Digital Imaging and PACS

Yudthaphon Vichianin, Ph.D.

1

Presentation File

Lab file: https://cutt.ly/jNnu35q

2

Pre-test

Yudthaphon Vichianin, Ph.D.

3

PACS and Related Components

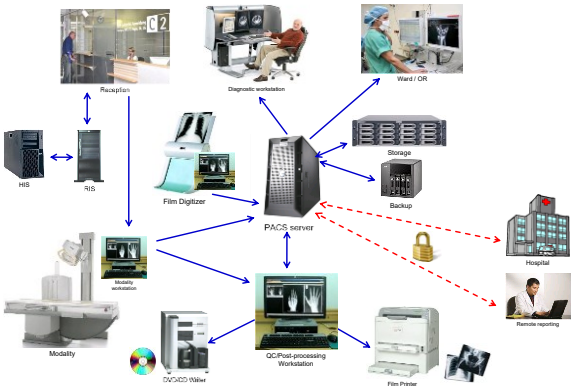
Yudthaphon Vichianin, Ph.D.
Department of Radiological Technology
Faculty of Medical Technology
Mahidol University

4

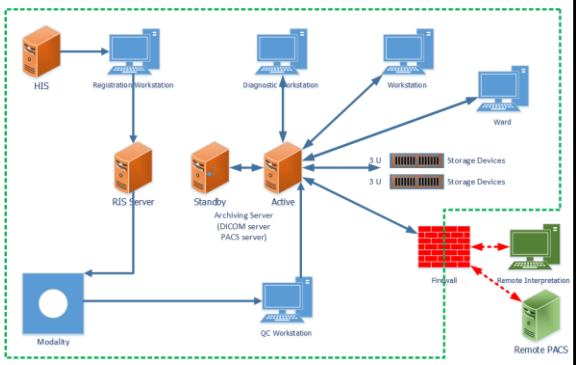
Agenda

- The Big picture
- Hardware & Software Components
- Storage Devices
- Fault Tolerance Techniques
- Network & Security

5



6



7

PACS: Components

- PACS is an Information System
  - Hardware: Workstation, Server, Monitor
  - Software: OS, Database, Application
  - Network: Communication Technologies
  - Data: i.e. images
  - People: i.e. Administrator, Users, Vendors
  - Policy: i.e. Workflow, Standards, Laws

8

PACS: Hardware & Software

- Monitor: Medical Grade Display with DICOM compliance
- Hardware:
  - Server: High performance machine serving multiple clients
- Software:
  - Vender specifics

9

10

Computer hardware

- **Computer hardware** is the collection of physical components that constitute a computer system. Computer hardware is the physical parts or components of a computer, such as monitor, keyboard, computer data storage, hard disk drive (HDD), graphic card, sound card, memory (RAM), motherboard, and so on, all of which are tangible physical objects.[1] By contrast, software is instructions that can be stored and run by hardware.

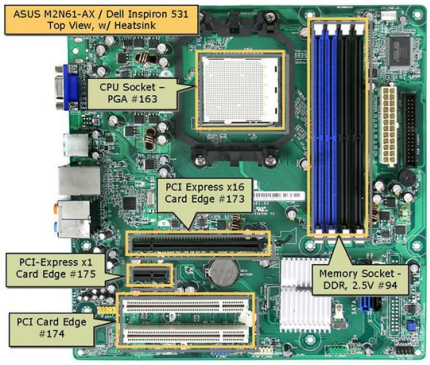
11

Computer hardware

- The **CPU** (Central Processing Unit), which performs most of the calculations which enable a computer to function, and is sometimes referred to as the brain of the computer. It is usually cooled by a heatsink and fan, or water-cooling system.
- The clock speed of CPUs governs how fast it executes instructions, and is measured in GHz; typical values lie between 1 GHz and 5 GHz.

12

13



Source: IHS

14

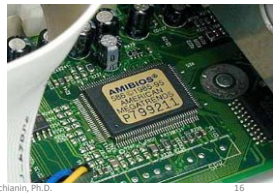
Computer hardware

- **Random-Access Memory** (RAM), a type of computer memory that can be accessed randomly; that is, any byte of memory can be accessed without touching the preceding bytes. RAM is the most common type of memory found in computers and other devices.
- **Read-Only Memory** (ROM), is a type of non-volatile memory used in computers and other electronic devices. Data stored in ROM can only be modified slowly, with difficulty, or not at all, so it is mainly used to store firmware (software that is closely tied to specific hardware, and unlikely to need frequent updates) or application software in plug-in cartridges.

15

Random-Access Memory

Read-Only Memory



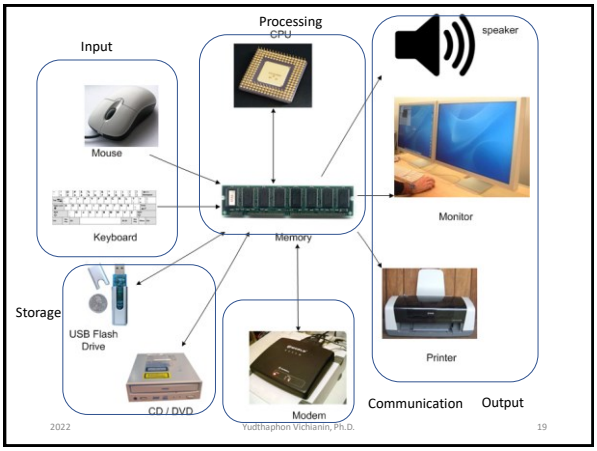
16

Computer hardware

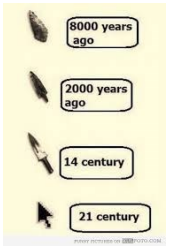
- The **video card** (also known as the graphics card), which processes computer graphics. More powerful graphics cards are better suited to handle strenuous tasks, such as playing intensive video games.

17

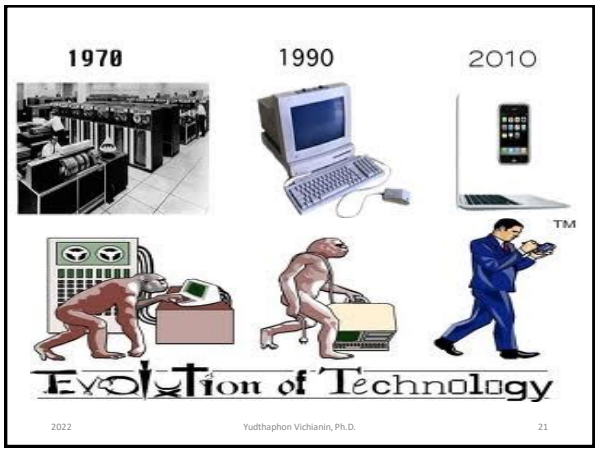
18



19



20



21

PACS Servers

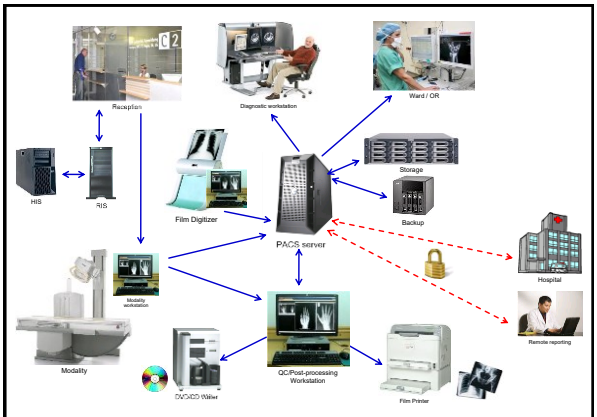
Yudthaphon Vichianin, Ph.D.
Department of Radiological Technology
Faculty of Medical Technology
Mahidol University

22

PACS

- A **picture archiving and communication system (PACS)** is a medical imaging technology which provides economical storage and convenient access to images from multiple modalities (source machine types).

23



24

Desktop Computer | **Server Computer**

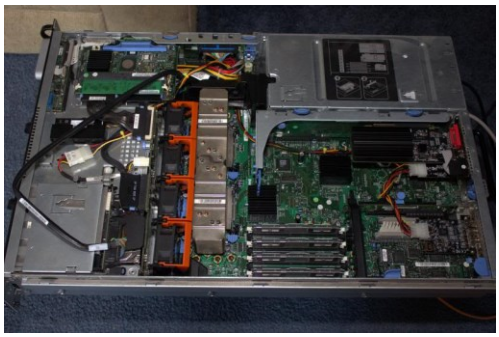
8/5 | **24/7**

25

26

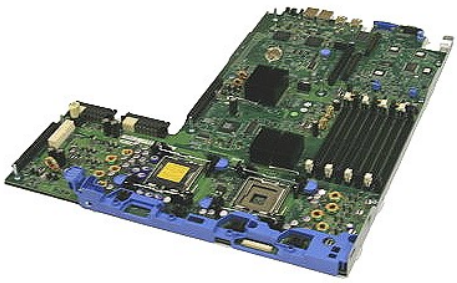
http://www.ithov.com/uploads/allimg/200903/20090330133124946.jpg

27



http://i77.photobucket.com/albums/j61/PockyFreak/fansinstelledinPE2950.jpg

28

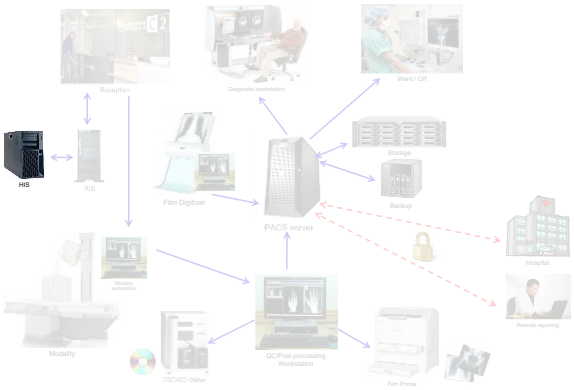


29

Redundant Power Supply

Hot Plug / Hot Swap

30

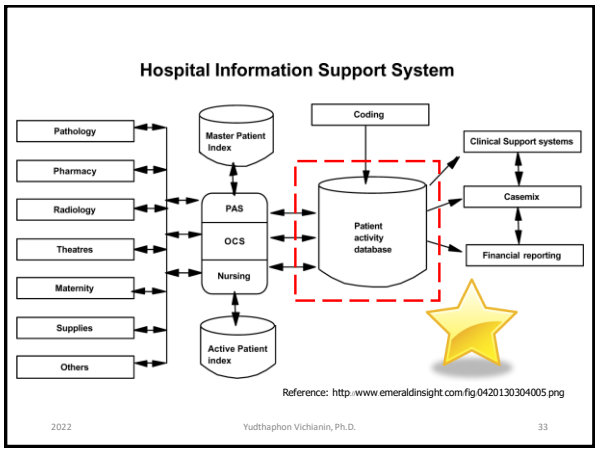


31

HIS

- A **hospital information system (HIS)** is essentially a computer system that can manage all the information to allow health care providers to do their jobs effectively.
- These systems have been around since they were first introduced in the 1960s and have evolved with time and the modernization of **healthcare** facilities

32

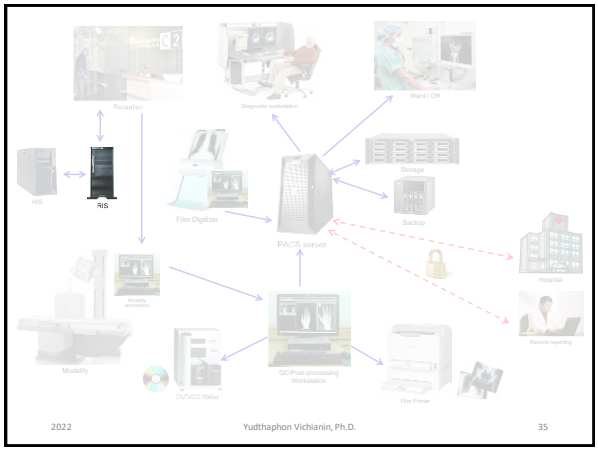


33

RIS

- **Radiology information systems (RIS)** are computerized databases that are utilized to track, manipulate, and distribute patient data and imagery.
- RIS is the core system for the electronic management of imaging departments.

34



35

RIS Functionality

- Patient registration and scheduling
- Patient list management
- Interface with modality via Work-list
- Radiology Department workflow management
- Request and document scanning
- Result(s) entry
- Reporting and printout
- Result(s) delivery including faxing and e-mailing of clinical reports
- Patient tracking
- Interactive documents
- Technical files creation
- Modality and material management

36

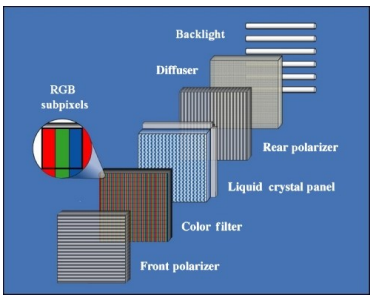
RIS Options

- HL7 interfaces with a PACS.
- HL7 also enables communication between HIS and RIS in addition to RIS and PACS.

37

Medical LED Monitor

38



Major components of an optical stack of a liquid crystal display. The color filters are omitted for inherently grayscale displays.

39

Medical Monitor (LCD/LED)

- Backlight
- Diffuser
- Rear polarizer
- Liquid crystal panel
- Color filter
- Front polarizer

40

Medical Monitor

https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3043865/

41

Medical Monitor: Factors

- Viewing Angle → Contrast
- Ambient Light → Reflection → Contrast
- Display Visual Noise

42

Display Calibration

- The luminance (and perceived) contrast of an uncalibrated LCD can vary greatly throughout the input digital driving level (DDL) range of a single display.
- For calibrating medical imaging grade displays, a photometer should be accurate to within 5%
- Except for very low luminance levels (0.5 cd/m2) where an accuracy of 10% may suffice.

43

Display Calibration

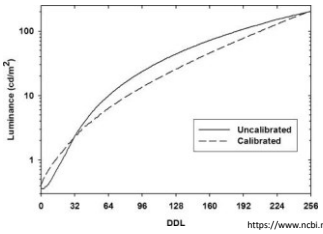
- The goal of grayscale calibration of electronic displays is to **ensure** that images presented to an observer have **equal perceived contrast** appearance **on all displays**, independent of the luminance range of the display.

https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3043865/

44

Display Calibration

- Typical contrast ratios are in the range of 250 to 400 for color displays and up to 600 (or more) for inherently grayscale displays.



$$C = \frac{L^d_{\max}}{L^d_{\min}}$$

https://www.ncbi.nlm.nlm.nih.gov/pmc/articles/PMC3043865/

45

Photometer

- A photometer is an appropriate device to measure the luminance emitted (or reflected) from a display.

http://www.baylandtechnologies.com/assets/useradds/024.png

46

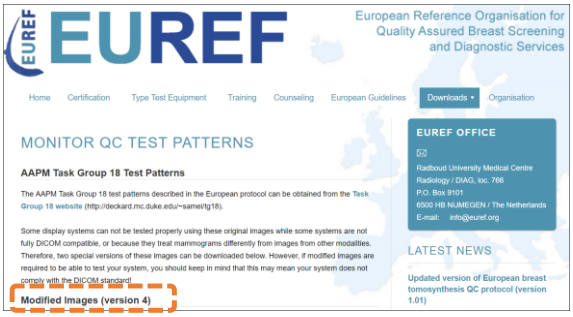
http://www.xrite.com/categories/calibration-profiling/i1display-pro

47

http://img.medicalexpo.com/images_me/photo-m2/83410-10333077.jpg

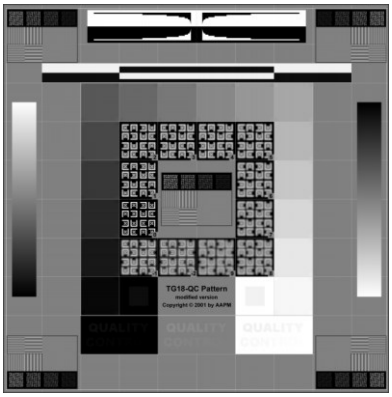
48

Test Pattern:



http://www.euref.org/downloads/software-physico-technical-protocol/monitor-qc-test-patterns

49



50

PACS checklists

- High availability: ready 24/7
- Good network: enough bandwidth for sending images and communicating the results
- Data interface with other systems: HIS/RIS via HL7
- Ensure images exchange: DICOM standard
- Scalable for future expansion: Well storage planning

51

What "High Availability" Means in Terms of Down-Time*

Availability (percentage)	Average per year (days)	Average per month (hours)	Average per week (hours)	Average per (minutes)
95%	18.25	36.5	8.42	72
98%	7.3	14.6	3.37	28.8
99%	3.65	7.3	1.69	14.4
99.9%	0.365	0.73	0.17	1.44
99.99%	0.0365	0.073	0.017	0.144
99.999%	0.00365	0.0073	0.0017	0.0144

*Excludes planned down time for maintenance and upgrades.

Reference: SCAR University Primer2: Archiving Issues in the Digital Medical Enterprise

52

Service-Level Agreement (SLA)

- A service-level agreement (SLA) is defined as an official commitment that prevails between a service provider and the customer.
- Particular aspects of the service – quality, availability, responsibilities – are agreed between the service provider and the service user.

https://en.wikipedia.org/wiki/Service-level_agreement

53

Service-Level Agreement (SLA)

- **Abandonment Rate**: Percentage of calls abandoned while waiting to be answered.
- **ASA (Average Speed to Answer):** Average time (usually in seconds) it takes for a call to be answered by the service desk.
- **TSF (Time Service Factor):** Percentage of calls answered within a definite timeframe, e.g., 80% in 20 seconds.
- **FCR (First-Call Resolution):** Percentage of incoming calls that can be resolved without the use of a callback or without having the caller call back the helpdesk to finish resolving the case.
- **TAT (Turn-Around Time):** Time taken to complete a certain task.
- **MTTR (Mean Time To Recover):** Time taken to recover after an outage of service.

https://en.wikipedia.org/wiki/Service-level_agreement

54

Service-Level Agreement (SLA)

- **Uptime** is also a common metric, often used for data services such as shared hosting, virtual private servers and dedicated servers.
- Common agreements include
  - **Percentage of network uptime** (the time during which a computer is operational. Downtime is the time when it isn't operational)
  - **Number of scheduled maintenance windows**

https://en.wikipedia.org/wiki/Service-level_agreement

55

Service Outages

- Outages caused by system failures can have a serious impact on the users of computer/network systems, in particular those industries that rely on a nearly 24-hour service:
  1. Medical informatics
  2. Nuclear power and other infrastructure
  3. Banks and other financial institutions
  4. Aeronautics, airlines
  5. News reporting
  6. E-commerce and online transaction processing
  7. Persistent online games

https://en.wikipedia.org/wiki/Downtime

56

Planned Outage

- A planned outage is the result of a planned activity by the system owner and/or by a service provider.
- These outages, often scheduled during the maintenance window, can be used to perform tasks including the following:
  1. Deferred maintenance, e.g., a deferred hardware repair or a deferred restart to clean up a garbled memory
  2. Diagnostics to isolate a detected fault
  3. Hardware fault repair
  4. Fixing an error or omission in a configuration database or omission in a recent configuration database change
  5. Fixing an error in application database or an error in a recent application database change
  6. Software patching/software updates to fix a software fault.

https://en.wikipedia.org/wiki/Downtime

57

Response and Reduction of Impact

- A process needs to be in place to detect a malfunction - network monitoring - and to restore the network to a working condition
- Risk may be minimized by using reliable components, by performing maintenance, such as upgrades, by using redundant systems or by having a contingency plan or business continuity plan.
- One of the biggest causes of downtime is misconfiguration, where a planned change goes wrong.

https://en.wikipedia.org/wiki/Downtime

58

Highly available system

- A **computer cluster** consists of a set of loosely or tightly connected computers that work together so that, in many respects, they can be viewed as a single system.

59

High-Availability Cluster

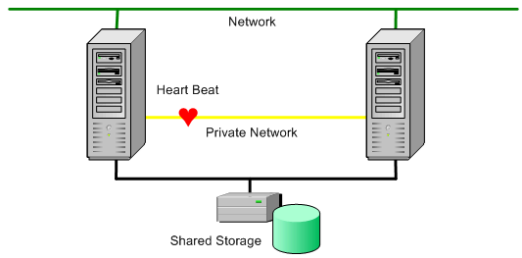
- **High-availability clusters** (also known as HA clusters or fail-over clusters) are groups of computers that support server applications that can be reliably utilized with a minimum amount of down-time.
- They operate by using high availability software to harness **redundant computers** in groups or clusters that provide continued service when system components fail.

60

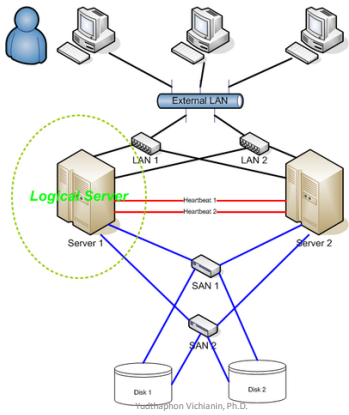
High-Availability Cluster

- Without clustering, if a server running a particular application crashes, the application will be unavailable until the crashed server is fixed.
- HA clustering remedies this situation by **detecting** hardware/software faults, **and immediately restarting the application** on another system **without requiring administrative intervention**, a process known as failover.

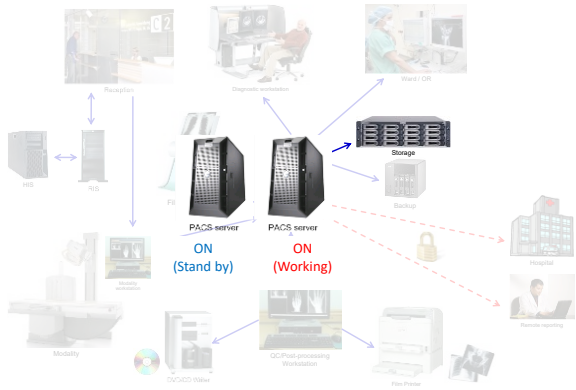
61



62



63

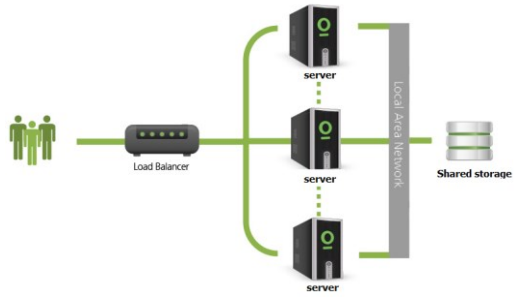


64

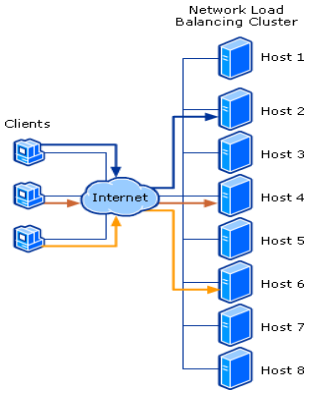
Load-Balancing Cluster

- Load balancing improves the distribution of workloads across multiple computing resources
- Load balancing aims to optimize resource use, maximize throughput, minimize response time, and avoid overload of any single resource.
- Using multiple components with load balancing instead of a single component may increase reliability and availability through redundancy.

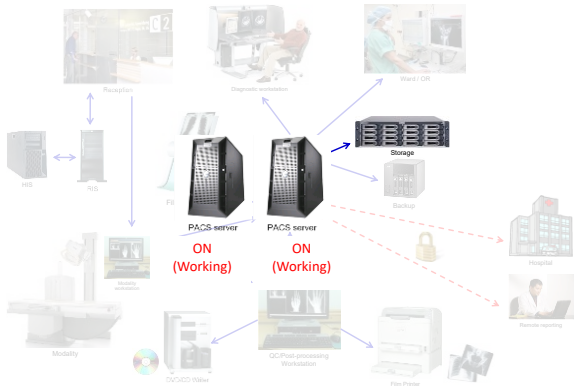
65



66



67

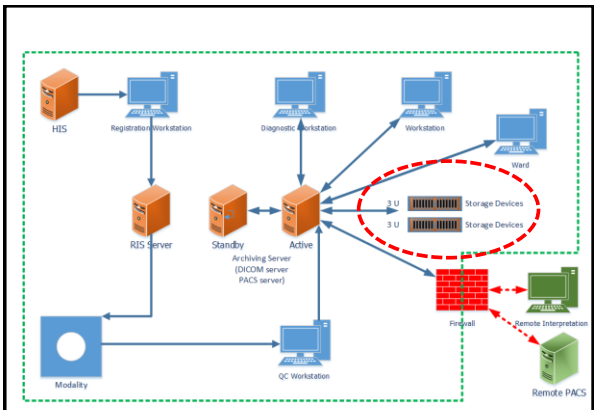


68

PACS Data Storage

Yudthaphon Vichianin, Ph.D.
Department of Radiological Technology
Faculty of Medical Technology
Mahidol University

69



70

PACS: Storage Devices

- Direct Attach Storage (DAS)
- Network Attach Storage (NAS)
- Storage Area Network (SAN)

71

Direct-attached storage (DAS)

- Direct-attached storage (DAS) is digital storage directly attached to the computer accessing it, as opposed to storage accessed over a computer network.




72

Network Attach Storage (NAS)

- A NAS unit is a computer **connected to a network** that provides only file-based data storage services to other devices on the network.
- It is a file-level computer data storage server connected to a computer network providing data access to a heterogeneous group of clients.

https://en.wikipedia.org/wiki/Network-attached_storage

73

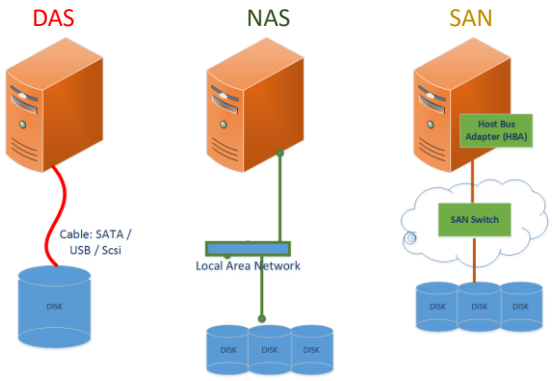


74

Storage Area Network (SAN)

- A storage area network (SAN) is a network which provides access to consolidated, **block level** data storage.
- A SAN does not provide file abstraction.
- **NAS** appears to the client OS (operating system) as a **file server** (the client can map network drives to shares on that server) whereas a disk available through a **SAN** still appears to the client OS as **a disk**, visible in disk and volume management utilities (along with client's local disks), and available to be formatted with a file system and mounted.

75



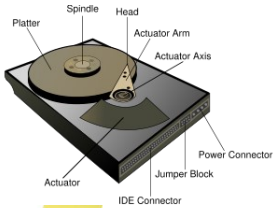
76

PACS: Storage Devices Comparison

Items of Interest	DAS	NAS	SAN
Cost	☺	☺	☹
Management	😐	😐	☺
Fault Tolerance	☹	☺	☺
PACS	😐	☺	☺

77

Hard Drive



- Platter:
- Spindle: Motor
- Actuator: read/write data
  - Arm:
  - Axis:
- Power Connector:
- IDE Connector: IDE: 16 MB/s
- SATA: 1.5 Gbit/sec

78

Hard Disk Drive - HDD Solid State Drive - SDD

79

80

TEN TIMES THE WORKLOAD CAPABILITY OF DESKTOP DRIVES

The workhorse of our datacenter portfolio. High performance, capacity and reliability make the WD Re drive ideal for data warehousing/mining and high-performance computing.

High Capacity Nearline Drive

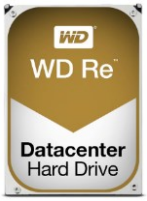
Massive capacities up to 6TB suit even the most demanding datacenter, enterprise server, or cloud storage needs.

Designed to Handle up to 550TB Per Year

Among the highest workload capability of any 3.5-inch hard drive that delivers performance and reliability to any datacenter environment.

Up to 2 Million Hours MTBF

The WD Re drive delivers a high level of reliability for 24×7×365 operation in the most demanding storage environments.[1]



81

Improvement of HDD characteristics

Parameter	Started with (1956)	Developed to (2016)	Improvement
Capacity (formatted)	3.75 megabytes	10 terabytes	2.7-million-to-one
Physical volume	68 cubic feet (1.9 m^3)	2.1 cubic inches (34 cm^3)	56,000-to-one
Weight	2,000 pounds (910 kg)	2.2 ounces (62 g)	15,000-to-one
Average access time	approx. 600 milliseconds	2.5 ms to 10 ms; RW RAM dependant	about 200-to-one
Price	US$9,200 per megabyte (1961)	US$0.032 per gigabyte by 2015	300-million-to-one
Data density	2,000 bits per square inch	1.3 terabits per square inch in 2015	650-million-to-one
Average lifespan	~2000 hrs	~22500 hrs	11-to-one

https://en.wikipedia.org/wiki/Hard_disk_drive

82

A newer 2.5-inch (63.5 mm) 6,495 MB HDD compared to an older 5.25-inch full-height 110 MB HDD

https://en.wikipedia.org/wiki/Hard_disk_drive

83

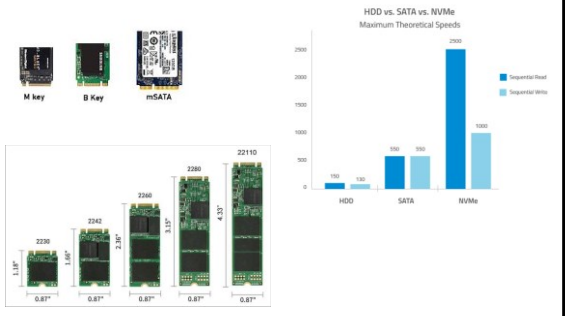
Decimal and binary unit prefixes interpretation

Capacity advertised by manufacturers		Capacity expected by some consumers		Reported capacity	
With prefix	Bytes	Bytes	Diff.	Windows, Linux	MacOS 10.6+
100 GB	100,000,000,000	107,374,182,400	7.37%	93.1 GB, 95,367 MB	100 GB
1 TB	1,000,000,000,000	1,099,511,627,776	9.95%	931 GB, 953,674 MB	1,000 GB, 1,000,000 MB

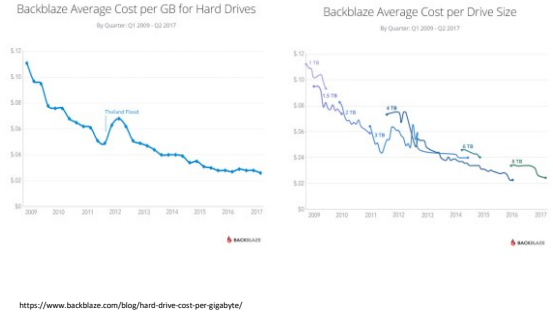
https://en.wikipedia.org/wiki/Hard_disk_drive

84

M.2

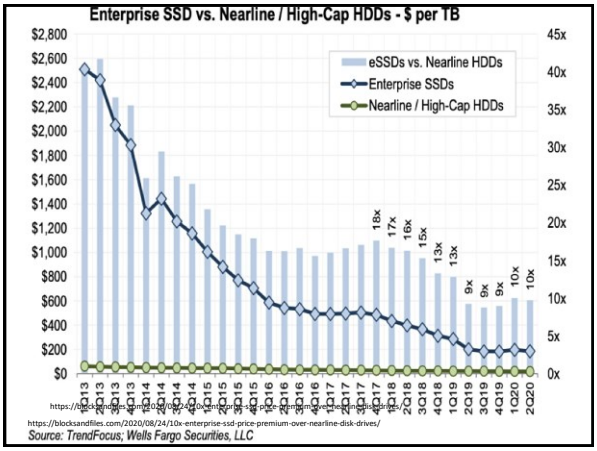


85



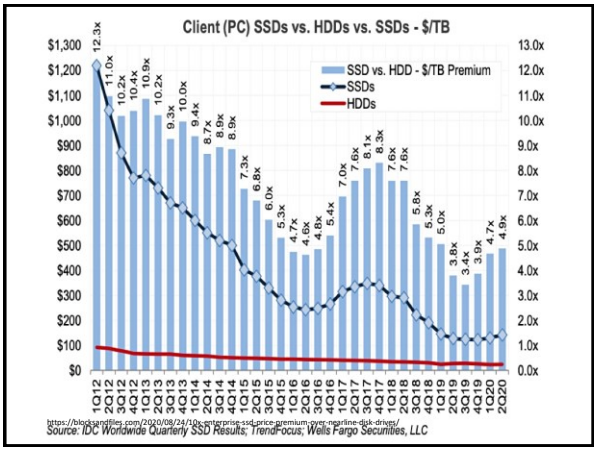
https://www.backblaze.com/blog/hard-drive-cost-per-gigabyte/

86



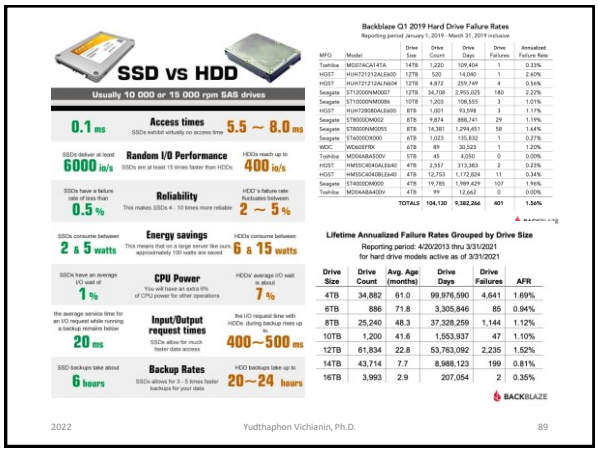
https://blocksandfiles.com/2020/08/24/10x-enterprise-ssd-price-premium-over-nearline-disk-drives/

87

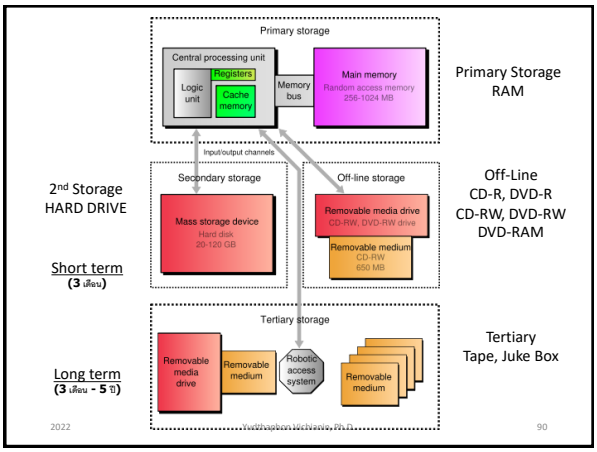


https://blocksandfiles.com/2020/08/24/10x-enterprise-ssd-price-premium-over-nearline-disk-drives/

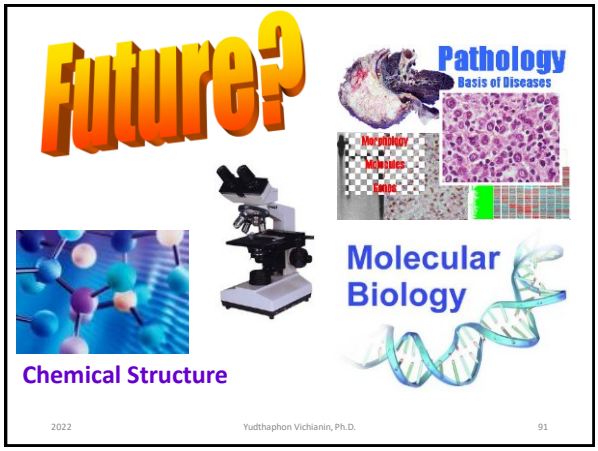
88


SSD vs HDD
Usually 10 000 or 15 000 rpm SAS drives
Access times
0.1 ms
5.5 ~ 8.0 ms
Random I/O Performance
6000 io/s
400 io/s
Reliability
0.5 %
2 ~ 5 %
Energy savings
2 & 5 watts
6 & 15 watts
CPU Power
1 %
7 %
Input/Output request times
20 ms
400~500 ms
Backup Rates
6 hours
20~24 hours
Backblaze Q1 2019 Hard Drive Failure Rates
Reporting period January 1, 2019 - March 31, 2019 inclusive
Lifetime Annualized Failure Rates Grouped by Drive Size
Reporting period: 4/20/2013 thru 3/31/2021
for hard drive models active as of 3/31/2021
Drive Size | Drive Count | Avg. Age (months) | Drive Days | Drive Failures | AFR
4TB | 34,882 | 61.0 | 99,976,590 | 4,641 | 1.69%
6TB | 886 | 71.8 | 3,305,846 | 85 | 0.94%
8TB | 25,240 | 48.3 | 37,328,259 | 1,144 | 1.12%
10TB | 1,200 | 41.6 | 1,553,937 | 47 | 1.10%
12TB | 61,834 | 22.8 | 53,763,092 | 2,235 | 1.52%
14TB | 43,714 | 7.7 | 8,988,123 | 199 | 0.81%
16TB | 3,993 | 2.9 | 207,054 | 2 | 0.35%
BACKBLAZE
2022
Yudthaphon Vichianin, Ph.D.
89

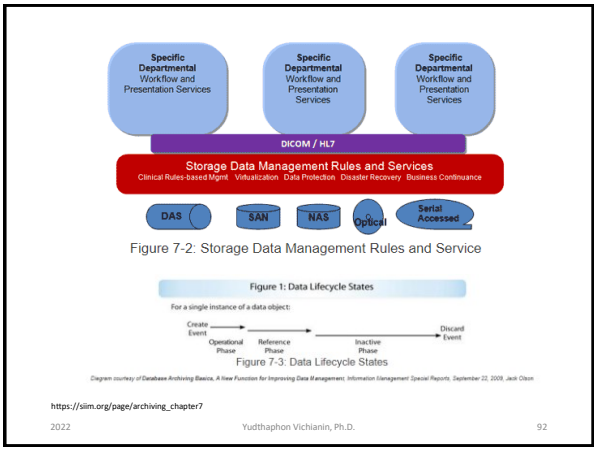
89


Primary storage
Central processing unit
Logic unit
Registers
Cache memory
Memory bus
Main memory
Random access memory
256-1024 MB
Primary Storage
RAM
Input/output channels
2nd Storage
HARD DRIVE
Secondary storage
Mass storage device
Hard disk
20-120 GB
Off-line storage
Removable media drive
CD-RW, DVD-RW drive
Removable medium
CD-RW
650 MB
Off-Line
CD-R, DVD-R
CD-RW, DVD-RW
DVD-RAM
Short term
(3 เดือน)
Tertiary storage
Removable media drive
Removable medium
Robotic access system
Removable medium
Tertiary
Tape, Juke Box
Long term
(3 เดือน - 5 ปี)
2022
Yudthaphon Vichianin, Ph.D.
90

90


Future?
Pathology
Basis of Diseases
Molecular
Biology
Chemical Structure
2022
Yudthaphon Vichianin, Ph.D.
91

91


Specific Departmental Workflow and Presentation Services
Specific Departmental Workflow and Presentation Services
Specific Departmental Workflow and Presentation Services
DICOM / HL7
Storage Data Management Rules and Services
Clinical Rules-based Mgmt Virtualization Data Protection Disaster Recovery Business Continuance
DAS
SAN
NAS
Optical
Serial Accessed
Figure 7-2: Storage Data Management Rules and Service
Figure 1: Data Lifecycle States
For a single instance of a data object:
Create Event
Operational Phase
Reference Phase
Inactive Phase
Discard Event
Figure 7-3: Data Lifecycle States
https://siim.org/page/archiving_chapter7
2022
Yudthaphon Vichianin, Ph.D.
92

92

Long-term archive costs is essential

- Costs of archiving data should consider that the retention period for the data will exceed the life of the technology used to keep the data.
- Long-term archives are now active elements of any clinical operation rather than just disaster recovery repositories.
- Data retention is a requirement that can extend **beyond 7 years up to 21+.**
- New data types are emerging that eclipse the archiving needs created by radiology by orders of magnitudes.
- Three types of cost models for data archive expenditure are linear, asymmetric, and symmetric.

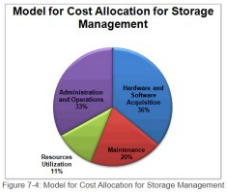


Figure 7-4: Model for Cost Allocation for Storage Management

https://siim.org/page/archiving_chapter7

93

Society for Imaging Informatics in Medicine

https://siim.org/page/archiving_additional

94

Calculation of Storage Requirements per Study Based on Institutional Procedure Protocol

Modality	Average number of images per study	Image size (pixels) X	Y	Pixel depth (bytes)	MB per study
Computed tomography	60	512	512	2	31.5
Magnetic resonance	160	256	256	2	21.0
Computed radiography	3	2048	2500	2	30.7
Ultrasound	30	640	480	2*	18.4
Nuclear medicine	10	256	256	2	1.3

* Monochrome ultrasound studies are 1 B deep and color US studies are 3 B deep; average of 2 B deep is used.

Reference: SCAR University Primer2: Archiving Issues in the Digital Medical Enterprise

95

Calculation of Storage Requirements per Day and per Year Based on Institutions' Procedure Volumes

	MB per study	Studies per year	Studies per day	Average MB of *storage required per day	Average GB of storage required per year
Computed tomography	31.5	16,120	62	1,953	508
Magnetic resonance	21.0	11,960	46	966	251
Computed radiography	30.7	59,800	230	7,061	1,836
Ultrasound	18.4	9,100	35	644	167
Nuclear medicine	1.3	8,320	32	42	11

*Averaged over the year, based on 5 days per week and 52 weeks per year.

Reference: SCAR University Primer2: Archiving Issues in the Digital Medical Enterprise

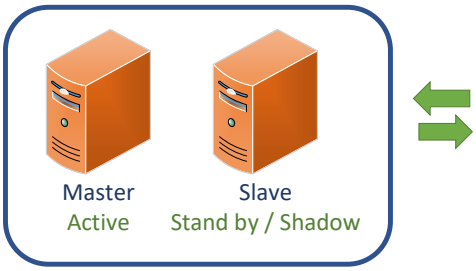
96

Fault Tolerance Technique

- Server
  - Clustering
    - High Availability Custer (HA)
    - Load Balancing Cluster
    - High Performance (HPC)

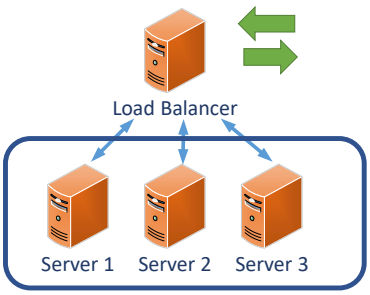
97

High Availability Custer (HA)



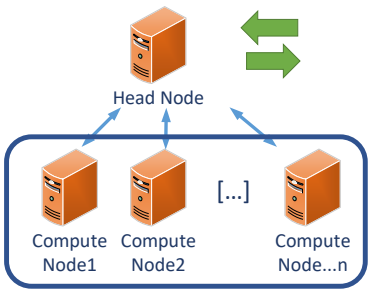
98

Load Balancing Cluster



99

High Performance (HPC)



100

Disk Fault Tolerance

- Data Failure
  - Virus/Malware
  - Hacking Attack
  - **Disk Failure**
- How to prevent disk failure?
  - **R**edundant **A**rray of **I**ndependent **D**isks **(RAID)**

101

RAID Techniques

- Stripping – data separation
- Mirroring – duplicated copy
- Error Correction – Electronic Calculation

102

Storage servers with 24 hard disk drives and built-in hardware RAID controllers supporting various RAID levels

https://en.wikipedia.org/wiki/RAID

103

RAID Techniques

- The configurations that employ the techniques of striping, mirroring, or parity to create large reliable data stores from multiple general-purpose computer hard disk drives (HDDs).
- RAID 0 - 6

https://en.wikipedia.org/wiki/Standard_RAID_levels

104

Standard RAID Levels

- RAID 0: Striped Set
- RAID 1: Mirrored (HOT SPARE)
- RAID 3 and RAID 4: Striped Set (min 3 HDDs) with Dedicated Parity
- RAID 5: Striped Set (min 3 HDDs) with Distributed Parity
- RAID 6: Striped Set (min 4 HDDs) with Double-Distributed Parity

105

RAID 0

- RAID 0 (also known as a **stripe set** or striped volume) splits ("**stripes**") data evenly across two or more disks, without parity information, redundancy, or fault tolerance.
- RAID 0 provides **no fault tolerance or redundancy**, the failure of one drive will cause the entire array to fail; as a result of having data striped across all disks, the failure will result in **total data loss**.
- RAID 0 is primarily used in applications that require **high performance** and are able to tolerate lower reliability, such as in **scientific computing.**

https://en.wikipedia.org/wiki/Standard_RAID_levels

106

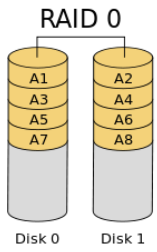
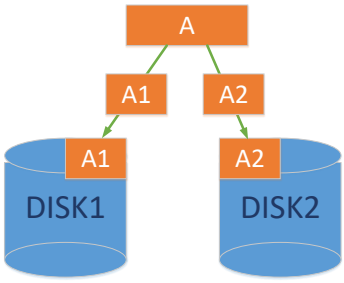


Diagram of a RAID 0 setup

https://en.wikipedia.org/wiki/Standard_RAID_levels

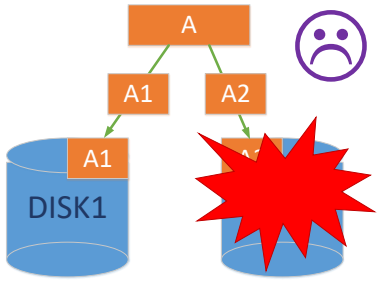
107

RAID Level 0 -- Stripping



108

RAID Level 0 -- Stripping



109

RAID 1

- RAID 1 consists of an **exact copy** (or **mirror**) of a set of data on two or more disks; a classic RAID 1 mirrored pair contains **two disks**.
- Random read performance of a RAID 1 array may equal up to **the sum of each member's performance** while the write performance remains at the level of a single disk.

https://en.wikipedia.org/wiki/Standard_RAID_levels

110

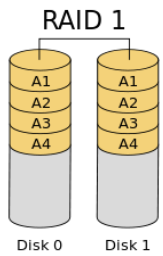
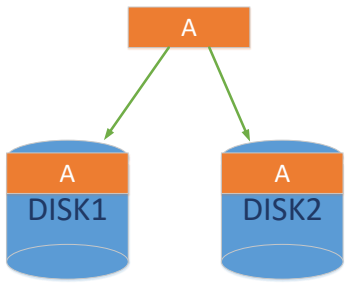


Diagram of a RAID 1 setup

https://en.wikipedia.org/wiki/Standard_RAID_levels

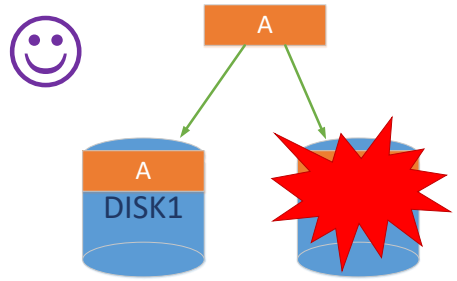
111

RAID Level 1-- Mirroring



112

RAID Level 1-- Mirroring



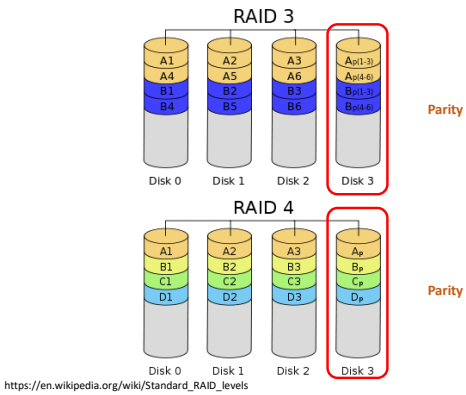
113

RAID 3 & 4

- RAID 3, which is rarely used in practice, consists of **byte-level** striping with a dedicated parity disk.
- RAID 4 consists of **block-level** striping with a dedicated parity disk.
- Applications that make **small reads and writes from random disk locations will get the worst performance** out of this level.
- The performance of random writes is low due to the need **to write all parity data to a single disk**.

https://en.wikipedia.org/wiki/Standard_RAID_levels

114



https://en.wikipedia.org/wiki/Standard_RAID_levels

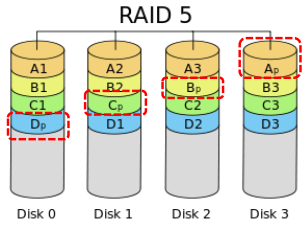
115

RAID 5

- RAID 5 consists of block-level striping with distributed parity. Unlike in RAID 4, parity information is distributed among the drives.
- **Write performance is increased** since all RAID members participate in serving of the write requests.

https://en.wikipedia.org/wiki/Standard_RAID_levels

116



https://en.wikipedia.org/wiki/Standard_RAID_levels

117

Error Correction or Parity

- Parity data is used by some RAID levels to achieve redundancy.
- If a drive in the array fails, remaining data on the other drives can be combined with the parity data (using the boolean XOR function) to reconstruct the missing data.

Exclusive-OR gate

A	B	Output
0	0	0
0	1	1
1	0	1
1	1	0

- **Drive 1: 01101101**
  Drive 2: 11010100
- To calculate parity data for the two drives,
- an XOR is performed on their data:

01101101
XOR 11010100
————————
10111001 -→ Store in Drive 3

- The resulting parity data, 10111001, is then stored on Drive 3.

https://en.wikipedia.org/wiki/Parity_bit

118

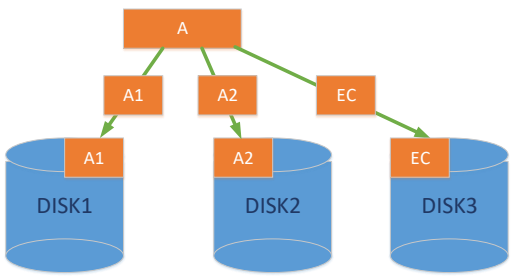
Error Correction or Parity

- **Drive 1: 01101101**
- ~~**Drive 2: 11010100**~~
- **Drive 3: 10111001**
- Parity check

10111001
XOR 01101101
————————
11010100

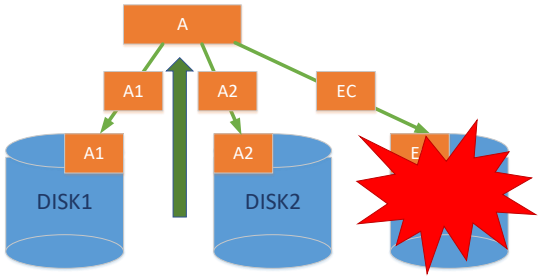
119

RAID Level 5 -- Stripping + Error Correction



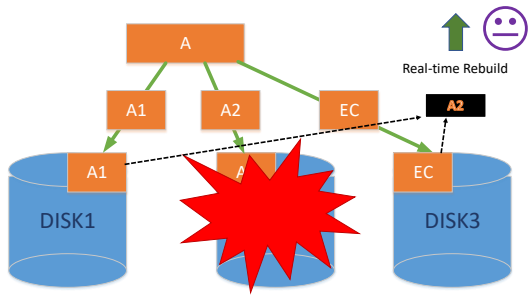
120

RAID Level 5 -- Stripping + Error Correction



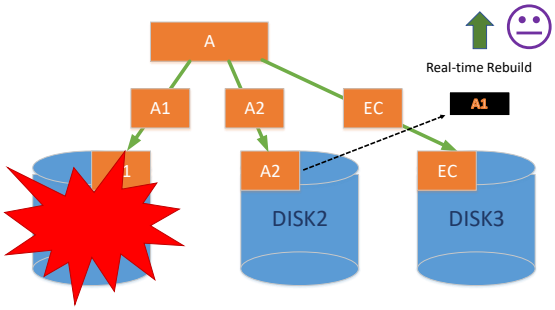
121

RAID Level 5 -- Stripping + Error Correction



122

RAID Level 5 -- Stripping + Error Correction



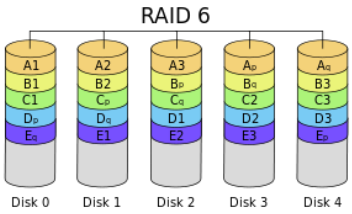
123

RAID 6

- RAID 6 extends RAID 5 by adding another parity block; thus, it uses block-level striping with **two parity blocks distributed across all member disks**.

https://en.wikipedia.org/wiki/Standard_RAID_levels

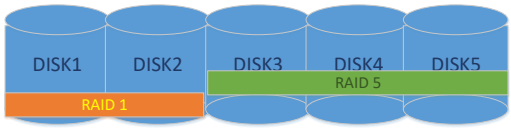
124



https://en.wikipedia.org/wiki/Standard_RAID_levels

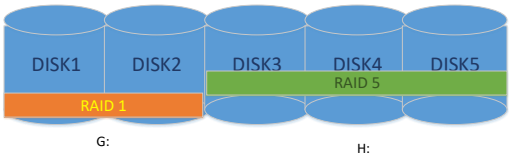
125

SAN Advantages



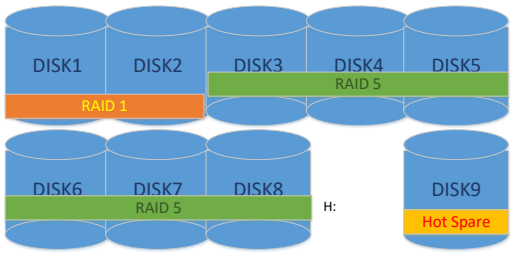
126

SAN Advantages



127

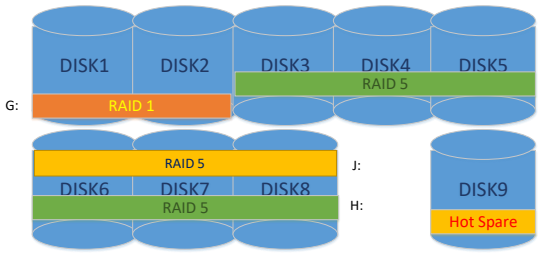
SAN Advantages



Why it is good for PACS?

128

SAN Advantages

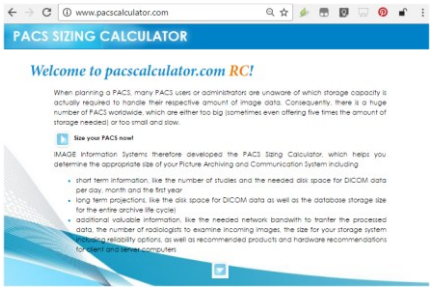


Why it is good for PACS?

129

PACS Sizing

http://www.pacscalculator.com/



130

Short Term Information

	Per Day	Per Month	Per year
Number of studies	240	7300	87600
Storage for DICOM data in GB	12	365	4380

Long Term Projections

Year	DICOM data in TB	Database storage in GB
1	5	5
2	9	9
3	14	14
4	18	18
5	22	23
6	27	27
7	31	32
8	36	36
9	40	41
10	44	45

131

Additional Information

Information	Value
Min. network bandwith in Mbit/s	2
Min. number of radiologists	2
Max. number of radiologists	4
RAID 5	3 x 4 TB HDD = 12 TB
Server recommendations	IQ-WEBX 5 XEON CPU(s) with 8 cores 16 - 32 GB RAM fast RAID storage + NAS or SAN 1 GBit/s Ethernet network card WINDOWS SERVER 2008 R2
Client recommendations	IQ-VIEW PRO 3D INTEL CORE i5 CPU 4 GB RAM 500 GB HDD 1 GBit/s Ethernet network card WINDOWS 7 PROFESSIONAL

Your calculation of 02-20-2017

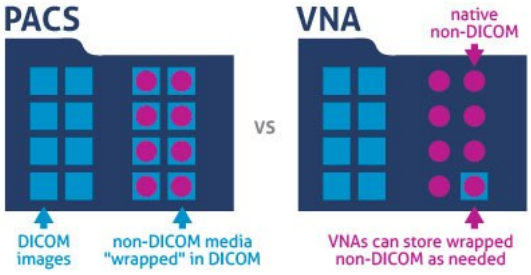
www.pacscalculator.com
session ID = 148756513113

132

Vendor Neutral Archive (VNS)

Yudthaphon Vichianin, Ph.D.
Department of Radiological Technology
Faculty of Medical Technology
Mahidol University

133



134

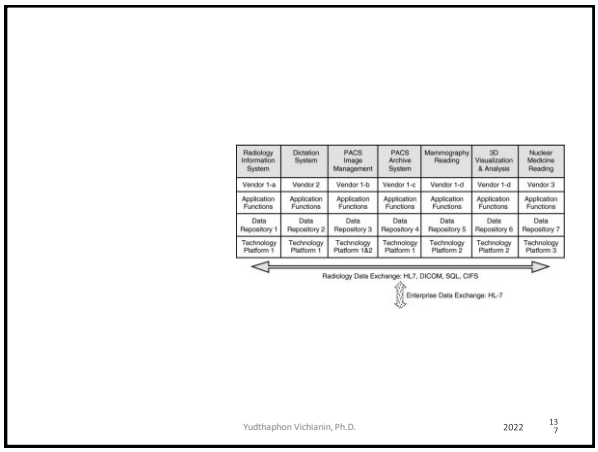
- A **Vendor Neutral Archive** (**VNA**) is a medical imaging technology in which images and documents (and potentially any file of clinical relevance) are stored (archived) in a standard format with a standard interface, such that they can be accessed in a vendor-neutral manner by other systems

135

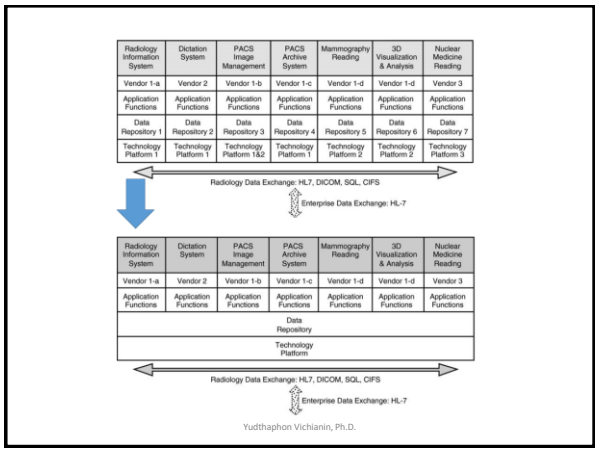
- The Memorial Sloan-Kettering Cancer Center (MSKCC) over the past 11 years. (New York)

System Consolidation

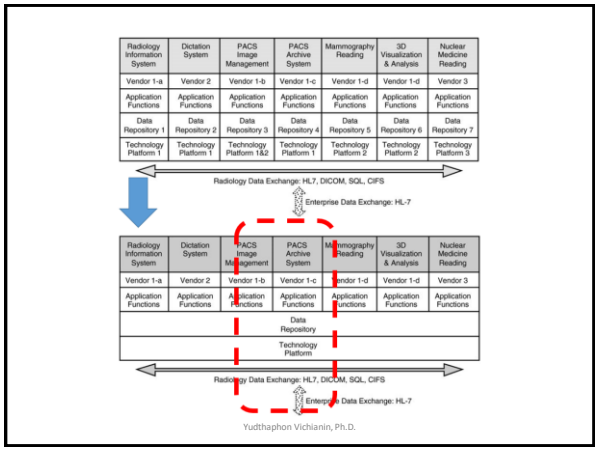
136



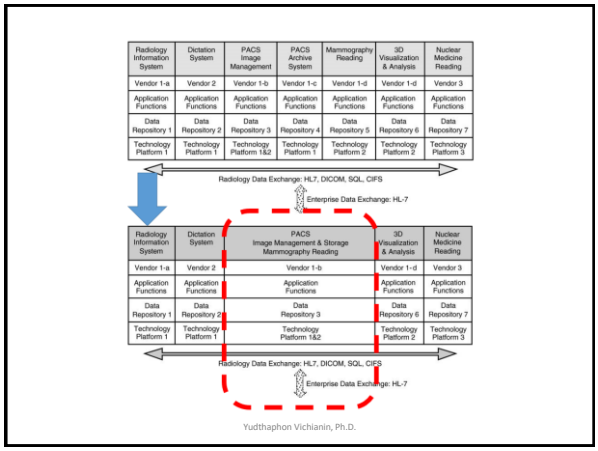
137



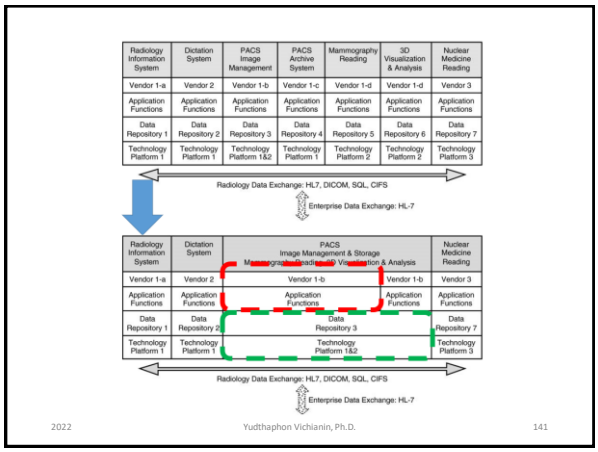
138



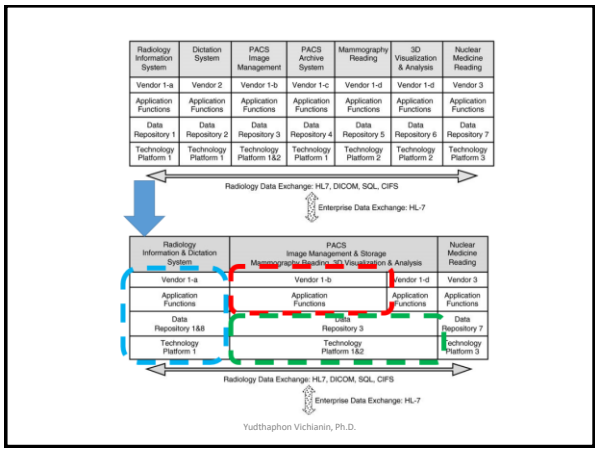
139



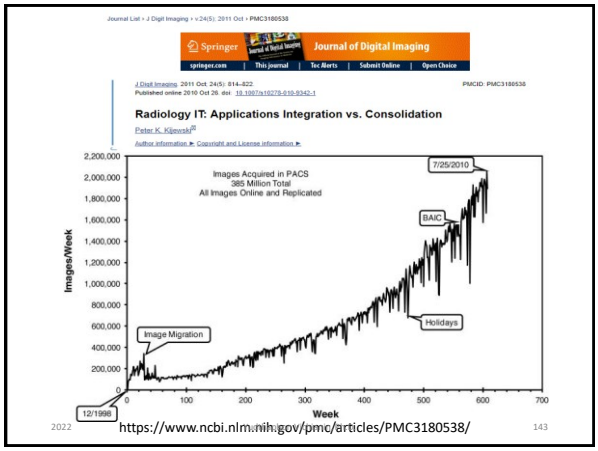
140



141



142



https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3180538/

143

144

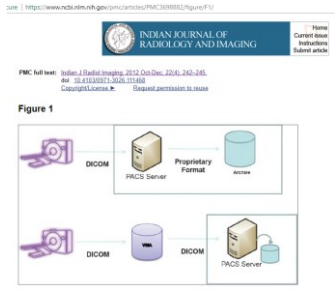
- When a hospital needs to migrate a PACS vendor, the complete **earlier data need to be migrated** in the format of the newly procured PACS.
- To address this issue, the new concept of **vendor neutral archive (VNA)** has emerged

145

An integral part of Picture Archiving and Communication System (PACS) is archiving

An archive is a **location** containing a **collection** of **records, documents, or other materials of historical importance**

146



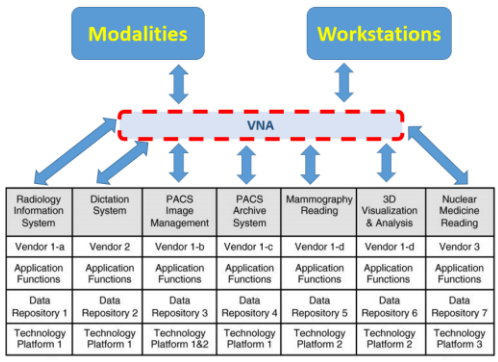
147

Dictation System	PACS Image Management	PACS Archive System	Mammography Reading	3D Visualization & Analysis
Vendor 2	Vendor 1-b	Vendor 1-c	Vendor 1-d	Vendor 1-d
Application Functions	Application Functions	Application Functions	Application Functions	Application Functions
Data Repository 2	Data Repository 3	Data Repository 4	Data Repository 5	Data Repository 6
Technology Platform 1	Technology Platform 1&2	Technology Platform 1	Technology Platform 2	Technology Platform 2

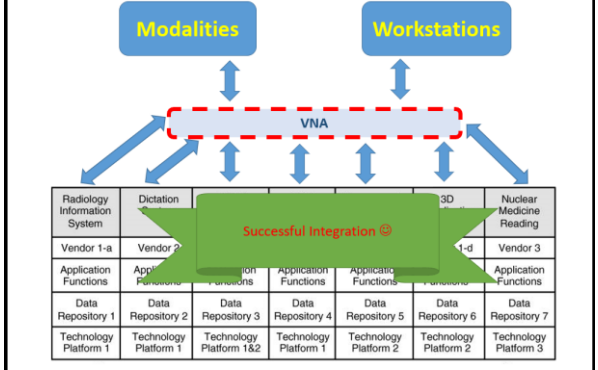
Radiology Data Exchange: HL7, DICOM, SQL, CIFS

Enterprise Data Exchange: HL-7

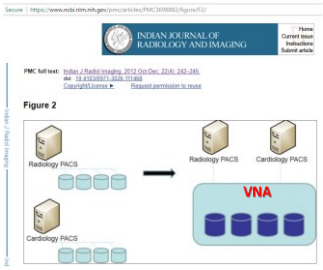
148



149



150



2022 Yudthaphon Vichianin, Ph.D. 151

151

Question & Answer

Thank you for your attention

☺☺☺

2022 Yudthaphon Vichianin, Ph.D. 152

152

Networking Technology

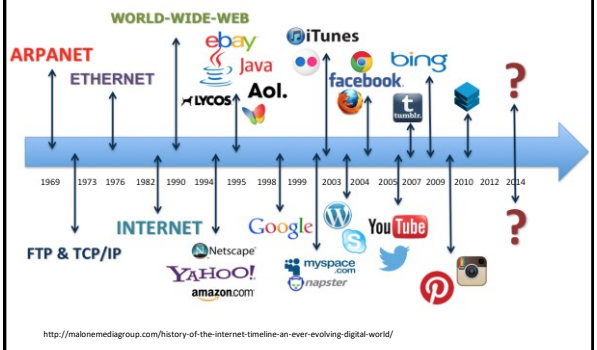
Yudthaphon Vichianin, Ph.D.
Department of Radiological Technology
Faculty of Medical Technology
Mahidol University

153

History of Computer Network

- In the late **1950s**, early networks of computers included the military radar system Semi-Automatic Ground Environment (**SAGE**).
- **In 1960**, the commercial airline reservation system semi-automatic business research environment (**SABRE**) went online with two connected mainframes.
- **In 1965**, Thomas Marill and Lawrence G. Roberts created the first wide area network (**WAN**). This was an immediate precursor to the **ARPANET**.
- **In 1973**, Robert Metcalfe wrote a formal memo at Xerox PARC describing **Ethernet**, a networking system that was based on the Aloha network, developed in the 1960s by Norman Abramson and colleagues at the University of Hawaii.
- **In 1995**, the transmission speed capacity for Ethernet increased from **10 Mbit/s to 100 Mbit/s**.
- **By 1998**, Ethernet supported transmission speeds of a **Gigabit**.

154



http://malonemediagroup.com/history-of-the-internet-timeline-an-ever-evolving-digital-world/

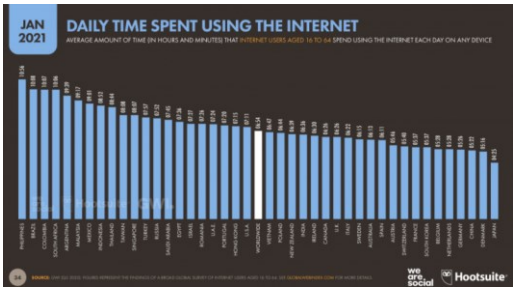
155

Network technology

- A **computer network** or **data network** is a telecommunications network which allows **nodes** to **share resources**.
- Networked computing devices exchange data with each other using a data **link**.
- The connections between nodes are established using either **cable media** or **wireless media**.

156

The best-known computer network is the Internet



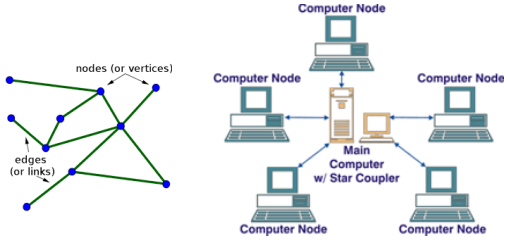
https://wearesocial.com/sg/blog/2021/03/southeast-asia-digital-life-intensified/

157

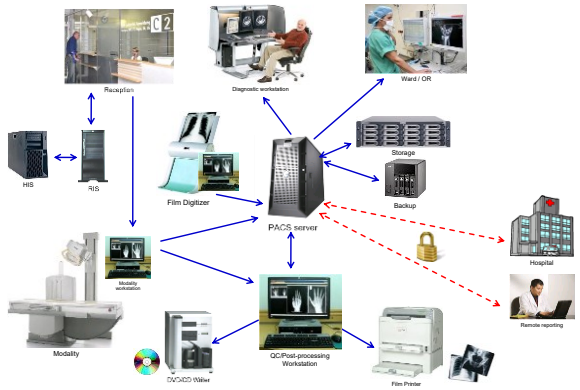
Network technology

- **Nodes** can include hosts such as personal computers, phones, servers as well as networking hardware.
- Two such devices can be said to be networked together **when one device is able to exchange information with the other device**, whether or not they have a direct connection to each other.

158



159



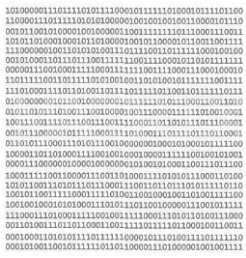
160

Data Transmission Schemes

- Computer communication links that do not support packets, such as **traditional point-to-point telecommunication links**, simply transmit data as a **bit stream**.

161

http://miriadna.com/preview/mounty-stream-on-the-green-valley



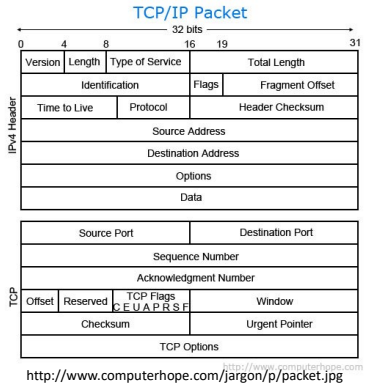
http://img10.deviantart.net/96ee/i/2006/217/c/1/matrix_bit_stream_by_kaizo_konpaku.jpg

162

Data Transmission Schemes

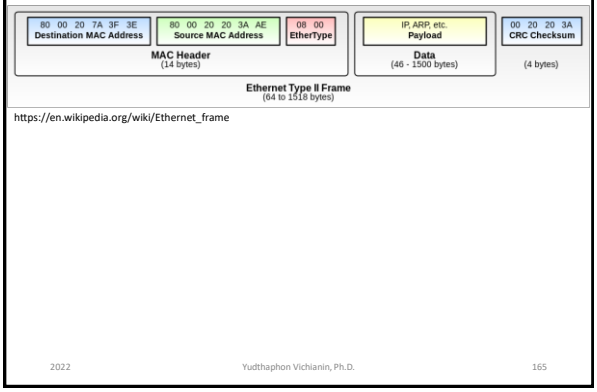
- In **packet networks**, the data is formatted into **packets** that are sent through the network to their destination. Once the packets arrive they are **reassembled into their original message**.

163



http://www.computerhope.com/jargon/p/packet.jpg

164



https://en.wikipedia.org/wiki/Ethernet_frame

165

Links

- A **wired network** connects devices to the Internet or other network using cables.

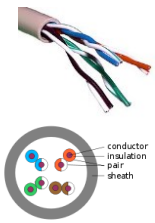
- A **wireless network** is any type of computer network that uses wireless data connections for connecting network nodes

http://www.cisco.com/c/en/us/solutions/small-business/resource-center/work-anywhere/wireless-network.html

166

Network Cables

- Unshielded twisted pair (UTP)
- A typical subset of these colors (**blue**, **blue**/white, **orange**, **orange**/white, **green**, **green**/white, **brown**, **brown**/white) shows up in most UTP cables.
- The cables are typically made with copper wires with the colored insulation typically made from an insulator.



167

https://en.wikipedia.org/wiki/Twisted_pair

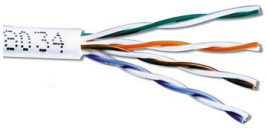
Name	Typical construction	Bandwidth	Applications	Notes
Level 1		0.4 MHz	Telephone and modem lines	Not described in EIA/TIA recommendations. Unsuitable for modern systems.[9]
Level 2		4 MHz	Older terminal systems, e.g. IBM 3270	Not described in EIA/TIA recommendations. Unsuitable for modern systems.[9]
Cat 3	UTP[10]	16 MHz[10]	10BASE-T and 100BASE-T4 Ethernet[14]	Described in EIA/TIA-568. Unsuitable for speeds above 16 Mbit/s. Now mainly for telephone cables[11]
Cat 4	UTP[10]	20 MHz[10]	16 Mbit/s[10] Token Ring	Not commonly used[10]
Cat 5	UTP[10]	100 MHz[10]	100BASE-TX & 1000BASE-T Ethernet[10]	Common for current LANs. Superseded by Cat5e, but most Cat5 cable meets Cat5e standards.[10]
Cat 5e	UTP[10]	100 MHz[10]	100BASE-TX & 1000BASE-T Ethernet[10]	Enhanced Cat5. Common for current LANs. Same construction as Cat5, but with better testing standards.[10]
Cat 6	UTP[15]	250 MHz[15]	10GBASE-T Ethernet	ISO/IEC 11801 2nd Ed. (2002), ANSI/TIA 568-B.2-1. Most commonly installed cable in Finland according to the 2002 standard EN 50173-1.
Cat 6$_A$	F/UTP, U/FTP	500 MHz	10GBASE-T Ethernet	Adds cable shielding. ISO/IEC 11801 2nd Ed. Am. 2. (2008), ANSI/TIA-568-C.1 (2009)
Cat 7	S/FTP, F/FTP	600 MHz	10GBASE-T Ethernet or POTS/CATV/1000BASE-T over single cable	Fully shielded cable. ISO/IEC 11801 2nd Ed. (2002)
Cat 7$_A$	S/FTP, F/FTP	1000 MHz	10GBASE-T Ethernet or POTS/CATV/1000BASE-T over single cable	Uses all four pairs. ISO/IEC 11801 2nd Ed. Am. 2. (2008)
Cat 8/8.1	F/UTP, U/FTP	1600-2000 MHz	40GBASE-T Ethernet or POTS/CATV/1000BASE-T over single cable	In development (ANSI/TIA-568-C.2-1, ISO/IEC 11801 3rd Ed.)
Cat 8.2	S/FTP, F/FTP	1600-2000 MHz	40GBASE-T Ethernet or POTS/CATV/1000BASE-T over single cable	In development (ISO/IEC 11801 3rd Ed.)

168

UTP/STP

Shielded twisted pair (STP)

Unshielded twisted pair (UTP)

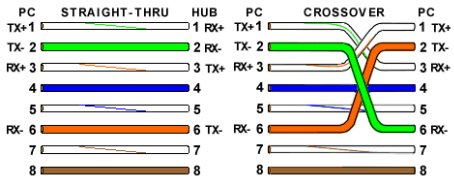


Source: http://networking.jobstown.net/images/utp%20and%20stp.jpg

169

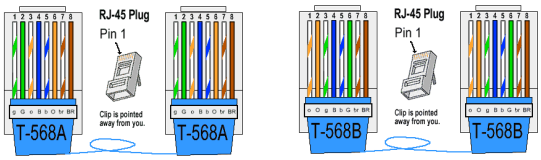
Basic Theory

Basic Theory:



170

RJ-45 & Cabling Color Code
Straight-Through cables



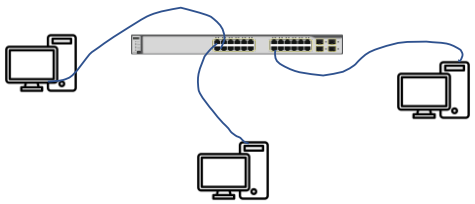
Both the T-568A and the T-568B standard Straight-Through cables are used most often as patch cords for your Ethernet connections.

http://www.incentre.net/wp-content/uploads/2015/02/ethcablerj45cr.gif

171

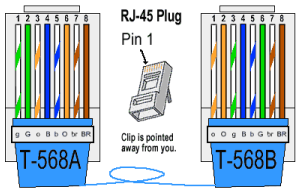
Straight-Through cables

- Connect different type of devices



172

RJ-45 & Cabling Color Code
RJ-45 Crossover Ethernet Cable



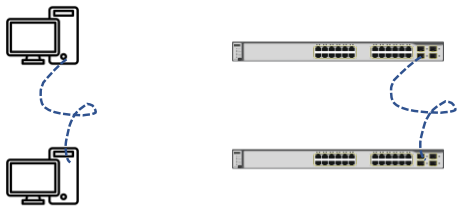
A good way of remembering how to wire a Crossover Ethernet cable is to wire one end using the T-568A standard and the other end using the T-568B standard.

http://www.incentre.net/wp-content/uploads/2015/02/ethcablerj45cr.gif

173

Crossover Ethernet Cable

- Connect same type of devices

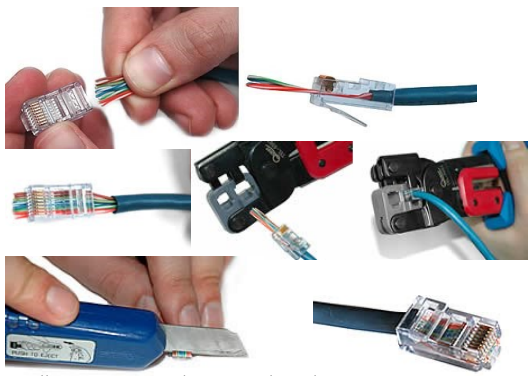


174

Ethernet Cable Tips:

- A straight-thru cable has identical ends.
- A crossover cable has different ends.
- A straight-thru is used as a patch cord in Ethernet connections.
- A crossover is used to connect two Ethernet devices without a hub or for connecting two hubs.
- Odd numbered pins are always striped, even numbered pins are always solid colored.
- Looking at the RJ-45 with the clip facing away from you, Brown is always on the right, and pin 1 is on the left.

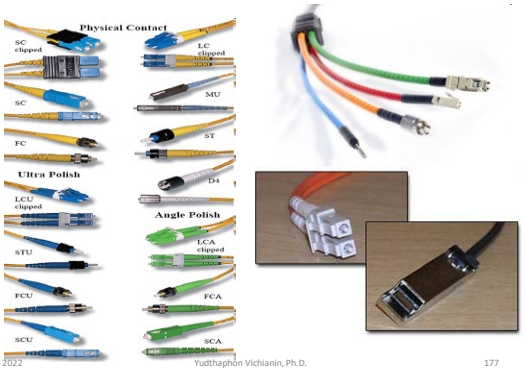
175



http://www.cableorganizer.com/learning-center/how-to/how-to-terminate-RJ45.htm

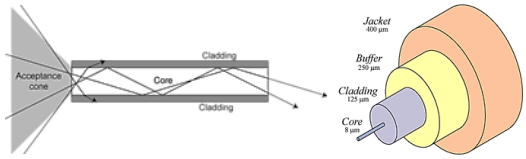
176

Fiber Optic Cable



177

Fiber Optic Cable



178

Network Interface Controller (NIC)

- A **network interface controller** (NIC, also known as a network interface card, network adapter, LAN adapter or physical network interface)
- **NIC** is a computer hardware component that connects a computer to a computer network.

179

Wire

Wireless

180

WIFI Standards

Standard	Maximum Speed	Frequency
802.11 (legacy)	1.2 Mbps	2.4 GHz
802.11a	54 Mbps	5.8 GHz
802.11b	11 Mbps	2.4 GHz
802.11g	54 Mbps	2.4 GHz
802.11n	150 Mbps	2.4 & 5 GHz
802.11ac	800 Mbps	5 GHz

https://propakistani.pk/wp-content/uploads/2016/01/Capture-3.jpg

Old Naming Convention	New Naming Convention
802.11b	Wi-Fi 1
802.11a	Wi-Fi 2
802.11g	Wi-Fi 3
802.11n	Wi-Fi 4
802.11ac	Wi-Fi 5
802.11ax	Wi-Fi 6

https://wifiadviser.com/blog/wifi-standards-explained/

181

Version/Features	Wi-Fi 4	Wi-Fi 5	Wi-Fi 6
IEEE standard	802.11n	802.11ac	802.11ax
Speed	Up to 150 Mbps max	433Mbits/sec-6.933Gbits/sec	600.4Mbits/sec-9.6078Gbits/sec
Frequency	2.4 & 5 GHz	5 GHz	2.4 & 5 GHz
Highest modulation	64-QAM	256-QAM	1024-QAM
MIMO	MIMO	MU-MIMO (downlink)	MU-MIMO (bidirectional)
Spatial streams	1	4	8
Range (indoor)	70 meters	80 meters along with 3 antennas	Better than Wi-Fi 5 since it supports beamforming
Range (outdoor)	250 meters	-	Better than Wi-Fi 5 since it supports beamforming

networkinterview.com
(An Initiative By ipwithease.com)

182

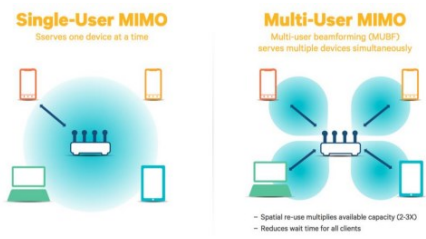


Figure 1. SU-MIMO vs. MU-MIMO

https://www.qualcomm.com/content/dam/qcomm-martech/dm-assets/documents/802.11ac_mu-mimo_bridging_the_mimo_gap_in_wi-fi.pdf

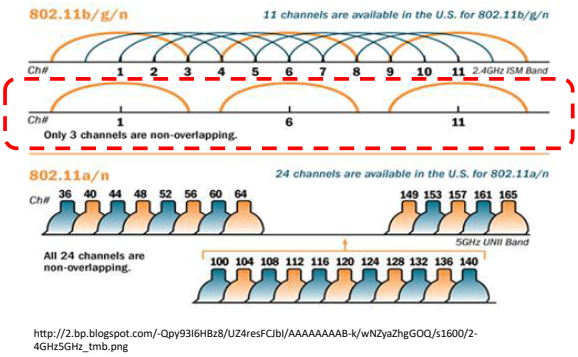
183

Figure 2. SU-MIMO and MU-MIMO operation

- 802.11ac improves congestion by allowing the router to communicate with multiple output devices simultaneously. But it has some limitations. It requires MU-MIMO compatible routers and clients, it only works on downlink.
- 802.11ax seeks to improve Wi-Fi in two ways. One is to increase the speed of each stream and the second is to make each router more efficient by allowing it to communicate with multiple devices simultaneously.

https://www.qualcomm.com/content/dam/qcomm-martech/dm-assets/documents/802.11ac_mu-mimo_bridging_the_mimo_gap_in_wi-fi.pdf
https://www.hardwarezone.com.sg/feature-wireless-80211ax-standard-networking-guide

184



http://2.bp.blogspot.com/-Qpy93I6HBz8/UZ4resFCJbI/AAAAAAAAB-k/wNZyaZhgGOQ/s1600/2-4GHz5GHz_tmb.png

185

Data Communication Component

- **Message** → Data / Images
- **Sender/Destination** → Workstation / Server
- **Transmission Medium** → wire / wireless
- **Protocol** → Procedure / Method

186

Network Devices

- Network devices are components used to connect computers or other electronic devices together so that they can share files or resources like printers or fax machines.

187

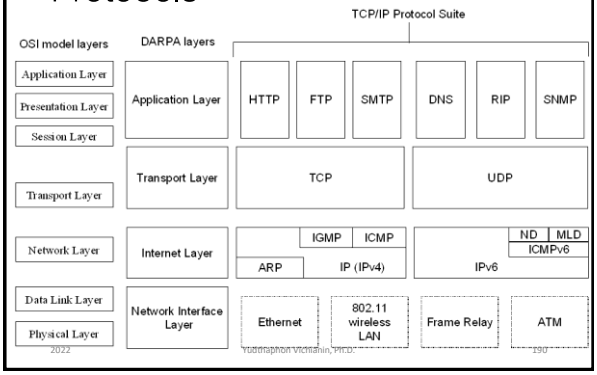
Network Switch

- A **network switch** (also called **switching** hub, bridging hub, officially MAC bridge) is a computer networking device that connects devices together on a computer network, by using packet switching to receive, process and forward data to the destination device.

188

189

Protocols



190

Network protocols

- **Network protocols** are formal standards and policies comprised of rules, procedures and formats that define communication between two or more devices over a network.

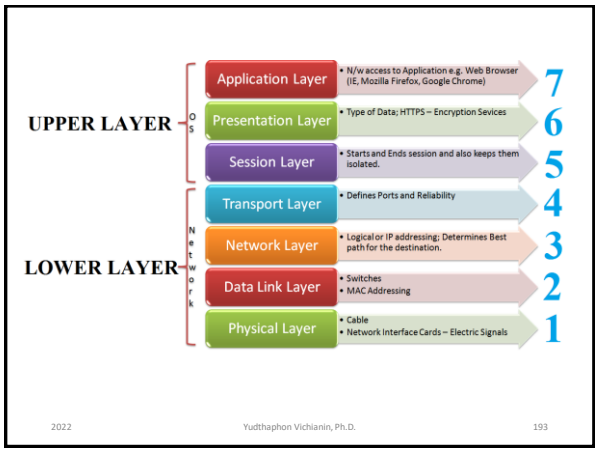
191

OSI Model

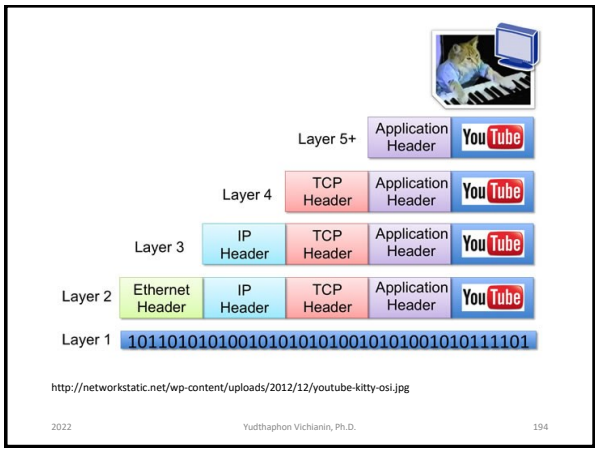
- The Open Systems Interconnection model (OSI model) is a **conceptual model** that characterizes and standardizes the communication **functions** of a telecommunication or computing system without regard to their underlying internal structure and technology.

https://en.wikipedia.org/wiki/OSI_model

192



193

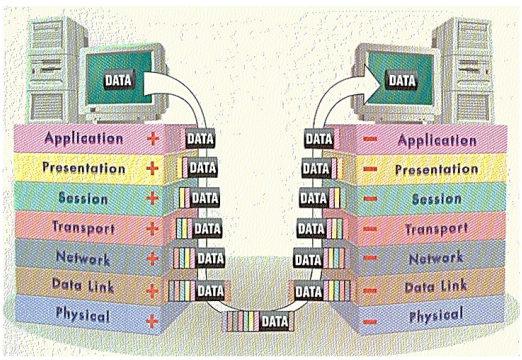


http://networkstatic.net/wp-content/uploads/2012/12/youtube-kitty-osi.jpg

194

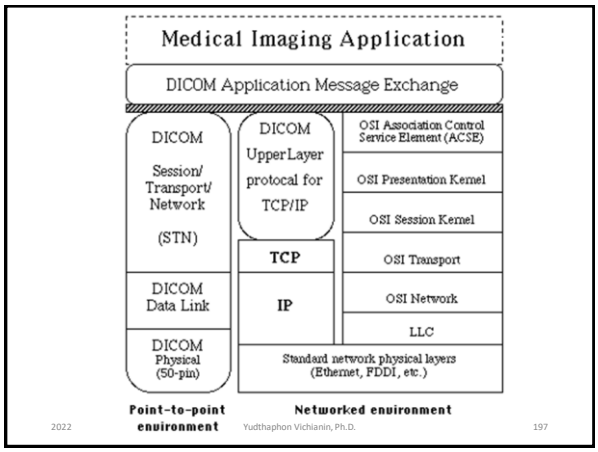
https://encrypted-tbn1.gstatic.com/images?q=tbn:ANd9GcSmoqI9GX6u0SiLEIjW9yECyLT_hv0zvaLjRQMwERddew0G1_MC

195

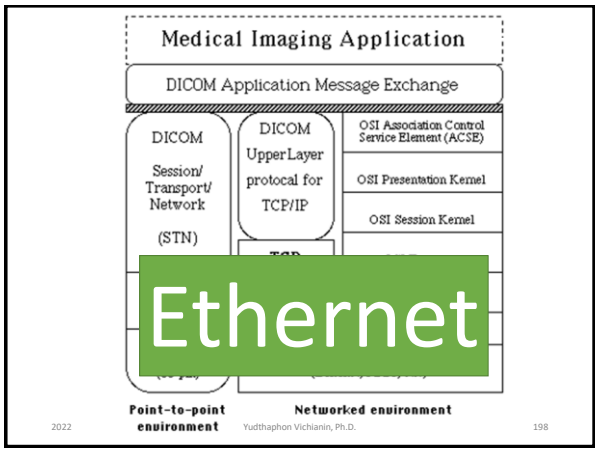


http://ccna-routingswitching-ciscochamp.netai.net/web_images/encapsulation3.png

196



197



198

Ethernet Network

- Ethernet initially assumed a shared medium
- Frame Based
- Broadcasting technique

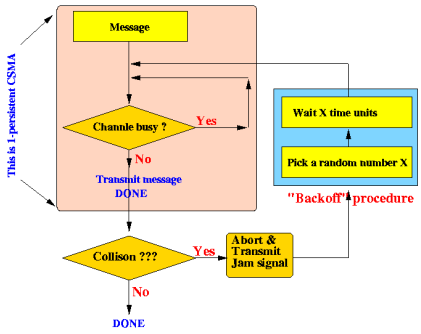
- Carrier Sense Multiple Access with Collision Detection (CSMA/CD).

199

CSMA/CD

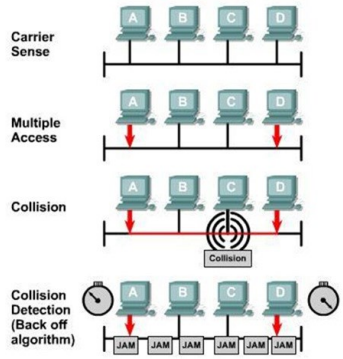
- Ethernet devices will **check** to see if anyone else is transmitting at the moment (carrier sense of multiple access) and if so (**collision detection**) will **wait** a short time before retrying the transmission.

200



http://www.mathcs.emory.edu/~cheung/Courses/558/Syllabus/00/CSMA/FIGS/1-pers-csmacd.gif

201

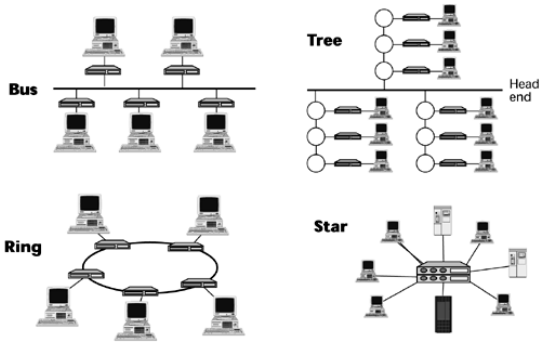


202

Network Topology

- A network topology is the **arrangement** of a network, including its nodes and connecting lines.
- There are two ways of defining network geometry: the **physical topology** and the **logical (or signal) topology.**
- **https://www.youtube.com/watch?v=gKW3BKvmhC0**

203



204

Bus Network Topology

- In the bus network topology, every workstation is connected to a main cable called the bus. Therefore, in effect, each workstation is directly connected to every other workstation in the network.

205

Star Network Topology

- In the star network topology, there is a central computer or server to which all the workstations are directly connected. Every workstation is indirectly connected to every other through the central computer.

206

Ring Network Topology

- In the ring network topology, the workstations are connected in a closed loop configuration. Adjacent pairs of workstations are directly connected. Other pairs of workstations are indirectly connected, the data passing through one or more intermediate nodes.
- If a Token Ring protocol is used in a star or ring topology, the signal travels in only one direction, carried by a so-called token from node to node.

207

Mesh Network Topology

- The mesh network topology employs either of two schemes, called full mesh and partial mesh. In the full mesh topology, each workstation is connected directly to each of the others. In the partial mesh topology, some workstations are connected to all the others, and some are connected only to those other nodes with which they exchange the most data.

208

Tree Network Topology

- The tree network topology uses two or more star networks connected together. The central computers of the star networks are connected to a main bus. Thus, a tree network is a bus network of star networks.

209

Logical (or signal) topology

- Logical (or signal) topology refers to the nature of the paths the signals follow from node to node. In many instances, the logical topology is the same as the physical topology. But this is not always the case. For example, some networks are physically laid out in a star configuration, but they operate logically as bus or ring networks.

210

Basic Computer Security

Yudthaphon Vichianin, Ph.D.
Department of Radiological Technology
Faculty of Medical Technology
Mahidol University

211

What is computer security?

- Also known as cybersecurity or IT security, is the protection of computer systems from the theft or damage to the hardware, software or the information on them, as well as from disruption or misdirection of the services

https://en.wikipedia.org/wiki/Computer_security

212

Computer Security

- Computer Security is concerned with four main areas:

1. Confidentiality: Only authorized users can access the data resources and information.
2. Integrity: Only authorized users should be able to modify the data when needed.
3. Availability: Data should be available to users when needed.
4. Authentication: Truly communicating with whom you think you are communicating with

213

Computer Security

- Controlling physical access to the hardware
- Protecting against harm that may come via
  - Network access
  - Data and code injection
  - Malpractice by operators (intentional or accidental)
  - Being tricked into deviating from secure procedures

214

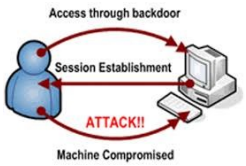
Vulnerabilities and attacks

- **Backdoors**: A backdoor in a computer system, a cryptosystem or an algorithm, is any secret method of bypassing normal authentication or security controls.
- **Denial of service attacks (DoS):** are designed to make a machine or network resource unavailable to its intended users.Attackers can deny service to individual victims, such as by deliberately entering a wrong password enough consecutive times to cause the victim account to be locked.

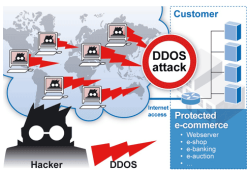
https://en.wikipedia.org/wiki/Computer_security#Vulnerabilities_and_attacks

215

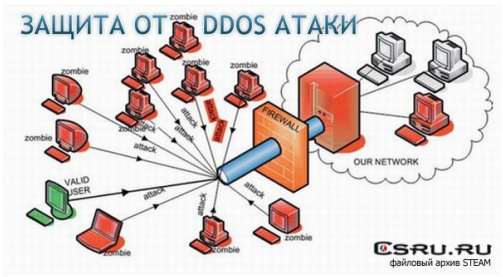
Backdoors



Denial of service attacks



216

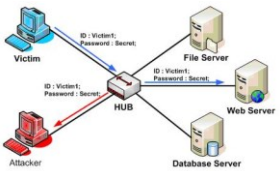


Denial of service attacks

217

Vulnerabilities and attacks

- **Eavesdropping:** is the act of surreptitiously listening to a private conversation, typically between hosts on a network.



https://en.wikipedia.org/wiki/Computer_security#Vulnerabilities_and_attacks

218

Vulnerabilities and attacks

- **Spoofing:** is a fraudulent or malicious practice in which communication is sent from an unknown source disguised as a source known to the receiver.

https://sites.google.com/site/ethicalhackingtutorials/account-hacking/email-spoofing-bombing-spamming

http://4.bp.blogspot.com/-SinT_2-4vw0/UC5Ept9c3AI/AAAAAAAAAQk/j1i2IPiEvcI/s1600/new.jpeg

219

Vulnerabilities and attacks

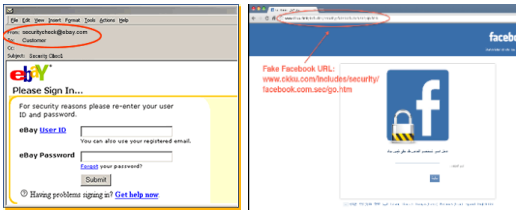
- **Privilege escalation**: describes a situation where an attacker with some level of restricted access is able to, without authorization, elevate their privileges or access level.

http://dataeducation.com/wp-content/uploads/2012/02/ownership-chains.jpg

220

Vulnerabilities and attacks

- **Phishing:** is the attempt to acquire sensitive information such as usernames, passwords, and credit card details directly from users. Phishing is typically carried out by email spoofing and it often directs users to enter details at a fake website



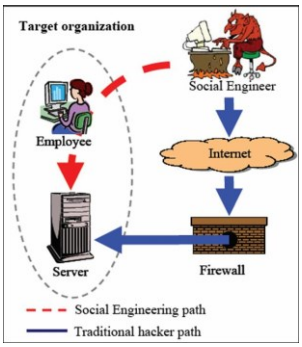
http://export.ebay.co.th/uploadfile/2011/0706/20110706060321249.gif

221

Vulnerabilities and attacks

- **Social engineering:** aims to convince a user to disclose secrets such as passwords, card numbers, etc. by, for example, impersonating a bank, a contractor, or a customer. A popular and profitable cyberscam involves fake CEO emails sent to accounting and finance departments.

222



Hermansson, 2005. illustrates how the social engineer exploits the weakest link of a computer system, the human user

http://faculty.nps.edu/ncrowe/oldstudents/laribeethesis_files/image002.jpg

223

Hospitals attacks

- There are many reports of hospitals and hospital organizations getting hacked, including **ransomware attacks**,Windows XP exploits,**viruses**,and **data breaches** of **sensitive data** stored on hospital servers.

https://en.wikipedia.org/wiki/Computer_security#Vulnerabilities_and_attacks

- The attackers sometimes go into a victim's network for months in order to infect the furthest corners of the network and encrypt or corrupt backup files, making payment the only way to get back the missing data.

http://www.forbes.com/sites/kalevleetaru/2016/03/29/hacking-hospitals-and-holding-hostages-cybersecurity-in-2016/#f98aec33e2ee

224

Security by design

- The principle of **least privilege**, where each part of the system has only the privileges that are needed for its function.
- Code **reviews** and unit **testing**.
- **Default secure settings**,
- **Audit trails tracking** system activity, so that when a security breach occurs, the mechanism and extent of the breach can be determined.
- **Full disclosure of all vulnerabilities**, to ensure that the "window of vulnerability" is kept as short as possible when bugs are discovered.

225

Security measures

- **User account access controls** and cryptography can protect systems files and data, respectively.
- **Firewalls** are by far the most common prevention systems from a network security perspective as they can (if properly configured) shield access to internal network services, and block certain kinds of attacks through packet filtering. Firewalls can be both hardware- or software-based.
- **Intrusion Detection System (IDS)** products are designed to detect network attacks in-progress and assist in post-attack forensics, while audit trails and logs serve a similar function for individual systems.

226

Vulnerability management

- Vulnerabilities can be discovered with a **vulnerability scanner**, which analyzes a computer system in search of known vulnerabilities
- Many organizations contract **outside security auditors** to run regular **penetration tests** (**hacking test**) against their systems to identify vulnerabilities.

227

Reducing vulnerabilities

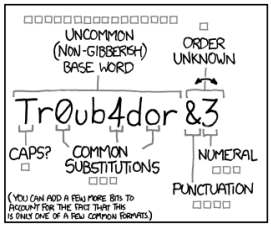
- Hardware protection mechanisms
  - **USB dongles** are typically used in software licensing schemes to unlock software capabilities
  - **Trusted platform modules** (TPMs) secure devices by integrating cryptographic capabilities onto access devices.
  - **Computer case intrusion detection** refers to a push-button switch which is triggered when a computer case is opened.
  - **Drive locks** are essentially software tools to encrypt hard drives, making them inaccessible to thieves.
  - **Disabling USB ports** is a security option for preventing unauthorized and malicious access to an otherwise secure computer.
  - **Limited mobile-enabled access**.
- Secure operating systems
- Secure coding

https://en.wikipedia.org/wiki/Computer_security#Vulnerabilities_and_attacks

228

Good password

- Easy to remember, but hard to guess



http://losingit.me.uk/wordpress/wp-content/uploads/2011/08/xkcd_-Password-Strength.png

My son Jayden was born in September 2005

MsJwbiS2

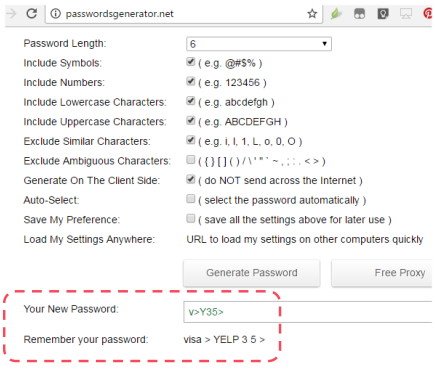
M2Jwb!sZ

http://www.nerdiosity.com/wp-content/uploads/2012/02/password-phrase1.png

229

230

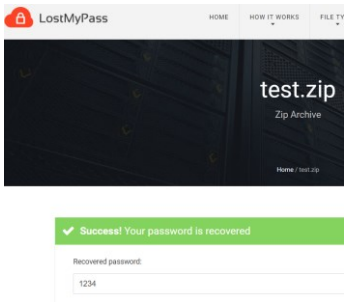
http://passwordsgenerator.net/



231

Multi-factor authentications

232



233

Risk Management in Digital Environment

Yudthaphon Vichianin, Ph.D.
Department of Radiological Technology
Faculty of Medical Technology
Mahidol University

234

Risk Management in Radiology

Chamaree Chuapetcharasopon, MD, MBA
President
Radiological Society of Thailand

235

Risk Management in Radiology

- Incident
- Problem
- Risk

236

Incident

1. Discrete **occurrence or event**.

2. Arising out of or associated with something more significant.

3. unexpected and inappropriate or inconvenient event which (depending on the circumstances) may lead to a damage, disaster, or loss.

- Incidents accumulate into "Problem(s)"
- Incident Management
- Problem Management

237

What is Risk?

- Risk is considered **to be the chance or possibility** of incurring loss or of a negative event happening that may cause injury to patients or medical practitioners.

238

What is RISK?

- **Possibility** of danger.
- **Possibility** that any activity could happen and harm.
- **Probability** of a hazard resulting in an adverse event.

http://mir-online.org/html/img/pool/MIR_ECR_2012_-_Senol_-_Risk_management_in_radiology.pdf

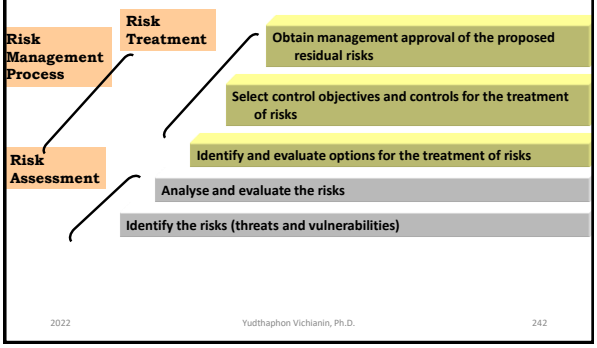
239

Risks may be managed

240

241

Risk Management Processes



242

Risk Assessment

Risk Value			Probability				
			Very Low	Low	Medium	High	Very High
			1	2	3	4	5
Impact	Very High	5	5	10	15	**20**	**25**
	High	4	4	8	12	16	**20**
	Medium	3	3	6	9	12	15
	Low	2	2	4	6	8	10
	Very Low	1	1	2	3	4	5

243

Risk Treatment

1. Reduce Risks
2. Transfer Risks
3. Avoid Risks
4. Accept Risks

244

Risk Management in Radiology

- Example: Risk management in PACS
  - Identify risks
  - Risk assessment
  - Plan
  - Review and evaluate
  - Implement
  - Control
  - Monitor

245

Planning for PACS

- Financial Justification
- Vendor Selection
- Technology Issues
  - Hardware
  - Software
  - Network And IT
- Disaster Plan
- Security
- Space And Environment Issues
- Project Implementation

246

Planning for PACS

- Financial Justification
- Vendor Selection
- Technology Issues
  - Hardware
  - Software
  - Network And IT
- Disaster Plan
- Security
- Space And Environment Issues
- Project Implementation

247

Risk management in PACS

What Is The Risk(s) In PACS/Radiology?

– Identify Risks

2 Types Of Potential Risks

- Hard Ware (Simple)
- Software/Man-made , Workflow/Policies (More Complicate)

248

Risk management in PACS

5 components in PACS – Identify risks

- Acquisition:
- Data:
- Server:
- Network
- Display workstation:

249

Risk management in PACS

5 components in PACS

- **Acquisition:**
  - Wrong patient identification
  - Wrong selection from work list
  - Wrong order selected/wrong barcode scanner process
  - Equipment down in the middle of study
  - Wrong registration of modality

250

Risk management in PACS

5 components in PACS

Data:

- Error input due to not fully integrated system or poor interface between system
- Wrong data processing
- Flipping error/ label error
- Wrong image sent(bad image, wrong IP address)
- Data corrupted/ loss during process and sending
- Local back up data corrupted/cannot bring back
- Different standards from different vendors for example digital mammography

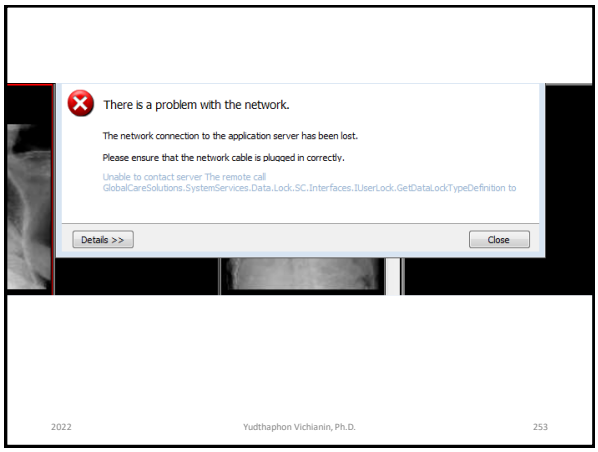
251

Risk management in PACS

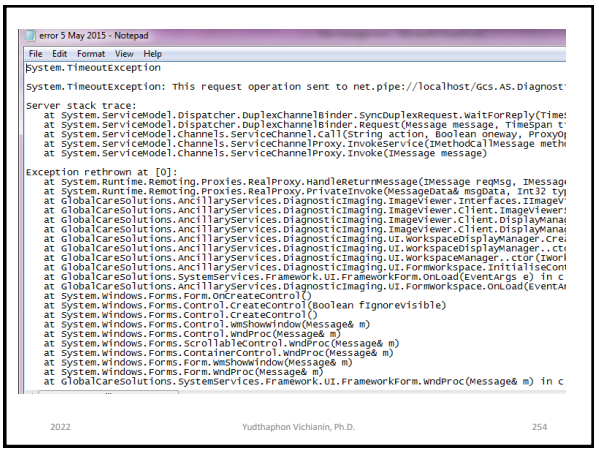
5 components in PACS

- **Server:**
  - Down
  - upgrade - wrong configuration, wrong set up
- **Network:**
  - Down
  - upgrade –wrong configuration, wrong set up

252



253



254

Risk management in PACS

5 components in PACS

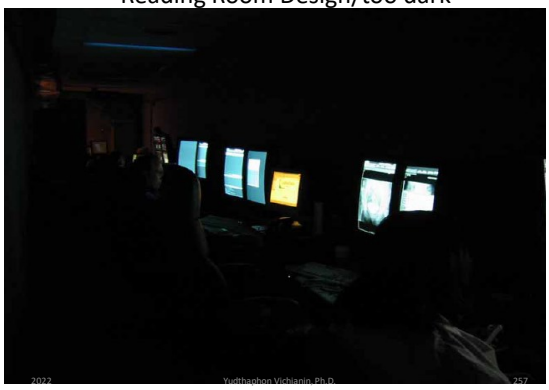
- **Display workstation**
  - Not proper specification
  - Not proper calibration
  - Not proper environment
- Results in Interpretation errors

255

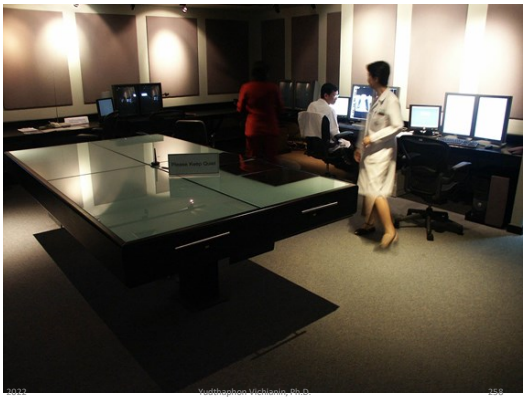
Reading Room Design/too bright

256

Reading Room Design/too dark



257



258

Figure 3

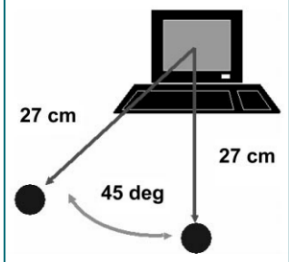


Figure 3: Diagram shows experimental viewing conditions for reference 26, where readers viewed a set of mammograms on axis and 45° off axis. Diagnostic accuracy decreased significantly for off-axis LCD viewing but not for CRT viewing.

Radiology: Volume 242: Number 3—March 2007

259

Risk management in Radiology

- Example: Risk management in PACS
  - Identify risks – 5 components
  - Risk assessment/analysis
    - scoring
  - Plan
    - department policies, work instructions
  - Review and evaluate the plan
    - every 3,6 or 12 months
  - Implement
  - Control
  - Monitor

260

Risk (may use prior incidents)	Probability	Impact	Score	Priority
Network down	2	5	10	2
CT scan down	4	4	16	1
Wrong data processing selected (Bad images)	4	2	8	3

261

Risk management in Radiology

- Example: Risk management in PACS
  - Risk assessment/analysis
    - scoring
  - Plan
    - 24/7 maintenance contract for CT machine
    - Disaster plan for Network down

262

Risk management in PACS

- DISASTER PLAN
  - Network/PACS is down - disaster plan, Business continuity plan (BCP), contingency plan
  - What does PACS down mean?
  - When to start using Contingency plan or disaster plan and BCP?
  - Who make decision and announce?

263

Risk management in PACS

- **Disaster plan:**
- Example: Scenario: System/Network down
  - Identify all PACS workflow and replace with manual workflow
  - Example:
    - Reroute data from X-ray machine (CR/DR) to film printer
    - Move view box to reading room beside computer
    - Set up report template for PACS down situation for radiologists. (Training/inform ALL radiologists)
    - Print report with film to clinic
    - Copy report from each computer back to the system when system up.

264

265

Planning for PACS

- Financial justification
- Vendor selection
- Technology issues
  - Hardware
  - Software
  - Network and IT
- Disaster plan
- Security
- Space and environment issues
- Project implementation

266

Risk management in PACS

- **Security (digital)**
  - Virus, Malware, Ransomware
    - USB or laptop from vendor engineer
    - Specific Internet direct to equipment/modality
    - Patient portal
    - Personal/staff practice:
  - Confidentiality and privacy/Patient information Data access
    - Personal/staff practice
  - Must follow hospital IT security policies

267

Risk Management in Radiology

- **One cannot predict all risks**.
- Injury to patients may occur even in the best hospitals where patients receive high-quality services and treatments.
- *Risk management is a **Proactive Concept*** that involves practices such as identification of risk, quantification and evaluation of risk and consideration of measures that can be used to eliminate or control risk in a medical setting.

268

Risk Management in Radiology

- *the major focus of risk management in medical setting is to **reduce and eliminate harm and injury to patients** through integration of various medical precautions.*

Craciun H, Mankad K, Lynch J. Risk management in radiology departments. *World J Radiol* 2015; 7(6): 134-138

269

Risk Management in Radiology

In summary

- ***Safeguarding patients and personnel***
- ***Transparency***
- ***Professional competence and equipment***
- ***Quality system***

270

Question & Answer

Thank you for your attention

☺☺☺

271

Clinical Perspectives of PACS and Digital Imaging

Yudthaphon Vichianin, Ph.D.
Department of Radiological Technology
Faculty of Medical Technology
Mahidol University

272

Healthcare information and integration

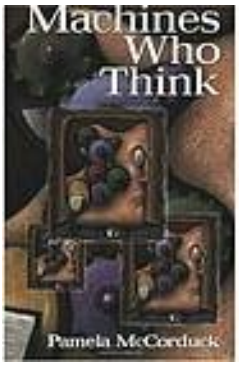
Yudthaphon Vichianin, Ph.D.
Department of Radiological Technology
Faculty of Medical Technology
Mahidol University

273

Use of Computer in Medicine

- Create the basis for the historical record
  - Detail information about individual patients
- Support communication among providers
  - Further investigation by medical specialist and team
- Anticipate future health problems
- Record standard prevention measure
  - Vaccination record
- Provide a legal record
- Support clinical research

274



- MYCIN, developed in 1972, diagnosed infectious blood diseases.
- To identify bacteria causing severe infections
- To recommend antibiotics, with the dosage adjusted for patient's body weight

McCorduck, Pamela (2004), Machines Who Think (2nd ed.), Natick, MA: A. K. Peters, Ltd., ISBN 1-56881-205-1, OCLC 52197627.

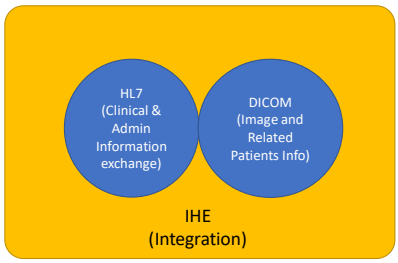
275

Issues in System Integration

- Many institutions seeks for integrated clinical workstations
- Clinical aspects
  - results of tests (labs/x-ray)
  - entry of orders
  - access to reports
- Non-clinical aspects
  - Administrative (ie. HR)
  - Financial (accounting / avg. cost of care for each diseases)
  - Research (analysis of patient information)
  - Knowledge base (journals)
  - Office automation (word / spread sheet/ presentation)

276

The Big Picture



277

IHE

Yudthaphon Vichianin, Ph.D.
Department of Radiological Technology
Faculty of Medical Technology
Mahidol University

278

IHE: What it is?

- Integrating the Healthcare Enterprise **(IHE)**
- A non-profit organization based in the US states
- Objective: To improve the way computer systems share information
- IHE was established in 1998 by a consortium of radiologists and information technology (IT) experts

279

IHE: Website

280

IHE: What it does?

- Address the area that the interoperability of health care IT systems can be improved
- Gathering case requirements, identifies available standards, and develops technical guidelines which manufacturers can **implement**.

https://en.wikipedia.org/wiki/Integrating_the_Healthcare_Enterprise

281

IHE: Example

- For example, the Digital Imaging and Communications in Medicine (DICOM) standards specify many different formats for image data
- A given set of images that might comply with some optional parts of the standards might still not be accepted by an application in use by a particular radiologist
- **Profiles** reduce the chances of these incompatibilities

https://en.wikipedia.org/wiki/Integrating_the_Healthcare_Enterprise

282

IHE: Profiles

Describe specific solutions to integration problems

- Anatomic Pathology
- Cardiology
- Eye Care
- IT Infrastructure
- Laboratory
- Pathology and Laboratory Medicine
- Patient Care Coordination
- Patient Care Device
- Pharmacy
- Quality, Research and Public Health
- Radiation Oncology
- Radiology

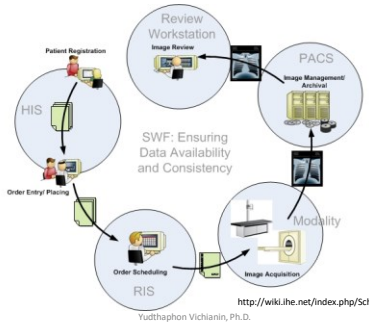
283

IHE: Radiology Profiles

- Profiles for Workflow (7)
- Profiles for Content (10)
- Profiles for Presentation (5)
- Profiles for Infrastructure (10)

284

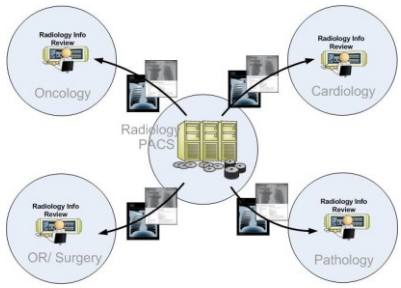
Scheduled Workflow (SWF) integrates the ordering, scheduling, imaging acquisition, storage and viewing activities associated with radiology exams.



http://wiki.ihe.net/index.php/Scheduled_Workflow

285

Access to Radiology Information (ARI) shares images, diagnostic reports, and related information inside a single network.



http://wiki.ihe.net/index.php/Access_to_Radiology_Information

286

IHE: Samples of Radiology Profile

- **[SWF]** Scheduled Workflow integrates ordering, scheduling, imaging acquisition, storage and viewing for Radiology exams.

  View example (HTML Scheduled Workflow - IHE Wiki.htm)

- **[MAMMO]** Mammography Image specifies how Mammography images and evidence objects are created, exchanged, used and displayed.

  View example (HTML Mammography Image - IHE Wiki.htm)

http://wiki.ihe.net/index.php/Profiles#IHE_Radiology_Profiles

287

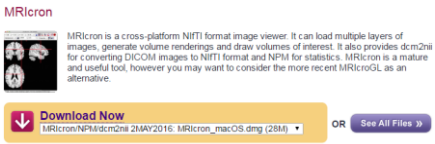
Clinical Perspectives

- Examples
  - Research
  - Quality Improvement
  - Dose Tracking

288

Research: Functional MRI

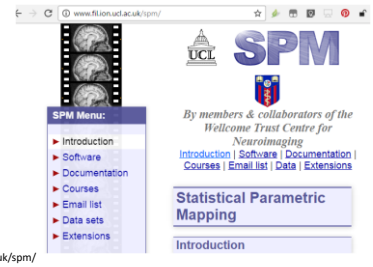
- Export DICOM to external storage
- Convert DICOM to appropriated file format
  - Niffty format for further processing
  - https://nifti.nimh.nih.gov/nifti-1



289

Research: Functional MRI

- Using External software such as
  - MATLAB
  - SPM

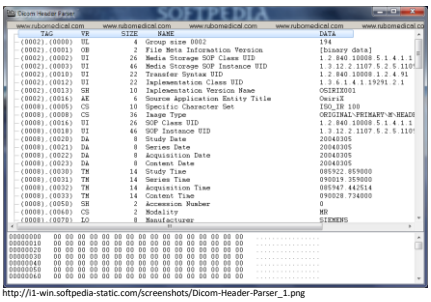


http://www.fil.ion.ucl.ac.uk/spm/

290

Quality Improvement

DICOM header information → KV, mas

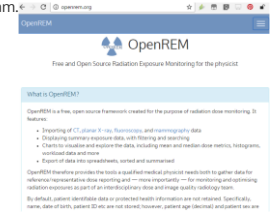


http://i1-win.softpedia-static.com/screenshots/Dicom-Header-Parser_1.png

291

Dose Tracking

OpenREM therefore provides the tools a qualified medical physicist needs both to gather data for reference/representative dose reporting and — more importantly — for monitoring and optimizing radiation exposures as part of an interdisciplinary dose and image quality radiology team.

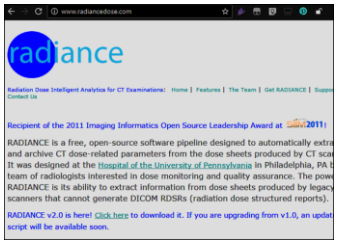


http://openrem.org/

292

Radiation Dose Tracking

RADIANCE is a free, open-source software pipeline designed to automatically extract and archive CT dose-related parameters from the dose sheets produced by CT scanners.



http://www.radiancedose.com/

293

Additional concerns on Clinical Settings

294

The 'Wannacry' ransomware attack

The attack has hit more than 200,000 victims in at least 150 countries, says Europol

295

296

CYBERSECURITY STATISTICS & FACTS FOR 2022

- **85%** of cybersecurity breaches are caused by human error. (Verizon)
- **94%** of all malware is delivered by email. (CSO Online)
- Ransomware attacks happen every **10 seconds**. (InfoSecurity Group)
- **71%** of all cyberattacks are financially motivated (followed by intellectual property theft, and then espionage). (Verizon)
- The annual global cost of cybercrime is estimated to be **$10.5 trillion** by 2025. (Cybersecurity Ventures)

297

F-35 fighter jets face greater threats from cyber-attacks than from enemy missiles

Source: Interesting Engineering

The cybersecurity industry is estimated to be worth over $400 billion by 2027

Source: Ce Pro

Over 80% of cybersecurity events involve phishing attacks

Source: CSO Online

Google discovered over 2.1 million phishing sites as of January 2021

Source: Tessian

298

299

Risk

- The term “information security risk” refers to the damage that attacks against IT systems can cause.
- IT risk encompasses a wide range of potential events, including data breaches, regulatory enforcement actions, financial costs, reputational damage, and more.

https://reciprocity.com/resources/what-is-information-security-risk/

300

Vulnerability

- Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

https://csrc.nist.gov/glossary/term/vulnerability

301

Threat

- Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability.

https://csrc.nist.gov/glossary/term/threat

302

Motivation

- Motivation of Hackers: Why Do Hackers Do What They Do?
- Hacker Motivation 1: Achieving Financial Gains
  - Misusing Data
  - Selling Data on the Dark Web
  - Blackmailing Victims
  - Selling Malware
- Hacker Motivation 2: Carrying Out Political Agendas
  - Stealing sensitive, confidential, or classified data (research, trade secrets, or even personal information on specific targets).
  - Manipulating or otherwise interfering with elections.
- Hacker Motivation 3: Performing Corporate Espionage
  - Some companies hire hackers for stealing confidential information from rival firms. In these situations, hackers are assigned to find leaky or vulnerable databases or launch attacks on the target organization's servers or websites.
- Hacker Motivation 4: Proving a Point (Hacktivist)
  - Some hackers don't care about money. Instead, they hack to prove their social, ethical, religious, or political views or to force their views upon others.

303

Motivation

- Hacker Motivation 5: Taking Personal Revenge
  - Locking their targets' devices.
  - Encrypting or deleting their data.
  - Hacking their social media profiles and posting false or inappropriate content.
- Hacker Motivation 6: Causing Harm for Personal Enjoyment
  - Some black hat hackers hack just to create chaos or to cause harm or panic. They relish ruining the reputation of a person or company, interrupting governments' activities, or destroying important data. They might be addicted to hacking and feel a sense of achievement when they hack a system or defraud someone.
- Hacker Motivation 7: Mitigating Cyber Threats
  - Hackers sometimes hack to attack or stop other hackers from doing bad things.

304

Risk analysis

- Risk analysis is the process of identifying and analyzing potential issues that could negatively impact key business initiatives or projects. This process is done in order to help organizations avoid or mitigate those risks.
- Performing a risk analysis includes considering the possibility of adverse events caused by either natural processes, like severe storms, earthquakes or floods, or adverse events caused by malicious or inadvertent human activities.
- An important part of risk analysis is identifying the potential for harm from these events, as well as the likelihood that they will occur.

https://www.techtarget.com/searchsecurity/definition/risk-analysis

305

Why is risk analysis important?

Enterprises and other organizations use risk analysis to:

- anticipate and reduce the effect of harmful results from adverse events;
- evaluate whether the potential risks of a project are balanced by its benefits to aid in the decision process when evaluating whether to move forward with the project;
- plan responses for technology or equipment failure or loss from adverse events, both natural and human-caused; and
- identify the impact of and prepare for changes in the enterprise environment, including the likelihood of new competitors entering the market or changes to government regulatory policy.

306

Steps in risk analysis process

The risk analysis process usually follows these basic steps:

- Conduct a risk assessment survey: This first step, getting input from management and department heads, is critical to the risk assessment process. The risk assessment survey is a way to begin documenting specific risks or threats within each department.
- Identify the risks: The reason for performing risk assessment is to evaluate an IT system or other aspect of the organization and then ask: What are the risks to the software, hardware, data and IT employees? What are the possible adverse events that could occur, such as human error, fire, flooding or earthquakes? What is the potential that the integrity of the system will be compromised or that it won't be available?
- Analyze the risks: Once the risks are identified, the risk analysis process should determine the likelihood that each risk will occur, as well as the consequences linked to each risk and how they might affect the objectives of a project.
- Develop a risk management plan: Based on an analysis of which assets are valuable and which threats will probably affect those assets negatively, the risk analysis should produce control recommendations that can be used to mitigate, transfer, accept or avoid the risk.
- Implement the risk management plan: The ultimate goal of risk assessment is to implement measures to remove or reduce the risks. Starting with the highest-priority risk, resolve or at least mitigate each risk so it's no longer a threat.
- Monitor the risks: The ongoing process of identifying, treating and managing risks should be an important part of any risk analysis process.

307

https://survey.charteredaccountantsanz.com/risk_management/midsize-firms/treat.aspx

308

Risk Treatment

- Risk treatment involves working through options to treat unacceptable risks to your business. Unacceptable risks range in severity; some require immediate treatment, others can be monitored and treated later.
- Before you decide which risks to treat, you need to gather information about the:
  - method of treatment
  - people responsible for treatment
  - costs involved
  - benefits of treatment
  - likelihood of success
  - ways to measure and assess treatments.

309

Risk avoidance

- **Avoidance:** Elimination of the vulnerability that gives rise to a particular risk so that it is avoided altogether. This is the most effective solution, but often not possible due to organizational requirements.
- Eliminating email to avoid the risk of email-borne viruses is an effective solution but not likely to be a realistic approach in the modern enterprise.
- You may decide not to proceed with the activity likely to generate the risk, where practical. Alternatively, you may think of another way to reach the same outcome.

310

Risk reduction

- Reduce the risk
- You can control a risk by:
- reducing the likelihood of the risk occurring – for example, through quality control processes, managing debtors, auditing, compliance with legislation, staff training, regular maintenance or a change in procedures
- reducing the impact if the risk occurs – for example, through emergency procedures, off-site data backup, minimising exposure to sources of risk or public relations.
- Transfer the

311

Risk transfer

- **Transference:** A risk or the effect of its exposure may be transferred by moving to hosted providers who assume the responsibility for recovery and restoration or by acquiring insurance to cover the costs emerging from equipment theft or data exposure.
- You may be able to shift some or all of the responsibility for the risk to another party through insurance, outsourcing, joint ventures or partnerships.

312

Risk deterrence

- **Mitigation/Deterrence:** Risk mitigation involves the reduction in likelihood or impact of a risk's exposure.
- Risk deterrence involves putting into place systems and policies to mitigate a risk by protecting against the exploitation of vulnerabilities that cannot be eliminated.
- Most risk management decisions focus on mitigation and deterrence, balancing costs and resources against the level of risk and mitigation that will result.

313

Risk acceptance

- **Acceptance:** Recognizing a risk, identifying it, and then accepting that it is sufficiently unlikely or of such limited impact that corrective controls are not warranted. Risk acceptance must be a conscious choice, documented, approved by senior administration, and regularly reviewed.
- You may accept a risk if it cannot be avoided, reduced or transferred. However, you will need to have plans for managing and funding the consequences of the risk if it occurs.

https://www.business.qld.gov.au/starting-business/protect-business/managing-risk/treating

314

Physical / Operational control

- Types of Controls
- You can apply three general types of controls to mitigate risks, typically by layering defensive controls to protect data with multiple control types when possible. This technique is called a layered defensive strategy or "defense in depth."
- Operational: Operational controls include organizational culture as well as physical controls that form the outer line of defense against direct access to data, such as protection of backup media; securing output and mobile file storage devices; and facility design details including layout, doors, guards, locks, and surveillance systems.

315

Technical control

- **Technical:** Technical controls include
- logical access control systems
- security systems
- Encryption
- data classification solutions

316

Management control

- Management: Management or administrative controls include business and organizational processes and procedures, such as security policies and procedures, personnel background checks, security awareness training, and formal change-management procedures.

317

Identifying Vulnerabilities

Many risks to enterprise networks relate to vulnerabilities present in system and service configurations and to network and user logon weaknesses. For the exam, you should be familiar with some of the more common tools used to conduct vulnerability assessments, including the following:

- Port scanners: This software utility scans a single machine or a range of IP addresses, checking for a response on service ports. A response on port 80, for example, might reveal the operation of an HTTP host. Port scanners are useful in creating an inventory of services hosted on networked systems. When applied to test ports on a single system, this is termed a port scan, whereas a scan across multiple hosts is referred to as a port sweep.
- Vulnerability scanners: This software utility scans a range of IP addresses, testing for the presence of known vulnerabilities in software configuration and accessible services. Unlike port scanners, which only test for the availability of services, vulnerability scanners may check for the particular version or patch level of a service to determine its level of vulnerability.
- Protocol analyzers: This software utility is used on a hub, a switch supervisory port, or in line with network connectivity to enable the analysis of network communications. Individual protocols, specific endpoints, or sequential access attempts can be identified using this utility, which is often referred to as a packet sniffer.

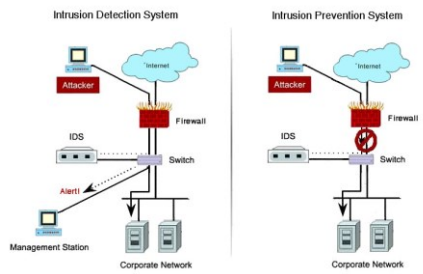
318

Identifying Vulnerabilities

- Network mappers: Another software utility used to conduct network assessments over a range of IP addresses, the network mapper compiles a listing of all systems, devices, and network hardware present within a network segment. This information can be used to identify simple points of failure, to conduct a network inventory, and to create graphical details suitable for reporting on network configurations.
- Password crackers: This software utility allows direct testing of user logon password strength by conducting a brute-force password test using dictionary terms, specialized lexicons, or mandatory complexity guidelines. Password crackers should provide only the relative strength of a password, rather than the password itself, to avoid weakening logon responsibility under evidentiary discovery actions.

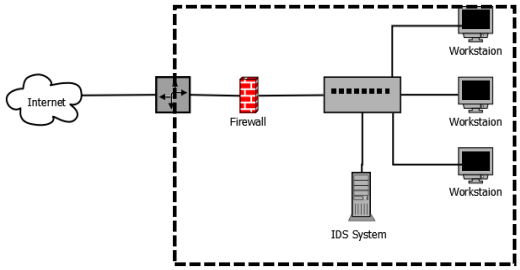
319

Intrusion Detection System



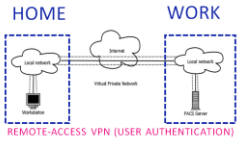
320

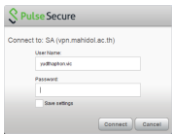
Firewall

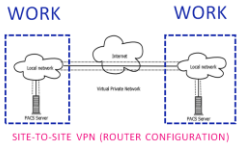


321

Virtual Private Network: VPN







322

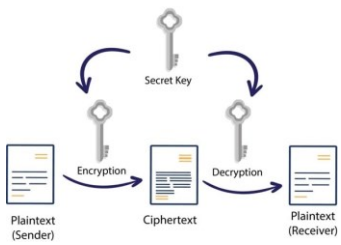
Encryption techniques

- **AES** – Advanced encryption standard, trusted by many standard organizations. It can encrypt 128-bit, 192-bit as well as 256-bit. AES is a symmetric encryption algorithm that is mostly in use today. AES is used for both rest data as well as at transit.

https://intellipaat.com/blog/tutorial/ethical-hacking-cyber-security-tutorial/encryption-techniques/

323

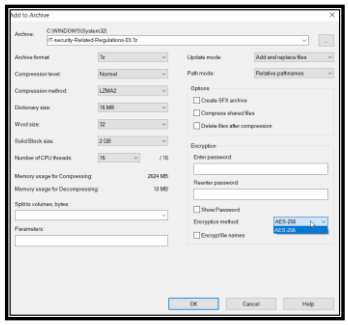
Symmetric Encryption



https://www.encryptionconsulting.com/what-are-encryption-protocols-and-how-do-they-work/

324

File Encryption using 7zip



325

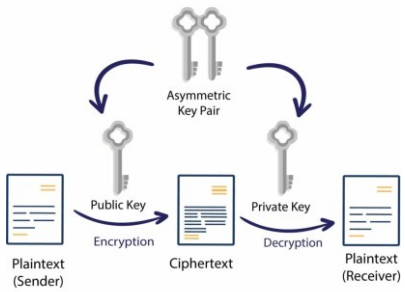
Encryption techniques

- **RSA** – Public encryption algorithm to protect the data over the internet. It is an asymmetric key encryption algorithm that uses public and private keys. RSA is an algorithm based on the factorization of the product of two prime numbers. If the receiver knows these numbers only then, he/she can decrypt the message. RSA finds its applications in digital signatures but is often slow when a large volume of data is to be encrypted.

https://intellipaat.com/blog/tutorial/ethical-hacking-cyber-security-tutorial/encryption-techniques/

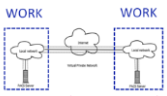
326

Asymmetric Encryption

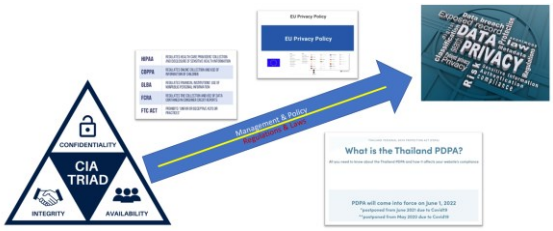


https://www.encryptionconsulting.com/what-are-encryption-protocols-and-how-do-they-work/

327



328



329

What is an Information Security Management System?

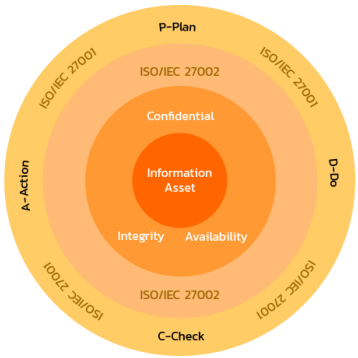
- ISO27001 (or to give its proper name, ISO/IEC 27001) is the international standard for Information Security Management Systems (ISMS)
- An ISMS is a set of processes that together help an organization to manage their information security by assessing their risks and taking action to reduce them.
- The management system is simply a set of things you must do to keep on top of your information security

330

Main components

- Information security policy – what are your rules on keeping your subject data secure?
- Objectives – what are you trying to do with your data?
- Risk assessment and treatment – what could go wrong like subject data leak and how can you stop it?
- Roles and responsibilities – who does what in your research?
- Competence – does everyone have the skills they need to work with the data?
- Awareness training – does everyone in your research team know about information security?
- Monitoring and measuring – quantifying what's going on accessing and using your subject data.
- Internal audit – independent checks that it's all happening as it should with your data.
- Management review – keeping everything in your subject data use under control.

331



332

Clinical Data Erasure

- How to securely delete files

File allocation table

File name	Creation Time	First cluster	Length
A	T1	1	2
B	T2	3	4
C	T3	7	5
D	T4	...	...
E	T5	...	...

File on disk

00	1	2	3	4	5	6	7	8	9	10
10	A	A	B	B	B	B	C	C	C	C
20	C	D	D	E	E	E	E			

333

File allocation table

File name	Creation Time	First cluster	Length
A	T1	1	2
B Deleted	T2	3	4
C	T3	7	5
D	T4	...	...
E	T5	...	...

*Marked as Deleted

Undeleting possible

File on disk

File content is still on the device

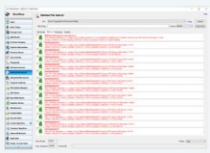
00	1	2	3	4	5	6	7	8	9	10
10	A	A	B	B	B	B	C	C	C	C
20	C	D	D	E	E	E	E			

Press: shift + delete (do not put into the recycle bin)

334

Recover Deleted Files

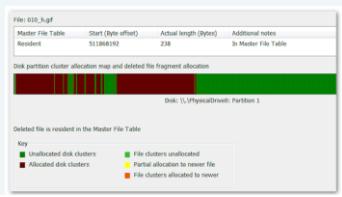
OSForensics™ allows you to recover and search deleted files, even after they have been removed from the Recycle Bin. This allows you to review the files that the user may have attempted to destroy.
Each deleted file found is displayed with a corresponding Quality indicator between 0-100. A value towards 100 means that the deleted file is largely intact, with only a few missing clusters of data.



335

Deleted File Cluster View

OSForensics also provides a graphical view of the allocation of the deleted file clusters on the physical disk.



336

Clinical Data Erasure

- Clearing
  - Clearing is the removal of sensitive data from storage devices in such a way that there is assurance that the data may not be reconstructed using normal system functions or software file/data recovery utilities. The data may still be recoverable, but not without special laboratory techniques.
  - Clearing is typically an administrative protection against accidental disclosure within an organization. For example, before a hard drive is re-used within an organization, its contents may be cleared to prevent their accidental disclosure to the next user.
- Purging
  - Purging or sanitizing is the physical rewrite of sensitive data from a system or storage device with the intent that the data cannot be recovered. Purging, proportional to the sensitivity of the data, is generally done before releasing media beyond control, such as before discarding old media, or moving media to a computer with different security requirements.
- Destruction
  - The storage media is made unusable for conventional equipment. Effectiveness of destroying the media varies by medium and method. Depending on recording density of the media, and/or the destruction technique, this may leave data recoverable by laboratory methods. Conversely, destruction using appropriate techniques is the most secure method of preventing retrieval.

337

Purging

- Sometimes referred to as data clearing, data wiping, or data destruction)
- A software-based method of overwriting the data that aims to completely destroy all electronic data residing on a hard disk drive or other digital media by using zeros and ones to overwrite data onto all sectors of the device.

338

Overwriting Standard	Date	Overwriting Rounds	Pattern	Notes
U.S. Navy Staff Office Publication NAVSO P-5239-26[13]	1993	3	A character, its complement, random	Verification is mandatory
U.S. Air Force System Security Instruction 5020[14]	1996	3	All zeros, all ones, any character	Verification is mandatory
Peter Gutmann's Algorithm	1996	1 to 35	Various, including all of the other listed methods	Originally intended for MFM and RLL disks, which are now obsolete
Bruce Schneier's Algorithm[15]	1996	7	All ones, all zeros, pseudo-random sequence five times	
U.S. DoD Unclassified Computer Hard Drive Disposition[16]	2001	3	A character, its complement, another pattern	
German Federal Office for Information Security[17]	2004	2–3	Non-uniform pattern, its complement	
Communications Security Establishment Canada ITSG-06[18]	2006	3	All ones or zeros, its complement, a pseudo-random pattern	For unclassified media
NIST SP-800-88[19]	2006	1	?	
U.S. National Industrial Security Program Operating Manual (DoD 5220.22-M)[12]	2006	?	?	No longer specifies any method.
NSA/CSS Storage Device Declassification Manual (SDDM)[20]	2007	0		Degauss or destroy only
Australian Government ICT Security Manual 2014 – Controls[21]	2014	1	Random pattern (only for disks larger than 15 GB)	Degauss magnetic media or destroy Top Secret media
New Zealand Government Communications Security Bureau NZSIT 402[22]	2008	1	?	For data up to Confidential
British HMG Infosec Standard 5, Baseline Standard[23]	?	1	Random Pattern	Verification is mandatory
British HMG Infosec Standard 5, Enhanced Standard	?	3	All ones, all zeros, random	Verification is mandatory
NIST SP-800-88 Rev. 1[24]	2014	1	All zeros	Outlines solutions based on media type.[25]

339

File allocation table

File name	Creation Time	First cluster	Length
A	T1	1	2
B Deleted	T2	3	4
C	T3	7	5
D	T4	...	...
E	T5	...	...

*Deleted and overwritten

File on disk

File content is overwritten depending on standards

00	1	2	3	4	5	6	7	8	9	10
10	A	A	0	0	0	0	C	C	C	C
20	C	D	D	E	E	E	E			

340

File Shredder Software (clearing + purging)

- File Shredder is a desktop application for shredding (destroying) unwanted files beyond recovery

341

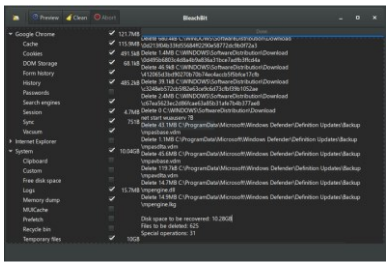
List of data-erasing software

342

BleachBit

Home | Download | Features | Contribute | Shop | Help

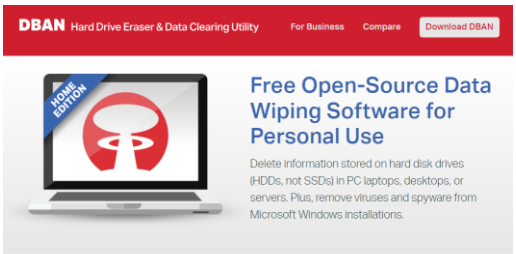
Clean Your System and Free Disk Space



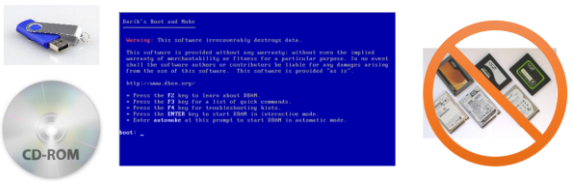
343

Darik's Boot and Nuke

https://dban.org/



344

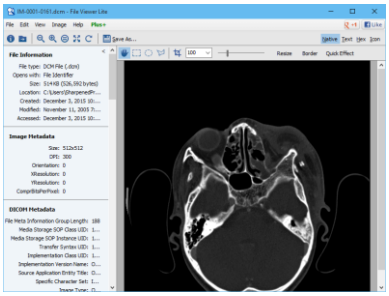


345

Destruction

346

DICOM Anonymizing



347

DICOM Anonymizing

General:

TAG	Name	Value
0002, 0012	Implementation Class UID	modified
0002, 0013	Implementation Class UID	"DICOMLIBRARY-100"
0002, 0016	Source Application Entity Title	"DICOMLIBRARY"
0002, 0100	Private Information Creator UID	empty
0002, 0102	Private Information	empty

UID Anonymity:

TAG	Name	Value
0002, 0003	Media Storage SOP Instance UID	unique
0008, 0018	SOP Instance UID	unique
0020, 000D	Study Instance UID	unique
0020, 000E	Series Instance UID	unique

Visit Anonymity:

TAG	Name	Value
0008, 0080	Institution Name	empty
0008, 0081	Institution Address	empty
0008, 0082	Institution Code Sequence	removed
0008, 0090	Referring Physician's Name	empty
0008, 0092	Referring Physician's Address	empty
0008, 0094	Referring Physician's Telephone Numbers	empty
0008, 0096	Referring Physician Identification Sequence	removed
0008, 0116	Responsible Organization	empty
0008, 1048	Physician(s) of Record	empty
0008, 1049	Physician(s) of Record Identification Sequence	removed
0008, 1050	Performing Physician's Name	empty
0008, 1052	Performing Physician Identification Sequence	removed
0008, 1060	Name of Physician(s) Reading Study	empty
0008, 1062	Physician(s) Reading Study Identification Sequence	removed
0008, 1070	Operators' Name	empty
0008, 1072	Operator Identification Sequence	removed
0038, 0010	Admission ID	empty
0038, 0011	Issuer of Admission ID	empty
0038, 0016	Route of Admissions	empty
0038, 001a	Scheduled Admission Date (RET)	empty
0038, 001b	Scheduled Admission Time (RET)	empty
0038, 001c	Scheduled Discharge Date (RET)	empty
0038, 001d	Scheduled Discharge Time (RET)	empty
0038, 001e	Scheduled Patient Institution Residence (RET)	empty
0038, 0020	Admitting Date	empty
0038, 0021	Admitting Time	empty
0038, 0030	Discharge Date (RET)	empty
0038, 0032	Discharge Time (RET)	empty
0038, 0040	Discharge Diagnosis Description (RET)	empty
0038, 0044	Discharge Diagnosis Code Sequence (RET)	removed
0038, 0300	Current Patient Location	empty
0038, 0400	Patient's Institution Residence	empty
0038, 0500	Patient State	empty

Patient Anonymization:

TAG	Name	Value
0010, 0010	Patient's Name	"Anonymized^^^"
0010, 0020	Patient ID	"0"
0010, 0021	Issuer of Patient ID	empty
0010, 0022	Type of Patient ID	empty
0010, 0030	Patient's Birth Date	empty
0010, 0032	Patient's Birth Time	empty
0010, 0050	Patient's Insurance Plan Code Sequence	removed
0010, 0101	Patient's Primary Language Code Sequence	removed
0010, 0102	Patient's Primary Language Code Modifier Sequence	removed
0010, 1000	Other Patient IDs	empty
0010, 1001	Other Patient Names	empty
0010, 1002	Other Patient IDs Sequence	removed
0010, 1005	Patient's Birth Name	empty
0010, 1040	Patient's Address	empty
0010, 1050	Insurance Plan Identification (RET)	empty
0010, 1060	Patient's Mother's Birth Name	empty
0010, 1080	Military Rank	empty
0010, 1081	Branch of Service	empty
0010, 1090	Medical Record Locator	empty
0010, 2150	Country of Residence	empty
0010, 2152	Region of Residence	empty
0010, 2154	Patient's Telephone Numbers	empty
0010, 2160	Ethnic Group	empty
0010, 2180	Occupation	empty
0010, 21b0	Additional Patient History	empty
0010, 2110	Pregnancy Status	empty
0010, 21d0	Last Menstrual Date	empty
0010, 21f0	Patient's Religious Preference	removed
0010, 2202	Patient Species Code Sequence	removed
0010, 2203	Patient's Sex Neutered	removed
0010, 2293	Patient Breed Code Sequence	removed
0010, 2294	Breed Registration Sequence	removed
0010, 2295	Breed Registration Number	empty
0010, 2296	Breed Registry Code Sequence	removed
0010, 2297	Responsible Person	empty
0010, 2298	Responsible Person Role	empty
0010, 2299	Responsible Organization	empty

348

Procedure Anonymity:

TAG	Name	Value
0040, 0001	Scheduled Station AE Title	empty
0040, 0006	Scheduled Performing Physician's Name	empty
0040, 0008	Scheduled Performing Physician Identification Sequence	removed
0040, 0010	Scheduled Station Name	empty
0040, 0011	Scheduled Procedure Step Location	empty
0040, 0012	Pre-Medication	empty
0040, 0241	Performed Station AE Title	empty
0040, 0242	Performed Station Name	empty
0040, 0243	Performed Location	empty
0040, 0296	Billing Item Sequence	removed

Results Anonymity:

TAG	Name	Value
4008, 0042	Results ID Issuer (RET)	empty

Interpretation Anonymity:

TAG	Name	Value
4008, 010c	Interpretation Author (RET)	empty
4008, 0114	Physician Approving Interpretation (RET)	empty
4008, 0119	Distribution Name (RET)	empty
4008, 011a	Distribution Address (RET)	empty
4008, 0202	Interpretation ID Issuer (RET)	empty

Equipment Anonymity:

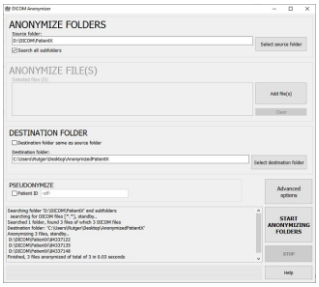
TAG	Name	Value
0008, 0070	Manufacturer	empty
0008, 1010	Station Name	empty
0008, 1040	Institutional Department Name	empty
0008, 1090	Manufacturer's Model Name	empty
0018, 1000	Device Serial Number	empty
0018, 1016	Secondary Capture Device Manufacturer	empty
0018, 1017	Hardcopy Device Manufacturer	empty
0018, 1018	Secondary Capture Device Manufacturer's Model Name	empty
0018, 1019	Secondary Capture Device Software Version(s)	empty
0018, 101a	Hardcopy Device Software Version	empty
0018, 101b	Hardcopy Device Manufacturer's Model Name	empty
0018, 1020	Software Version(s)	empty
0018, 1200	Date of Last Calibration	empty
0018, 1201	Time of Last Calibration	empty
0018, 700c	Date of Last Detector Calibration	empty
0018, 700e	Time of Last Detector Calibration	empty
0018, 7010	Exposures on Detector Since Last Calibration	empty
0018, 7011	Exposures on Detector Since Manufactured	empty

Study Anonymity:

TAG	Name	Value
0020, 0010	Study ID	"1"
0008, 0050	Accession Number	empty
0032, 000a	Study Status ID (RET)	empty
0032, 000c	Study Priority ID (RET)	empty
0032, 0012	Study ID Issuer (RET)	empty
0032, 0032	Study Verified Date (RET)	empty
0032, 0033	Study Verified Time (RET)	empty
0032, 0034	Study Read Date (RET)	empty
0032, 0035	Study Read Time (RET)	empty
0032, 1000	Scheduled Study Start Date (RET)	empty
0032, 1001	Scheduled Study Start Time (RET)	empty
0032, 1010	Scheduled Study Stop Date (RET)	empty
0032, 1011	Scheduled Study Stop Time (RET)	empty
0032, 1020	Scheduled Study Location (RET)	empty
0032, 1021	Scheduled Study Location AE Title (RET)	empty
0032, 1030	Reason for Study (RET)	empty
0032, 1031	Requesting Physician Identification Sequence	removed
0032, 1032	Requesting Physician	empty
0032, 1033	Requesting Service	empty
0032, 1040	Study Arrival Date (RET)	empty
0032, 1041	Study Arrival Time (RET)	empty
0032, 1050	Study Completion Date (RET)	empty
0032, 1051	Study Completion Time (RET)	empty
0032, 1055	Study Component Status ID (RET)	empty
0032, 1060	Requested Procedure Description	empty
0032, 1064	Requested Procedure Code Sequence	removed
0032, 1070	Requested Contrast Agent	empty
0032, 4000	Study Comments	empty
0040, 2008	Order Entered By	empty
0040, 2009	Order Enterer's Location	empty
0040, 2010	Order Callback Phone Number	empty

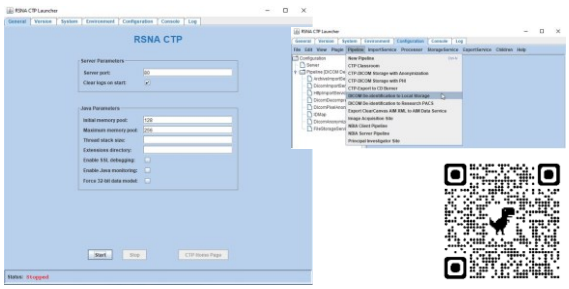
349

DICOM Anonymizer



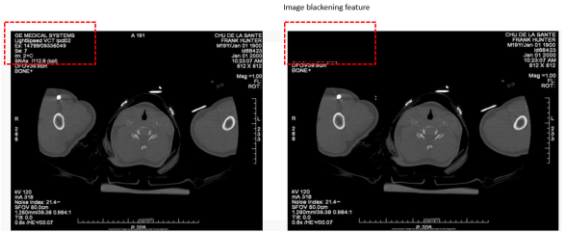
350

RSNA Clinical Trial Processor (CTP)



351

Image blackening feature



https://www.imaios.com/en/Company/blog/Top-5-Best-DICOM-De-identification-tools

352

Question & Answer

Thank you for your attention

☺☺☺

353

DICOM Standard

Yudthaphon Vichianin, Ph.D.
Department of Radiological Technology
Faculty of Medical Technology
Mahidol University

354

DICOM: History

DICOM™ Digital Imaging and Communications in Medicine

NEMA, Suite 900
1300 North 17th Street
Rosslyn, VA 22209
Ph: (703) 475-9217
http://dicom.nema.org
dicom@medicalimaging.org

- Developed by American College of Radiology (ACR) and National Electrical Manufacturers Association (NEMA).
- ACR and NEMA joined forces and formed a standard committee in 1983
- The first standard was released in 1985 (ACR/NEMA 300)
- In 1988 the second version was released (ACR/NEMA 2.0)
- In 1993 the third version of the standard was released. Its name was then changed to "DICOM"
- Current DICOM 3 2016

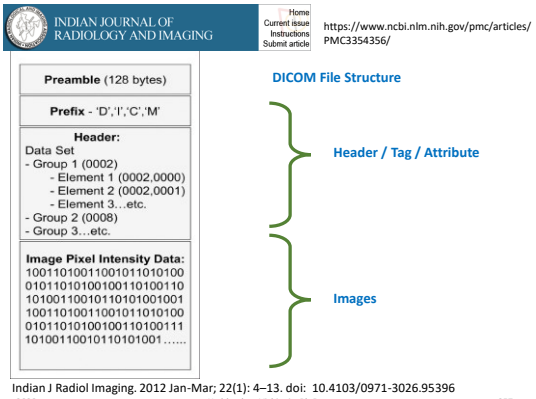
http://dicom.nema.org/

355

DICOM

- **D**igital **I**maging and **Co**mmunications in **M**edicine (DICOM)
- A standard for handling, storing, printing, and transmitting information in medical imaging.
- Including a file format definition and a network communications protocol.
- TCP/IP to communicate between systems

356



Indian J Radiol Imaging. 2012 Jan-Mar; 22(1): 4–13. doi: 10.4103/0971-3026.95396

357

File format	Advantages	Disadvantages	Applications in clinical radiology
JPEG (.jpg)	Permits setting compression level; small image size	Low image quality at higher degrees of compression	Images for on-screen display (websites and PowerPoint® presentations)
GIF (.gif)	Good internet browser support; good for displaying animations	Larger file sizes; limited color support (256 colors or 256 shades of gray)	Images for display on a website
PNG (.png)	Good internet browser support; good image quality	Limited acceptance with earlier web browsers	Teaching files; publication; images for display on a website
TIFF (.tif)	High image quality	Large file size	Master copies of teaching file; format preferred by journals for publication

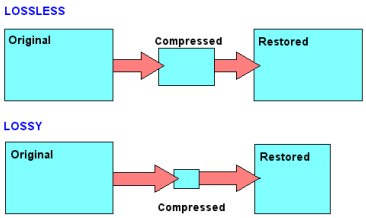
Indian J Radiol Imaging. 2012 Jan-Mar; 22(1): 4–13.
doi: 10.4103/0971-3026.95396

358

Modalities	Pixel matrix	Total pixels	Size of images
Nuclear medicine	128 × 128	16,384	0.16 MP
MRI	256 × 256	65,536	0.06 MP
USG	512 × 512	262,144	0.25 MP
DSA	512 × 512	262,144	0.25 MP
CT scan	512 × 512	262,144	0.25 MP
CR / DR	2048 × 2048	4,194,304	4 MP
Digital mammography	4000 × 5000	20,000,000	81 MP
Digital cameras	User defined	User defined	3–20 MP

Indian J Radiol Imaging. 2012 Jan-Mar; 22(1): 4–13.
doi: 10.4103/0971-3026.95396

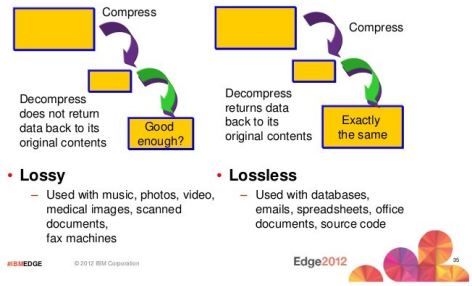
359



Lossless formats are better when higher image quality is desired, such as for archiving, teaching, and submission for publication.

360

Lossy vs. Lossless Methods



- **Lossy**
  - Used with music, photos, video, medical images, scanned documents, fax machines
- **Lossless**
  - Used with databases, emails, spreadsheets, office documents, source code

361

Lossless compression

- Huffman coding
- Run-length encoding
- Dictionary coders
- Prediction by partial matching
- Dynamic Markov Compression
- Adaptive Huffman coding
- Wavelet compression

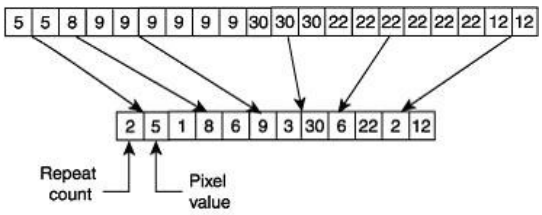
362

Data Compression Example

- Run-length encoding (RLE) - TIFF
- WWWWWWWWWWWWBWWWWWWWWW WWWWBBBWWWWWWWWWWWWWW WWWWWWWWWWBWWWWWWWWW WWWW
- Replace with **12WB12W3B24WB14W**

363

RLE image compression



364

Lossy Compression

- Discrete cosine transform
- Fractal transform
- Wavelet compression
- Vector quantization
- Linear predictive coding
- Interpolative encoding

365

JPEG2000

- JPEG 2000 includes a lossless mode based on a special integer wavelet filter.
- JPEG 2000 is a wavelet-based image compression standard.
- It was created by the Joint Photographic Experts Group committee in the year 2000.
- The standardized filename extension is **.jp2**

366

DICOM: PS3.14: Grayscale Standard Display Function

PS 3.14 -2011
Page 12

7.1 GENERAL FORMULAS

The Grayscale Standard Display Function is defined by a mathematical interpolation of the 1023 Luminance levels derived from Barten's model. The Grayscale Standard Display Function allows us to calculate luminance, L, in candelas per square meter, as a function of the Just-Noticeable Difference (JND) Index, j:

$$\log_{10} L(j) = \frac{a + c \cdot Ln(j) + e \cdot (Ln(j))^2 + g \cdot (Ln(j))^3 + m \cdot (Ln(j))^4}{1 + b \cdot Ln(j) + d \cdot (Ln(j))^2 + f \cdot (Ln(j))^3 + h \cdot (Ln(j))^4 + k \cdot (Ln(j))^5}$$

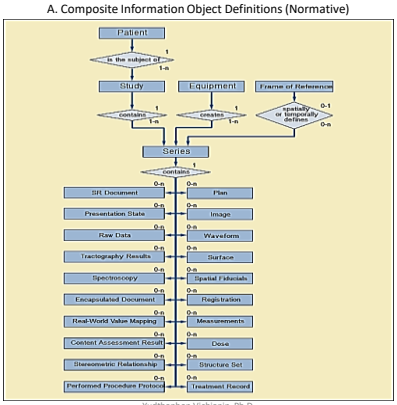
with Ln referring to the natural logarithm, j the index (1 to 1023) of the Luminance levels L_j of the JNDs, and a = -1.3011877, b = -2.5840191E-2, c = 8.0242636E-2, d = -1.0320229E-1, e = 1.3646699E-1, f = 2.8745620E-2, g = -2.5468404E-2, h = -3.1978977E-3, k = 1.2992634E-4, m = 1.3635334E-3.

The logarithms to the base 10 of the Luminance L_j are very well interpolated by this function over the entire Luminance Range. The relative deviation of any log(Luminance)-value from the function is at most 0.3%, and the root-mean-square-error is 0.0003. The continuous representation of the Grayscale Standard Display Function permits a user to compute discrete JNDs for arbitrary start levels and over any desired Luminance Range.

PS3.14.htm http://dicom.nema.org/medical/dicom/current/output/html/part14.html

367

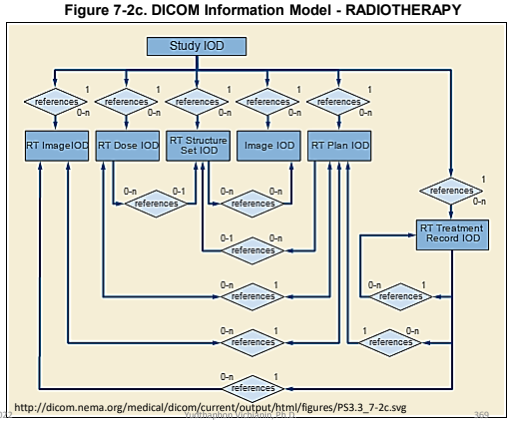
7 DICOM Model of the Real World
A. Composite Information Object Definitions (Normative)



http://dicom.nema.org/medical/dicom/current/output/html/part03.html#chapter_A

368

Figure 7-2c. DICOM Information Model - RADIOTHERAPY



http://dicom.nema.org/medical/dicom/current/output/html/figures/PS3.3_7-2c.svg

369

DICOM:

- Example of CR Image file in DICOM standard perspective
  - PS3.3.htm -- A.2. Computed Radiography Image IOD
- Example of MR Image file in DICOM standard perspective
  - PS3.3.htm -- A.4. Magnetic Resonance Image IOD
- Example of US Image file in DICOM standard perspective
  - PS3.3.htm -- A.6. Ultrasound Image IOD

370

Table A.2-1. CR Image IOD Modules

IE	Module	Reference	Usage
Patient	Patient	C.7.1.1	M
	Clinical Trial Subject	C.7.1.3	U
Study	General Study	C.7.2.1	M
	Patient Study	C.7.2.2	U
	Clinical Trial Study	C.7.2.3	U
Series	General Series	C.7.3.1	M
	CR Series	C.8.1.1	M
	Clinical Trial Series	C.7.3.2	U
Equipment	General Equipment	C.7.5.1	M
Image	General Image	C.7.6.1	M
	General Reference	C.12.4	U
	Image Pixel	C.7.6.3	M
	Contrast/Bolus	C.7.6.4	C - Required if contrast media was used in this image
	Display Shutter	C.7.6.11	U
	Device	C.7.6.12	U
	Specimen	C.7.6.22	U
	CR Image	C.8.1.2	M
	Overlay Plane	C.9.2	U
	Modality LUT	C.11.1	U
	VOI LUT	C.11.2	U
	SOP Common	C.12.1	M
	Common Instance Reference	C.12.2	U

Mandatory = M
Conditional = C
User Option = U

371

Table A.4-1. MR Image IOD Modules

IE	Module	Reference	Usage
Patient	Patient	C.7.1.1	M
	Clinical Trial Subject	C.7.1.3	U
Study	General Study	C.7.2.1	M
	Patient Study	C.7.2.2	U
	Clinical Trial Study	C.7.2.3	U
Series	General Series	C.7.3.1	M
	Clinical Trial Series	C.7.3.2	U
Frame of Reference	Frame of Reference	C.7.4.1	M
Equipment	General Equipment	C.7.5.1	M
Image	General Image	C.7.6.1	M
	General Reference	C.12.4	U
	Image Plane	C.7.6.2	M
	Image Pixel	C.7.6.3	M
	Contrast/Bolus	C.7.6.4	C - Required if contrast media was used in this image
	Device	C.7.6.12	U
	Specimen	C.7.6.22	U
	MR Image	C.8.3.1	M
	Overlay Plane	C.9.2	U
	VOI LUT	C.11.2	U
	SOP Common	C.12.1	M
	Common Instance Reference	C.12.2	U

Mandatory = M
Conditional = C
User Option = U

372

DICOM service classes

Yudthaphon Vichianin, Ph.D.

373

PACS 12. DICOM service classes

Yudthaphon Vichianin, Ph.D.

374

DICOM Service Class Examples

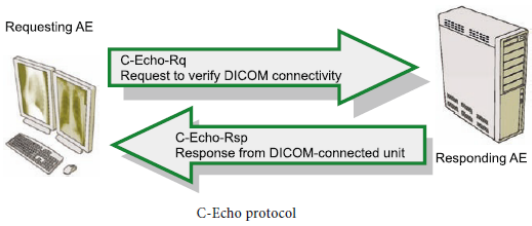
- Verification service
- Storage service
- Query/Retrieve service
- Modality Worklist service

375

Verification Service

Yudthaphon Vichianin, Ph.D.

376



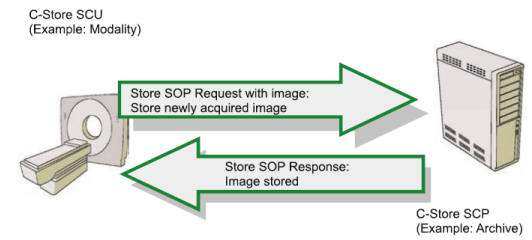
C-Echo protocol

377

Storage Service

Yudthaphon Vichianin, Ph.D.

378



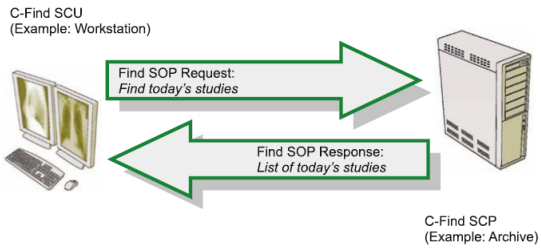
DICOM C-Store

379

Query/Retrieve Service

Yudthaphon Vichianin, Ph.D.

380



DICOM C-Find example: retrieving a list of all today's studies from an archive

381

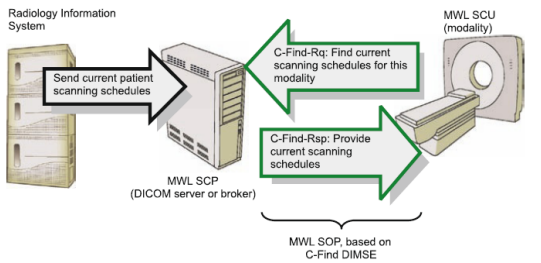
Modality Worklist Service

Yudthaphon Vichianin, Ph.D.

382

Modality Worklist SOP

SOP Class name	SOP Class UID
Modality Worklist	1.2.840.10008.5.1.4.31



DICOM MWL example: populating imaging modalities with basic patient data

383

HL7

Yudthaphon Vichianin, Ph.D.
Department of Radiological Technology
Faculty of Medical Technology
Mahidol University

384

HL7: Health Level 7

- Definition: a set of international standards for transfer of clinical and administrative data between software applications used by various healthcare providers.
- Objective: Healthcare systems can communicate with each other.

95% of US healthcare organizations use HL7 V2

More than 35 countries have HL7 V2.x implementations

https://en.wikipedia.org/wiki/Health_Level_7

385

HL7: Website

http://www.hl7.org/

386

HL7: Health Level 7

- Standard series of predefined logical format for packaging healthcare data in the form of messages to be transmitted among computer system.
- Message: a collection of data that sends information about an event in the healthcare organization.
- Interface: data connection between 2 (or more) computer systems
- Level 7: in the OSI model (7 layers)

387

HL7: Events

- Registration
- Orders (Clinical & none clinical)
- Results and observations
- Queries
- Finance
- Master files and indexes
- Document control
- Scheduling and logistics
- Personnel administration
- Patient care planning
- Network synchronization
- Laboratory automation

388

HL7: Events

- HL7 messages are used to communicate events that occur in the clinical order entry module of the HIS/EMR as well as events that occur in the Radiology Information System (RIS). These include

1. Creating, amending and canceling a radiology request in the HIS/EMR sent as HL7 order messages (HL7 ORM)
2. Creating, amending and canceling a radiology request in the RIS sent as HL7 order messages (HL7 ORM)
3. Progressing the exam in the RIS (arrival, exam start, exam complete) sent as HL7 order messages (HL7 ORM)
4. Notifying the HIS of a radiology report (result) being available (interim, final, corrected) sent as HL7 result messages (HL7 ORU)

389

HL7: Versions

- Version 2.x Messaging Standard – an interoperability specification for health and medical transactions (current 2.8.2)
- Version 3 Messaging Standard – an interoperability specification for health and medical transactions

390

HL7: Example of Version 2.x Messaging

```
MSH|^~\&|MegaReg|XYZHospC|SuperOE|XYZImgCtr|20060529090131
EVN||200605290901||||200605290900
PID|||56782445^^^UAReg^PI||KLEINSAMPLE^BARRY^Q^JR||1962091
PV1||I|W^389^1^UABH^^^^3||||12345^MORGAN^REX^J^^^MD^0010^U
OBX|1|NM|^Body Height||1.80|m^Meter^ISO+|||||F
OBX|2|NM|^Body Weight||79|kg^Kilogram^ISO+|||||F
AL1|1||^ASPIRIN
DG1|1||786.50^CHEST PAIN, UNSPECIFIED^I9|||A
```

https://en.wikipedia.org/wiki/Health_Level_7

391

HL7: Example of Version 3 Messaging

```
<POLB_IN224200 ITSVersion="XML_1.0" xmlns="urn:hl7-org:v3"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <id root="2.16.840.1.113883.19.1122.7" extension="CNTRL-3456"/>
  <creationTime value="200202150930-0400"/>
  <!-- The version of the datatypes/RIM/vocabulary used is that of May 2006 -->
  <versionCode code="2006-05"/>
  <!-- interaction id= Observation Event Complete, w/o Receiver Responsibilities -->
  <interactionId root="2.16.840.1.113883.1.6" extension="POLB_IN224200"/>
  <processingCode code="P"/>
  <processingModeCode nullFlavor="OTH"/>
  <acceptAckCode code="ER"/>
  <receiver typeCode="RCV">
    <device classCode="DEV" determinerCode="INSTANCE">
      <id extension="GHH LAB" root="2.16.840.1.113883.19.1122.1"/>
      <asLocatedEntity classCode="LOCE">
        <location classCode="PLC" determinerCode="INSTANCE">
          <id root="2.16.840.1.113883.19.1122.2" extension="ELAB-3"/>
        </location>
      </asLocatedEntity>
    </device>
```

https://en.wikipedia.org/wiki/Health_Level_7

392

HL7: Structure of a Message

- Default encoding: | delimiter
- Example of HL7 message (Admission)

```
MSH|^~\&|MegaReg|XYZHospC|SuperOE|XYZImgCtr|20060529090131-
   0500||ADT^A01^ADT_A01|01052901|P|2.5
EVN||200605290901||||200605290900
PID|||56782445^^^UAReg^PI||KLEINSAMPLE^BARRY^Q^JR||19620910|M||2028-
   9^^HL70005^RA99113^^XYZ|260 GOODWIN CREST DRIVE^^BIRMINGHAM^AL^35
   209^^M~NICKELL'S PICKLES^10000 W 100TH AVE^BIRMINGHAM^AL^35200^^O
   ||||||0105I30001^^^99DEF^AN
PV1||I|W^389^1^UABH^^^^3||||12345^MORGAN^REX^J^^^MD^0010^UAMC^L||678
   90^GRAINGER^LUCY^X^^^MD^0010^UAMC^L|MED|||||A0||13579^POTTER^SHER
   MAN^T^^^MD^0010^UAMC^L|||||||||||||||||||||||||||200605290900
OBX|1|NM|^Body Height||1.80|m^Meter^ISO+|||||F
OBX|2|NM|^Body Weight||79|kg^Kilogram^ISO+|||||F
AL1|1||^ASPIRIN
DG1|1||786.50^CHEST PAIN, UNSPECIFIED^I9|||A
```


393

Message segments

- Message header (MSH)
- Event information (EVN)
- Patient Identification (PID)
- Patient visit information (PV)
- Observation (OBX) Used to transmit amount, unit, reference range, and status information about single observation
- Allergy (AL)
- Diagnostic (DG)

394

HL7: Elements of messages

```
MSH|^~\&|MegaReg|XYZHospC|SuperOE|XYZImgCtr|20060529090131-
   0500||ADT^A01^ADT_A01|01052901|P|2.5
EVN||200605290901||||200605290900
PID|||56782445^^^UAReg^PI||KLEINSAMPLE^BARRY^Q^JR||19620910|M||2028-
   9^^HL70005^RA99113^^XYZ|260 GOODWIN CREST DRIVE^^BIRMINGHAM^AL^35
   209^^M~NICKELL'S PICKLES^10000 W 100TH AVE^BIRMINGHAM^AL^35200^^O
   ||||||0105I30001^^^99DEF^AN
PV1||I|W^389^1^UABH^^^^3||||12345^MORGAN^REX^J^^^MD^0010^UAMC^L||678
   90^GRAINGER^LUCY^X^^^MD^0010^UAMC^L|MED|||||A0||13579^POTTER^SHER
   MAN^T^^^MD^0010^UAMC^L|||||||||||||||||||||||||||200605290900
OBX|1|NM|^Body Height||1.80|m^Meter^ISO+|||||F
OBX|2|NM|^Body Weight||79|kg^Kilogram^ISO+|||||F
AL1|1||^ASPIRIN
DG1|1||786.50^CHEST PAIN, UNSPECIFIED^I9|||A
```

- Segment: a collection of data elements relating to one side of a message.
- Segment ID : 3 first characters.

395

HL7: OBX Imaging Procedure

- Modality worklist

```
MSH|^~\&|SuperOE|XYZHospC|ImgScheduler|XYZImgCtr|20060529090136-050
   0||ORM^O01|01052906|P|2.5
PID|||56782445^^^UAReg^PI||KLEINSAMPLE^BARRY^Q^JR||19620910|M||2028
   -9^^HL70005^RA99113^^XYZ|260 GOODWIN CREST DRIVE^^BIRMINGHAM^AL^3
   5209^^M~NICKELL'S PICKLES^10000 W 100TH AVE^BIRMINGHAM^AL^35200^^
   O||||||0105I30001^^^99DEF^AN
PV1||I|W^389^1^UABH^^^^3||||12345^MORGAN^REX^J^^^MD^0010^UAMC^L||67
   890^GRAINGER^LUCY^X^^^MD^0010^UAMC^L|MED|||||A0||13579^POTTER^SHE
   RMAN^T^^^MD^0010^UAMC^L
ORC|NW|U123456|01E29005||||1^^^200605291100||200605290900|54321^SOM
   ETECH^AGNES^Z^^^MT^^^UAMC^L||67890^GRAINGER^LUCY^X^^^MD^^^UAMC^L|
   |^WPN^CP^^1^311^5552368~^ASN^PH^^1^311^5551212|||^UAMC
OBR||U123456|01E29005|93000^ELECTROCARDIOGRAM^CPT4||||||||||67890
   ^GRAINGER^LUCY^X^^^MD^^^UAMC^L||U123456|U123456|U123456||||ECG|||
   1^^^200605291100
ZDS|1.2.33.444.5555.4565432|ZOTZArchive|Application|DICOM
```


396

Message segments

- MSH|^~\&|MegaReg|XYZHospC|SuperOE|XYZImgCtr|20060529090131-0500||ADT^A01^ADT_A01|01052901|P|2.5
- EVN||200605290901||||200605290900
- PID|||56782445^^^UAReg^PI||KLEINSAMPLE^BARRY^Q^JR||19620910|M||2028-9^^HL70005^RA99113^^XYZ|260 GOODWIN CREST DRIVE^^BIRMINGHAM^AL^35209^^M~NICKELL'S PICKLES^10000 W 100TH AVE^BIRMINGHAM^AL^35200^^O|||||||0105I30001^^^99DEF^AN

397

Message segments

- PV1|1|I|W^389^1^UABH^^^^3||||12345^MORGAN^REX^J^^^MD^0010^UAMC^L||67890^GRAINGER^LUCY^X^^^MD^0010^UAMC^L|MED|||||A0||13579^POTTER^SHERMAN^T^^^MD^0010^UAMC^L|||||||||||||||||||||||||200605290900
- OBX|1|NM|^Body Height||1.80|m^Meter^ISO+|||||F
  OBX|2|NM|^Body Weight||79|kg^Kilogram^ISO+|||||F
- Allergy
  AL1|1||^ASPIRIN
- Diagnostic
  DG1|1||786.50^CHEST PAIN, UNSPECIFIED^I9|||A

398

Delimiter

- Field separator: 4th character → |
- Component separator: caret → ^

MSH|^~\&|MegaReg|XYZHospC|ImgOrdMgr|XYZImgCtr|20010529090131-0500||ADT^A01^ADT_A01|01052901|P|2.5

- Repetition separator: tilde → ~

PID|||56782445^^^UAReg^PI||KLEINSAMPLE^BARRY^Q^JR||19620910|M||2028-9^^HL70005^RA99113^^XYZ|260 GOODWIN CREST DRIVE^^BIRMINGHAM^AL^35209^^M~NICKELL'S PICKLES^10000 W 100TH AVE^BIRMINGHAM^AL^35200^^O|||||||0105I30001^^^99DEF^AN

- Field# 11→ address→ 2 addresses repeating

399

Patient Identification segment:PID

- PID|||56782445^^^UAReg^PI||KLEINSAMPLE^BARRY^Q^JR||19620910|M||2028-9^^HL70005^RA99113^^XYZ|260 GOODWIN CREST DRIVE^^BIRMINGHAM^AL^35209^^M~NICKELL'S PICKLES^10000 W 100TH AVE^BIRMINGHAM^AL^35200^^O|||||||0105I30001^^^99DEF^AN
- PID|||56782445^^^UAReg^PI||KLEINSAMPLE^BARRY^Q^JR|19620910|M||2028-9^^HL70005^RA99113^^XYZ|260 GOODWIN CREST DRIVE^^BIRMINGHAM^AL^35209^^M~NICKELL'S PICKLES^10000 W 100TH AVE^BIRMINGHAM^AL^35200^^O|||||||0105I30001^^^99DEF^AN

- PID-8: Gender
- PID-11 Patient Address

400

PV1 Segment: Patient Visit

- PV1-2: Patient Class (in/out)

```
PV1|1|I|W^389^1^UABH^^^^3||||12345^MORGAN^REX^J^^^MD^0010^UAMC^L||678
   90^GRAINGER^LUCY^X^^^MD^0010^UAMC^L|MED|||||A0||13579^POTTER^SHER
   MAN^T^^^MD^0010^UAMC^L|||||||||||||||||||||||||||200605290900
```

- PV1-3: Assigned Patient Location

```
PV1|1|I|W^389^1^UABH^^^^3||||12345^MORGAN^REX^J^^^MD^0010^UAMC^L||678
   90^GRAINGER^LUCY^X^^^MD^0010^UAMC^L|MED|||||A0||13579^POTTER^SHER
   MAN^T^^^MD^0010^UAMC^L|||||||||||||||||||||||||||200605290900
```

- PV1-7 Attending Doctor
- PV1-8: Referring Doctor
- PV1-9: Consulting Doctor
- PV1-10: Hospital Service (ie. MED/SURG/RAD)
- PV1-44: Admit date/time
- PV1-45 Discharge date/time

401

Observation Segment: OBX

- Used to transmit amount, unit, reference range, and status information about single observation.
- Vital sign, blood pressure
- Laboratory result
- Send report (text)

402

OBX

- OBX|1|NM|^Body Height||1.80|m^Meter^ISO+|||||F
- OBX-3: Observation Identifier
- OBX|1|NM|^Body Height||1.80|m^Meter^ISO+|||||F
- OBX|1|NM|^Body Height||1.80|m^Meter^ISO+|||||F

403

OBX: Imaging Procedure

- MSH|^~\&|SuperOE|XYZHospC|ImgScheduler|XYZImgCtr|20060529090136-0500||ORM^O01|01052906|P|2.5
  PID|||56782445^^^UAReg^PI||KLEINSAMPLE^BARRY^Q^JR||19620910|M||2028-9^^HL70005^RA99113^^XYZ|260 GOODWIN CREST DRIVE^^BIRMINGHAM^AL^35209^^M~NICKELL'S PICKLES^10000 W 100TH AVE^BIRMINGHAM^AL^35200^^O||||||0105I30001^^^99DEF^AN
  PV1|1|I|W^389^1^UABH^^^^3||||12345^MORGAN^REX^J^^^MD^0010^UAMC^L||67890^GRAINGER^LUCY^X^^^MD^0010^UAMC^L|MED|||||A0||13579^POTTER^SHERMAN^T^^^MD^0010^UAMC^L
  ORC|NW|U123456|01E29005||||1^^^200605291100||200605290900|54321^SOMETECH^AGNES^Z^^^MT^^^UAMC^L||67890^GRAINGER^LUCY^X^^^MD^^^UAMC^L||^WPN^CP^^1^311^5552368~^ASN^PH^^1^311^5551212|||^UAMC
  OBR||U123456|01E29005|93000^ELECTROCARDIOGRAM^CPT4|||||||||||67890^GRAINGER^LUCY^X^^^MD^^^UAMC^L||U123456|U123456|U123456|||ECG|||1^^^200605291100
  ZDS|1.2.33.444.5555.4565432|ZOTZArchive|Application|DICOM

404

HL7: OBX Imaging Procedure

- OBX-18: Accession Number
- OBX-24: DICOM Modality
- ZDS: Study instance UID

* Z segments are custom and can vary from vendor to vendor

405

Basic Network Design

Yudthaphon Vichianin, Ph.D.
Department of Radiological Technology
Faculty of Medical Technology
Mahidol University

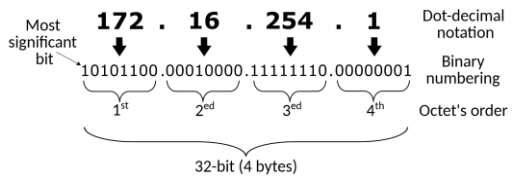
406

IP address

- An Internet Protocol address (IP address) is a numerical label such as 192.0.2.1 that is connected to a computer network that uses the Internet Protocol for communication.
- Internet Protocol version 4 (IPv4) defines an IP address as a 32-bit number.

407

IP address

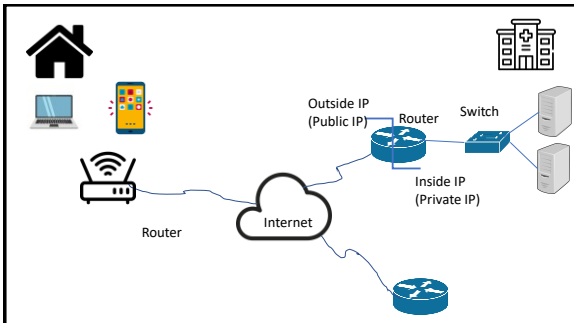


https://en.wikipedia.org/wiki/IP_address

408

https://conceptdraw.com/a886c3/p1/preview/640

409



410

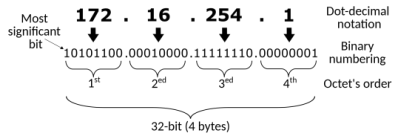
Private IP Address

- A public IP address is a globally unique, meaning that the address is not an address reserved for use in private networks
- Computers not connected to the Internet, such as hospital machines that communicate only with each other via TCP/IP, need not have globally unique IP addresses.
- Today, such private networks are widely used and typically connect to the Internet with network address translation (NAT), when needed.

411

Reserved private IPv4 network ranges[9]

Name	CIDR block	Address range	Number of addresses	Classful description
24-bit block	10.0.0.0/8	10.0.0.0 – 10.255.255.255	16 777 216	Single Class A.
20-bit block	172.16.0.0/12	172.16.0.0 – 172.31.255.255	1 048 576	Contiguous range of 16 Class B blocks.
16-bit block	192.168.0.0/16	192.168.0.0 – 192.168.255.255	65 536	Contiguous range of 256 Class C blocks.



https://en.wikipedia.org/wiki/IP_address

412

Pop quiz

- 8.8.8.8
- 8.8.4.4
- 202.28.162.1
- 172.16.255.254
- 192.168.100.2

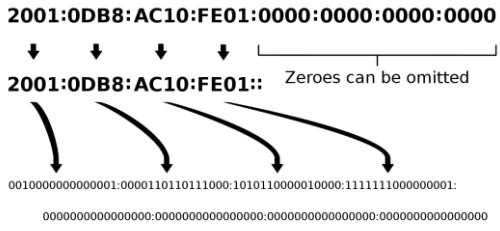
413

IP address version 6

- In IPv6, the address size was increased from 32 bits in IPv4 to 128 bits, thus providing up to 2128 (approximately 3.403×1038) addresses. This is deemed sufficient for the foreseeable future.

414

An IPv6 address (in hexadecimal)



https://en.wikipedia.org/wiki/IP_address

415

IP address assignment

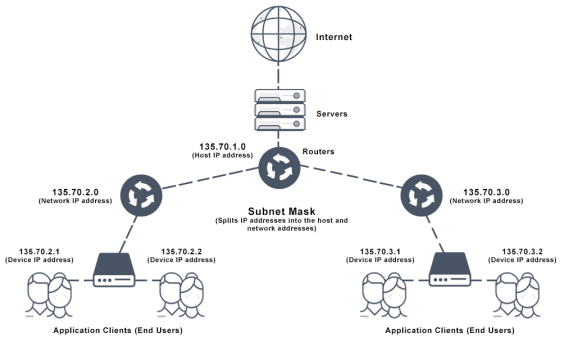
- IP addresses are assigned to a host either dynamically as they join the network, or persistently by configuration of the host hardware or software.
- Persistent configuration is also known as using a **static IP address**.
- In contrast, when a computer's IP address is assigned each time it restarts, this is known as using a **dynamic IP address**.

416

Subnet Mask

- Every device has an IP address with two pieces: the client or host address and the server or network address.
- IP addresses are either configured by a DHCP server or manually configured (static IP addresses).
- The subnet mask splits the IP address into the host and network addresses, thereby defining which part of the IP address belongs to the device and which part belongs to the network.

417



418

Subnet Mask

- A subnet mask is a 32-bit number created by setting host bits to all 0s and setting network bits to all 1s.
- In this way, the subnet mask separates the IP address into the network and host addresses.

419

Subnet Mask

- Class A, B, and C networks have natural masks, or default subnet masks:
- Class A: 255.0.0.0
- Class B: 255.255.0.0
- Class C: 255.255.255.0

420

Subnet Mask

- Typically, although the phrase “subnet mask” is preferred, you might use “IP/Mask” as a shorthand to define both the IP address and subnet mask at once.
- In this situation, the IP address is followed by the number of bits in the mask. For example:

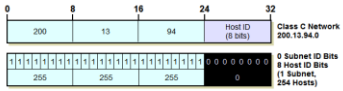
- 10.51.2.1/8
- 192.168.30.5/24

421

192.168.100.1/24

IP Address:	192	.	168	.	100	.	1
IP (Binary):	11000000	.	10101000	.	01100100	.	00000001
	Network ID						Host ID
SM (Binary):	11111111	.	11111111	.	11111111	.	00000000
Subnet Mask:	255	.	255	.	255	.	0

422



http://www.tcpipguide.com/free/t_IPCustomSubnetMasks-3.htm

423

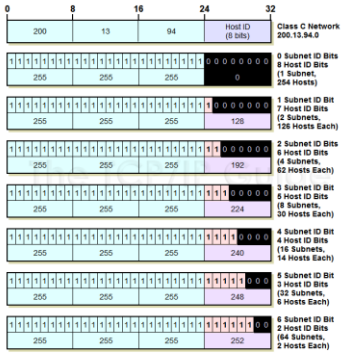


Figure 69: Custom Subnet Masks for Class C Networks

http://www.tcpipguide.com/free/t_IPCustomSubnetMasks-3.htm

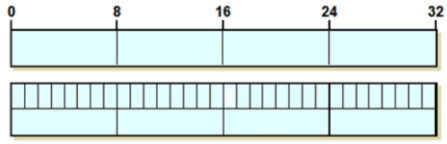
424

Exercise

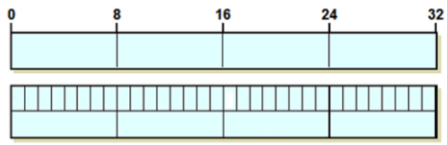
- Ex1: 10.51.2.1/8
- Subnet mask =
- Host ID=
- Network ID=
- Ex2: 192.168.30.5/24
- Subnet mask =
- Host ID =
- Network ID =

425

Ex1: 10.51.2.1/8



Ex2: 192.168.30.5/24



426

Dynamic IP addresses

- Dynamic IP addresses are assigned by network using Dynamic Host Configuration Protocol (DHCP).
- DHCP is the most frequently used technology for assigning addresses. It avoids the administrative burden of assigning specific static addresses to each device on a network.

427

Dynamic IP addresses

- The address assigned with DHCP is associated with a *lease* and usually has an expiration period.
- If the lease is not renewed by the host before expiry, the address may be assigned to another device.

428

Broadcast addressing

- Broadcasting is an addressing technique available in IPv4 to address data to all possible destinations on a network in one transmission operation as an all-hosts broadcast.
- All receivers capture the network packet. The address 255.255.255.255 is used for network broadcast.

429

Standard Ports

- Hypertext Transfer Protocol (HTTP) = 80
- Digital Imaging and Communications in Medicine = 104 (DICOM; also port 11112)
- Hypertext Transfer Protocol Secure = 443

430

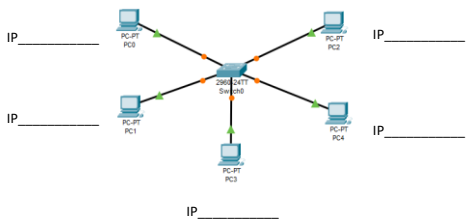
Well-known ports [hide]

Port	TCP	UDP	SCTP	DCCP	Description
0	Reserved				In programming APIs (not in communication between hosts), requests a system-allocated (
1	Yes	Assigned			TCP Port Service Multiplexer (TCPMUX). Historic. Both TCP and UDP have been assigned
2	Assigned				compressnet (Management Utility)[3]
3	Assigned				compressnet (Compression Process)[3]
5	Assigned				Remote Job Entry[8] was historically using socket 5 in its old socket form, while MIB PIM ha UDP 5 to it.
7	Yes				Echo Protocol[10][11]
9	Yes		Yes[12]	Assigned	Discard Protocol[13]
	No	Unofficial			Wake-on-LAN[14]
11	Yes				Active Users (systat service)[15][16]
13	Yes				Daytime Protocol[17]
15	Unofficial	No			Previously netstat service[2][15]
17	Yes				Quote of the Day (QOTD)[18]
18	Yes				Message Send Protocol[19][20]
19	Yes				Character Generator Protocol (CHARGEN)[21]
20	Yes	Assigned	Yes[12]		File Transfer Protocol (FTP) data transfer[11]
21	Yes	Assigned	Yes[12]		File Transfer Protocol (FTP) control (command)[11][12][22][23]
22	Yes	Assigned	Yes[12]		Secure Shell (SSH),[11] secure logins, file transfers (scp, sftp) and port forwarding
23	Yes	Assigned			Telnet protocol—unencrypted text communications[11][24]
25	Yes	Assigned			Simple Mail Transfer Protocol (SMTP),[11][25] used for email routing between mail servers
27	Assigned				nsw-fe (NSW User System FE)[3]

https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

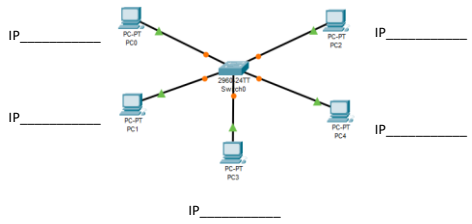
431

Class A Network



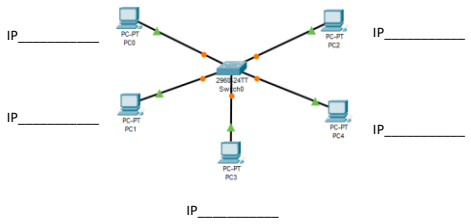
432

Class B Network



433

Class C Network



434

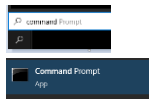
Basic Network Troubleshooting

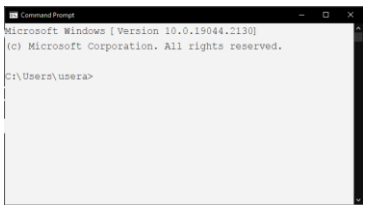
Yudthaphon Vichianin, Ph.D.
Department of Radiological Technology
Faculty of Medical Technology
Mahidol University

435

Window command box

- Open search in widow
- Type command *<enter>*





436

Ping command

- ping *hostname*
- ping *ipaddress*

437

ipconfig

- In command box
- Type ipconfig

```
C:\Users\usera>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::2439:d4b3:bac3:f2be%17
   IPv4 Address. . . . . . . . . . . : 192.168.2.17
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.2.1
```


438

ipconfig

- In command box
- Type ipconfig /all

439

```
C:\Users\usera>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : ytp-ws-ill
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Ethernet Connection (14) I219-LM
   Physical Address. . . . . . . . . : 30-D0-42-EF-62-C4
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::2439:d4b3:bac3:f2be%17(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.2.17(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.2.1
   DHCPv6 IAID . . . . . . . . . . . : 573624386
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2A-80-CA-58-30-D0-42-EF-62-C4
   DNS Servers . . . . . . . . . . . : 8.8.8.8
                                       4.4.4.4
   NetBIOS over Tcpip. . . . . . . . : Enabled
```


440

Command Prompt

```
Microsoft Windows [Version 10.0.19044.2075]
(c) Microsoft Corporation. All rights reserved.

C:\Users\USER>ping google.com

Pinging google.com [216.58.200.14] with 32 bytes of data:
Reply from 216.58.200.14: bytes=32 time=314ms TTL=111
Reply from 216.58.200.14: bytes=32 time=381ms TTL=111
Reply from 216.58.200.14: bytes=32 time=402ms TTL=111
Reply from 216.58.200.14: bytes=32 time=159ms TTL=111

Ping statistics for 216.58.200.14:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 159ms, Maximum = 402ms, Average = 314ms

C:\Users\USER>
```


441

Ping command

```
C:\Users\USER>ping 216.58.200.14

Pinging 216.58.200.14 with 32 bytes of data:
Reply from 216.58.200.14: bytes=32 time=33ms TTL=111
Reply from 216.58.200.14: bytes=32 time=29ms TTL=111
Reply from 216.58.200.14: bytes=32 time=30ms TTL=111
Reply from 216.58.200.14: bytes=32 time=30ms TTL=111

Ping statistics for 216.58.200.14:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 29ms, Maximum = 33ms, Average = 30ms
```


442

Cable Checking

443

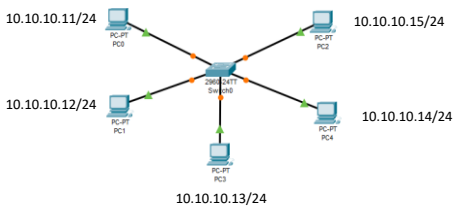
444

Hand-on

Group of 4

445

Class A network in Cisco Packet Tracer

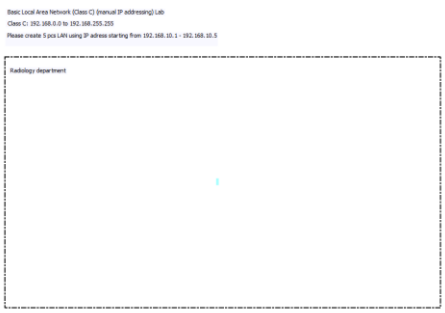


446

Network Lab Day

447

LAN – class C

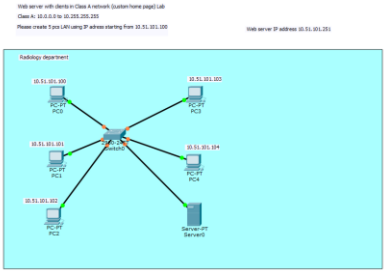


448

LAN – class B

449

LAN – class A



450

Very basic HTML

```
<!DOCTYPE html>
<html>
<body>

<h2>HTML Links</h2>
<p>HTML links are defined with the a tag:</p>

<a href="https://www.w3schools.com">This is a link</a>

</body>
</html>
```

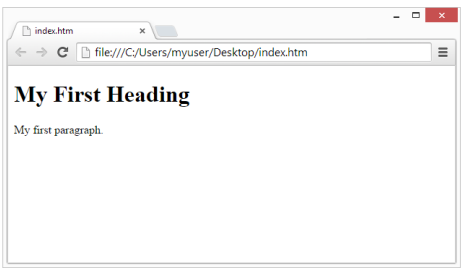
HTML Links

HTML links are defined with the a tag:

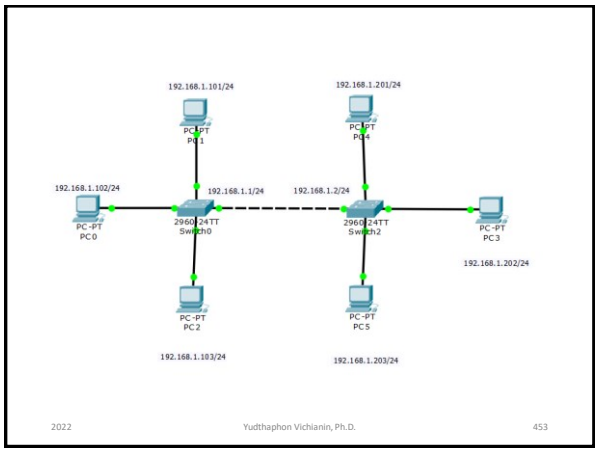
This is a link

451

Index.htm



452


192.168.1.101/24
PC-PT
PC1
192.168.1.201/24
PC-PT
PC4
192.168.1.102/24
PC-PT
PC0
192.168.1.1/24
2960-24TT
Switch0
192.168.1.2/24
2960-24TT
Switch2
PC-PT
PC3
192.168.1.202/24
PC-PT
PC2
192.168.1.103/24
PC-PT
PC5
192.168.1.203/24
2022
Yudthaphon Vichianin, Ph.D.
453

453