

Information Technology Infrastructure

Various Kinds of Architecture

- ❖ Business architecture
- ❖ Enterprise architecture
- ❖ Data architecture,
- ❖ Application architecture and
- ❖ Infrastructure architecture

Is there a General Definition of IT Infrastructure?

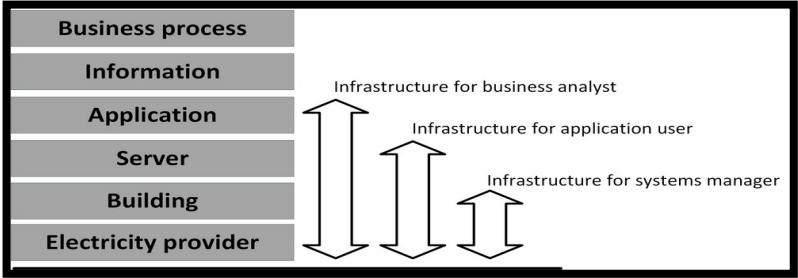
No generally accepted definition of IT infrastructure seems to exist
In literature, many definitions of IT infrastructure are described. Some of them are:

IT Infrastructure

IT infrastructure consists of the equipment, systems, software, and services used in common across an organization, regardless of mission/program/project. IT Infrastructure also serves as the foundation upon which mission/program/project-specific systems and capabilities are built.

What infrastructure comprises dependents on:

- Who you ask
- What their point of view is



For most people, infrastructure is invisible and taken for granted

Introduction to Non-Functional Attributes

- IT infrastructure provides services to applications
- Many of these services can be defined as functions such as
 - Disk space,
 - Processing,
 - Connectivity

However most of these services are non-functional in nature

Non-Functional Attributes

Non-functional attributes describe the qualitative behavior of the system rather than its specific functionality and these include

- Availability

- Security
- Performnace
- Recoverability
- Testtability
- Scalability

Handling Conflicting NFRs

It is unusual to encounter conflicting NFRs for instance users may want a system that is secure but not want to be bothered by passwords

- It is the task of the infrastructure architect to balance these NFRs, in some cases some NFRs may take priority over others and the architect must involve the relevant stakeholders

AVAILABILITY

- Everyone expects their infrastructure to be available all the time
- A 100% guaranteed availability of an infrastructure is impossible

A fact of life

- There is always a chance of downtime.

Calculationon of Aavailability

- ❖ Availability can neither be calculated, nor guaranteed upfront
 - It can only be reported on afterwards, when a system has run for some years
- ❖ Over the years, much knowledge and experience is gained on how to design high available systems
 - Failover
 - Redundancy
 - Structured programming
 - Avoiding Single Points of Failures (SPOFs)
 - Implementing systems management
- ❖ The availability of a system is usually expressed as a percentage of uptime in a given time period, usually one year or one month
- ❖ Example for downtime expressed as a percentage per year

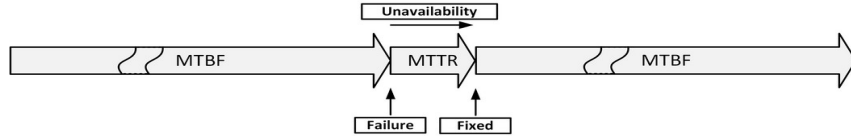
Availability %	Downtime per year	Downtime per month	Downtime per week
99.8%	17.5 hours	86.2 minutes	20.2 minutes
99.9% ("three nines")	8.8 hours	43.2 minutes	10.1 minutes
99.99% ("four nines")	52.6 minutes	4.3 minutes	1.0 minutes
99.999% ("five nines")	5.3 minutes	25.9 seconds	6.1 seconds

Typical requirements used in service level agreements today are 99.8% or 99.9% availability per month for a full IT system

- ❑ The availability of the infrastructure must be much higher
 - Typically in the range of 99.99% or higher
- ❑ 99.999% uptime is also known as carrier grade availability
 - For one component, higher availability levels for a complete system are very uncommon, as they are almost impossible to reach
- ❑ It is a good practice to agree on the maximum frequency of unavailability

MTBF and MTTR

- ❑ Mean Time Between Failures (MTBF)
 - The average time that passes between failures
- ❑ Mean Time To Repair (MTTR)
 - The time it takes to recover from a failure



- Some components have higher MTBF than others
- Some typical MTB's:

Component	MTBF (hours)
Hard disk	750,000
Power supply	100,000
Fan	100,000
Ethernet Network Switch	350,000
RAM	1,000,000

MTTR

- ❑ MTTR can be kept low by:
 - Having a service contract with the supplier
 - Having spare parts on-site
 - Automated redundancy and failover
- ❑ Steps to complete repairs:
 - Notification of the fault (time before seeing an alarm message)
 - Processing the alarm
 - Finding the root cause of the error
 - Looking up repair information
 - Getting spare components from storage

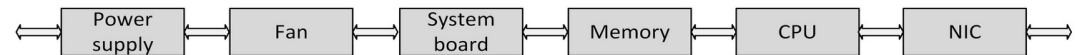
- Having technician come to the datacenter with the spare component
- Physically repairing the fault
- Restarting and testing the component

❑ Calculation Examples

$$\text{Availability} = \frac{\text{MTBF}}{(\text{MTBF} + \text{MTTR})} \times 100\%$$

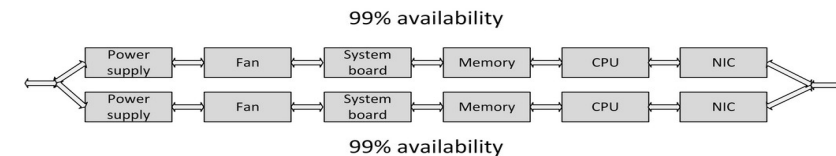
Component	MTBF (h)	MTTR (h)	Availability	in %
Power supply	100,000	8	0.9999200	99.99200
Fan	100,000	8	0.9999200	99.99200
System board	300,000	8	0.9999733	99.99733
Memory	1,000,000	8	0.9999920	99.99920
CPU	500,000	8	0.9999840	99.99840
Network Interface Controller (NIC)	250,000	8	0.9999680	99.99680

Serial components: One defect leads to downtime



- Example: the above system's availability is:
 $0.9999200 \times 0.9999200 \times 0.9999733 \times 0.9999920 \times 0.9999840 \times 0.9999680 = 0.9999200$
 (each components' availability is at least 99.99%)

Parallel components: One defect: no downtime!



- Calculate availability:

$$A = 1 - \bar{A}$$

- Total availability $\bar{A} 1 - \bar{A} = 99.99\%$

Sources of Unavailability - Human Errors

- 80% of outages impacting mission-critical services is caused by people and process issues

Examples:

- Performing a test in the production environment
- Switching off the wrong component for repair
- Swapping a good working disk in a RAID set instead of the defective one

- Restoring the wrong backup tape to production
- Accidentally removing files
 - Mail folders, configuration files
- Accidentally removing database entries
 - Drop table x instead of drop table y

Sources of Unavailability - Software Bugs

- Because of the complexity of the software, it is nearly impossible (and very costly) to create bug-free software
- Application software bugs can stop an entire system
- Operating systems are software too
 - Operating systems containing bugs can lead to
- corrupted file systems,
- network failures, or
- other sources of unavailability

Sources of Unavailability - Planned Maintenance

- ❑ Sometimes needed to perform systems management tasks:
 - ❖ Upgrading hardware or software
 - ❖ Implementing software changes
 - ❖ Migrating data
 - ❖ Creation of backups
- ❑ During planned maintenance the system is more vulnerable to downtime than under normal circumstances
 - ❖ A temporary SPOF could be introduced
 - ❖ Systems managers could make mistakes

Sources of Unavailability - Physical Defects

- ❑ Everything breaks down eventually
- ❑ Mechanical parts are most likely to break first
- ❑ Examples:
 - ❖ **Fans for cooling equipment** usually break because of dust in the bearings
 - ❖ **Disk drives** contain moving parts
 - ❖ **Tapes** are very vulnerable to defects as the tape is spun on and off the reels all the time
 - ❖ **Tape drives** contain very sensitive pieces of mechanics that can break easily

❑ Sources of Unavailability - Bathtub Curve

- ❑ A component failure is most likely when the component is new

- ❑ Sometimes a component doesn't even work at all when unpacked for the first time. This is called a DOA component—Dead On Arrival.
- ❑ When a component still works after the first month, it is likely that it will continue working without failure until the end of its life

Sources of Unavailability - Environmental Issues

- Environmental issues can cause downtime. Issues with
 - Power
 - Cooling
 - External factors like:
 - Disasters
 - Fire
 - Earthquakes
 - Flooding

Sources of Unavailability - Complexity of the Infrastructure

- Adding more components to an overall system design can undermine high availability
- Even if the extra components are implemented to achieve high availability
- Complex systems
- Have more potential points of failure
- Are more difficult to implement correctly
- Are harder to manage
- Sometimes it is better to just have an extra spare system in the closet than to use complex redundant systems

Availability Patterns

- A single point of failure (SPOF) is a component in the infrastructure that, if it fails, causes downtime to the entire system.
- SPOFs should be avoided in IT infrastructures as they pose a large risk to the availability of a system.
- We just need to know what is shared and if the risk of sharing is acceptable.
- To eliminate SPOFs, a combination of redundancy, failover, and fallback can be used.
- **Redundancy**
- Redundancy is the duplication of critical components in a single system, to avoid a single point of failure (SPOF)

Examples:

- A single component having two power supplies; if one fails, the other takes over
- Dual networking interfaces
- Redundant cabling

Failover

- Failover is the (semi)automatic switch-over to a standby system or component

Examples:

- Windows Server failover clustering
- VMware High Availability
- Oracle Real Application Cluster (RAC) database

Fallback

- Fallback is the manual switchover to an identical standby computer system in a different location
- Typically used for disaster recovery
- Three basic forms of fallback solutions:
- Hot site
- Cold site
- Warm site

Natural disasters:	Manmade disasters:
Floods	Hazardous material
Hurricanes	spills
Tornadoes	Infrastructure failure
Earthquakes	Bio-terrorism

Business Continuity

- In case of a disaster, the infrastructure could become unavailable, in some cases for a longer period of time.
- Business continuity is about identifying threats an organization faces and providing an effective response.
- To handle the effect of disasters, following processes are
- Business Continuity Management (BCM) and
- Disaster Recovery Planning (DRP)
- **Business Continuity**
- An IT disaster is defined as an irreparable problem in a datacenter, making the datacenter unusable

WEEK#3

Performance Concepts

- Performance is a typical hygiene factor
- Nobody notices a highly performing system
- But when a system is not performing well enough, users quickly start complaining

Perceived Performance

- Perceived performance refers to how quickly a system appears to perform its task
- In general, people tend to overestimate their own patience
- People tend to value predictability in performance
 - ❑ When the performance of a system is fluctuating, users remember a bad experience
 - ❑ Even if the fluctuation is relatively rare
- Inform the user about how long a task will take
 - ❑ Progress bars
 - ❑ Splash screens

Performance during Infrastructure Design

- A solution must be designed, implemented, and supported to meet the performance requirements Even under increasing load
- Calculating performance of a system in the design phase is:

❑ Extremely difficult

❑ Very unreliable

- Performance must be considered:

- When the system works as expected
- When the system is in a special state, like:

❑ Failing parts

❑ Maintenance state

❑ Performing backup

❑ Running batch jobs

Some ways to do this are:

- Benchmarking
- Using vendor experience
- Prototyping and User Profiling

Benchmarking

❑ A benchmark uses a specific test program to assess the relative performance of an infrastructure component

❑ Benchmarks compare:

- Performance of various subsystems
- Across different system architectures

❑ CPU benchmarking is the practice of determining how a processor will perform in a standardized way. This is typically done using special software packages. Some popular benchmarking packages include Whetstone, Dhrystone, 3DMark, PCMark and others.

- ❑ Benchmarks comparing the raw speed of parts of an infrastructure
 - Like the speed difference between processors or between disk drives
 - Not taking into account the typical usage of such components
 - Examples:
 - Floating Point Operations Per Second – FLOPS
 - Million Instructions Per Second – MIPS of a CPU

Prototyping

- ❑ Also known as proof of concept (PoC)
- ❑ Prototypes measure the performance of a system at an early stage
- ❑ Building prototypes:
 - Hiring equipment from suppliers
 - Using data centre capacity at a vendor's premise
 - Using cloud computing resources
- ❑ Focus on those parts of the system that pose the highest risk, as early as possible in the design process

Vendor Experience

- ❑ The best way to determine the performance of a system in the design phase: use the experience of vendors
- ❑ They have a lot of experience running their products in various infrastructure configurations
- ❑ Vendors can provide:
 - Tools
 - Figures
 - Best practices

User Profiling

- ❑ Predict the load a new software system will pose on the infrastructure before the software is actually built
- ❑ Get a good indication of the expected usage of the system
- ❑ Steps:
 - Define a number of typical user groups (personas)
 - Create a list of tasks personas will perform on the new system
 - Decompose tasks to infrastructure actions
 - Estimate the load per infrastructure action
 - Calculate the total load

Performance of a Running System

Managing Bottlenecks

- ❑ The performance of a system is based on:
 - The performance of all its components
 - The interoperability of various components
- ❑ A component causing the system to reach some limit is referred to as the bottleneck of the system
- ❑ Every system has at least one bottleneck that limits its performance
- ❑ If the bottleneck does not negatively influence performance of the complete system under the highest expected load, it is OK

Performance Testing

- ❑ **Load testing** - shows how a system performs under the expected load
- ❑ **Stress testing** - shows how a system reacts when it is under extreme load
- ❑ **Endurance testing** - shows how a system behaves when it is used at the expected load for a long period of time
- ❑ **Performance Testing - Breakpoint**
- ❑ Ramp up the load
 - Start with a small number of virtual users
 - Increase the number over a period of time
- ❑ The test result shows how the performance varies with the load, given as number of users versus response time.

Performance Testing

- ❑ Performance testing software typically uses:
 - One or more servers to act as injectors
 - Each emulating a number of users
 - Each running a sequence of interactions
 - A test conductor
 - Coordinating tasks
 - Gathering metrics from each of the injectors
 - Collecting performance data for reporting purposes
- ❑ Performance testing should be done in a production-like environment
 - Performance tests in a development environment usually lead to results that are highly unreliable
 - Even when underpowered test systems perform well enough to get good test results, the faster production system could show performance issues that did not occur in the tests
- ❑ To reduce cost:
 - Use a temporary (hired) test environment

Performance Patterns

Increasing Performance on Upper Layers

- ❑ 80% of the performance issues are due to badly behaving applications
- ❑ Application performance can benefit from:
 - Database and application tuning
 - Prioritizing tasks
 - Working from memory as much as possible (as opposed to working with data on disk)
 - Making good use of queues and schedulers
- ❑ Typically more effective than adding compute power

Disk Caching

- ❑ Disks are mechanical devices that are slow by nature
- ❑ Caching can be implemented i:
 - Disks
 - Disk controllers
 - Operating system
- ❑ Cache memory:
 - Stores all data recently read from disk
 - Stores some of the disk blocks following the recently read disk blocks

❑ Caching

Component	Time it takes to fetch <u>1 MB</u> of data (ms)
Network, 1 Gbit/s	675
Hard disk, 15k rpm, 4 KB disk blocks	105
Main memory DDR3 RAM	0.2
CPU L1 cache	0.016

Web Proxies

- ❖ When users browse the internet, data can be cached in a web proxy server
 - A web proxy server is a type of cache
 - Earlier accessed data can be fetched from cache, instead of from the internet
- ❖ Benefits:
 - Users get their data faster
 - All other users are provided more bandwidth to the internet, as the data does not have to be downloaded again

Grid Computing

- ❖ A computer grid is a high performance cluster that consists of systems that are spread geographically
- ❖ The limited bandwidth is the bottleneck

❖ Examples:

- SETI@HOME
- CERN LHC Computing Grid (140 computing centers in 35 countries)

❖ Broker firms exist for commercial exploitation of grids

❖ Security is a concern when computers in the grid are not under control

Capacity Management

- ❖ Capacity management guarantees high performance of a system in the long term
- ❖ To ensure performance stays within acceptable limits, performance must be monitored
- ❖ Trend analyses can be used to predict performance degradation
- ❖ Anticipate on business changes (like forthcoming marketing campaigns)

WEEK#4

Security

- Security is the combination of:
 - Availability
 - Confidentiality
 - Integrity
- Focused on the recognition and resistance of attacks
- For IT infrastructures availability is a non-functional attribute in its own right

Computer Crimes

- Reasons for committing crime against IT infrastructures:
 - Personal exposure and prestige
 - Creating damage
 - Financial gain
 - Terrorism
 - Warfare

Personal Exposure and Prestige

- In the past, the hacker community was very keen on getting personal or group exposure by hacking into a secured IT infrastructure. When hackers proved that they could enter a secured system and made it public, they gained respect from other hackers.
- While nowadays most hacking activity is done for other reasons, there are still large communities of hackers that enjoy the game.

Creating Damage

- Creating damage to organizations to create bad publicity
- For instance, by defacing websites, bringing down systems or websites, or
- making internal documents public

Financial Gain

- For instance, by holding data hostage and asking for ransom money, stealing credit card data, changing account data in bank systems
- Stealing passwords of customers and ordering goods on their behalf

Terrorism

- The main purpose of terrorism is creating fear in a society
- A well-planned attack targeted at certain computer systems, like the
- Computer system that manages the water supply
- A nuclear power plant, could result in chaos and fear amongst citizens

Warfare

- Certain governments use hacking practices as acts of war
- Since economies and societies today largely depend on the IT infrastructures, bringing important IT systems down in a certain country could cause the economy to collapse.
- Bringing down the internet access of a country for example means: no access to social media, no e-mails, no web shops, no stock trading, no search engines, etc.

Risk management

- ❖ Managing security is all about managing risks
- ❖ The effort we put in securing the infrastructure should be directly related to the risk at hand
- ❖ Risk management is the process of:
 - ❑ Determining an acceptable level of risk
 - ❑ Assessing the current level of risk
 - ❑ Taking steps to reduce risk to the acceptable level
 - ❑ Maintaining that level

Risk list

A risk list can be used to quantify risks

Risk is calculated based on:

Asset name - component that needs to be protected

Vulnerability - weakness, process or physical exposure that makes the asset susceptible to exploits

Exploit - a way to use one or more vulnerabilities to attack an asset

Probability - an estimation of the likelihood of the occurrence of an exploit

Impact - the severity of the damage when the vulnerability is exploited

Example of Part of a Risk List

Asset	Vulnerability	Exploit	P	I	R
Laptop	Laptop gets stolen	Sensitive data on hard disk is exposed	5	3	15
Printer	Printer hard disk contains sensitive data	Repair man could swap hard disk and the hard disk could get on the market with sensitive data	1	3	3
Work-stations	Virus attack unknown to virus scanner	Unavailability or disclosure of data	2	3	6
SAN storage system	Data protection via LUN masking contains error	Data could get exposed to wrong server	1	2	2

Risk Response

- Controls can be designed and implemented based on identified severity of the risk in the risk list.
- There four risk responses:
 - o Acceptance of the risk
 - o Avoidance of the risk - do not perform actions that impose risk
 - o Transfer of the risk - for instance transfer the risk to an insurance company
 - o Mitigation of the risk and accepting the residual risk

Exploits

- Information can be stolen in many ways
- Examples:
 - o Key loggers can send sensitive information like passwords to third parties
 - o Network sniffers can show network packages that contain sensitive information or replay a logon sequence
 - Data on backup tapes outside of the building can get into wrong hands
 - Disposed PCs or disks can get into the wrong hands
 - Corrupt or dissatisfied staff can copy information
 - End users are led to a malicious website that steals information (phishing)

Security Controls

CIA

- Three core goals of security (CIA):
 - ❑ Confidentiality

- ❑ Integrity
- ❑ Availability

- Confidentiality - prevents the intentional or unintentional unauthorized disclosure of data
- Integrity - ensures that:
 - ❑ No modifications to data are made by unauthorized staff or processes
 - ❑ Unauthorized modifications to data are not made by authorized staff or processes
 - ❑ Data is consistent
- Availability - ensures the reliable and timely access to data or IT resources

Example of confidentiality levels

Confidentiality Level	Description
1	Public information
2	Information for internal use only
3	Information for internal use by restricted group
4	Secret: reputational damage if information is made public
5	Top secret: damage to organization or society if information is made public

Example of integrity levels

Integrity Level	Description
1	Integrity of information is of no importance
2	Errors in information are allowed
3	Only incidental errors in information are allowed
4	No errors are allowed, leads to reputational damage
5	No errors are allowed, leads to damage to organization or society

Example of availability levels

Availability Level	Description
1	No requirements on availability
2	Some unavailability is allowed during office hours
3	Some unavailability is allowed only outside of office hours
4	No unavailability is allowed, 24/7/365 availability, risk for reputational damage
5	No unavailability is allowed risk for damage to organization or society

Security Controls

- ❑ Controls mitigate risks
- ❑ Security controls must address at least one of the CIA
- ❑ Information can be classified based on CIA levels
- ❑ Controls can be designed and implemented based on the identified risk level for CIA

Attack Vectors

❑ Malicious code

- Applications that, when activated, can cause network and server overload, steal data and passwords, or erase data

❑ Worms

- Self-replicating programs that spread from one computer to another, leaving infections as they travel

❑ Virus

- Self-replicating program fragment that attaches itself to a program or file enabling it to spread from one computer to another, leaving infections as it travels

❑ Trojan Horse

- Appears to be useful software but will actually do damage once installed or run on your computer

❑ Denial of service attack

- An attempt to overload an infrastructure to cause disruption of a service
- Can lead to downtime of a system, disabling an organization to do its business
- In a Distributed Denial of Service (DDoS) attack the attacker uses many computers to overload the server
- Groups of computers that are infected by malicious code, called botnets, perform an attack

❑ Preventive DDoS measures:

- Split business and public resources
- Move all public facing resources to an external cloud provider
- Setup automatic scalability (auto scaling, auto deployment) using virtualization and cloud technology
- Limit bandwidth for certain traffic
- Lower the Time to Live (TTL) of the DNS records to be able to reroute traffic to other servers when an attack occurs
- Setup monitoring for early detection

❑ Phishing

- A technique of obtaining sensitive information
- The phisher sends an e-mail that appears to come from a legitimate source, like a bank or credit card company, requesting "verification" of information
- The e-mail usually contains a link to a fraudulent web page

Security Patterns

Identity and Access Management (IAM)

- ❑ The process of managing the identity of people and systems, and their permissions
- ❑ The IAM process follows three steps:
 - Users or systems claim who they are: **identification**
 - The claimed identity is checked: **authentication**
 - Permissions are granted related to the identity and the groups it belongs to: **authorization**

Layered Security

- ❑ Layered security (also known as a Defense-In-Depth strategy) implements various security measures in various parts of the IT infrastructure
 - Instead of having one big firewall and have all your security depend on it, it is better to implement several layers of security
- ❑ Preferably security layers make use of different technologies
 - This makes it harder for hackers to break through all barriers, as they will need specific knowledge for each step
- ❑ Disadvantage: increases the complexity of the system

Cryptography

- ❑ The practice of **hiding information** using encryption and decryption techniques

Encryption is the conversion of information from a readable state to apparent random data

- ❑ Only the receiver has the ability to **decrypt** this data, transforming it back to the original information
- ❑ A **cipher** is a pair of algorithms that implements the encryption and decryption process. The operation of a cipher is controlled by a **key**
- ❑ **Block ciphers**
 - Input:
 - A block of plaintext
 - A key

- Output:
 - A block of cipher text
- Used across a wide range of applications, from ATM machine data encryption to e-mail privacy and secure remote access
- Standards:
 - Data Encryption Standard (DES)
 - Advanced Encryption Standard (AES)

❑ Stream ciphers

- Create an arbitrarily long stream of key material
- Combines key stream with the plaintext bit-by-bit or character-by-character
- Used when data is in transit over the network
- RC4 is a widely-used stream cipher

Cryptographic Attacks

- Every encryption method can be broken using a brute force attack
 - Except a one-time pad cipher with the key of equal or greater length than the message
- A brute force attack consists of systematically checking all possible keys until the correct key is found
- The amount of effort needed is exponentially dependent on the size of the key
- Effective security could be achieved if it is proven that no efficient method (as opposed to the time consuming brute force method) can be found to break the cipher
- Most successful attacks are based on flaws in the implementation of an encryption cipher
- To ensure a cipher is flawless, the source code is usually open source and thus open to inspection to everyone

WEEK#5

Data Center :

- Centralized facility used by an organizations to store, manage, and disseminate large amounts of data.
- Houses servers, networking equipment, storage devices, and other infrastructure required to support data processing and storage.
- Provides power supply, cooling, fire prevention and detection, equipment racks, and other facilities needed to host the installed infrastructure components.

Data Center Categories :

Typical data centre categories:

- **Sub Equipment Room (SER)** – a SER is also known as a patch closet
- **Main Equipment Room (MER)** – a MER is a small datacenter in the organization's subsidiaries or buildings
- **Organization owned datacenter** – a datacenter that contains all central IT equipment for the organization
- **Multi-tenant datacenter** – used by service providers that provide services for multiple other organizations. These datacenters are typically the largest

Datacenter location

Environment

Utilities

Visibility

Located in foreign countries

Physical structure

The physical structure of a datacentre includes components that need special attention:

Floors, Walls, Doors, Windows, Water & Gas Pipe

Floors

- One fully filled 19" computer rack weighs up to 700 kg
- In a typical datacenter, the floor must be able to carry 1500 to 2000 kg/m²
- Raised floors consist of a metal framework carrying removable floor tiles

Advantages

- Tiles are usually 60×60 cm
- Tiles can be lifted individually to reach cables installed under the raised floor
- Vents provide cool air flow to the racks placed on the floor
- Under the raised floor, data and power cables are installed
- As alternative, overhead cable trays can be used

Disadvantages

- They are expensive
- The maximum floor load is limited
- Doors and equipment loading slopes are hard to install due to the difference in floor height
- Under the raised floor, a fire could easily spread through the entire datacenter.

Walls, windows, and doors

- ❖ Walls should reach from the floor to the building's ceiling
 - Because of fire safety and physical intrusion prevention
- ❖ Windows are not desirable in a datacenter
- ❖ Windows must be:
 - Translucent
 - Shatterproof
 - Impossible to open
- ❖ Doors should be large enough to have equipment brought in
- ❖ Doors must resist forced entry

Water and gas pipes

- Water or gas pipes may have been installed:
 - Under the floor
 - In the walls
 - Above the ceiling of the datacenter
- Datacenter operators should know where the shutoff valves are

Power supply

- Energy usage is a key issue for datacenters
- Power drawn by datacenters:
 - A few kilowatts (kW) for one rack of servers
 - Dozens of megawatts (MW) for large facilities.

Power supply in a datacenter includes:

- Utility power supply
- Backup power systems(UPS, Generators)
- Power Distribution units

Utility Power Supply (UPS)

Power issues can occur in the utility power supply.

- Types of power issues:
 - ☐ Blackout
 - ☐ Surge
 - ☐ Spike
 - ☐ Waveform issues
- Possibly leading to:
 - ☐ Downtime
 - ☐ Damage to equipment

Backup Power Systems

Uninterruptable Power Supply (UPS)

- Independent of the Utility power supply
- Provide power for short period of time

Power Generators

- Power the data centre for an indefinite period of time as long as fuel is available

Power distribution

A power distribution unit (PDU) is a device with multiple power outlets

- Distributes power to equipment located in the datacenter

Two types of PDUs:

- Large floor mounted PDUs take main feeds (usually 3 phase power) and distribute it into multiple smaller feeds to computer racks
- Power Strips that feed equipment in racks

Most Infrastructure components can be equipped with two power supplies for redundancy. For availability reasons at least two power strips are needed to power equipment in a rack

Cooling

90% of all power used by IT infrastructure components is converted into heat, all heat has to be dissipated by a cooling system

Two types of cooling systems:

➤ Computer Room Air Conditioners (CRAC)

Refrigerant-based units connected to outside condensing units

➤ Computer Room Air Handlers (CRAH)

A chiller produces chilled water via a refrigeration process

Airflow

Data center airflow management controls temperatures in and around IT gear to maintain and increase efficiency. Poor airflow can prevent cool air from reaching overheated components or cause warm air to remain trapped in one area.

Data center airflow management addresses common problems by implementing solutions that control room temperatures, reduce fan speeds and create ideal air circulation channels.

Humidity and dust

The humidity of the air in a datacenter is critical for the IT infrastructure components

- Air humidity should be between 40% and 60%

The number of dust particles in a datacenter should be minimized

- Don't allow visitors in the datacenter

- People should wear dust-free clothing (like white coats) and protective sleeves around their shoes

Operating temperatures

Infrastructure components have maximum operating temperatures:

- Servers shut themselves down at an air inlet temperature of 40 degrees Celsius
- The air temperature in the datacenter usually ranges from 18 degrees to 27 degrees Celsius.

Fire prevention, detection, and suppression

Fire is one of the main enemies of a datacenter

- A short circuit in a cable
- Defect equipment

Fires can spread around very quickly

- Because of the air flow in the datacenter and the frequent use of raised floors

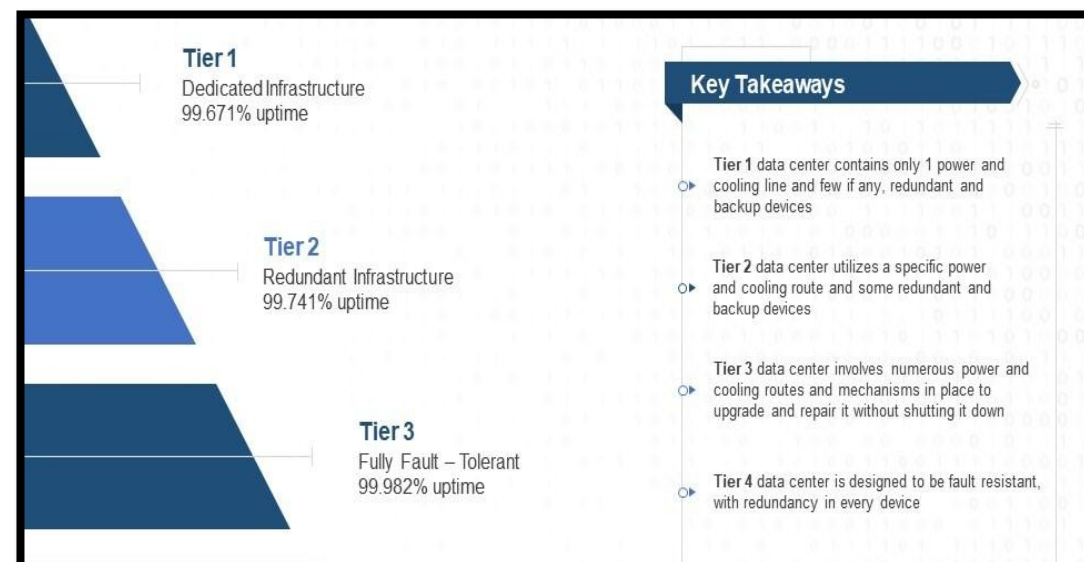
Smoke could damage equipment in the datacenter

- Even if a fire starts outside of the datacenter's computer room

Datacenter energy efficiency

- The Power Usage Effectiveness (PUE) metric measures the power used by the datacenter
- The PUE is calculated by dividing the amount of power used by the datacenter, by the power used to run the IT equipment in it
- Typical PUE value of a datacenter is between 1.1 and 2.0

Datacenter availability (Datacenter tier)



Tier	Measures	Expected downtime
Tier 1 <u>Availability</u> 99.671% <u>Type</u> Basic	Single path for power and cooling distribution No redundant components	Downtime very likely for planned and unplanned maintenance
Tier 2 <u>Availability</u> 99.741% <u>Type</u> Redundant components	Fulfills all Tier 1 requirements Single path for power and cooling distribution Redundant components	Downtime likely for planned and unplanned maintenance
Tier 3 <u>Availability</u> 99.982% <u>Type</u> Concurrently maintainable	Fulfills all Tier 1 and Tier 2 requirements Multiple active power and cooling distribution paths Only one path active Redundant components All IT equipment must be dual-powered	No downtime due to planned maintenance Downtime unlikely for unplanned maintenance
Tier 4 <u>Availability</u> 99.995% <u>Type</u> Fault tolerant	Fulfills all Tier 1, Tier 2, and Tier 3 requirements Multiple active power and cooling distribution paths Redundant components All cooling equipment is independently dual-powered, including chillers and Heating, Ventilating and Air Conditioning (HVAC) systems	No downtime due to planned or unplanned maintenance

Datacentre Performance

The data center itself does not provide performance to IT Infrastructures, except for the bandwidth of the internet connectivity and the scalability of the location.

Performance can be measured by :

- Uptime
- Response time
- Throughput
- Scalability

Datacenter security

Physical security

- Ensure that equipment is physically safe behind the datacenter doors
- Physical access to the datacenter must be restricted to selected and qualified staff

- An entry registration system should be used
- A log should be maintained containing all staff entering and leaving the datacenter
- Doors must be secured using conventional locks (for instance for dock loading doors) or electronic locks
 - Electronic locks should open only after proper authentication

WEEK#6

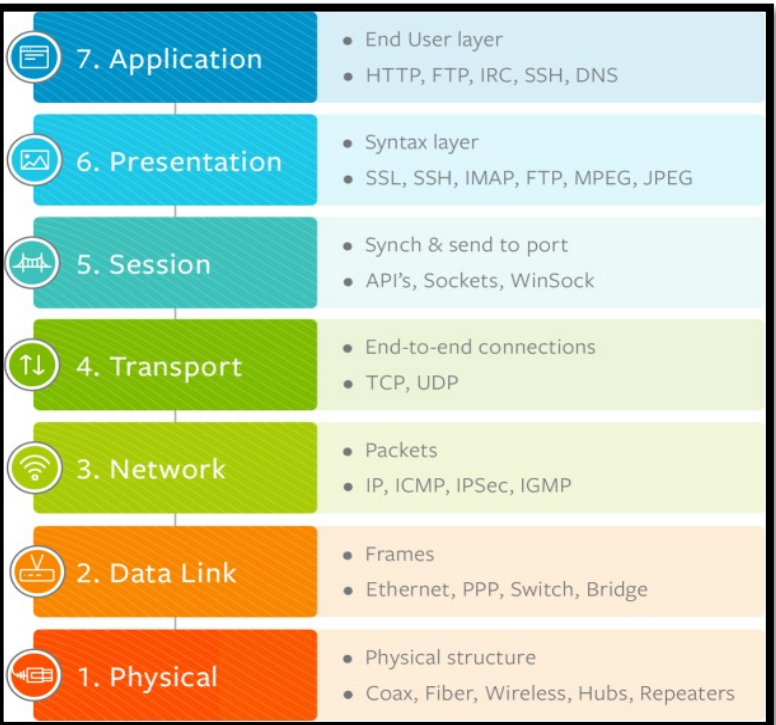
Networking – Part 1

- IT Infrastructure-Networking
- Stand-alone machines Mainframe Computers in the 1960s-Computing and Punching machines
- ARPANET-Late 1960s, a number of computers were connected by The interface message processor (IMPS) was the first packet-router.
- The predecessor of the Internet
- With PCs in the 1980s, local Area Networks (LANs) were introduced

Networking Building Blocks

OSI Reference Model

- The OSI Reference Model (OSI-RM) was developed in 1984 by the International Organization for Standardization (ISO)
- Seven layers define the different stages that data must go through to travel from one host to another over a network



- The Media Access Control (MAC) sublayer is responsible for managing access and permissions to transmit data between the network nodes. The data is transmitted sequentially and the layer expects acknowledgement for the encapsulated raw data sent between the nodes.

3. Network layer

The network layer has two main functions. One is breaking up segments into network packets, and reassembling the packets on the receiving end. The other is routing packets by discovering the best path across a physical network.

4Transport

The transport layer provides mechanisms such as error control, flow control, and congestion control to keep track of the data packets, check for errors and duplication, and resend the information that fails delivery. It involves the service-point addressing function to ensure that the packet is sent in response to a specific process (via a port address).

5. Session

Common Session Layer protocols include:

- Remote procedure call protocol (RPC)
- Point-to-Point Tunneling Protocol (PPTP)
- Session Control Protocol (SCP)
- Session Description Protocol (SDP),

6. Presentation layer

Responsibilities of the presentation layer include:

- Data conversion
- Character code translation
- Data compression
- Encryption and decryption

7. Application layer

Common application layer protocols include:

- File Transfer Protocol (FTP)
- Simple Mail Transfer Protocol (SMTP)
- Domain Name System (DNS)

OSI References model

- The OSI stack allows:
 - Implementing network components independently of each other
 - Ensuring all components work together

1. Physical

- Electrical, mechanical, and physical systems and networking devices that include specifications such as cable size, signal frequency, voltages, etc.
- Topologies such as Bus, Star, Ring, and Mesh
- Communication modes such as Simplex, Half Duplex, and Full Duplex
- Data transmission performance, such as Bit Rate and Bit Synchronization
- Modulation, switching, and interfacing with the physical transmission medium
- Common protocols including Wi-Fi, Ethernet, and others
- Hardware including networking devices, antennas, cables, modem, and intermediate devices such as repeaters and hubs.

2. Data Link layer

- The Logical Link Control (LLC) sublayer is responsible for flow controls and error controls that ensure error-free and accurate data transmission between the network nodes.

- Provides freedom to implement the network stack in an optimal way for a certain usage
- Each layer's payload contains the protocol for the next layer

Physical Layer

Cables

At the most elementary level, networking is about cables

Copper based cables:

Coax

Twisted pair

UTP comes in several quality ratings called categories

Fibber optic cable

Multiple strands of fibre glass or plastic

Each provide an optical path for light pulses

Light source:

Light-emitting diode (LED)

Laser

Two types of fiber optic cable are most common:

Multi-Mode Fiber (MMF)

Single Mode Fiber (SMF)

Patch Panels

- Cables in buildings are most visible in patch panels
 - In racks in the datacenter
 - In patch closets in various locations in (office) buildings
- They connect systems in a flexible way, without having to change the installed cabling in the building
- Patch panels are passive connecting devices
- Connecting systems is done using patch cables

Vertical and Horizontal Cabling

- The main distribution cabling in buildings connects the patch panels on the floors to the datacentre (vertical cabling)
- Endpoints in the walls are connected to the patch panels (horizontal cabling)

Leased Lines

Leased lines are dedicated data connections between two locations, provided by a telecom provider

Leased lines are based on: T or E carrier lines, SONET, SDH and Dark fiber

Internet Access

Three ways to connect to the internet:

Leased line

Cable internet access

- Uses cable television infrastructure

Digital Subscriber Line (DSL)

- Asymmetric DSL (ADSL)
- Symmetric DSL (SDSL)
- Very High DSL (VDSL)

Network Interface Controllers (NICs)

- Hardware component that connects a server or end user device to a physical network cable
- The NIC is actually both a physical layer and data link layer device
 - Provides physical access to a networking cable and an implementation of a datalink protocol like Ethernet
- A NIC has a fixed MAC address that is uniquely assigned to its network interface

Data link Layer

Ethernet

- **Developed at Xerox PARC between 1973 and 1975**

Ethernet is a networking technology that includes the protocol, port, cable, and computer chip needed to plug a desktop or laptop into a local area network (LAN) for speedy data transmission via coaxial or fiber optic cables.

Types of ethernet

1. Ethernet connections that use coaxial cables
2. Connections via fiber optic cables
3. Ethernet connections via twisted pair cables
4. Fast Ethernet
5. Gigabit Ethernet
6. Gigabit Ethernet
7. Switch-based Ethernet
8. Wired Ethernet, which uses cables
9. Wireless Ethernet – i.e., without cables
10. SOHO Ethernet LAN

Uses of Ethernet

- ❖ Improves consumer internet experiences
- ❖ Offers high bandwidth connections
- ❖ Provides different options of speed, based on budget, region, and requirements

- ❖ Strikes a balance between cost and performance. Amplifies the capabilities of your Wi-Fi network
- ❖ Enforces greater security
- ❖ Supports direct current (DC) power transmission

Ethernet CSMA/CD

- Carrier Sense Multiple Access with Collision Detection
- Any machine can start transmitting packets when the shared carrier is not in use
 - ❖ Coax cable, twisted-pair hub or Wi-Fi radio signal spectrum
- Carrier sensing circuitry checks the activity on the carrier
- When two machines start to transmit a packet at the same time, a packet collision occurs
 - ❖ This is detected by all sending machines
 - ❖ They will stop the transmission immediately
 - ❖ After a short waiting time, they will retransmit their packet when the carrier is not in use anymore

WLAN (Wi-Fi)

Wi-Fi vs. WLAN vs. Wireless

Wi-Fi is a certain type of WLAN that use specification of the 802.11 wireless standard.

The term WLAN are often linked and use the interchangeably. A WLAN can be built on various wireless technologies.

Wi-Fi networks are WLANs but Wi-Fi is not only type of WLAN.

- Wi-Fi range is about 30 m
- Access points are base stations for a wireless network
- Data encryption: Wi-Fi Protected Access (WPA)
 - WPA dynamically generates a new key for each packet
 - WPA includes a Message Integrity Check
 - Prevents an attacker from capturing, altering and/or resending data packets

Switching

- **Switches split a single network segment into multiple segments**
 - Each segment has one device
- **Switches learn which MAC address is connected to which port**
 - Data sent to a certain MAC address will only be forwarded to the switch port that has that MAC address connected

- **On a switched network, many simultaneous data transfers can take place, in full-duplex**

WAN

- Wide Area Networks (WANs) started in the 1980s
- Packet Switching technologies
- in WLAN
- Reliable Network
- Most WAN Connections Converted to VPN using
 - MPLS network of a network provider
 - The internet using IPsec or SSL
 - Dark fiber

Public Wireless Networks

- Public wireless (mobile) networks are getting more popular every day
- Public wireless networks are much less reliable than private wireless networks and have lower bandwidth
- Technologies:
 - 1G and 2G: GSM, CDMA, GPRS and EDGE
 - 3G: UMTS and HSDPA
 - 4G: LTE

Network Layer

The IP Protocol

- 🚩 IP is the defining set of protocols that enable the modern internet.
- 🚩 IP, in combination with TCP, was invented by Robert Kahn and Vinton Cerf in 1973
- 🚩 The IP protocol-mostly used layer 3 protocol in the world
- 🚩 IPv4 is the dominant protocol on the internet today
- 🚩 The IP protocol assumes that the network is inherently unreliable and that it is dynamic in terms of availability of links and nodes
- 🚩 IP uses data packets that contain:
 - Source address
 - Destination address
 - Payload data (typically an Ethernet packet)
- 🚩 IP routing protocols dynamically define the path of IP packets from source to destination

Routing issues:

- Due to network disruption, IP packets can get lost or corrupted

Class	First byte	Max numb hosts
A	0-127	16,777,214
B	128-191	65,534
C	192-223	254

- When an error is detected, the IP packet is dropped by the node that found the error
 - Since each IP packet is routed individually, IP packets can arrive at the destination out of order
- 🚩 The effects of dropped IP packets and IP packets arriving out of order is handled by upper layer protocols like TCP

IPv4 Addresses

- IPv4 addresses are composed of 4 bytes (32 bits)
- An IP address has a network prefix and a host number
- All hosts with the same network prefix can communicate directly to each other
- Hosts in other networks can only be reached using a router

IPv4 Classes

- First three bits of the first byte of an IP address define the class of the address
- Three classes of networks are defined

IPv4 Subnetting

- Subnetting is used to split up the host part of an IP network in smaller subnets, each forming a new IP network

IPv4 - Private IP Ranges

- Private IP addresses should be used for **LANs**
 - The number of unique IP addresses on the internet is limited
 - Hosts with public internet IP addresses can reach the internet directly
- Private IP address ranges:
 - 10.0.0.0 to 10.255.255.255 (class A address range)
 - 172.16.0.0 to 172.31.255.255 (class B address range)
 - 192.168.0.0 to 192.168.255.255 (class C address range)
- Private IP addresses:

- Are not used on the internet
- Are not routed by internet routers

IPv6

- IPv6 was introduced in 1998 as a successor of IPv4 to solve the problem of limited IP address space
- IPv6 uses 128-bit addresses represented in eight groups of four hexadecimal digits separated by colons
- Example: 2001:0bb8:86a2:0000:0000:8b1e:1350:7c34

Benefits of IPv6

- IPv6 has the following benefits over IPv4:
 - ☐ Expanded address space
 - ☐ Better support for mobile IP
 - ☐ Fixed header length
 - ☐ Auto configuration
 - ☐ Quality of Service
 - ☐ Security
 - ☐ MTU discovery

- IPv6 is not backwards compatible with IPv4

- Deployment models for IPv6

- ☐ Use IPv6 on the LAN and on dedicated WAN links
- ☐ Protocol translation
- ☐ Dual stack
- ☐ IPv6 over IPv4 tunnels

CIDR prefix	Subnet mask	Available subnets	Hosts per subnet
/24	255.255.255.0	1	254
/25	255.255.255.128	2	126
/26	255.255.255.192	4	62
/27	255.255.255.224	8	30
/28	255.255.255.240	16	14
/29	255.255.255.248	32	6
/30	255.255.255.252	64	2
/31	255.255.255.254	128	2 (only point-to-point)

- Dual stack is the simplest way to begin deploying IPv6

ICMP

- The Internet Control Message Protocol (ICMP) is an integral part of the IP protocol
- The best-known use of ICMP:
 - 'ping'
 - 'traceroute'

Routing

- A router copies IP packages between (sub)networks
- Routers compile routing tables to make IP packet forwarding decisions
- Routing and switching functionality may be combined in one device

- A switch capable of handling routing protocols is also known as a layer 3 switch

Routing Protocols

- Dynamic routing protocols automatically create routing tables
 - Based on information exchange with neighboring routers
- When a network connection experiences problems, the routing protocol automatically reconfigures the routing tables to use alternative routes
- LAN and WAN routing protocols can be divided in three classes:
 - Distance vector protocols (like RIP and IGRP)
 - Link state protocols (like OSPF and IS-IS)
 - Path vector routing (like BGP)

Multiprotocol Label Switching

- Multiprotocol Label Switching (MPLS) routes data from one network node to the next with the help of labels
- MPLS allows setting up end-to-end circuit
 - Across any type of physical transport medium
 - Using any protocol
- In practice, MPLS is mainly used to forward IP and Ethernet traffic.

Transport Layer

- The transport layer can maintain flow control, and can provide error checking and recovery of data between network devices
- The most used transport layer protocols are TCP and UDP

TCP

- Transmission Control Protocol (TCP) uses the IP protocol to create reliable transmission of so-called TCP/IP packets
 - TCP provides reliable, ordered delivery of a stream of data between applications
 - TCP introduces much overhead

UDP

- User Datagram Protocol (UDP) emphasizes reduced latency over reliability
 - It sends data without checking if the data arrived
 - Reduces much overhead
 - UDP is typically used when some packet loss is acceptable
 - Real-time voice and video streams
 - When only small amounts of data are transmitted, that fit in one IP packet

TCP and UDP Ports

- TCP and UDP use logical port numbers
- Each side of a TCP or UDP connection uses an associated port number between 0 and 65,535
- Received TCP or UDP packets are identified as belonging to a specific connection by its combination of the IP address, and the TCP or UDP port number
 - ✚ For instance: 192.168.1.2:80, the number after the colon represents the port number (80 in this case)
- Servers running a specific service listen to well-known ports:
 - ✚ FTP (port 21)
 - ✚ SSH (port 22)
 - ✚ SMTP (port 25)
 - ✚ DNS (port 53)
 - ✚ HTTP (port 80)

Network Address Translation (NAT)

- NAT allows the use of a private addressing space within an organization, while using globally unique addresses for routing data to the internet
- As a packet passes a NAT enabled router from its internal network interface to its internet interface, NAT replaces the packet's private IP address with its public IP address

Session Layer

The session layer provides mechanisms for opening, closing and managing a session between end-user application processes

Virtual Private Network (VPN)






- ❑ A Virtual Private Network (VPN) uses a public network to interconnect private sites in a secure way
 - Also known as a VPN tunnel
- ❑ VPN uses "virtual" connections based on IPsec/SSL
- ❑ Most network providers also offer private VPNs based on MPLS
- ❑ VPNs use strong encryption and strong user authentication
 - Using the internet for transmitting sensitive data is considered safe
- ❑ VPN tunnels are often used for remote access to the LAN by users outside of the organization's premises
- ❑ Most common VPN communications protocol standards:
 - Point-to-Point Tunneling Protocol (PPTP) for individual client to server connections

- Layer 2 Tunneling Protocol (L2TP) for individual client to server connections
- IPsec for network-to-network connectivity
- ☐ IPsec is built into IPv6 standard and is implemented as an add-on to IPv4

Presentation Layer

- This layer takes the data provided by the application layer and converts it into a standard format that the other layers can understand
- Many protocols are implemented in the presentation layer
 - SSL and TLS are the most important ones

SSL and TLS

- Allow applications to communicate securely over the internet using data encryption
- Secure Sockets Layer (SSL)
 -  SSL is considered insecure and should not be used
- Transport Layer Security (TLS)
 -  TLS is securing WWW traffic carried by HTTP to form HTTPS
 -  Version 1.2 is considered secure
 -  Version 1.3 is in a draft state
 -  TLS relies on an application capable of handling the protocol (like a Web browser)

Application Layer

- This layer interacts with the operating system or application
- Examples:
 - ☐ HTTP
 - ☐ FTP
 - ☐ SMTP and POP3 (e-mail)
 - ☐ CIFS Windows file sharing
- This layer also contains the relatively simple infrastructure services
- Examples:
 - ☐ BOOTP
 - ☐ DHCP
 - ☐ DNS
 - ☐ NTP
- These infrastructure services are used by the infrastructure itself
 - ☐ Not necessarily used by upper layer applications
- If infrastructure services fail, usually the entire infrastructure fails!

BOOTP and DHCP

- BOOTP automatically assigns IP addresses to hosts
 - ☐ Uses a centralized BOOTP server
 - ☐ BOOTP requires manual configuration for each host in the network
- DHCP is an extension to BOOTP
 - ☐ It superseded BOOTP because it has more options
- DHCP dynamically assigns network related parameters to hosts:
 - ☐ IP addresses
 - ☐ Subnet masks
 - ☐ Default gateway to be used for routing
 - ☐ DNS server to be used
- A DHCP assigned IP address has a limited life span
 - ☐ Typically a few hours
 - ☐ This is called a lease

DNS

- ☐ DNS is a distributed database that links IP addresses with domain names
- ☐ Translates domain names, meaningful to humans, into IP addresses
- ☐ For example, *www.sjaaklaan.com* is translated to 217.149.139.184
- ☐ This IP address is used by the browser to connect to the web server
- ☐ DNS distributes the responsibility of mapping domain names to IP addresses by designating authoritative name servers for each domain

DNSSEC

- DNS has a number of security issues
 - DNS was not designed with security in mind
 - Updates to DNS records are done in non-encrypted clear text
 - Authorization is based on IP addresses only
- DNSSEC is a set of extensions to DNS
 - Provides origin authentication of DNS data
 - Provides data integrity
- DNSSEC is not in wide spread use today
 - All DNS servers must implement DNSSEC in order to make full use of all benefits

IPAM Systems

- IP address management (IPAM) systems are appliances that can be used to plan, track, and manage IP addresses in a network
- IPAM systems integrate DNS, DHCP, and IP address administration in one high available redundant set of appliances

Network Time Protocol (NTP)

- ❑ NTP ensures all infrastructure components use the same time in their real-time clocks
- ❑ Particularly important for:
 - Log file analysis
 - Clustering software
 - Kerberos authentication
- ❑ NTP can maintain time:
 - ❖ To within 10 milliseconds over the internet
 - ❖ Accurate to 0.2 milliseconds or better in LANs
- ❑ When the time in an operating system is incorrect, the NTP client in the operating system changes the operating system clock
- ❑ NTP servers can be implemented as:
 - ❖ Software on operating systems, routers, and switches
 - ❖ Dedicated hardware appliances – often using some external signal like long wave radio clocks or GPS clocks
 - ❖ NTP time synchronization services on the internet
- ❑ NTP provides time in Coordinated Universal Time (UTC, previously known as GMT)
- ❑ The translation to the local time zone, including the switch to and from daylight saving time, is done at the operating system level, not in NTP clocks
- ❑ NTP operates within a hierarchy
- ❑ Each level in the hierarchy is assigned a number called the stratum
- ❑ The stratum defines its distance from the reference clock