IPCONFIG you can find out your IP Address, find your Default Gateway and find your Subnet Mask. This is a very handy network tool for finding your local IP address.

IPCONFIG Command

ipconfig /all

To display all your IP information for all adapters. With ipconfig /all you can also find out your DNS Server and MAC Address. This will show your full TCP/IP configuration for all adapters on your Windows machine. You can find out your own IP Address as well as your default gateway.

IPCONFIG Command

ipconfig /release

To release your current IP information and obtain a new IP Address from the DHCP server.

IPCONFIG Command

ipconfig /renew

Used to renew your IP Address if you have it set to obtain IP Address automatically.

IPCONFIG Command

ipconfig /displaydns

This shows your current DNS Resolver Cache Logs.

IPCONFIG Command

ipconfig /flushdns

The Flush DNS Command flushes or clears your current DNS Resolver Cache Logs.

Getmac Command

- How do I find my MAC Address you might ask?
- If you open up the command prompt you simply type getmac to get your computers local MAC address.

Contact Me ...

Email : thilina.jiat@gmail.com

THANK YOU