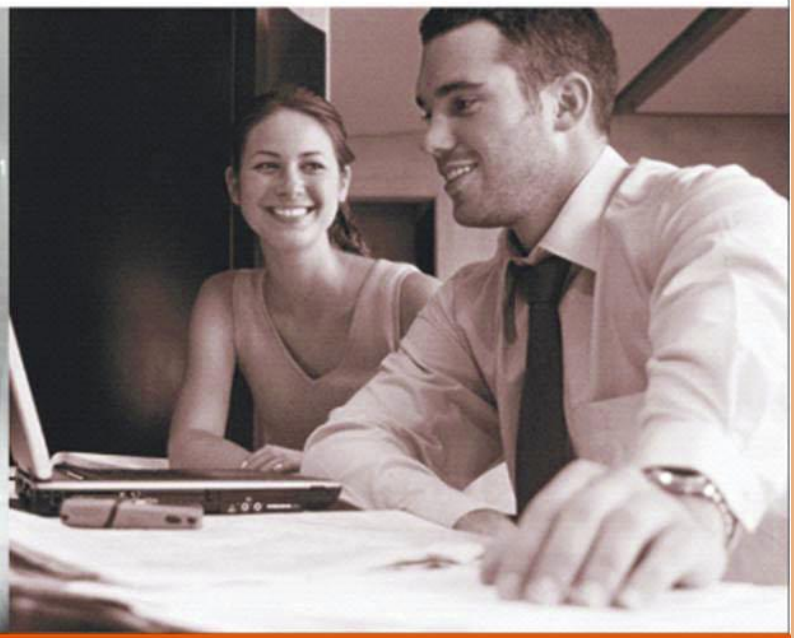
D-Link Network Associate

Version 1.2



Outline

- Module 1: What is Networking
- Module 2: OSI Reference Model and TCP/IP
- Module 3: IP Addressing and Subnetting
- Module 4: WLAN Fundamental
- Module 5: Cloud Computing Basics
- Module 6: Network Application

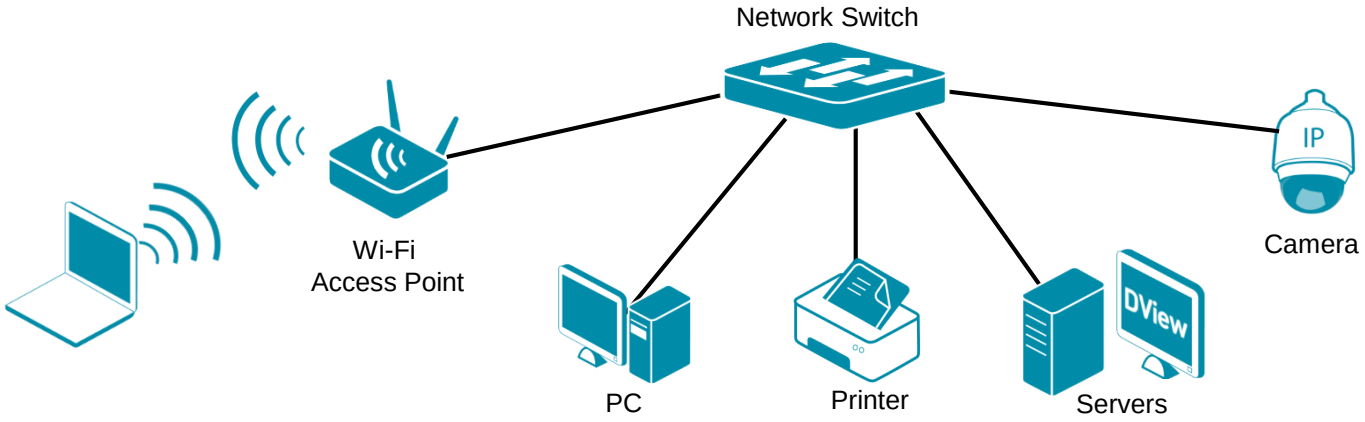
Module 1

What is Networking

What is Networking

- Networking is linking two or more computing devices together for the purpose of sharing resources:
  - Files (documents, images, media, etc.)
  - Data (application data, streaming video, audio, etc.)
  - Services (websites, printing, storage, etc.)
  - Hardware devices (cameras, printers, scanners, etc.)

- Networks can be small with just two devices or large consisting of thousands of devices.

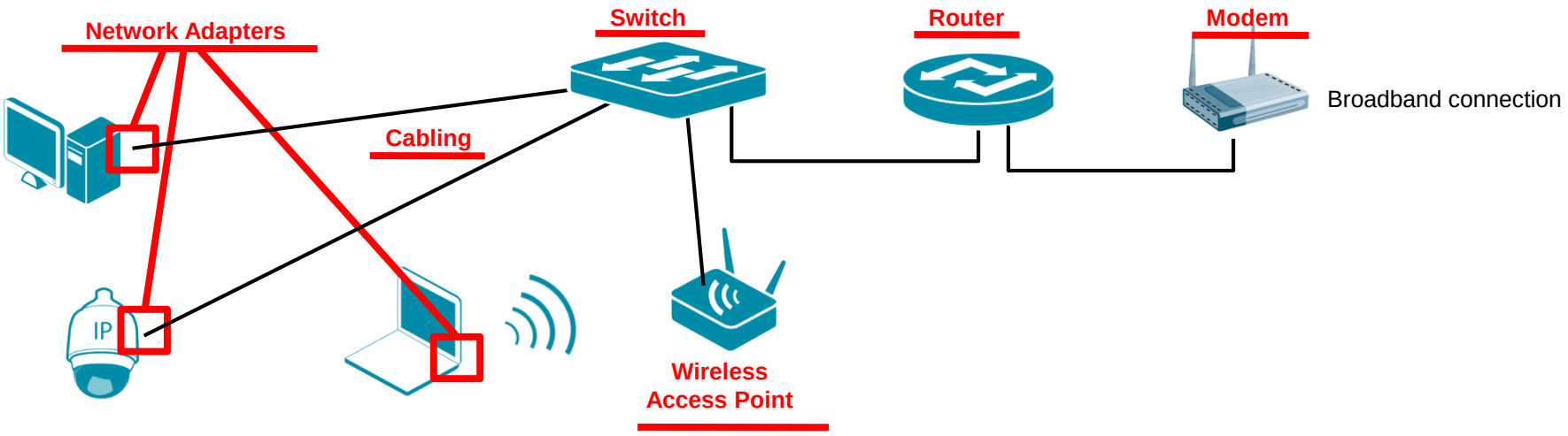


Purpose of a Network

- Communication
  - E-mail, chat, messaging
- Information
  - Web services, search engines
- Interconnectivity
  - Virtual Private Networks (VPNs) through the Internet
- Business
  - E-commerce, video conferencing
- Entertainment
  - Gaming, movies
- Education
  - E-learning, etc.

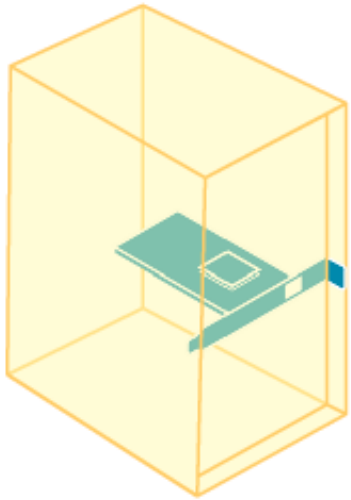
Network components

- Common components which are used to create a network:
  - Network adapter (Network Interface Controller, NIC). Can be wired or wireless;
  - Cable;
  - Switch or hub;
  - Wireless Access Point;
  - Router (to connect to other LANs or WAN);
  - Modem (to connect to WAN).



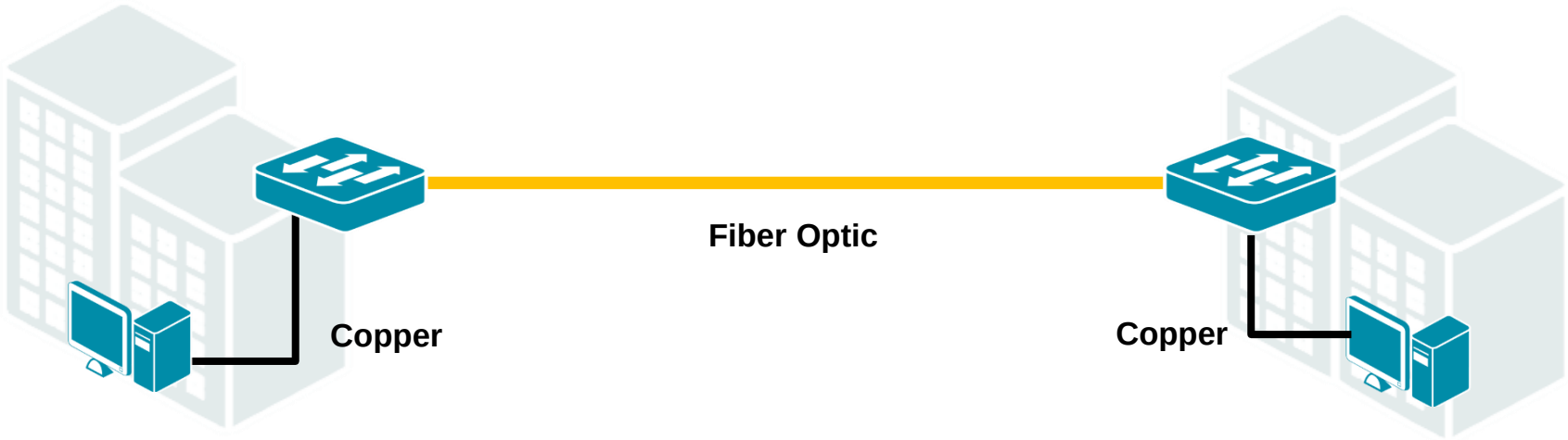
Network components – Network adapter

- A network adapter, network card more commonly referred to as a Network Interface Card (NIC),
- A NIC is a piece of computer hardware that physically makes the connection between the computer and the network cable
- A NIC can make the connection between the computer and the radio wave over a wireless network.
- The NIC is assigned a unique address called an MAC (media access control) address.

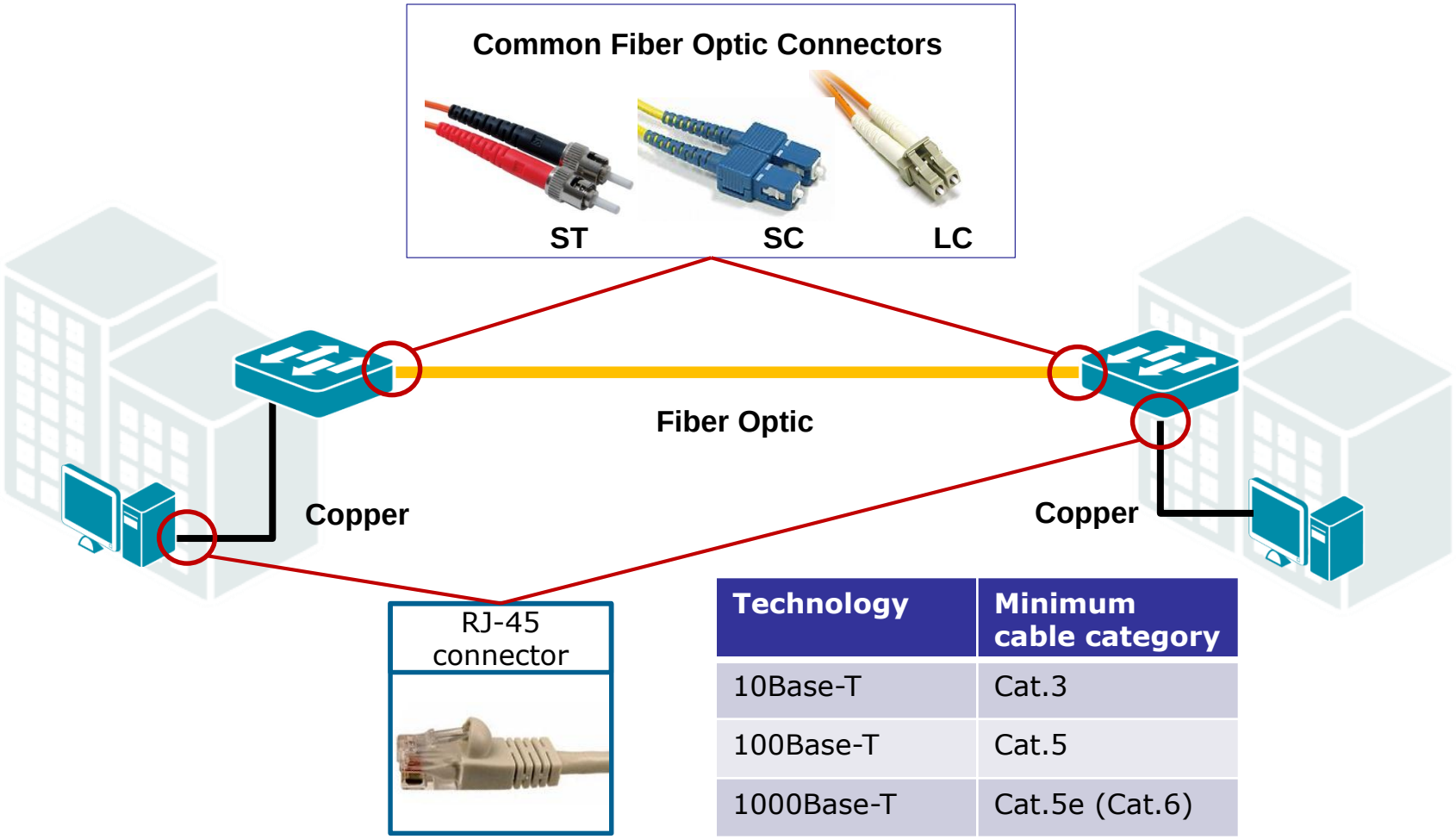


Network component - cable

- Copper
  - UTP – Unshielded Twisted Pair, STP – Shielded Twisted Pair
  - 100m maximum
  - Most common on LANs
- Fiber Optic
  - Used where cable length is over 100m
  - Single mode fiber – longer distances, more expensive
  - Multimode fiber – shorter distances, less expensive
  - Common for site-to-site, switch-to-switch connections



Network component - cable

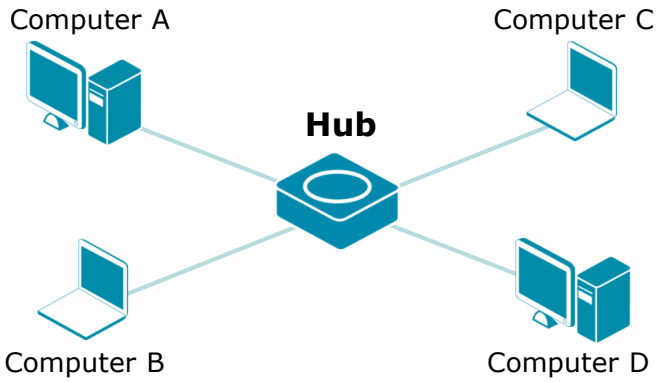


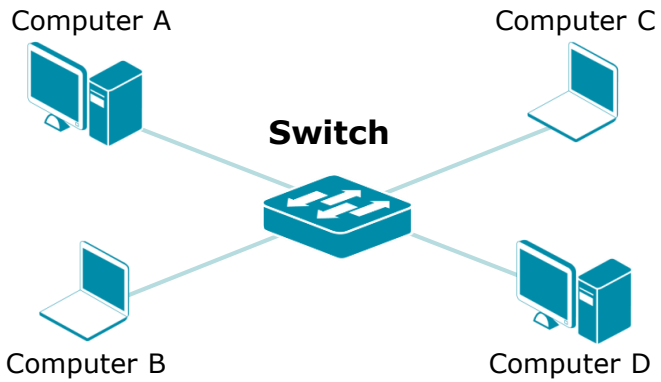
Technology	Minimum cable category
10Base-T	Cat.3
100Base-T	Cat.5
1000Base-T	Cat.5e (Cat.6)

Network component – hub and switch

- Hub:
  - A hub is defined as the networking device that is used to aggregate computers to build a small network. A hub does not manage any of the traffic that comes through them.

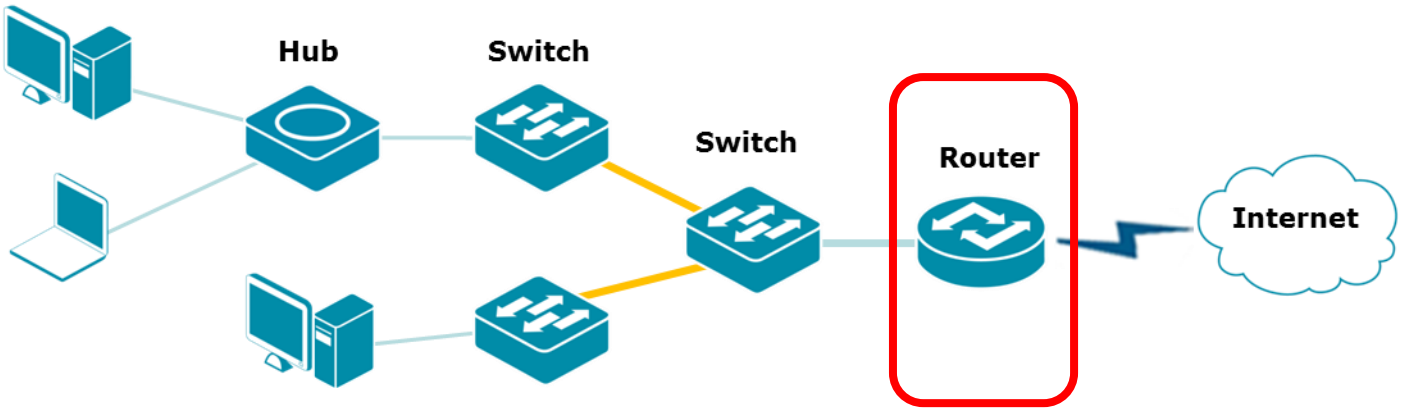
- Switch :
  - A network switch is a hardware device that joins multiple computers together to form one local area network. Mostly network switches appear nearly identical to network hubs, but a hub is less intelligent than a switch.





Network component - router

- A router is a network devices which is used to deliver data packets from one network to another.
- It also make a decision where packets should move based on the destination information in a packet header
- Routers are classified as Network Layer devices in the OSI model



Network component - wireless access point

- A wireless access point(AP) device acts as a central connection point or 'Hub' for any clients wirelessly.
- Access Points can be divided into two categories:
  - Standalone access points have switch-like intelligence.
  - Unified access points get their configuration from a centralized device called a WLAN controller.
- The Service Set Identifier (SSID) is the WLAN's logical name. It differentiates one WLAN from another, so all devices attempting to connect to a specific WLAN must use the same SSID.

Types of networks

- **LAN** - Local Area Network

  Network in a small geographical area such is home, office, school.

- **MAN** – Metropolitan Area Network

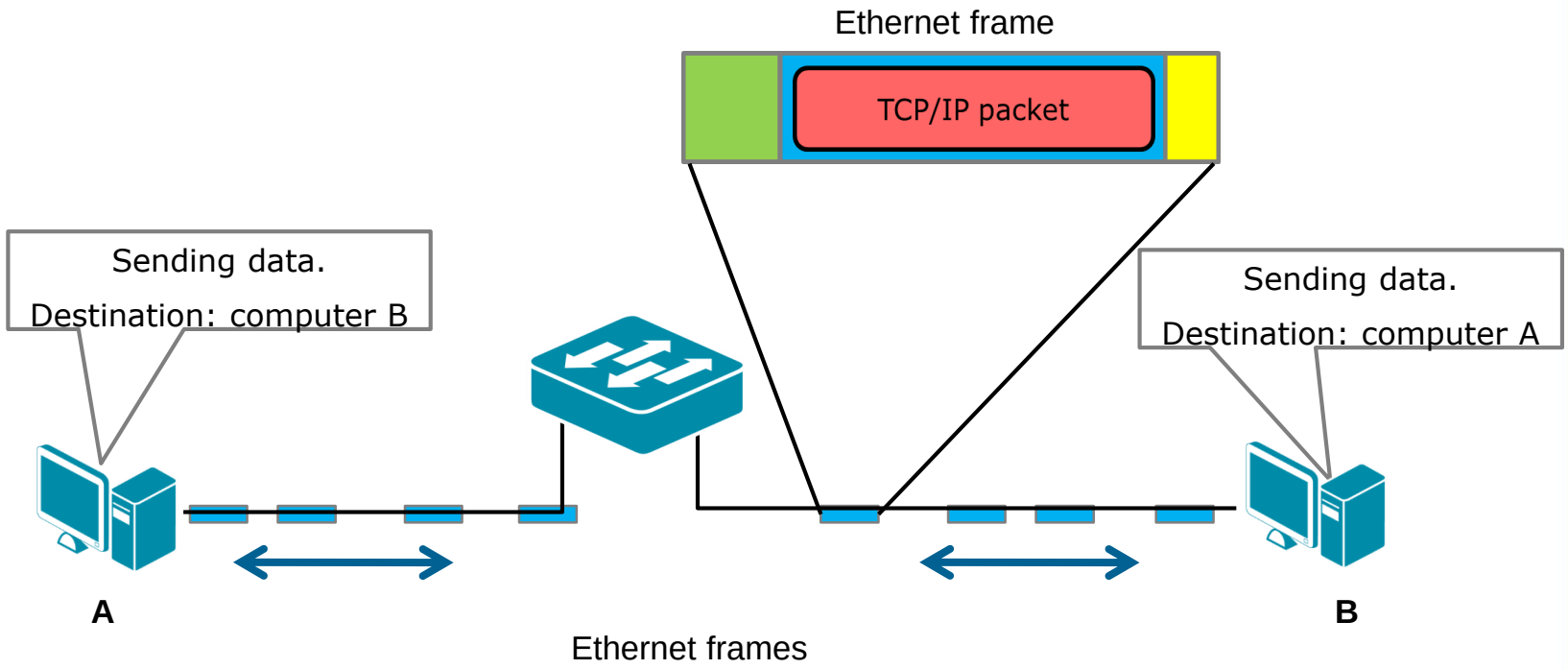
  Network over a larger geographical area such as a City or a University Campus.

- **WAN** – Wide Area Network

  Network over an extremely large areas, it can reach across cities, states, or even across the world. The Internet is the world's largest public WAN.

Common LAN communication protocols

- Ethernet is a communication protocol embedded in LAN devices. Devices on LAN communicate using Ethernet frames.
- Ethernet frames carry other protocol's information, i.e. TCP/IP protocol.
- Legacy protocols such as Token Ring and FDDI are almost obsolete.



Common WAN connection methods

- **PPPoE** (Point-to-Point Protocol over Ethernet)
  Username/password based authentication. PPP packets are encapsulated inside Ethernet frame.
- **DHCP** (Dynamic Host Configuration Protocol)
  Hosts automatically obtain IP addresses. No authentication required. The obtained IP address may change every time host connects, but may also be a specific allocated address.
- **Static IP**
  Hosts need to be set with IP address information manually. Connections may be allocated with a single IP or with multiple IP's (routed IP subnet).

Types of networks

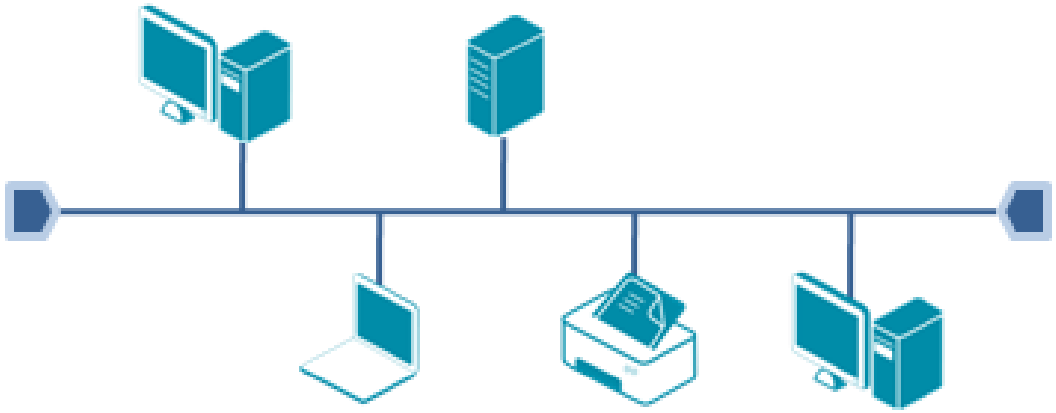
Different view of network type:

- Public networks
  - Internet, service provider network
- Private Networks
  - Corporate network, home network

Networks can be wired or wireless.

Types of network topology

- **Bus Topology**
  - Clients are connected via a shared communications line (normally a coaxial cable).
  - Not very effective due to clients interrupting each other (collisions).
  - Not very reliable – if a cable breaks, the whole network goes down.
  - Old technology, no longer being used.

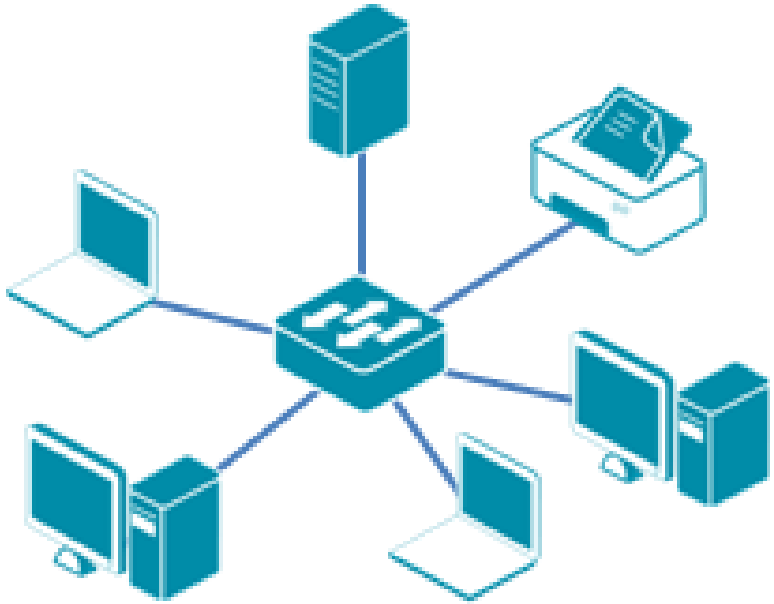


Types of network topology

- **Ring Topology**
  - Uses a token to pass information from one computer to another.
  - A failure in any cable or device breaks the loop and take down the entire network.
  - Rarely used nowadays.

Types of network topology

- **Star Topology**
  - All devices are connected to a central hub (switch).
  - Less collisions, best performance.
  - Easily scalable.
  - The most common type of LAN topology.



Summary

- Network definition
- Network components
  - NIC
  - Cable
  - Hub and switch
  - Wireless access point
- Network type
- Network topology
  - Bus
  - Ring
  - Star

Module 2

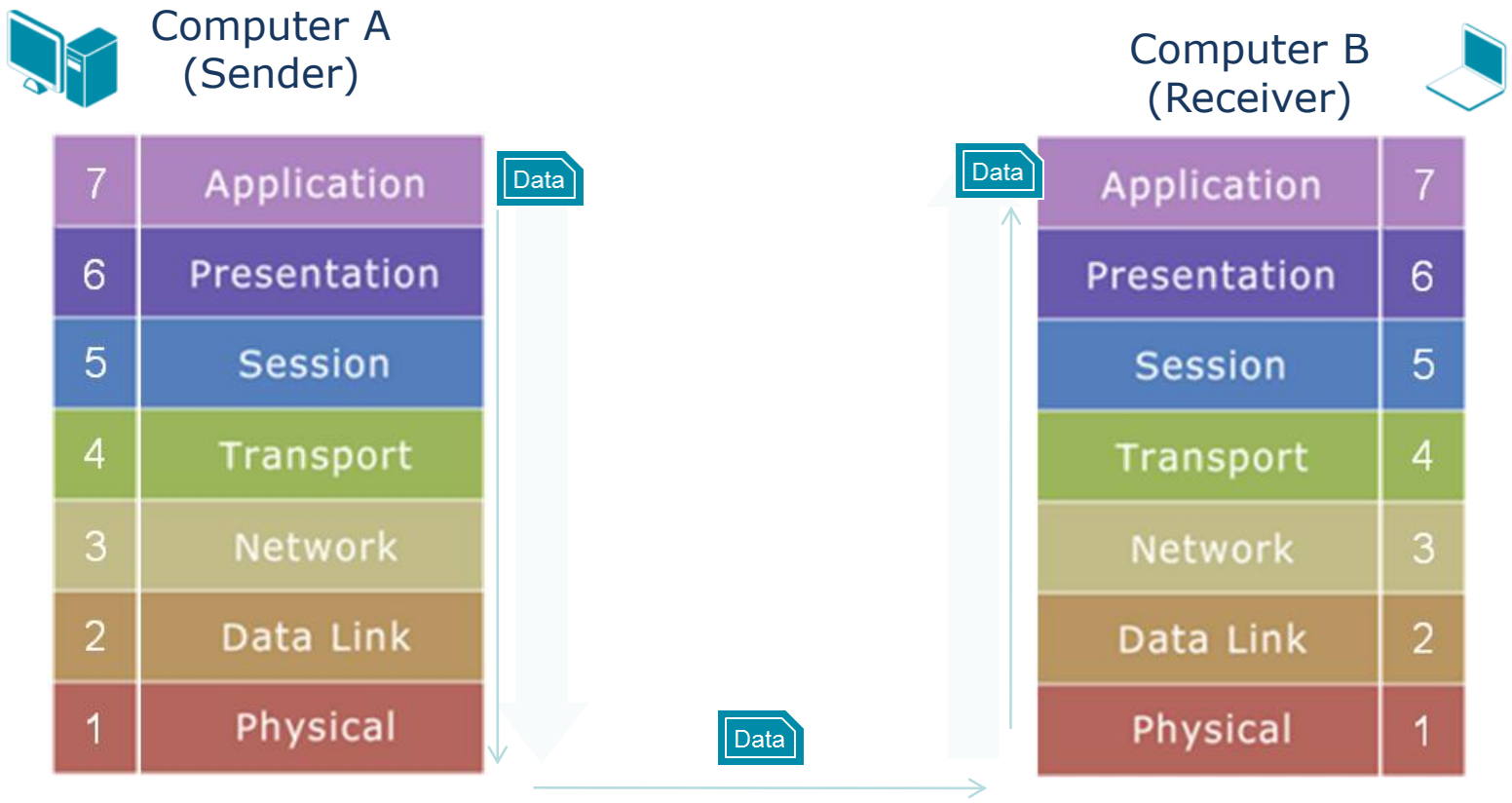
OSI Reference Model and TCP/IP

OSI Reference Model

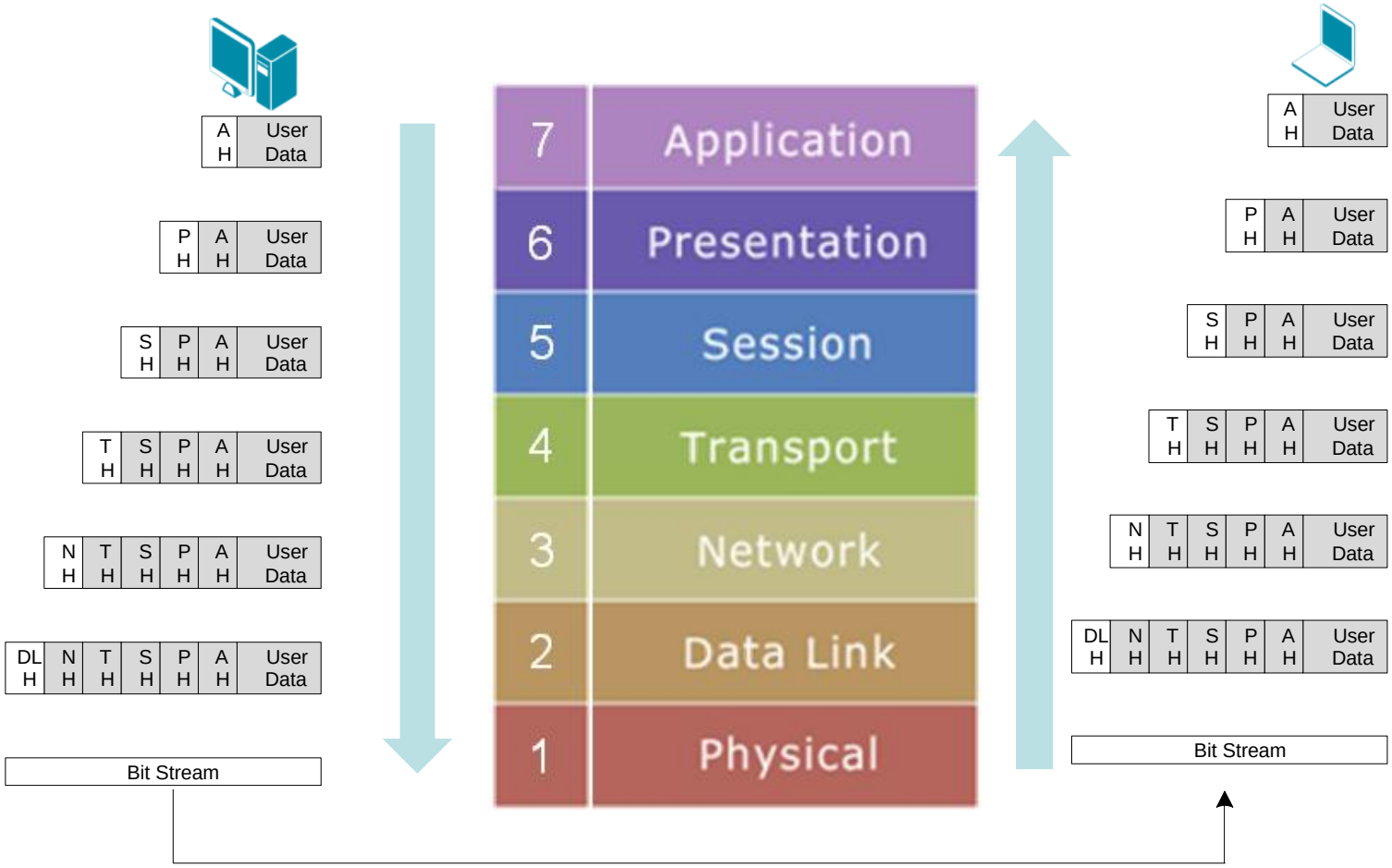
- The OSI Reference Model was implemented by the International Organization for Standardization as a guideline to help different vendors to create a network environment that would be compatible with other networks.

- The OSI Reference Model provides vendors with a set of standards to ensure not only compatibility, but also interoperability between different network technologies.

Network Communication



Encapsulation and Decapsulation

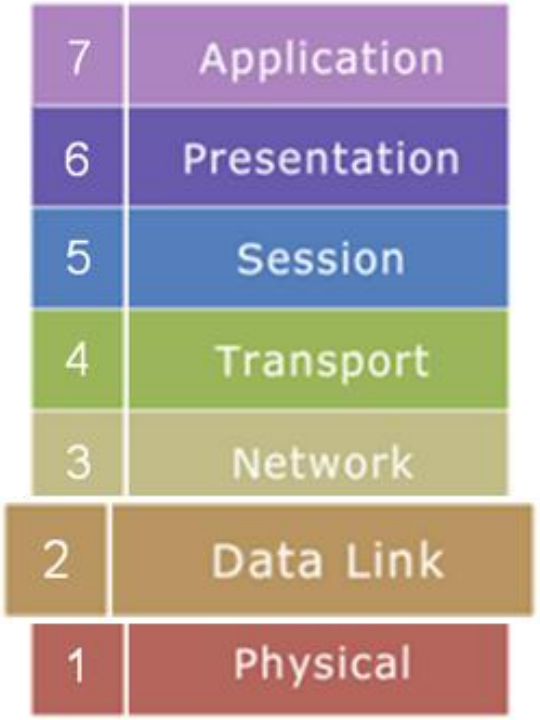


Physical Layer

- The physical layer provides a raw bit stream service. It moves 1s and 0s between the systems.
- The physical layer includes the mechanical, electrical, functional and procedural specifications for moving binary digits over a physical medium.
- Common devices which we use in the Physical Layer are hubs, network adaptors, repeaters and transceivers.

Data Link Layer

- The Data Link Layer manages communications on a single circuit, or a single link.
- It is divided into two sub layers:
  - Media Access Control (MAC) layer
  - Logical Link Control (LLC) layer
- The Media Access Control (MAC) layer controls the access to the shared channel in a broadcast network
- The Logical Link Control (LLC) layer handles frame synchronization, flow control and error checking.
- Common devices which we use in the Data Link are bridge, switch and wireless access points.



Network Layer

- The Network Layer determines how to route data from the sender network to the destination network
- There are different types of routes
  - Static routes
  - Dynamic routes
- The Network Layer is also responsible for addressing, called IP address*.
- The IP address consists of two parts:
  - Network part
  - Host part
- Common devices which we use in the Network Layer are routers and layer 3 switches.

* IP addressing detailed will be addressed in the "Internet Protocol" module.

Transport Layer

- The transport layer provides end-to-end data transfer
- The two main protocols in the Transport Layer are TCP and UDP.
  - Transmission Control Protocol (TCP): connection-oriented
  - User Datagram Protocol (UDP): connectionless
- The Transport Layer uses a service number to differentiate between applications.
  - For example, HTTP uses TCP port 80 while DNS uses UDP port 53.

Transport Layer – service port number

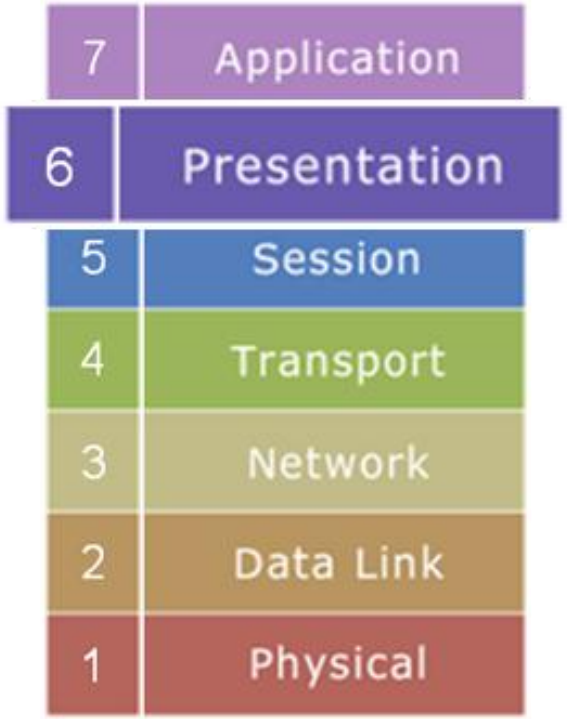
Port #	Common Protocol	Service	Port #	Common Protocol	Service
7	TCP	echo	80	TCP	http
9	TCP	discard	110	TCP	pop3
13	TCP	daytime	111	TCP	sunrpc
19	TCP	chargen	119	TCP	nntp
20	TCP	ftp-control	123	UDP	ntp
21	TCP	ftp-data	137	UDP	netbios-ns
23	TCP	telnet	138	UDP	netbios-dgm
25	TCP	smtp	139	TCP	netbios-ssn
37	UDP	time	143	TCP	IMAP
43	TCP	whois	161	UDP	snmp
53	TCP/UDP	dns	162	UDP	snmp-trap
67	UDP	bootps	179	TCP	bgp
68	UDP	bootpc	443	TCP	https (http/ssl)
69	UDP	tftp	520	UDP	rip
70	TCP	gopher	1080	TCP	socks
79	TCP	finger	33434	UDP	traceroute

Session Layer

- The Session Layer manages sessions between applications
- Usually this is visible to the user by having to log on with a password.

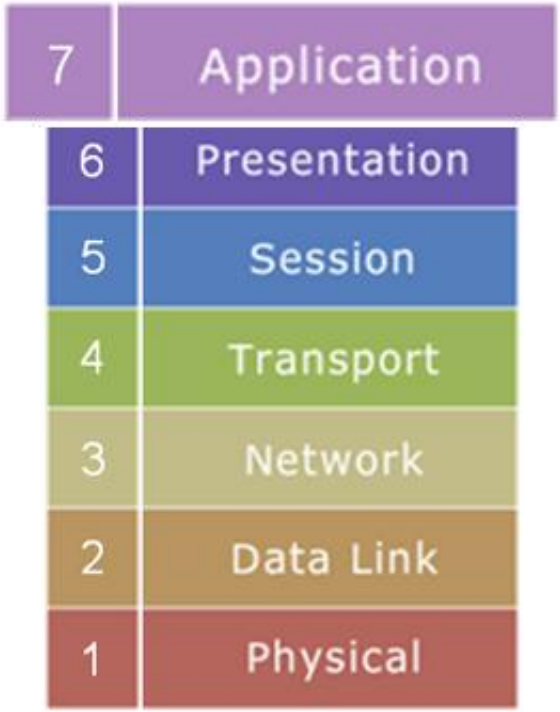
Presentation Layer

- The Presentation Layer is concerned with information syntax and semantics.
- Compression and encryption are also handled in the presentation layer.



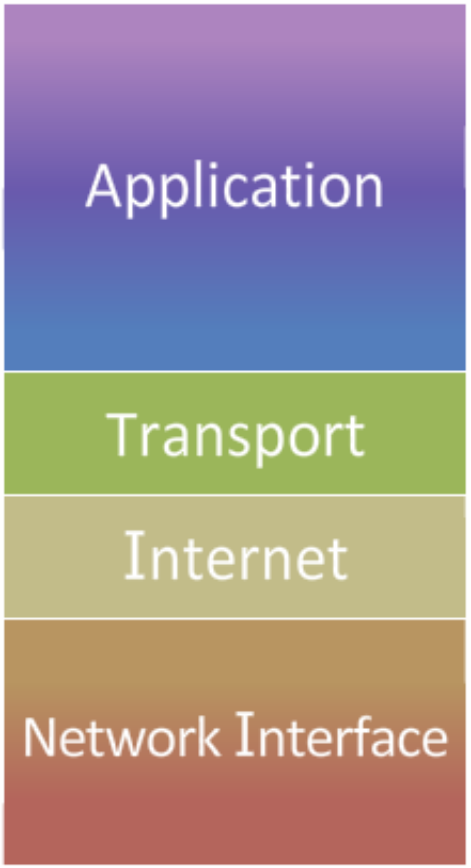
Application Layer

- The Application Layer handles the details of a particular application.
- It is usually bundled with a Human-Machine Interface - use to get access to distributed computing and communications.
- Commonly used network applications are:
  - Web browser (Internet Explorer, Chrome, Firefox, Safari)
  - Client software (Outlook, Skype)
  - Instant Message software (MSN, Yahoo Messenger)
  - File transfer software (FTP) and
  - Terminal emulation software (Telnet)
  - Social networking(Facebook, Google plus)

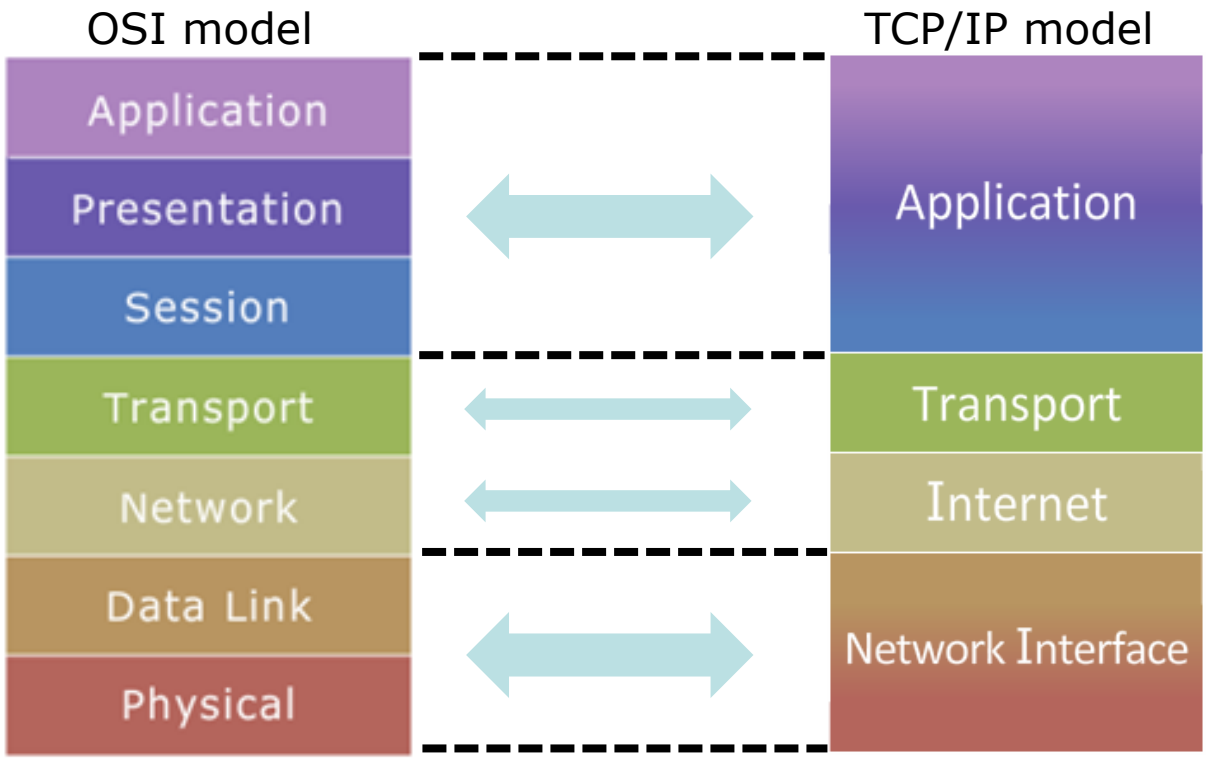


TCP/IP Protocol Suites

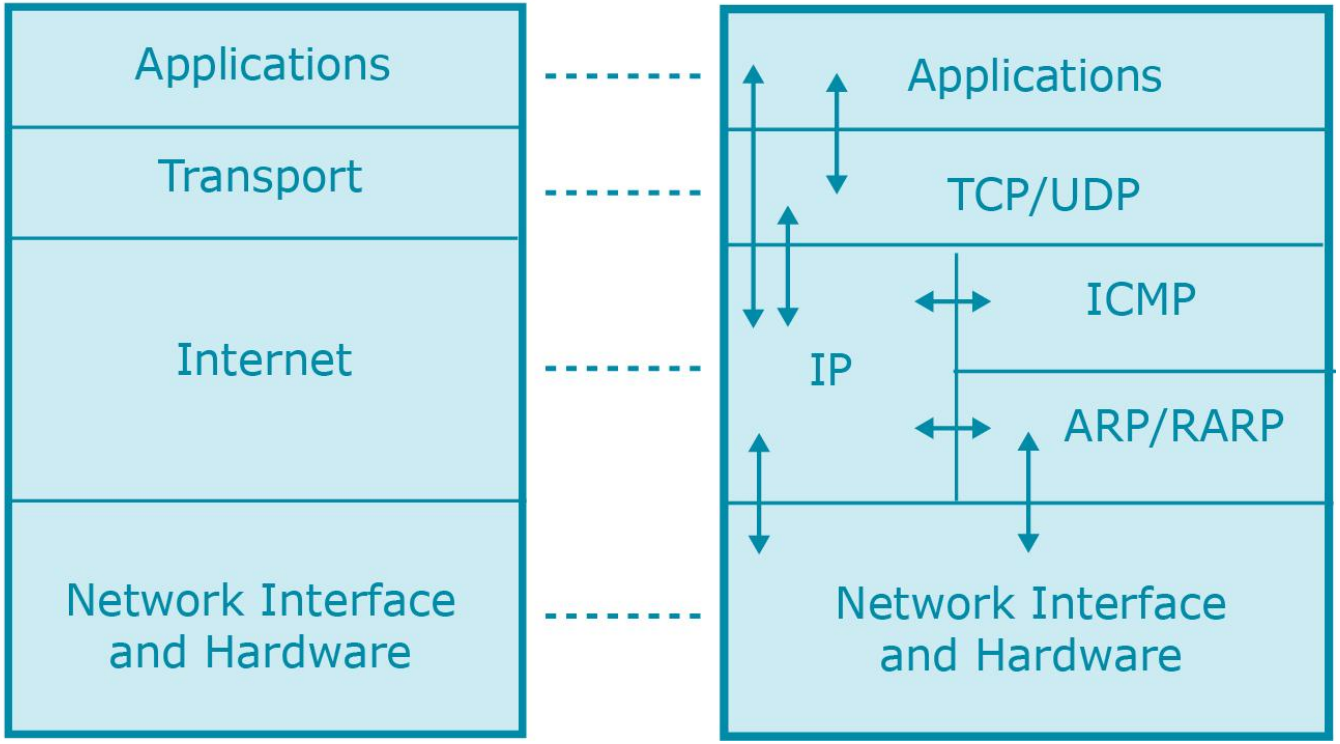
- TCP/IP is a set of protocols designed to allow networking devices to communicate and exchange information.
- TCP/IP is the de facto standard for internetworking.
- TCP – Transmission Control Protocol resides in the transport layer (layer 4) of the OSI model.
- IP – Internet Protocol resides in the network layer (layer 3) of the OSI model.



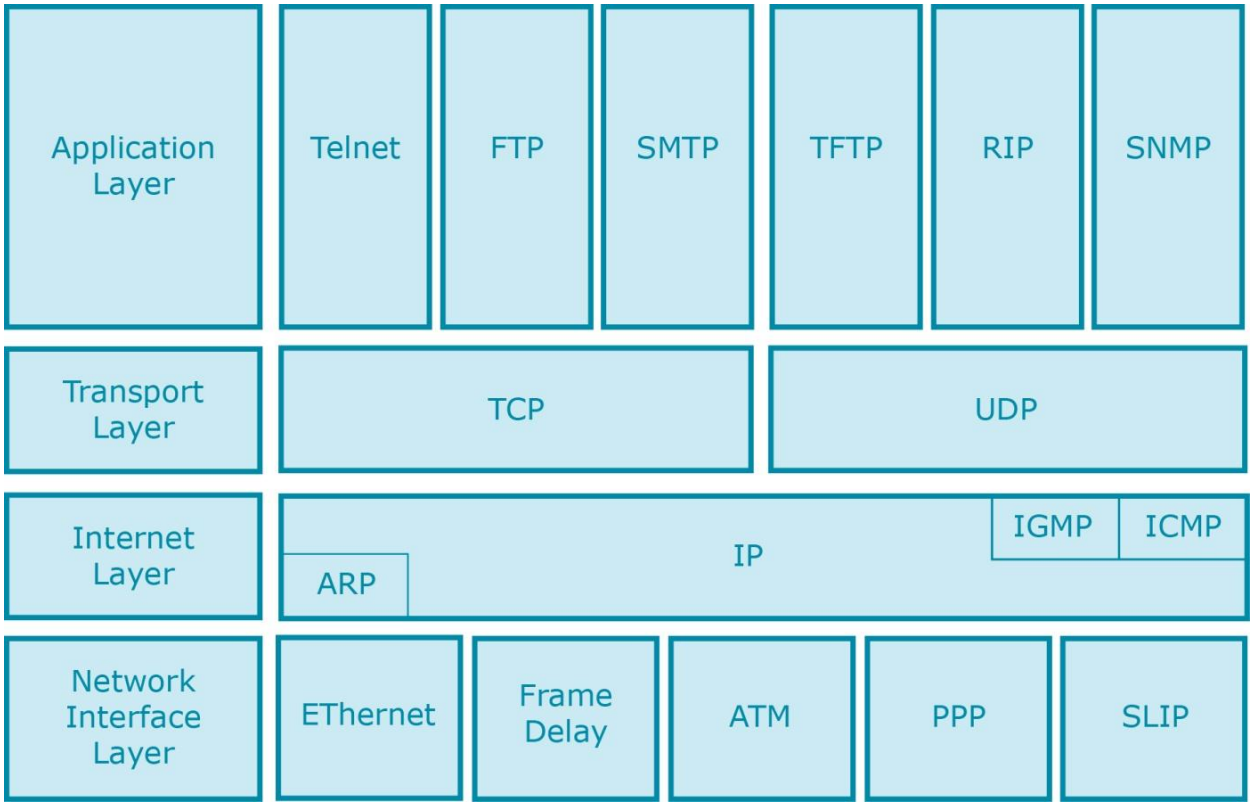
OSI vs. TCP/IP Model



TCP/IP Protocol Layers



TCP/IP Protocol Layers – cont'd



TCP/IP Protocol Layers summary

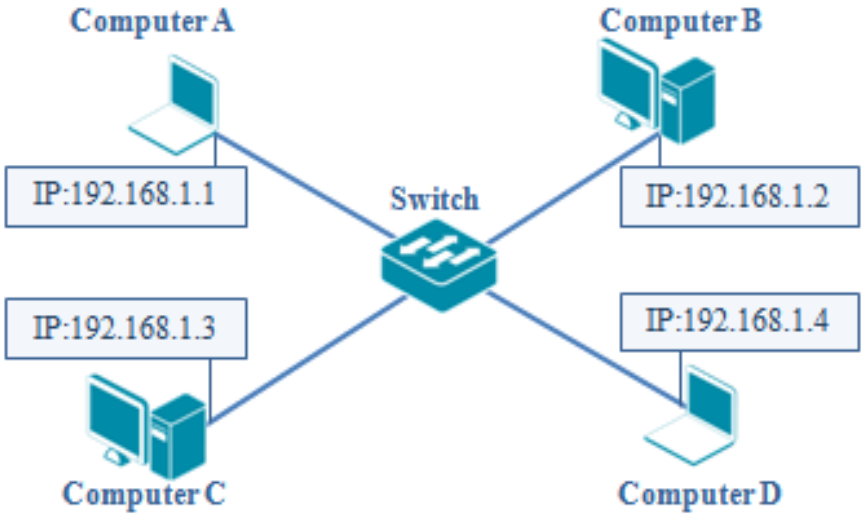
- The Network Interface Layer is the interface to the actual network hardware.
- The Internet Layer provides addressing and routing functions.
- The Transport Layer provides the end-to-end data transfer by delivering data from an application to its remote peer.
- The Application Layer is provided by the program that uses TCP/IP for communication. An application is a user process cooperating with another process, usually on a different host.

Module 3

IP Addressing and Subnetting

What is IP address

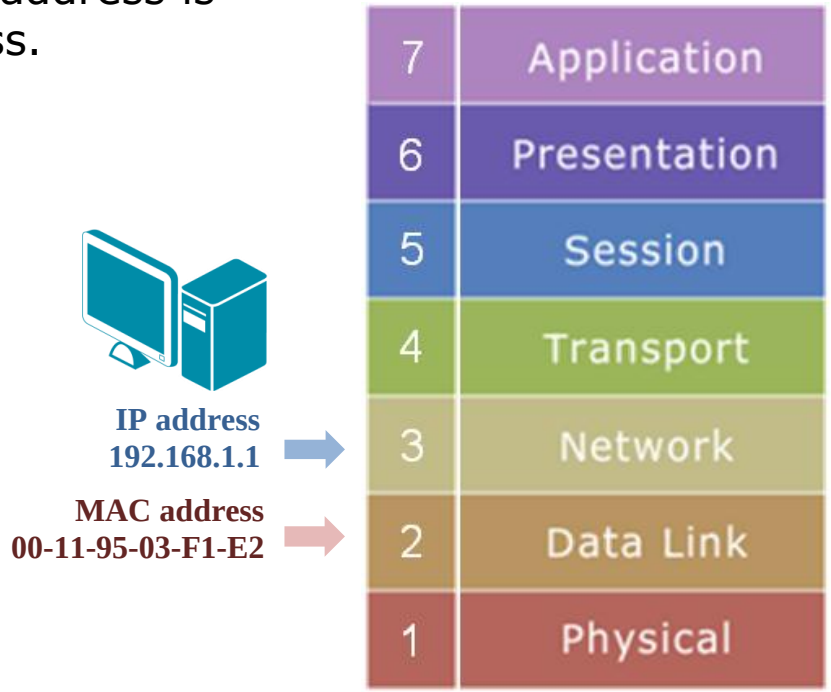
- An IP address is a unique address that network devices use in order to identify and communicate with each other on a computer network.
- It can be regarded as the identification of a computer in a network.
- Unlike MAC address, IP address is logical and can be changed on a device.
- IP addresses can be assigned to devices manually or automatically via a service on the network (DHCP).
- No two devices can have the same IP address on the same network.



IP ADDRESS
w. x. y. z

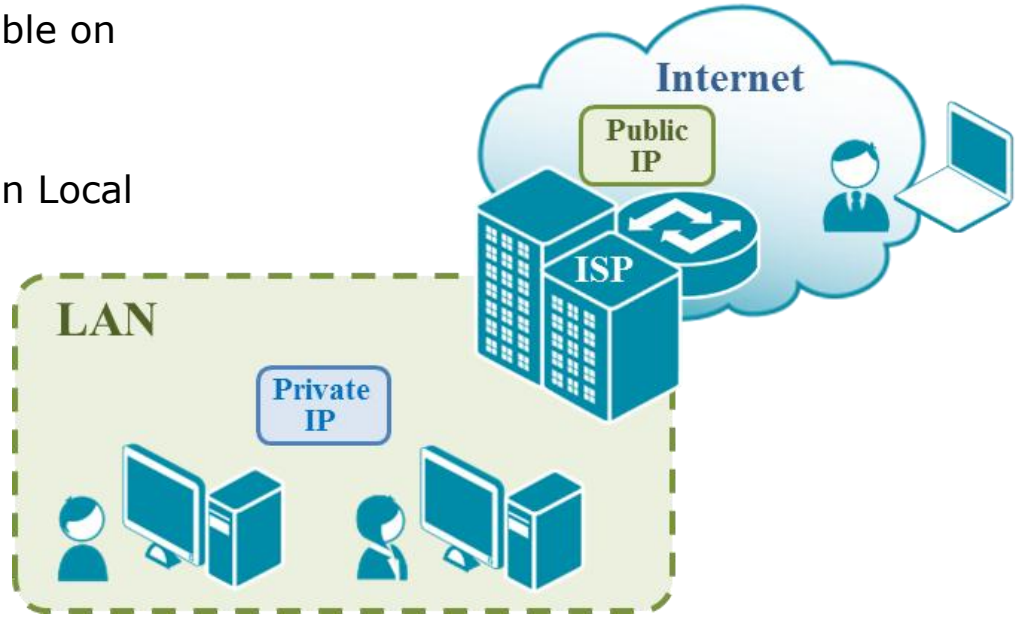
IP Address versus MAC Address

- A computer is also identified by a MAC address.
- A MAC address is layer two, physical address while IP address is layer three, logical address.

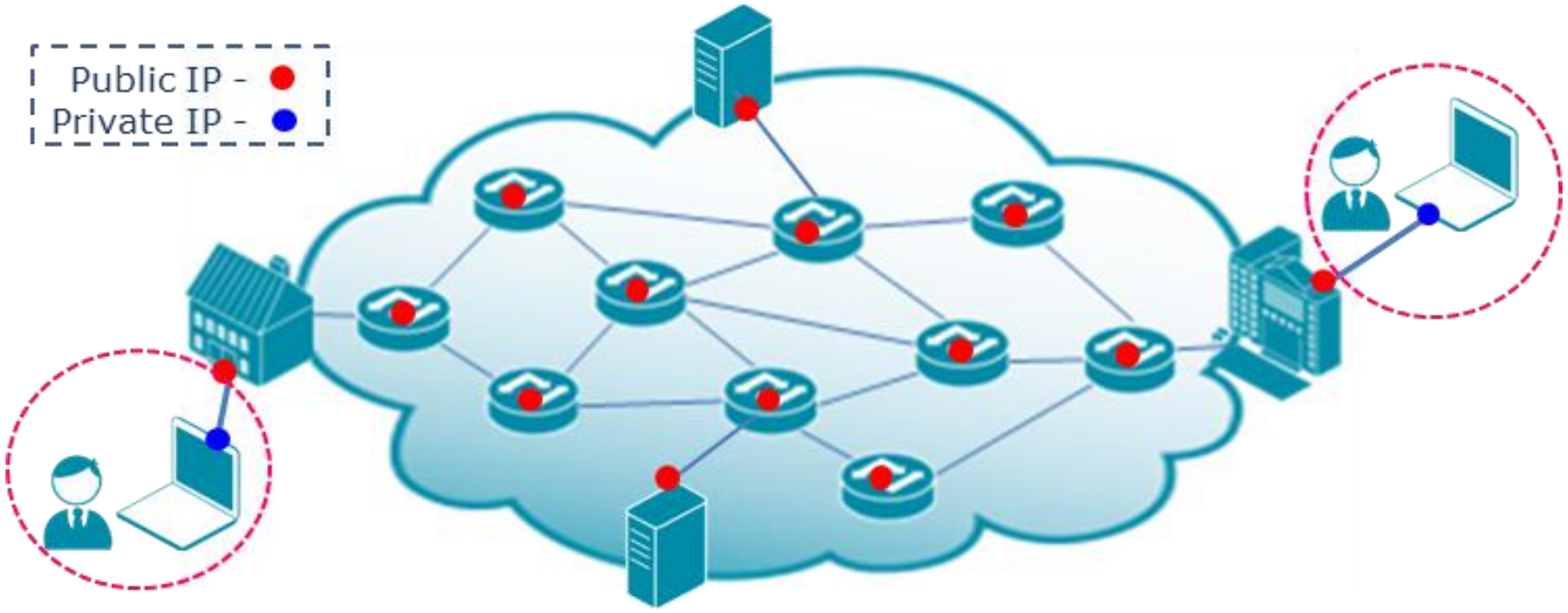


Major Types of IP Address

- Public IP addresses
  - The Internet community is based on public IP addresses.
  - Public IP addresses are assigned strictly by Internet Service Providers.
  - Public IP addresses are routable on the Internet.
- Private IP addresses
  - Private IP can only be used on Local Area Networks within an organization.
  - It is not routable on the Internet.



Major Types of IP Address



Reserved Private IP Address Ranges

- The Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks (RFC 1918):

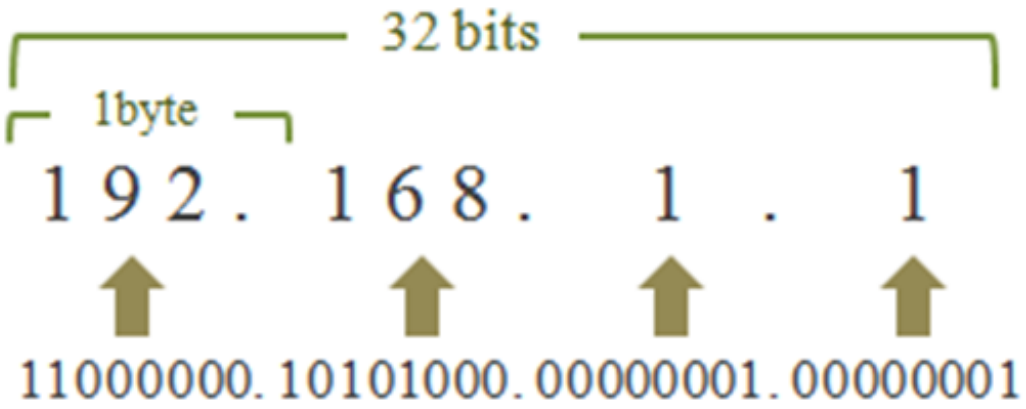
10.0.0.0 - 10.255.255.255

172.16.0.0 - 172.31.255.255

192.168.0.0 - 192.168.255.255

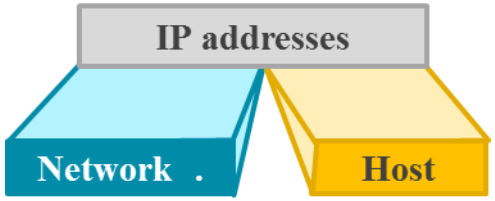
IP Address Format

- IP addresses are 32 bits in length and written as a sequence of one byte which are separated by periods.
- It is usually known as dotted decimal.
- The format of an IP address is **xxx.xxx.xxx.xxx**
- A sample IP address is 192.168.1.1.



IP Address Class

- IP address consists of two parts:
  - Network Identifier (Net ID), and
  - Host Identifier (Host ID)
- In IPv4, the IP address is categorized into different classes:
  - Class A
  - Class B
  - Class C
  - Class D
  - Class E



IP Address Class	IP Address Range (First Octet decimal value)
Class A	1-126(00000001 to 01111110)*
Class B	128-191(10000000 to 10111111)
Class C	192-223(11000000 to 11011111)
Class D	224-239(11100000 to 11101111)
Class E	240-255(11110000 to 11111111)

*127 (011111111) is a Class A address reserved for loopback testing and cannot be assigned to a network host.

Subnet Mask

- A subnet mask is used to identify the network bits and the host bits in an IP address. A binary one in the subnet mask represents the network bits, and a binary 0 represents the host bits.

Class	Subnet Mask	Number of Network Bits
A	255.0.0.0	8
B	255.255.0.0	16
C	255.255.255.0	24

IP Address and Subnet Mask

192.168.1.1	IP address. Unique address of a networking device on a network.
255.255.255.0	Subnet Mask. Determines how many IP addresses are in the subnet.

Subnet mask 255.0.0.0 gives you subnets with 16777214 addresses.

Subnet mask 255.255.255.0 gives you subnets with 254 addresses.

Subnet mask 255.255.255.192 gives you subnets with 62 addresses.

With 255.255.255.252 subnet mask the range of usable IP addresses in each subnet is narrowed down to two:

Subnet #1:	192.168.1.1 – 192.168.1.2	(Subnet ID: 192.168.1.0)
Subnet #2:	192.168.1.5 – 192.168.1.6	(Subnet ID: 192.168.1.4)

… etc.

Decimal versus Binary Numbers

- To understand how to calculate subnets, it is essential to learn how to convert binary numbers to decimal numbers, and vice versa.

Decimal	Binary	Decimal	Binary
0	0	10	1010
1	1	11	1011
2	10	12	1100
3	11	13	1101
4	100	14	1110
5	101	15	1111
6	110	16	10000
7	111	17	10001
8	1000	18	10010
9	1001	19	10011

Decimal-to-Binary Conversion

- Example: Convert decimal 81 to a binary number

Base **Exponent**	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Place Value	128	64	32	16	8	4	2	1
Example: Convert decimal 81 to binary	0	1	0	1	0	0	0	1

Binary-to-Decimal Conversion

- Example: Convert binary 10101000 to a decimal number

Base **Exponent**	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Place Value	128	64	32	16	8	4	2	1
Example: Binary Number	1	0	1	0	1	0	0	0
Decimal Number: 168	128	0	32	0	8	0	0	0

Subnet Masks in Binary Format

- Subnet mask can also be represented as number of bits:
  - 192.168.1.0/24 – means network with 255.255.255.0 subnet mask.
  - 10.1.1.0/8 – network with 255.0.0.0 subnet mask.

- Subnet mask in binary code:

Decimal format	Binary format
255.255.255.240	**11111111.11111111.11111111.11110000**

- 255.255.255.240 subnet mask has 28 bits.

- Example:
  10.1.1.4/30 – network with 255.255.255.252 subnet mask.
  Usable IP addresses 10.1.1.5 - 10.1.1.6.

Subnet Mask in Binary and Decimal Format

- These are the possible values (shown in binary and decimal formats) that can be used in a subnet mask.

0	0	0	0	0	0	0	0	=	0
1	0	0	0	0	0	0	0	=	128
1	1	0	0	0	0	0	0	=	192
1	1	1	0	0	0	0	0	=	224
1	1	1	1	0	0	0	0	=	240
1	1	1	1	1	0	0	0	=	248
1	1	1	1	1	1	0	0	=	252
1	1	1	1	1	1	1	0	=	254
1	1	1	1	1	1	1	1	=	255

Subnet ID and Broadcast Address

- For 255.255.255.0 subnet mask the number of available IP addresses is 256. The very first and the very last addresses are reserved leaving 254 usable addresses:
  - 192.168.1.1 – 192.168.1.254
  - 192.168.1.0 is reserved for Subnet ID.
    192.168.1.255 is reserved for Broadcast IP.

How to calculate how many IP addresses are available in a subnet:

256 – [subnet mask] = [number of IP's in the subnet]

Note: two addresses are reserved for Subnet ID and Broadcast IP.

Example: Subnet mask 255.255.255.224

256 – 224 = 32 (30 usable)

32 addresses available in the subnet, 30 of them are usable.

Subnet ID Calculation

- Use Windows calculator to come out the Subnet ID.
  - Programmer mode in Windows 7
- Example: 172.16.1.123 with 255.255.255.248 subnet mask.
- Apply logical "AND" function to the last octets of IP address and the Subnet Mask:

- 123 "And" 248 = 120

- 172.16.1.120 is the Subnet ID.

Check if IP addresses are in the same subnet

- Hosts in different IP subnets need a router (Layer 3 device) to communicate with each other.
- How do you know if two IP's are in the same subnet?
  Answer: Check their Subnet ID's. Same Subnet ID = same subnet.

Example:

- Subnet Mask for all addresses below is 255.255.255.192

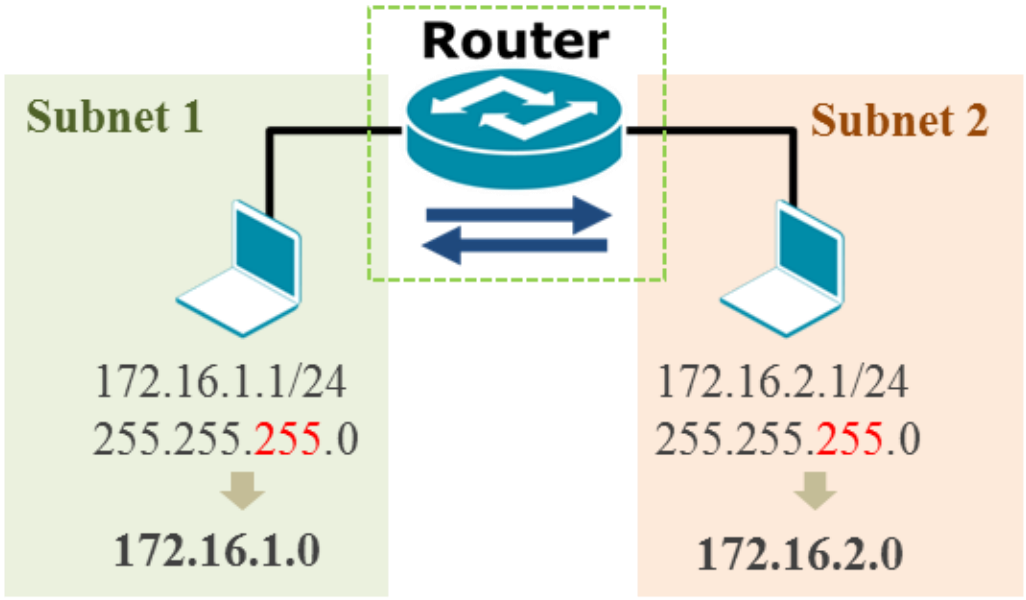
IP Address	Subnet ID
192.168.1.10	192.168.1.0
192.168.1.60	192.168.1.0
192.168.1.70	192.168.1.64
192.168.1.130	192.168.1.128
192.168.1.200	192.168.1.192
192.168.1.250	192.168.1.192

Although the addresses look similar, the subnet mask divides them into different IP subnets (see Subnet ID).

But if these addresses would have subnet mask 255.255.255.0 they would all be on the same subnet (with Subnet ID 192.168.1.0).

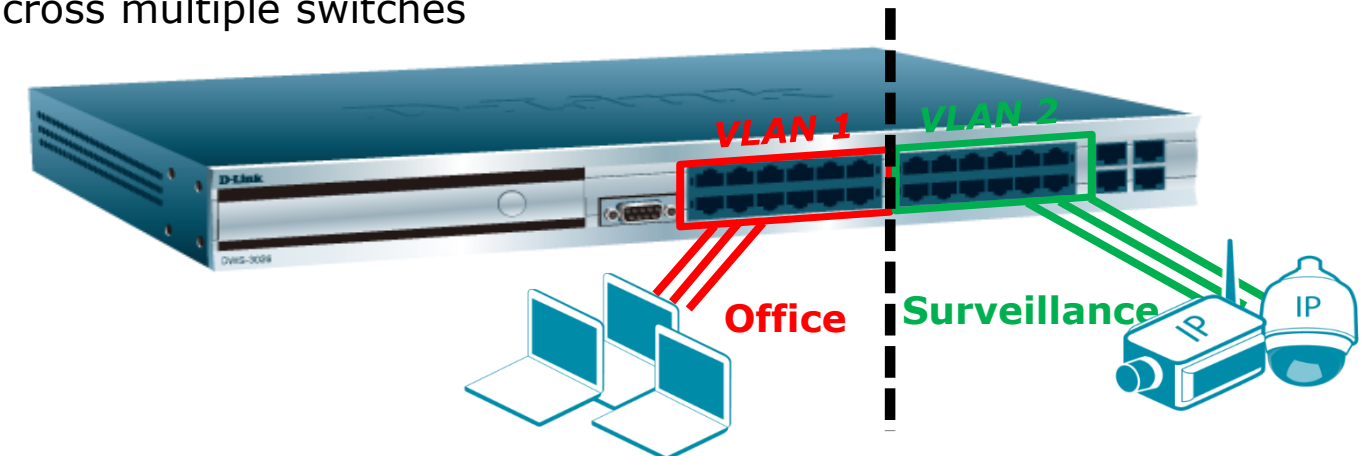
IP Subnet connectivity

- IP addresses can be on the same IP subnet or on different subnets.
- Hosts in different IP subnets need a router (Layer 3 device) or a Layer 3 switch to communicate with each other.



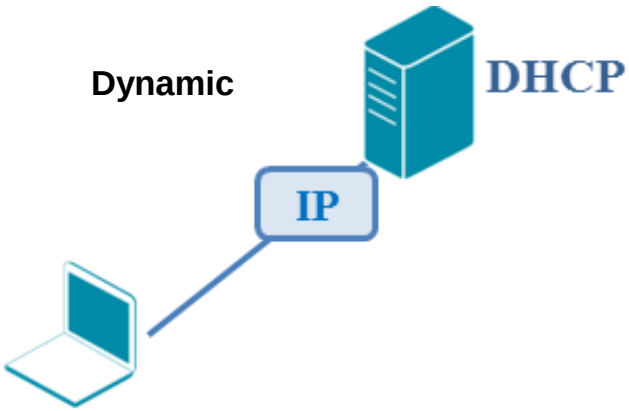
VLAN

- VLAN stands for virtual local area network or virtual LAN.
- It is a Logical subgroup within LAN.
- Why VLAN?
  - To subdivide network into smaller segments in order to reduce broadcast traffic.
  - To isolate one part of network users from the other.
  - To subdivide a group of users and apply different data priority, security restrictions to each group.
- Method to create a VLAN
  - Port-based VLANs:
    Simple and standalone solution
  - Tag-based (802.1q) VLANs:
    Can span across multiple switches



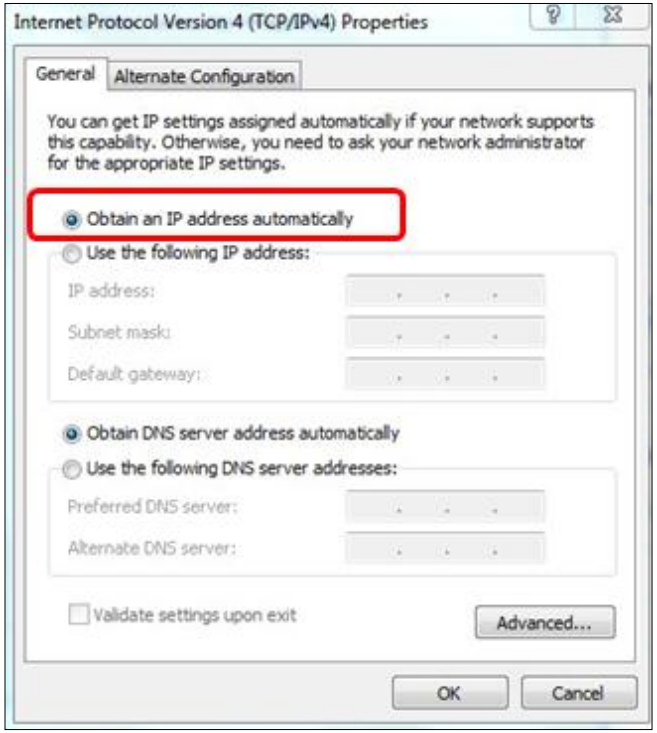
IP Address Assignment

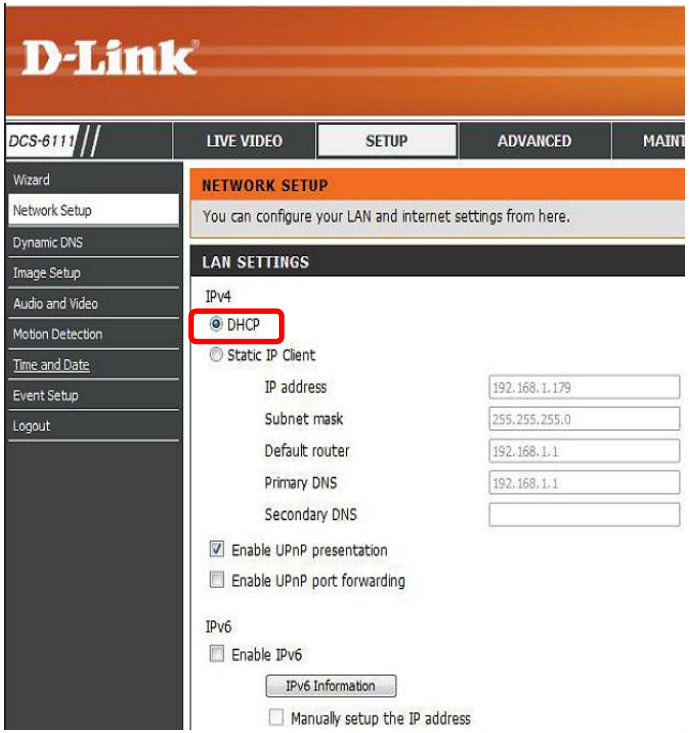
- There are two ways for IP address assignment: dynamic IP setting and static IP setting.
- Dynamic IP setting: the computer can obtain IP settings automatically from a DHCP server on the network.
- Static IP setting: you have to specify the IP address information manually.



Dynamic IP address assignment

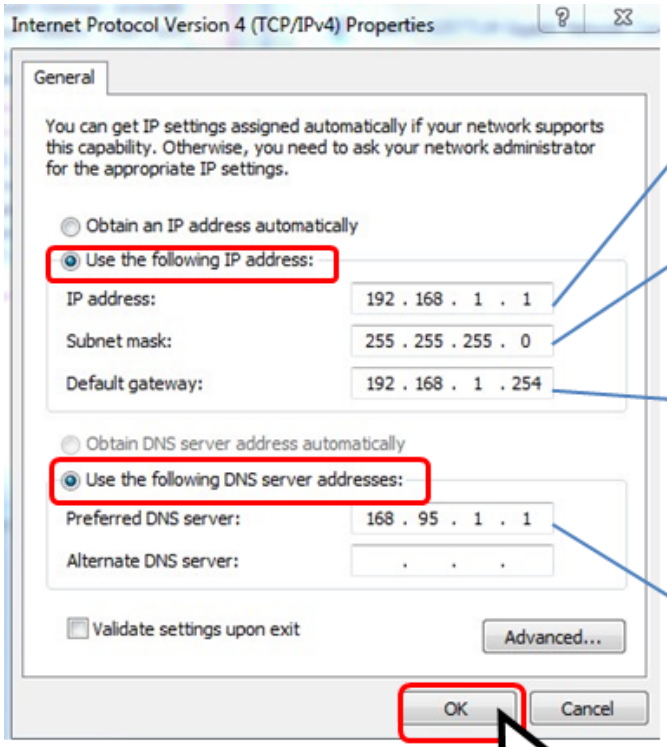
- The default IP setting of a Windows computer is to obtain IP information from a DHCP server.
- There is no need to change the configuration. Connect your computer to the network. Within one minute, your computer will obtain an IP address.





Static IP assignment

- When you want to specify the IP settings manually on a Windows computer, first connect your computer to the network.
- You will be requested to specify the 'IP addresses' , 'Subnet mask', 'Default gateway' and DNS servers



IP address- to identify your PC on the network

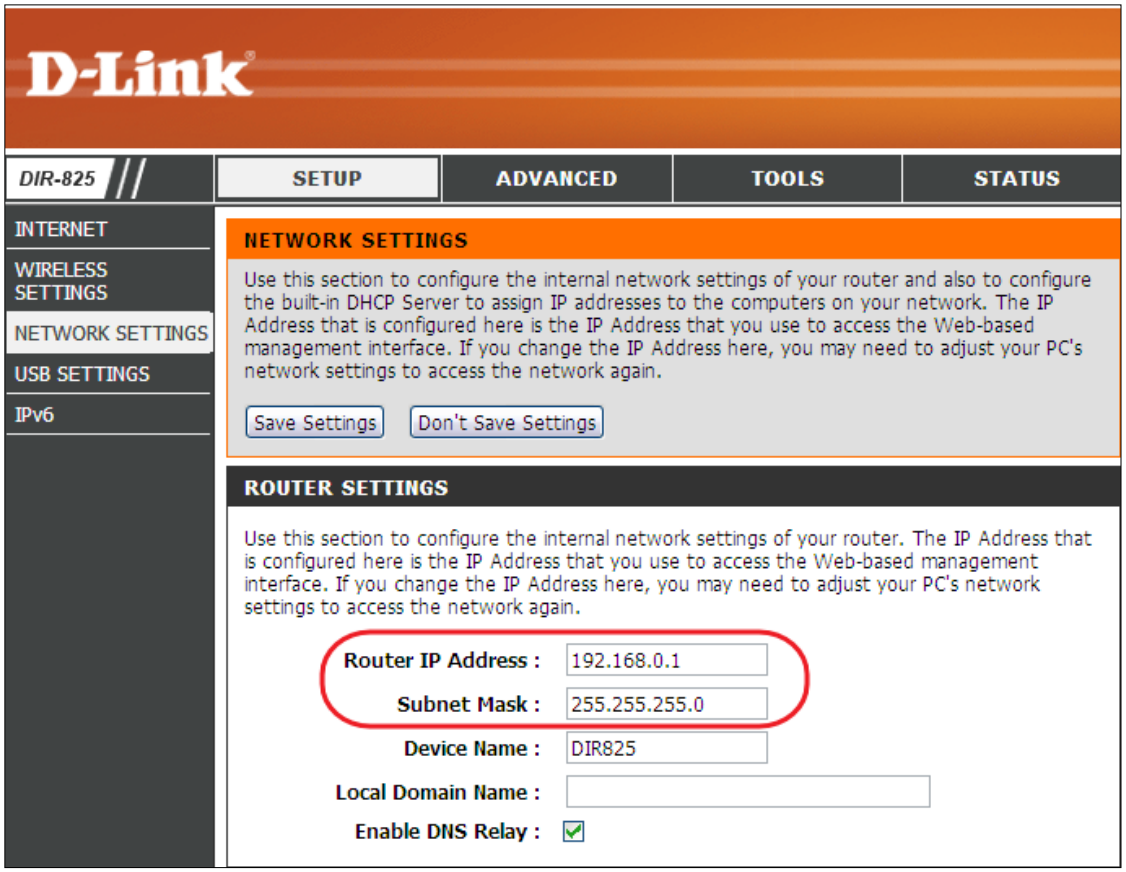
Subnet mask- to specify the size of your IP network.

Default Gateway- normally router's address. That's how your computer gets onto other networks, e.g. Internet.

DNS server- that's how your PC resolves names into IP address and can browse websites, e.g. wwww.dlink.com 207.232.83.10

Static IP Assignment

- You can also specify IP address on any network devices, such as residential gateway or wireless router.

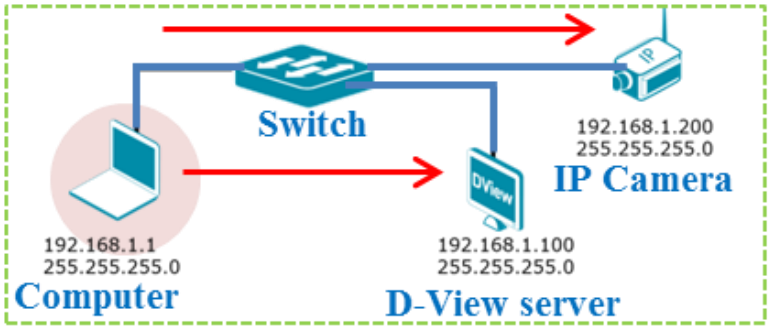


Verify the IP Configuration

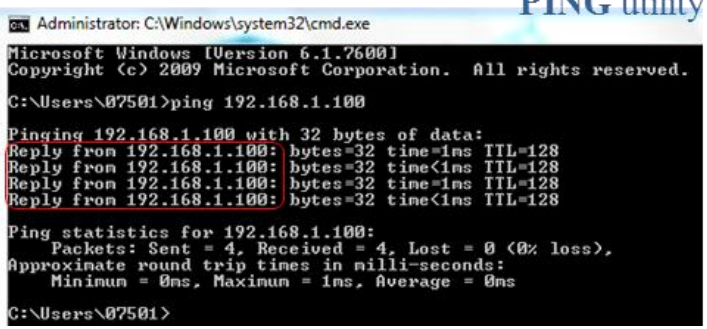
- After the configuration is done, you can launch the Windows command prompt and use “ipconfig” to verify the IP configuration.

Verify Network Connectivity

- As soon as you finish the IP setting of the network devices, you can use the PING utility to verify the network connectivity
- PING can be launched from the Windows command prompt. In the diagram, you use the PING utility from the computer at the left side to verify the network connectivity to the D-View server and the IP camera.
- "Reply from 192.168.1.100" indicates good network connectivity between the computer and the D-View server.

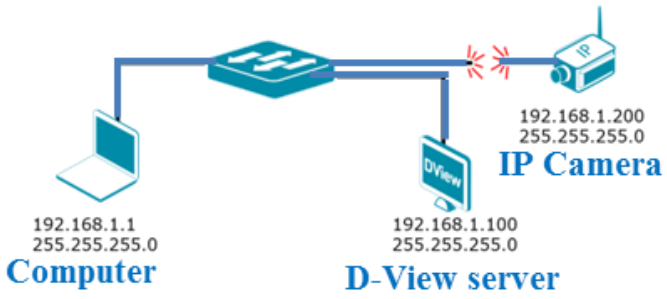


PING utility



Verify Network Connectivity

- Perform PING to verify the network connectivity between the computer and the IP camera.
- "Request timed out" indicates loss of network connectivity.



PING utility

```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\07501>ping 192.168.1.200

Pinging 192.168.1.200 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.200:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\07501>
```

IPv6

- IPv6 stands for IP version 6.
- IPv6 is a new version of the Internet Protocol, which is built on IPv4, and is expected to replace IPv4. IPv6 is the solution for the expansion of the Internet.
- IPv6 is described in RFC 2460, which is a good IPv6 document to start with.
- Evolution from IPv4:
  - Increase in IP address size
  - Support for different traffic types
  - Extensions to support authentication, data integrity, and data confidentiality

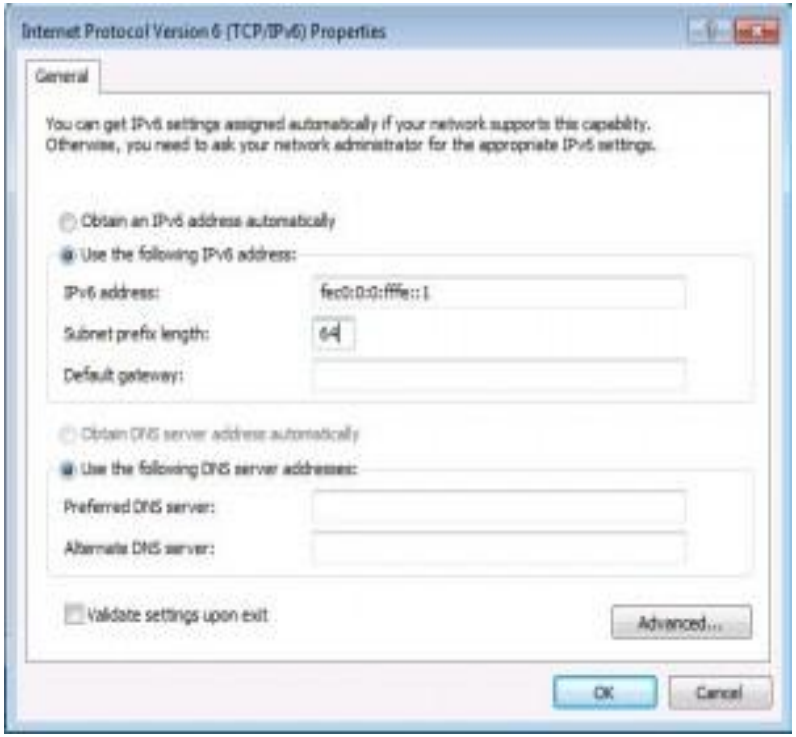
IPv4 and IPv6 Addressing Comparison

IPv4 address	32 bits
11000000.10101000.0000001.00001111	
192.168.1.15	
4,294,467,295 IP addresses	

IPv6 address	128 bits
00100001.11011010.11010011.00000000. 00000000.00000000.00101111.00111011. 00000010.10101010.00000000.11111111. 11111110.00101000.10011100.01011010	
21DA:00D3:2F3B:0000:02AA:00FF:FE28:9C5A	
3.4 x 10^{38} IP addresses	

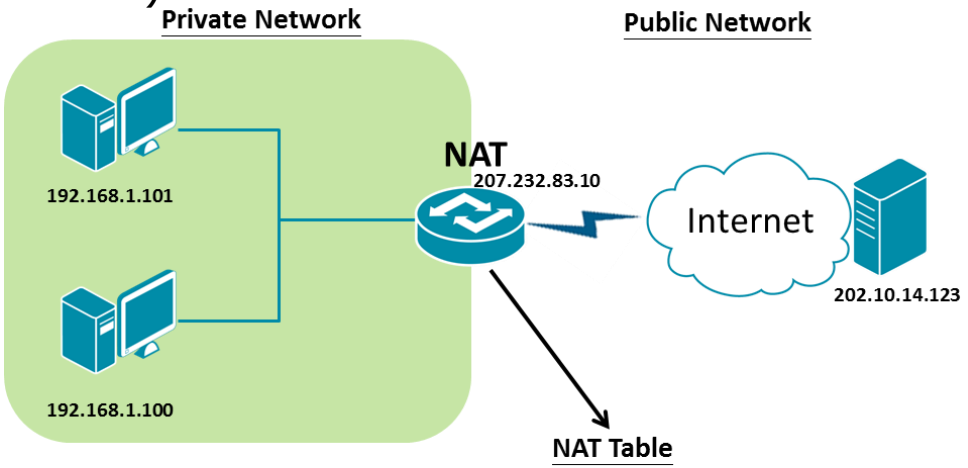
IPv6 Configuration

- IPv6 setting can be made from Windows computer after IPv6 is enabled.
- IPv6 address can also be specified in IPv6-enabled network devices, such as residential gateway or wireless router.



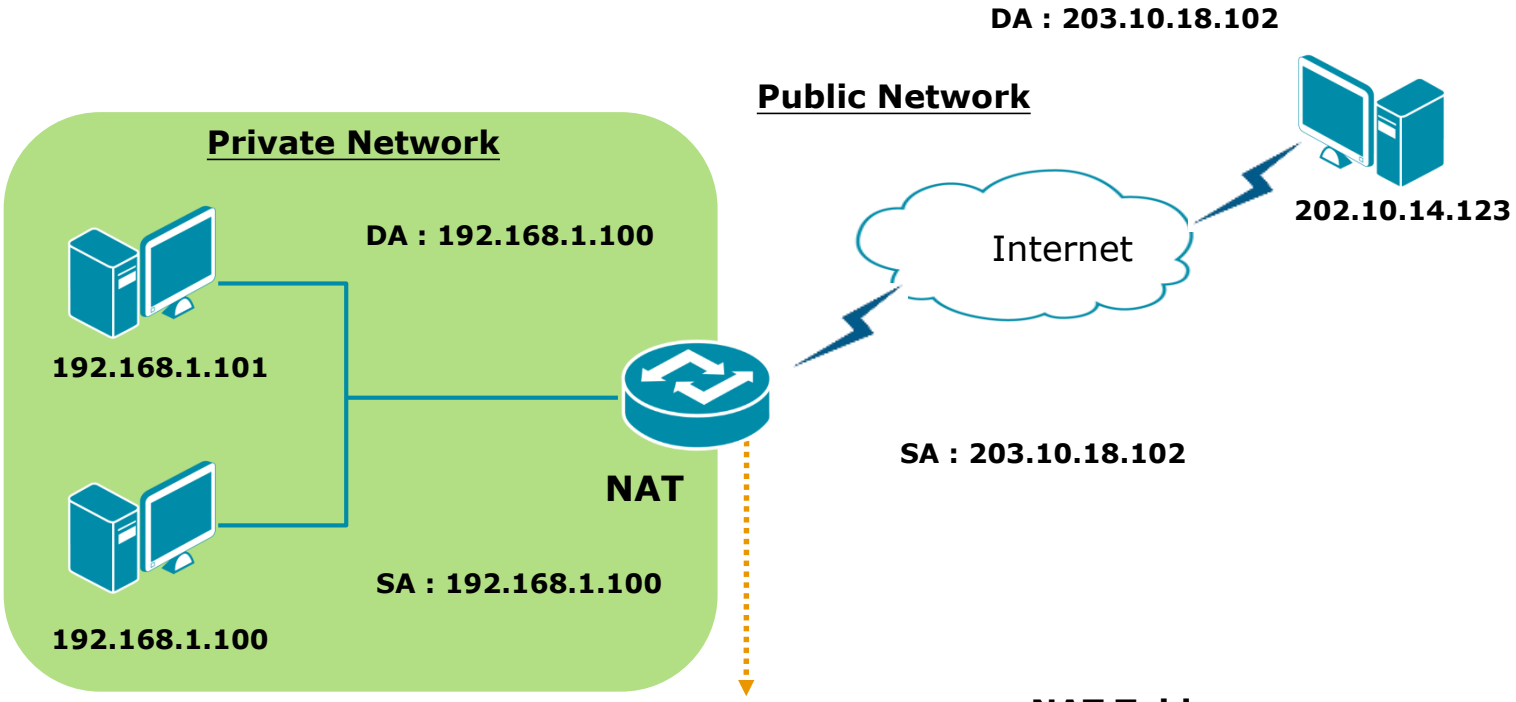
Network Address Translation

- NAT translates an IP address in one network to a different IP address in another network.
- It is usually implemented on a router or firewall and converts private IP addresses to public IP addresses.
- One of the purposes of using NAT is to allow a single IP address to represent a group of computers as IPv4 is running out of IP addresses. This is known as PAT (Port Address Translation).



Protocol	Private IP address :	Public IP address :
	Port	Port
TCP	192.168.1.100 : 1123	207.232.83.10 : 1123
TCP	192.168.1.101 : 1234	207.232.83.10 : 1234

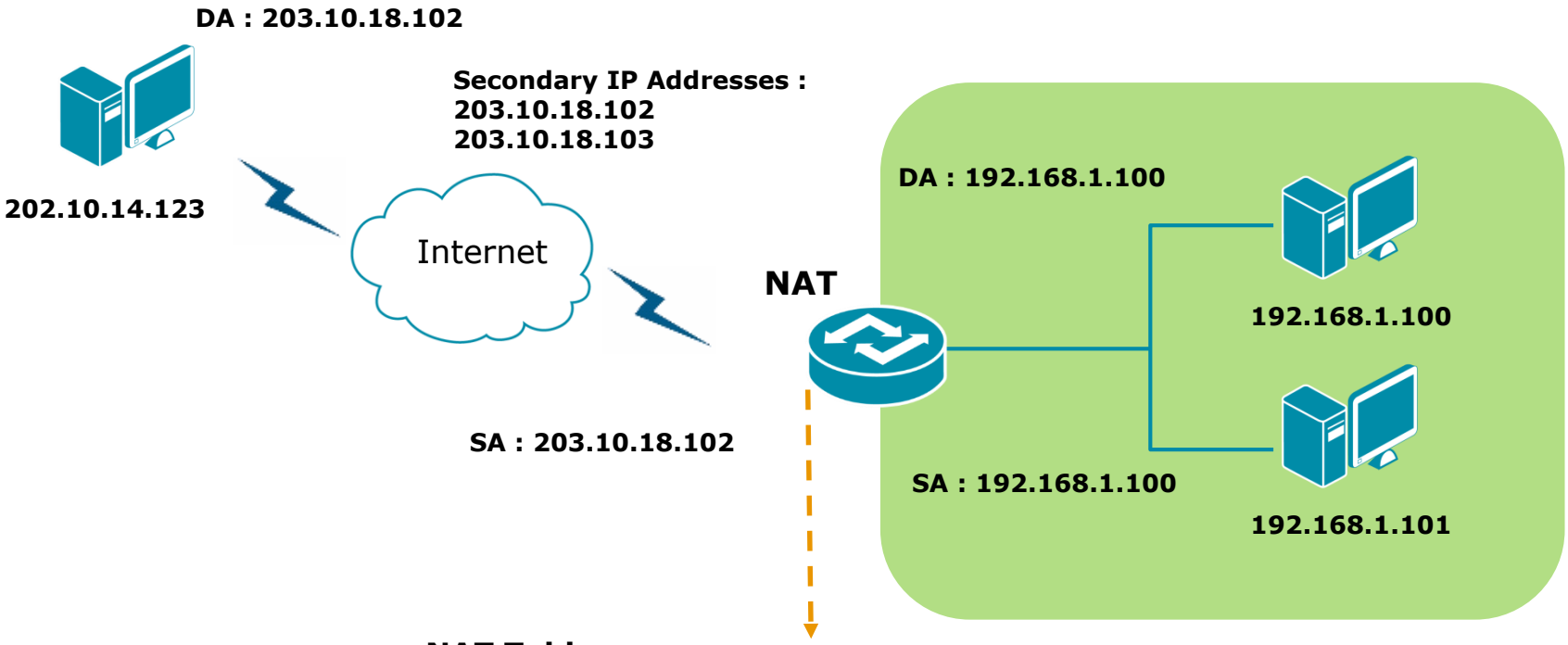
Network Address Translation - PAT



NAT Table

Protocol	Private IP address:	Public IP address:
	Port	Port
TCP	192.168.1.100 : 1123	203.10.18.102 : 1123
TCP	192.168.1.101 : 1234	203.10.18.102 : 1234

Network Address Translation – inbound translation

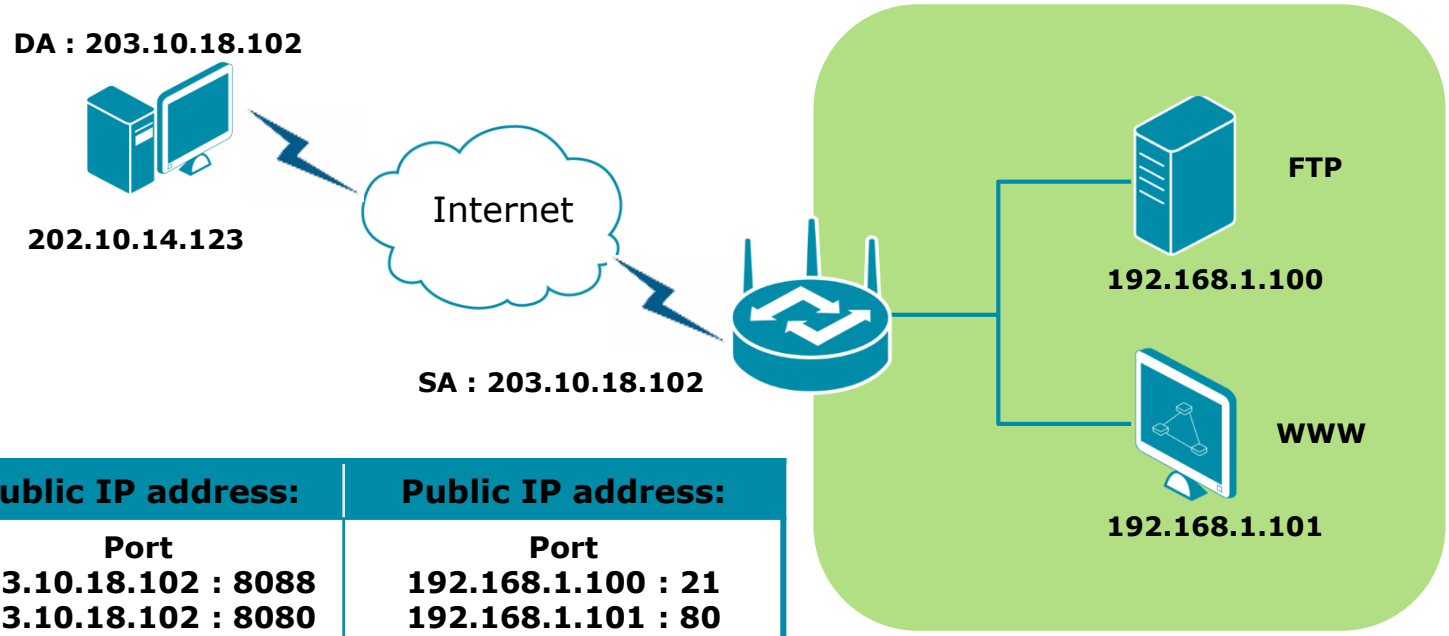


NAT Table

Protocol	Private IP address:	Public IP address:
TCP TCP	192.168.1.100 192.168.1.101	203.10.18.102 203.10.18.103

Virtual Server

- The Virtual Server is common function on wireless router.
- It allows remote users to have access to servers, such as Web or FTP, in the private network by means of port-redirection.
- Multiple virtual service can be created for different servers behind the gateway device.



Protocol	Public IP address:	Public IP address:
	Port	Port
TCP	203.10.18.102 : 8088	192.168.1.100 : 21
TCP	203.10.18.102 : 8080	192.168.1.101 : 80

Module 4

Wireless LAN Fundamental

Wireless LAN Technology Overview

- Wireless Local Area Network (WLAN) definition
  - Network infrastructure where all data is transmitted and received using radio signals over the air instead of via network cables
- Advantages of implementing WLAN technology
  - Mobility
  - Simple network expansion
  - Scalability
- Differences between wired LAN and wireless LAN

Wired LAN	Wireless LAN
• Network cable installation required • Limited by network media • Depends on physical location • Data sent through network cable	• Free of network cabling • Not limited by network media • Independent of physical location • Data sent over the air

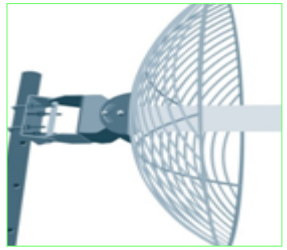
Basic Components of a Wireless Network

- Wireless client/station (STA)
  - Wi-Fi phone, Smart phone or PDA…etc. with Wi-Fi built in.
  - Wireless adapter for client devices (used only for clients that do not support wireless)
    - Wireless USB Adapter
    - PCMCIA Adapter
    - Express Card and PCIe
- Wireless device
  - Access point
  - Wireless router
- Antenna

D-Link Wireless USB Adapter

D-Link PCMCIA Wireless Network Adapter

D-Link Access Point

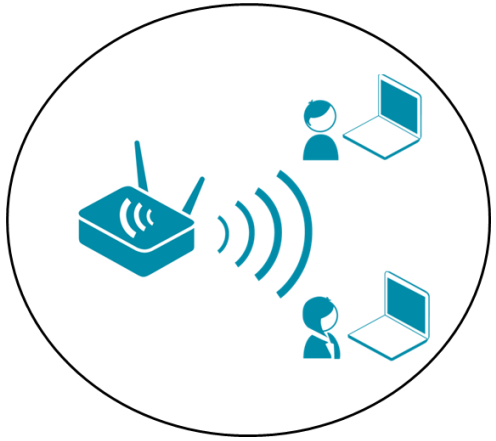


Antenna

Types of wireless networks

- **Ad-Hoc**
  Connect to other wireless client devices without the use of any wireless media.
  Useful for establishing a network where wireless infrastructure does not exist or where services are not required.
  Not suitable for large scale networks.

- **Infrastructure**
  Connect to other wireless client device with the use of any wireless media to act as a central point.
  Suitable to be deployed for a large scale network.



Antenna Types

- **Omnidirectional**
  - Radiates RF signals to roughly all directions

- **Directional**
  - Radiates RF signals in a specific direction

Regulatory Compliance

- Usage of radio frequency spectrum is controlled by governments
- Defining available frequencies and EIRP
  - **FCC** for U.S.
  - **ETSI** for Europe
- Products must pass CE or FCC certification

ISM and UNII bands

- Radio bands reserved internationally for the use of RF energy
- Do not require a license to transmit
- **ISM**

Band	Frequency Range
ISM-900	902-928 MHz
ISM-2400	2400-2484 MHz
ISM-5800	5725-5850 MHz

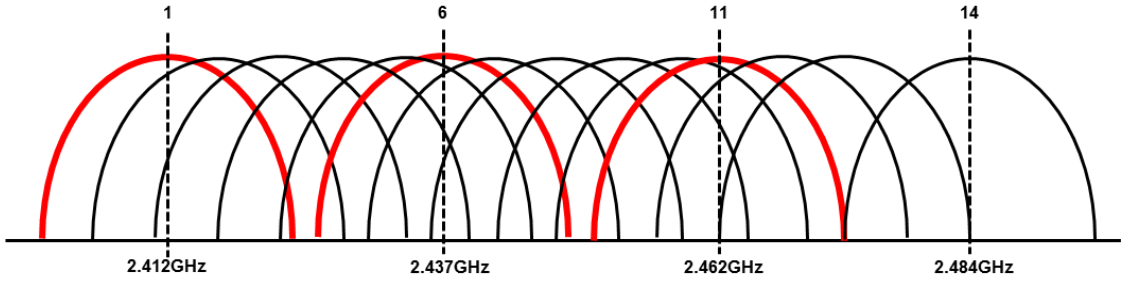
- **U-NII**

Band	Frequency Range
UNII-1	5150-5250 MHz
UNII-2	5250-5350 MHz
UNII-2 Extended	5470-5725 MHz
UNII-3	5725-5825 MHz

2.4 GHz ISM Channels

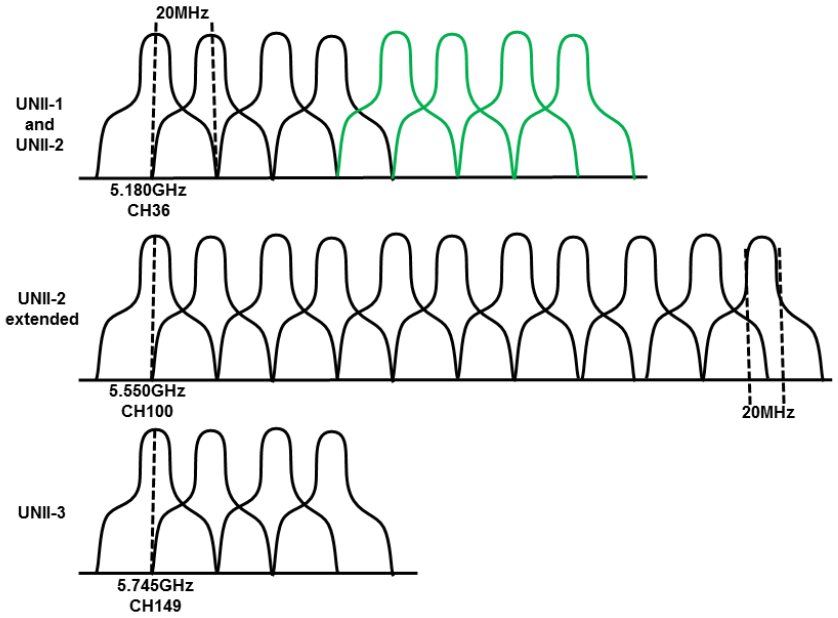
- FCC: 11 channels
- ETSI: 13 channels
- Japan: 14 channels

- Non-overlapping channels
  - 3 for FCC/ESTI
  - 4 for Japan
  - 1, 6, 11 are most common



5 GHz U-NII Channels

- 5.725 to 5.875 GHz (not allowed in all countries)
- 20 MHz channels
  - U-NII-1 (5.15 to 5.25 GHz): 4 channels
  - U-NII-2 (5.25 to 5.35 GHz): 4 channels
  - U-NII-2 extended (5.47 to 5.725 GHz): up to 11 channels
  - U-NII-3 (5.725 to 5.825 GHz): 4 channels



WLAN Standards Comparison

Standards	802.11a	802.11b	802.11g	802.11n
Release year	1999	1999	2003	2009
Max. data rate	54 Mbps	11 Mbps	54 Mbps	600 Mbps
Modulation technique	OFDM	DSSS	OFDM/DSSS	OFDM/DSSS
Frequency band	5 Ghz	2.4 Ghz	2.4 Ghz	2.4 Ghz and 5 Ghz

IEEE and Wi-Fi Alliance

- **IEEE** defines standards for advanced technology
  - IEEE 802.11 deals with Wireless LAN (WLAN)
    - Services and protocols on Layer 1 and Layer 2
    - Best practices
- **Wi-Fi Alliance** certifies interoperability of WLAN devices
- Based on IEEE 802.11

Wi-Fi Alliance Overview

- Certifies interoperability of WLAN products
  - Based on IEEE 802.11 standards
  - Interoperability of equipment from different vendors
- Wi-Fi Alliance's mission:
  - Provide a collaboration forum
  - Grow the Wi-Fi industry
  - Develop new specifications and programs
  - Support industry standards
  - Provide testing and certification

Certifications

- Wi-Fi CERTIFIED
  - Program improves user experience
  - Logo ensures interoperability
- Two types
  - Mandatory
  - Optional

Mandatory Programs

- **Core interoperability**
  - 802.11 a/b/g/n
  - Vendor-independent interoperability
- **Robust security**
  - WPA2 is mandatory
  - EAP authentication for enterprise solutions

Optional Programs

- **Wi-Fi Protected Setup**
  - Easy and secure setup
- **Wi-Fi Multimedia (WMM)**
  - Audio, video and voice priority – low delay is crucial!
- **WMM-Power Save**
  - Conserving battery life (sleep mode)
- **Wi-Fi Direct**
  - Clients connecting without the use of an AP
- **Voice Personal**
  - Interoperability and quality of VoWLAN

Wireless LAN Interference

- RF Interference causes network performance issues.
- 2.4GHz frequency band is more likely to get interference with other devices and networks.

Sources of 2.4GHz interference

Microwave Ovens

Other Wireless Networks

Baby Monitors

Cordless Phones

Air-con. Sensors

Bluetooth devices

WLAN Security

- Legacy security standards were defined from IEEE 802.11-1997 until IEEE 802.11-2004
- Static Wired Equivalent Privacy (WEP), 64-bit or 128-bit
- Open system authentication
- Shared-key authentication
- MAC filtering
- SSID hiding

Robust WLAN Security

- Legacy WLAN security considered inadequate for data privacy
- WPA as an interim solution for weak policies
- Stronger WLAN security began with the 802.11i amendment
- After 802.11i ratification, Wi-Fi Alliance introduced WPA2
- Current 802.11-2007 standard requirements
  - 802.1X/EAP for enterprise
  - Pre-shared key or passphrase for SOHO

	Standard	Encryption	Security Level	Key Type
WPA	Announced by Wi-Fi Alliance, not a standard	TKIP/RC4	Strong	Dynamic Key
WPA2	Follows IEEE 802.11i	CCMP/AES	Strongest	Dynamic Key

Wi-Fi Protected Setup (WPS)

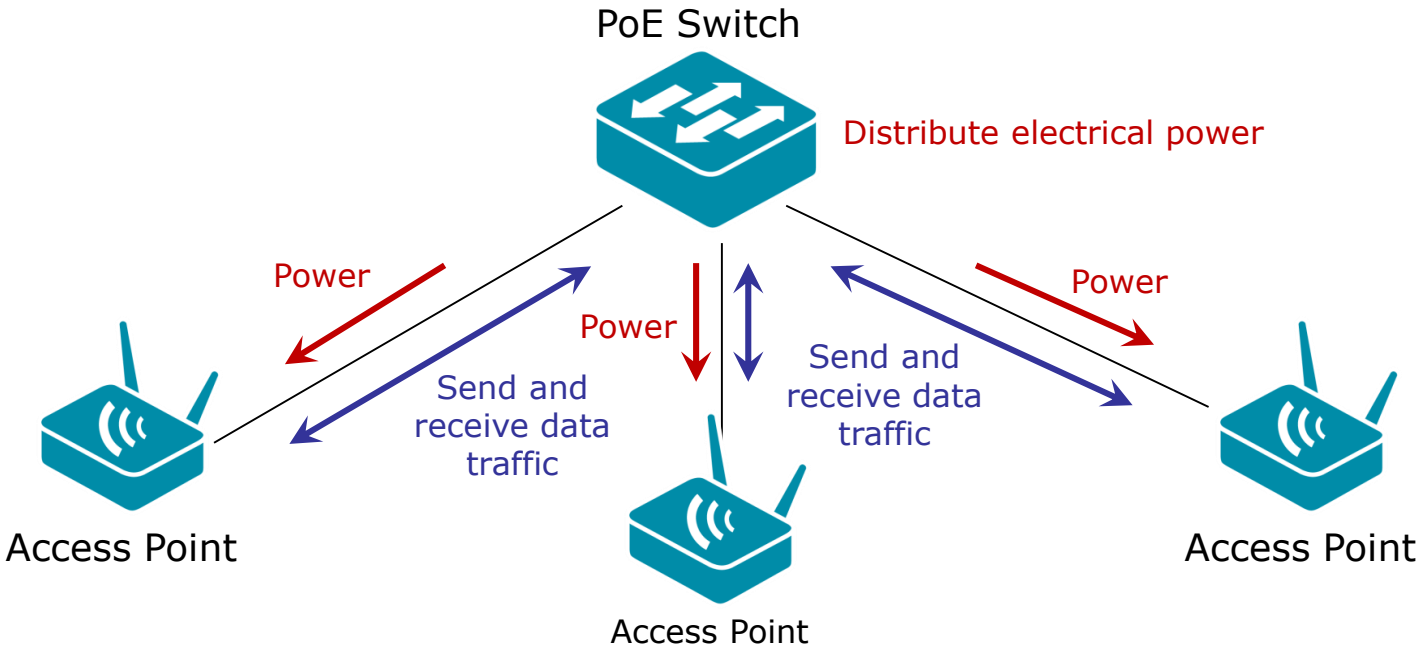
- Simple to use
- Provides automatic security configuration for SOHO environment
- Achieved by pressing a button or entering correct PIN
- Main goal is configuring WLAN clients and APs using WPA/WPA2
- Not all Wi-Fi Certified products support WPS
- WEP not supported

WPS Activation Methods

- D-Link SOHO AP/routers, two methods:
  - **PBC:** User presses WPS Push Button Configuration (PBC) button on AP/router and then clicks Connect button on wireless client within 120 seconds
  - **PIN:** User generates WPS Personal Identification Number (PIN) on AP/router and enters it on WLAN client within 120 seconds (or vice versa)

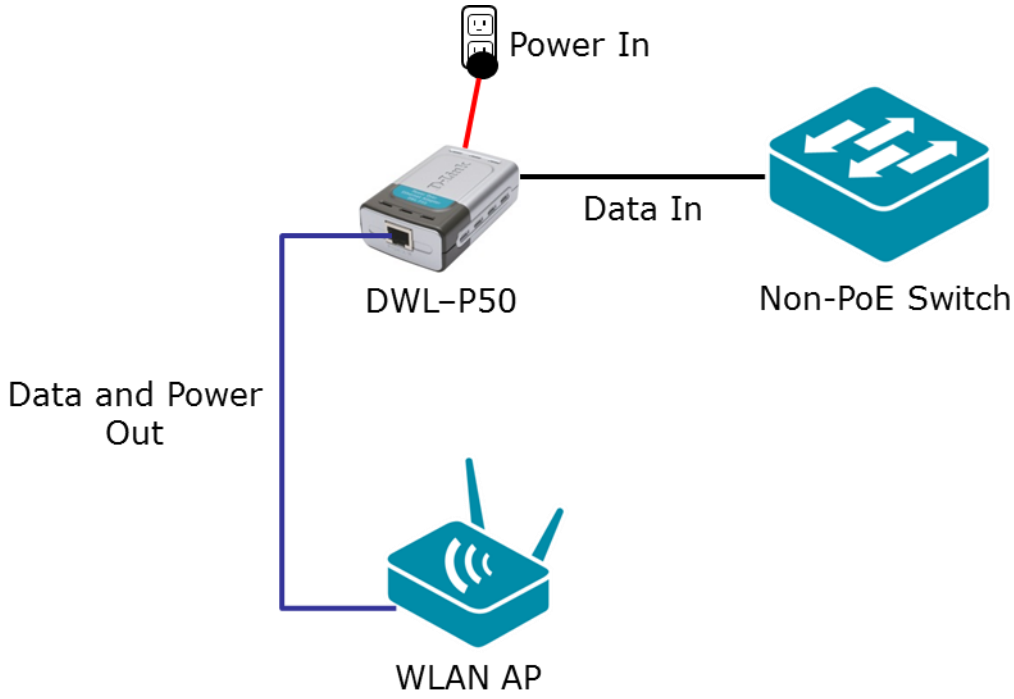
Power over Ethernet (PoE)

- Network cable delivers data and electrical power
- Benefits
  - Easier deployment of new Access Points
  - Fewer cables



PoE Delivery Methods

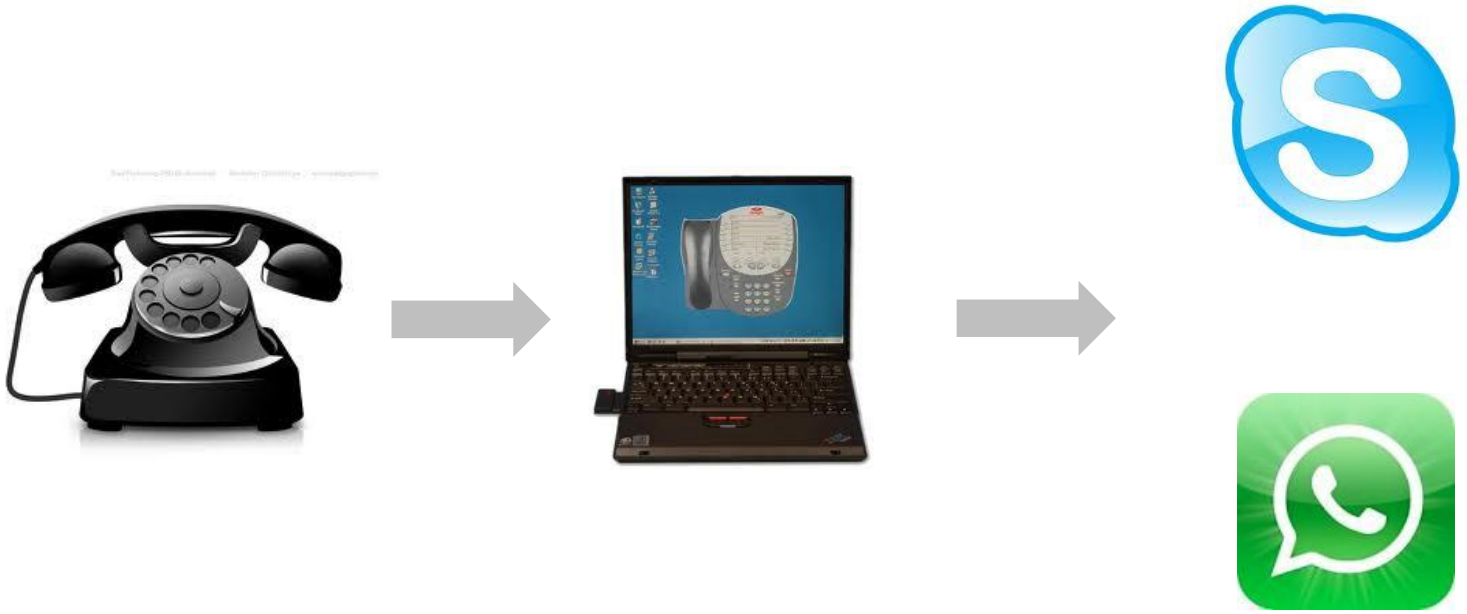
- Two types of devices
  - Powered devices
  - Power-sourcing equipment
- Two types of delivery
  - PoE-enabled switches
  - PoE external injectors



Module 5

Cloud Computing Basics

Evolution – Telephone Service



Evolution – Mail Service

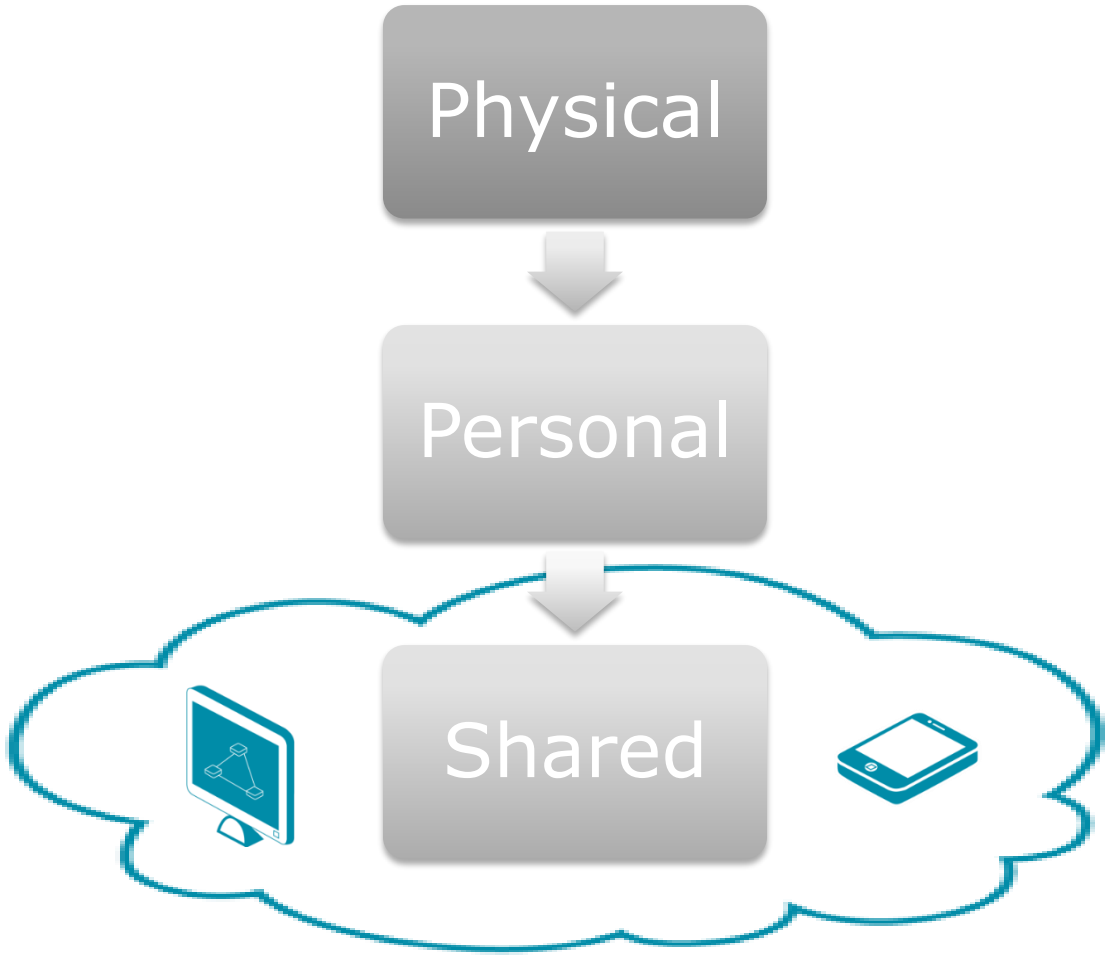
Evolution – Publishing Service

Evolution – Document Service

Microsoft Office

Google Docs

Service Evolution → Cloud Service



Why do We Need Cloud Service

- Data Explosion
- Cost Down
- Mobility

What is Cloud Computing

- A Definition

"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction."

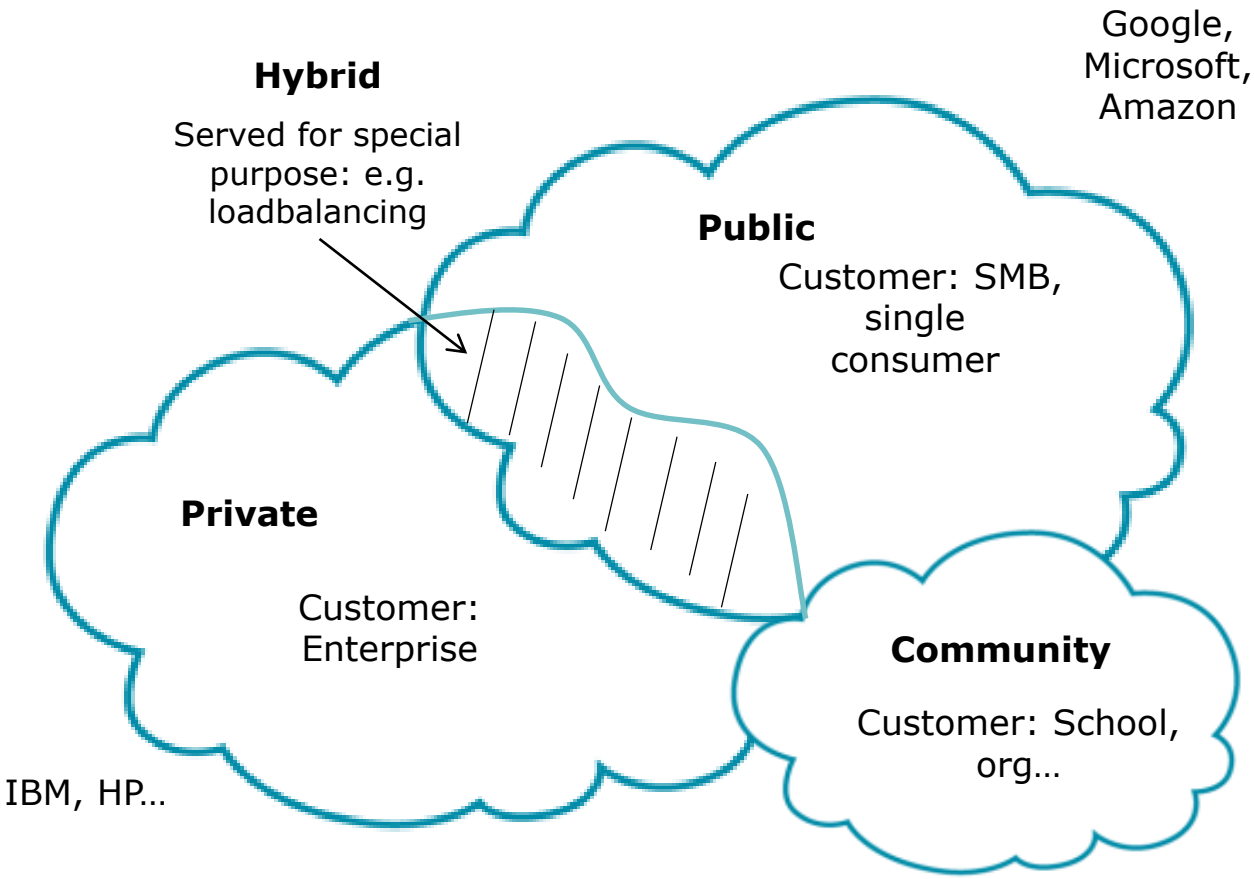
- NIST (The American National Institute of Standards and Technology)

5 Essential Characteristics

- On-demand self-service
- Broad network access
- Resource pooling
- Rapid elasticity
- Measured service

4 Deployment Models

- Private cloud
- Public cloud
- Hybrid cloud
- Community cloud



3 Service Models

- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)

salesforce.com RightNow jive Concur click. done. NETSUITE
SuccessFactors Business Execution Software workday. webex Taleo

Windows Azure heroku Google App Engine Engine Yard
force.com platform as a service vmware

GOGRID DELL hp openstack
amazon web services rackspace IT HOSTING

Source: IDC: 2010 June

Main Idea

- Any time…
- Anywhere…
- Have access to any service…
- With any devices.

Cloud in the Market

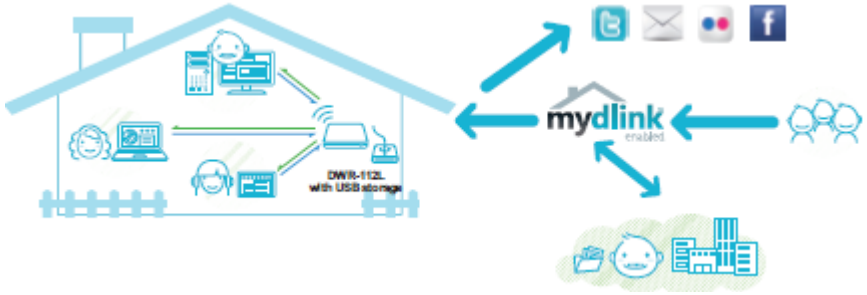
- Access
  - Anytime, Anywhere
  - mydlink-enable
  - User-friendly by design
  - No networking knowledge required

- View
  - Keep an eye on your home even when you're out
  - Share the view
  - All your files at your fingertips
  - A place for everything

Cloud in the Market

- Control
  - Stay safe
  - Stay productive
  - Stay secure
  - Stay in control

- Share
  - A personal cloud for family and friends
  - Be social, yet private
  - Sharing without the hassle
  - Safe and sound



Cloud Solutions

- Cloud Routers
  - Convenient and time-saving - Access your personal files and multimedia anywhere, anytime.
  - Better privacy – Your personal information is stored on your own device to ensure data security.
  - Limitless disk space - Swappable USB drives offer unlimited storage options.
  - Free mobile app available for iPhone, iPad and Android

Cloud Solutions

- Cloud Camera
  - Enjoy peace of mind by monitoring your kids, pets, possessions, and more
  - View and record important events
  - Compatible with mobile Internet devices such as iPhones, iPads, Android Phones, Android Tablets, Windows PCs, Macs, etc.
  - Complete easy installation in a few steps without requiring much networking knowledge.
  - Connect to mydlink to view live camera feeds and recordings.
  - Upload video clips to social networks for sharing.

Cloud Solutions

- Cloud Storages
  - Easy to install without any technical knowledge.
  - Family and friends can access your personal content with an easy-to remember URL.
  - Create a personal cloud at home which only authorized people can access.
  - Less power consumption than a typical PC server.
  - Enjoy many additional features like audio/video streaming, web server, photo gallery, etc.

Module 6

Network Application

Scenario 1: Residential Internet Access

- Requirement:
  - Internet access (PPPoE or DHCP or Static)
  - Network connection for:
    - Wireless Desktop PC
    - Wireless Smart Phone and Laptop
  - Secure wireless connection with WPA2-Personal (SSID: DNAcertification)
  - Web service for external users
- Time: 40 minutes

Scenario 2: Residential Cloud Access and Management

- Requirement:
  - Internet access (PPPoE or DHCP or Static)
  - Network connection for:
    - Wireless Desktop PC
    - Wireless Smart Phone and Laptop
  - Remote monitoring from mobile devices
  - Remote management from mobile devices
- Time: 20 minutes

Scenario 3: Traveler network access sharing

- Requirement: (DIR-505)
  - Wired Internet access sharing for wireless users
  - Wireless Internet access sharing for wired and wireless users
  - USB flash disk file sharing
- Time: 20 minutes