Requirements Analysis

Joao.Neves@fe.up.pt

Requirements Analysis

- Requirements are descriptions of the network functions and performance needed in order for the network to successfully support its users, applications, and devices.
- Requirements analysis helps the designer to better understand the probable behavior of the network being built. Such as:
  - More objective, informed choices of network technologies and services;
  - The ability to apply technology and topology candidates to networks;
  - Networks and elements properly sized to users and applications;
  - A better understanding of where and how to apply services in the network.

Requirements Organization

- Users
- Applications
- Devices
- Network
- Other

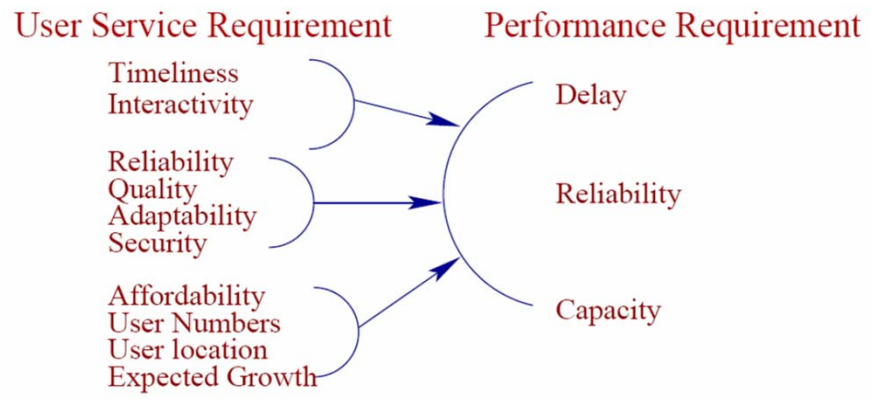
Requirements Organization

- ***Users***
- Applications
- Devices
- Network
- Other

Users Requirements

- Timeliness
- Interactivity
- Reliability
- Presentation quality
- Adaptability
- Security
- Affordability
- Functionality
- Supportability
- Future growth & Scalability

Users Requirements - Performance



- *Timeliness* is a requirement that the user be able to access, transfer, or modify information within a tolerable time frame

Requirements Organization

- Users
- ***Applications***
- Devices
- Network
- Other

Network RMA & Applications

- *Reliability* is a statistical measure of the frequency of failure of the network and its components (can be seen as the representation of the unscheduled outages of service);
- *Maintainability* is a statistical measure of the time to restore the system to fully operational status, after a failure;
- *Availability* is a measure of the relationship between the frequency of mission-critical failures and the time to restore service.

Applications Requirements - Application Types

Based on service and performance requirements, the following application types can be recognized:

- *Mission-critical* applications have predictable, guaranteed, and/or high-performance RMA requirements;
- *Rate-critical* applications have predictable, guaranteed, and/or high-performance capacity requirements;
- *Real-time* and *interactive* applications have predictable, guaranteed, and/or high-performance delay requirements.

RMA non-compliance

- Loss of revenue or customers (e.g. lost transactions of applications and money, such as investment banking, airline reservation, etc.)
- Unrecoverable information or situation (e.g. telemetry and teleconferencing applications)
- Loss of sensitive data (e.g. customer ID/billing and intelligence gathering applications)
- Loss of life (e.g. transportation or health-care applications)

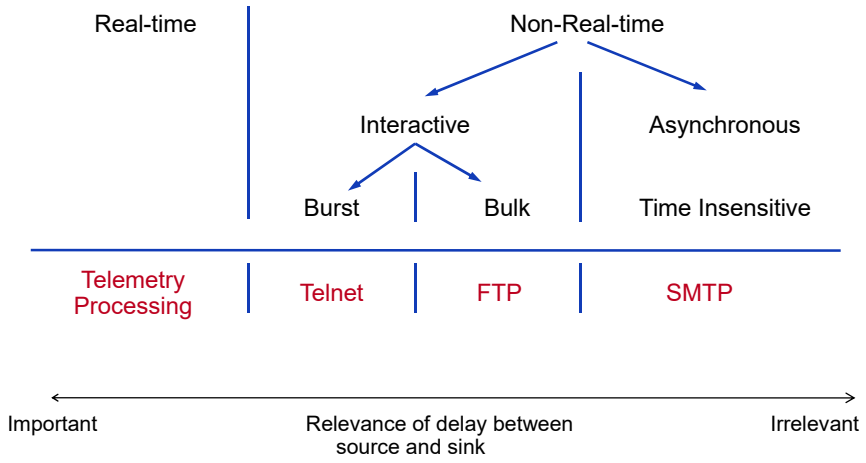
Applications - Capacity

- *Rate-critical applications* - Applications that require a predictable, bounded, or high degree of capacity
  - Voice, non-buffered video, and some “tele*service” applications (e.g. telemedicine, teleconferencing)
  - May require thresholds, limits, or guarantees on minimum, peak, and/or sustained capacities
- *Best-effort applications* - While at times there may be a high degree of capacity, it is inconsistent, and there is no control over the resources in the network to predict or guarantee a specific capacity

Applications - Delay

- Real-time applications
- Non-real-time applications
  - Interactive burst
  - Interactive bulk
  - Asynchronous

Applications - Delay types



Applications - Delay Sources

- Multiple sources of delay:
  - propagation,
  - transmission,
  - queuing,
  - processing,
  - routing.
- E.g. end-to-end and round-trip delay

Application Groups

It is advisable to develop application groups, e.g.:

- Telemetry, Command-and-Control;
- Visualization, 2D or 3D, VR;
- Distributed-Computing;
- Web Development, Access, and Use;
- Bulk Data Transport (without performance requirements);
- Tele∗Service;
- Operations, Administration, Maintenance, and Provisioning;
- Client-Server Applications.

Requirements Organization

- Users
- Applications
- ***Devices***
- Network
- Other

Device Requirements

- Device Types
- Performance Characteristics
- Device Locations

Device Types

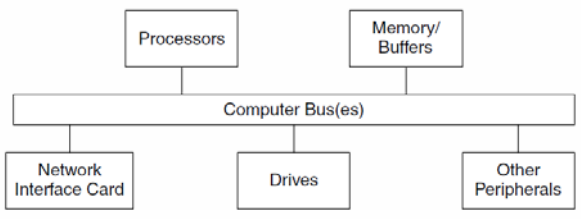
- *Generic computing devices*: PCs, laptops, handheld devices and workstations
- *Servers*: network servers, storage servers, application servers
- *Specialized devices* that provide specific functions to their users: data gathering and processing systems, medical devices, networked cameras or tools, IoT devices (wearable devices, environmental sensors, components in a vehicle or devices in homes…)

“Last Mile” & “Last Foot”

- “Last Mile” problem is: the difficulty in getting infrastructure, networking, and services into a campus or building;
- “Last Foot” problem is: getting services and performance from the device’s network interface through to its applications and users.

Device “Last Foot” Performance

- The “Last Foot” problem focuses on the performance of various components of the device: hardware, firmware, and software;
- Device problems frequently are misinterpreted as network problems



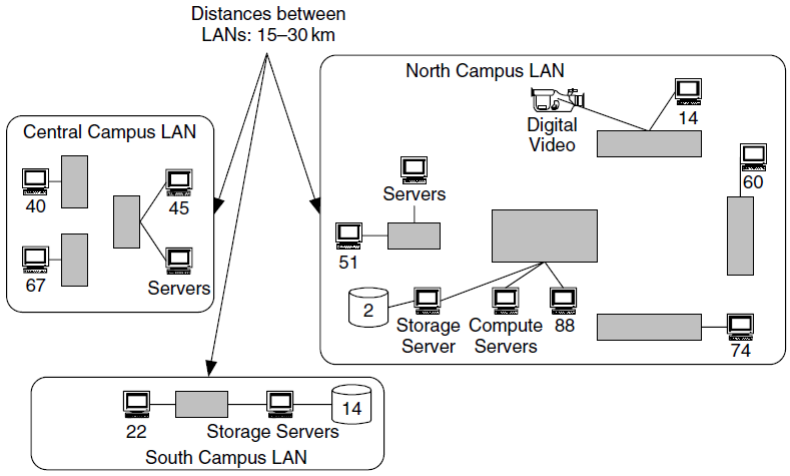
Performance Factors

- Storage: flash, solid state drive, disk drive, or tape
  - Disk-access speed;
  - Disk Caching size.
- Device driver performance
- Processor (CPU) performance
- Memory performance
  - Real and virtual memory access time
- Bus performance
  - Capacity and arbitration methods
- Operating System inefficiencies or bugs
- Application inefficiencies or bugs

Device Locations

- Knowing the locations of existing generic computing devices, servers, and specialized devices can be helpful in determining the relationships among users, applications, and networks.
- Is the start toward determining traffic flow characteristics for the system.
- Location information is particularly important for networks whose system components or functions are outsourced.

Device Locations



Requirements Organization

- Users
- Applications
- Devices
- ***Network***
- Other

Network Requirements

- Today most network designs need to integrate existing networks, including:
  - System upgrades;
  - Adding new applications;
  - Migrating to a new or different technology or protocol;
  - Upgrading the network infrastructure;
  - Expansion or reduction of a system's size or scope.
- Sometimes the network architecture and design must accommodate any dependencies and constraints imposed by the existing network.

Network Requirements

- Scaling dependencies
- Location dependencies
- Performance constraints
- Network, system, and support service dependencies
- Interoperability dependencies
- Network obsolescence

Scalability

- Scalability is how much growth can be accommodated in a network solution
- Not all technologies scale well
  - Hierarchically flat networks do not scale well
- Need to know
  - How much will grow the network in a short/medium term (one, two years...)
  - Number of sites to be added
  - What will be needed at each of these sites
  - How many users will be added
  - How many more servers will be added

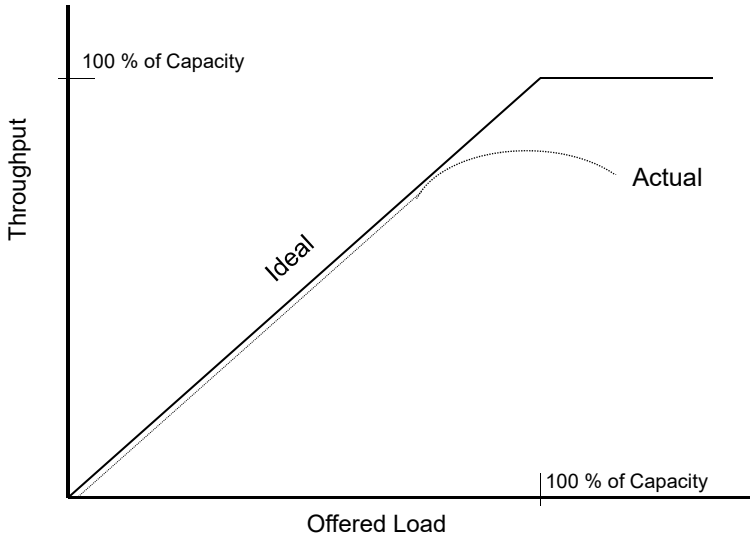
Network Performance

- Common performance factors include
  - Bandwidth
  - Throughput
  - Bandwidth utilization
  - Offered load
  - Accuracy
  - Efficiency
  - Delay (latency) and delay variation
  - Response time

Bandwidth vs. Throughput

- Bandwidth and throughput are not the same
- Bandwidth is the data carrying capacity of a circuit
  - Usually specified in bit per second
- Throughput is the quantity of error free data transmitted per unit of time (or the average rate of successful message delivery over a communication channel)
  - Measured in bit/s, byte/s, octet/s, or packet per second

Bandwidth, Throughput, Load



Other Factors that Affect Throughput

- The size of packets
- Inter-frame gaps between packets
- Packets-per-second ratings of devices that forward packets
- Client speed (CPU, memory, and HD access speeds)
- Server speed (CPU, memory, and HD access speeds)
- Network design
- Protocols
- Distance
- Errors
- Time of day, etc.

Throughput vs. *Goodput*

You need to decide what you mean by throughput:

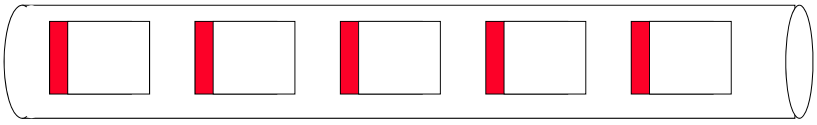
- Are you referring to byte per second, regardless of whether the bytes are user data bytes or packet header bytes?
- Or are you concerned with application-layer throughput of user bytes, sometimes called *goodput* or the Effective bandwidth?
- In that case, you have to consider that bandwidth is being “wasted” by the headers in every packet

Efficiency

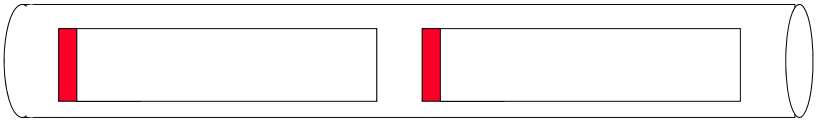
- Efficiency
  - How much overhead is required to deliver an amount of data?
  - How large can packets be?
    - » Larger better for efficiency (and goodput)
    - » But too large means too much data is lost if a packet is damaged
    - » How many packets can be sent in one bunch without an acknowledgment**?**

Efficiency

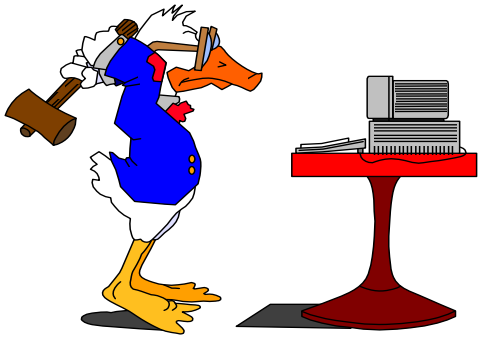
Small Frames (Less Efficient)



Large Frames (More Efficient)



Delay from the User's Point of View

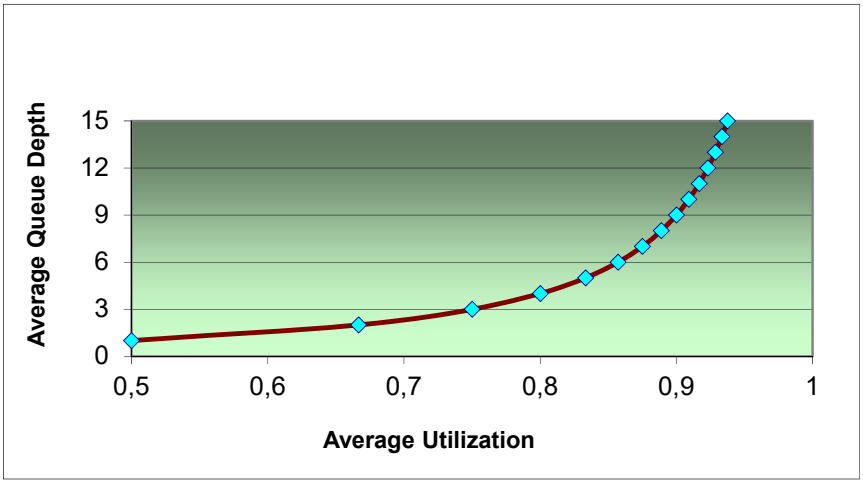


- Response Time
  - A function of the application and the equipment the application is running on, not just the network
  - Most users expect to see something on the screen in 100 to 200 milliseconds

Delay from the Engineer's Point of View

- Propagation delay
  - A signal travels in a cable at about 2/3 the speed of light in a vacuum
- Transmission delay (also known as serialization delay)
  - Time to put digital data onto a transmission line
    - » For example, it takes about 5 ms to output a 1024 byte packet on a 1.544 Mb/s T1 line
- Packet-switching delay
- Queuing delay

Queuing Delay and Bandwidth Utilization



- Number of packets in a queue increases exponentially as utilization increases

Example

- A packet switch has 5 users, each offering packets at a rate of 10 packet per second
- The average length of the packets is 1024 bit
- The packet switch needs to transmit this data over a 56 kbit/s WAN circuit
  - Load: 5 x 10 x 1,024 = 51,200 bit/s
  - Utilization: 51,200 / 56,000 = 91.4 %
  - Average number of packets in queue:
    0.914 / (1 – 0.914) = 10.63 packets

Delay Variation

- The amount of time average delay varies
  - Known as jitter
- Voice, video, and audio are intolerant of delay variation
- So forget everything said about maximizing packet sizes
  - There are always tradeoffs
  - Efficiency for high-volume applications versus low and non-varying delay for multimedia

Network Management Requirements

Management Tasks:

- Event processing
- Monitoring (metrics of: capacity, reliability, delay)
- Configuration
- Failure detection and troubleshooting
- Accounting
- Security

Network Management Requirements

Management Requirements:

- Monitoring methods
- Management protocols and tools
- Sets of characteristics for monitoring
- Intrusive monitoring: in-band vs. out-of-band
- Centralized vs. distributed monitoring
- Performance

Financial Requirements

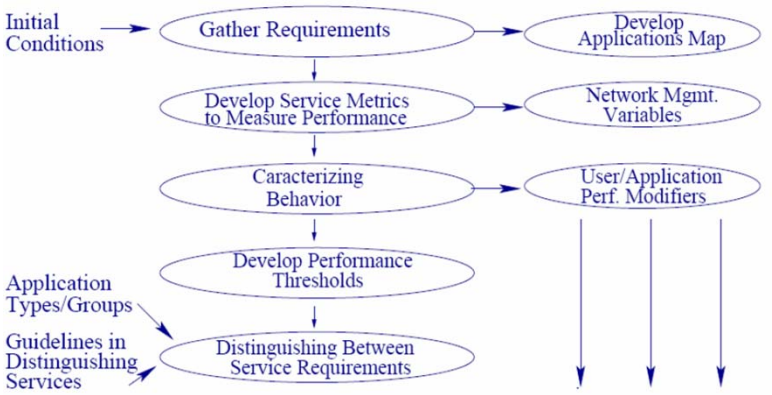
Budget necessary for the design and installation:

- Hardware
- Software
- Cabling
- …

Budget necessary for the production phase:

- Circuit rentals
- Staff
- Spare replacement
- …

Requirements Analysis Process



Technical Goals for the Requirement Analysis Process

- Scalability
- Availability
- Performance
- Security
- Manageability
- Usability
- Adaptability
- Affordability

Metrics – Quantify RMA

- *Reliability* is an indicator of the frequency of failure, and a related measure is the mean time between failures (MTBF);
- *Maintainability* is generally expressed as mean time to repair (MTTR);
- *Availability* also known as operational availability, does not reflect exactly the percentage of time that the system is operational, since scheduled maintenance is not included in this calculation.

Availability

- Usually means how much time the network is operational
- Availability can also be expressed as a mean time between failures (MTBF) and mean time to repair (MTTR)
- Availability = MTBF/(MTBF + MTTR)
  - For example:
    - » The network should not fail more than once every 4 000 hours (166 days) and it should be fixed within one hour
    - » 4 000 / 4 001 = 99.98% availability

Availability

- It can be expressed as a percentage of uptime for a period of time (month, week, day, etc.) in relation to the total time of that period
  - For example, in a 24/7 operation
    If the network is up for 166 hours in a week (168 h)
    then the Availability is 98.81 %
- Service Providers usually refer 95 % or 97 % of service availability…
  - A service evaluation for a day (1440 min) with 95 % availability means that it can be down for 80 min, i.e. 1 h 20 min… Or 8 h 24 min in a 24/7 week operation
  - And for 97 % it can be down circa 43 min!

Availability
Downtime in Minutes

T * (1-A) = D

Availability	Hourly	Daily	Weekly	Yearly	Yearly
99.999 %	0.0006	0.01	0.10	5	
99.98 %	0.012	0.29	2	105	1h 45min
99.95 %	0.03	0.72	5	263	4h 23min
99.90 %	0.06	1.44	10	526	8h 46min
99.70 %	0.18	4.32	30	1577	26h 17min
99.50 %	0.3	7.2	50.4	2628	43h 48min

E.g. 99.70 % Availability

- 99.70 % availability looks good, but it could mean that the network is down for 0.18 minutes (11 sec) every hour.
- Notice that 99.70 % availability for a year also could mean one catastrophic problem caused the network to be down for 1,577 minutes (26 h) all at once. *If it were on a Saturday and the network was never down for the rest of the year, that might actually be OK.*
- Should be considered time frames with percent availability numbers.

99.999 % Availability

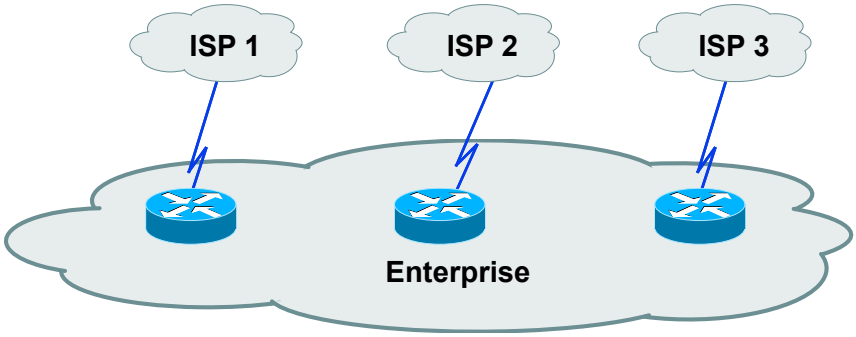
Considering the Holy Grail:

"Five Nines" availability…

- Which means 5 minutes downtime per year!
- But be sure to remember or explain to the customers that scheduled maintenance and upgrades don't count!
- Either that or plan for a network with triple redundancy (that could be extremely expensive to setup and manage).

99.999 % Availability

- Some enterprises want to require 99.999 %, known as “Five Nines” availability



- Can the customer afford this redundancy?
- Are maintenance operations included?

Service Level Agreement

Service Level Indicator (SLI)
Metric that is measured

Service Level Objective (SLO)
Acceptable range of values for the SLI

Service Level Agreement (SLA)
Legal document or contract with end users defining consequences if SLO is not met

SLA

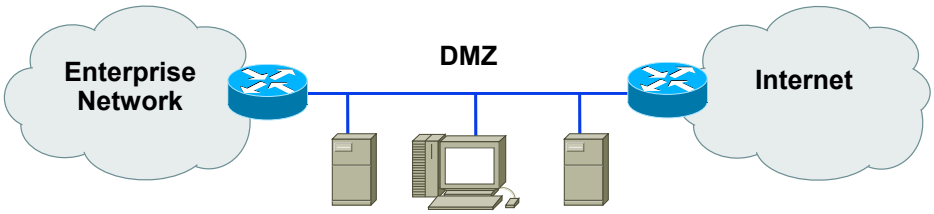
A **S**ervice **L**evel **A**greement is the formalization of the 'Quality of the Service' in a contract between the Customer and the Service Provider.

"If you can't measure it, don't negotiate it..."

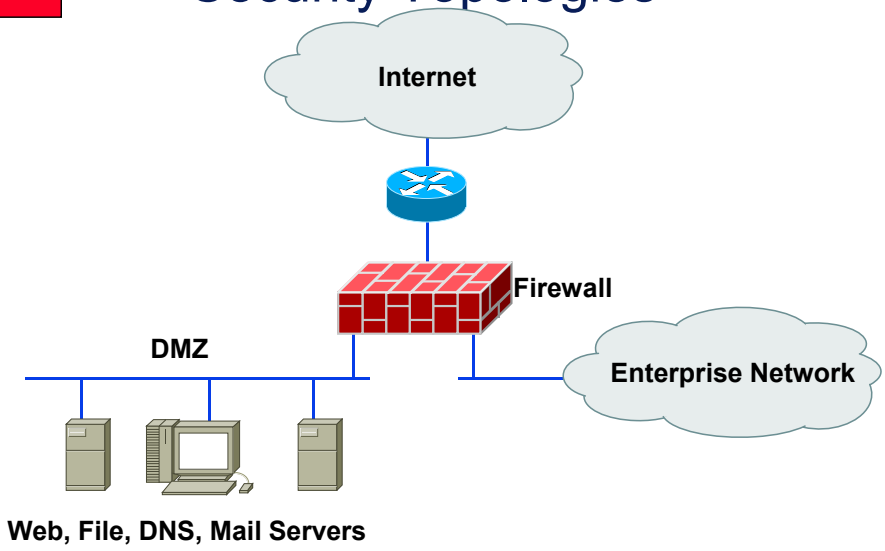
Security

- Focus on requirements first
- Detailed security planning
- Identify network assets
  - Including their value and the expected cost associated with losing them due to a security problem
- Analyze security risks

Security Topologies



Security Topologies



Network Assets

- Hardware
- Software
- Applications
- Data
- Intellectual property
- Trade secrets
- Company's reputation

Top Ten Vulnerabilities 2018

The top ten most commonly exploited vulnerabilities in 2018:

1. CVE-2018-8174 – Microsoft
2. CVE-2018-4878 – Adobe
3. CVE-2017-11882 – Microsoft
4. CVE-2017-8750 – Microsoft
5. CVE-2017-0199 – Microsoft
6. CVE-2016-0189 – Microsoft
7. CVE-2017-8570 – Microsoft
8. CVE-2018-8373 – Microsoft
9. CVE-2012-0158 – Microsoft
10. CVE-2015-1805 – Google Android

Source: https://www.recordedfuture.com/top-vulnerabilities-2018/

Top Ten Vulnerabilities 2019

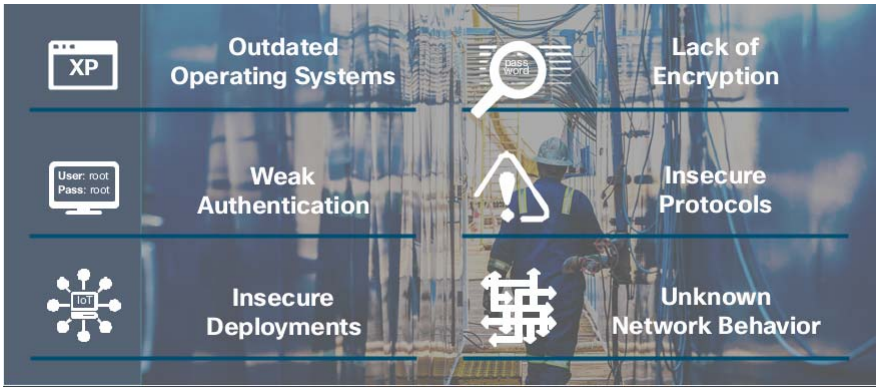
The top ten most commonly exploited vulnerabilities in 2019:

1. CVE-2018-15982 – Adobe Flash Player
2. CVE-2018-8174 – Microsoft Internet Explorer ↑1
3. CVE-2017-11882 – Microsoft Office =
4. CVE-2018-4878 – Adobe Flash Player ↑2
5. CVE-2019-0752 – Microsoft Internet Explorer
6. CVE-2017-0199 – Microsoft Office ↓5
7. CVE-2015-2419 – Microsoft Internet Explorer
8. CVE-2018-20250 – Microsoft WinRAR
9. CVE-2017-8750 – Microsoft Internet Explorer ↑4
10. CVE-2012-0158 – Microsoft Office ↓9

Source: https://www.verdict.co.uk/top-software-vulnerabilities-2019/

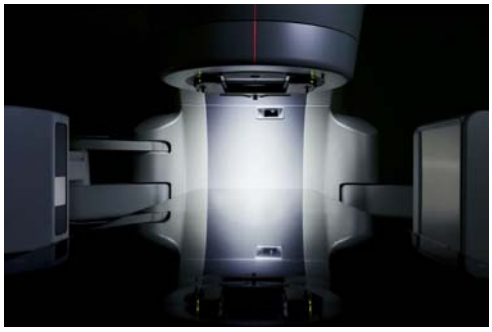
New Security Problems

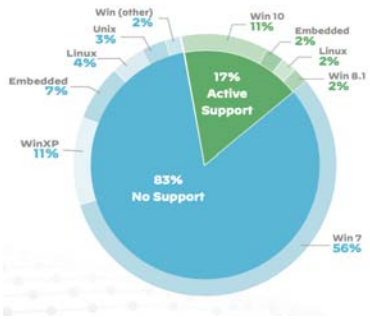
- Vulnerabilities of IoT in Manufacturing



Outdated Operating Systems

- E.g. 83 % of medical imaging devices run on operating systems that are so old they no longer receive any software updates at all.





Source: https://unit42.paloaltonetworks.com/iot-threat-report-2020/
https://www.wired.com/story/most-medical-imaging-devices-run-outdated-operating-systems/

Security Risks

- Hacked network devices
  - Data can be intercepted, analyzed, altered, or deleted
  - User passwords can be compromised
  - Device configurations can be changed
- Reconnaissance attacks ⇔ scout for failures
- Denial-of-service attacks

Manageability

- Performance management
- Fault management
- Configuration management
- Security management
- Accounting management

Usability

- Usability: the ease of use with which network users can access the network and services
- Networks should make users' jobs easier
- Some design decisions will have a negative affect on usability:
  - Strict security, for example

Adaptability

- Avoid incorporating any design elements that would make it hard to implement new technologies in the future
- Change can come in the form of new protocols, new business practices, new fiscal goals, new legislation
- A flexible design can adapt to changing traffic patterns and Quality of Service (QoS) requirements

Affordability

- A network should carry the maximum amount of traffic possible for a given financial cost
- Affordability is especially important in campus network designs
- WANs are expected to cost more, but costs can be reduced with the proper use of technology
  - Quiet routing protocols, for example

Network Applications Technical Requirements

Name of Application	Cost of Downtime	Acceptable MTBF	Acceptable MTTR	Throughput Goal	Delay Must be Less Than:	Delay Variation Must be Less Than:

Making Tradeoffs

Scalability	20
Availability	30
Network performance	15
Security	5
Manageability	5
Usability	5
Adaptability	5
Affordability	15
Total (must add up to 100)	100

Summary

- Continue to use a systematic, top-down approach
- Don't select products until you understand goals for scalability, availability, performance, security, manageability, usability, adaptability, and affordability
- Tradeoffs are almost always necessary

Bibliography

- **McCabe, James D.**
  Network Analysis, Architecture and Design
  3rd Ed., The Morgan Kaufmann Series in Networking, (2007)
  ISBN: 978-0-12370-480-1
  eBook ISBN: 978-0-08054-875-3

Chapters 2 - 3

- **Oppenheimer, Priscilla**
  Top-Down Network Design
  3rd Ed., Cisco Press (May 2012)
  ISBN-13: 978-1-58720-283-4
  ISBN-10: 1-58720-283-2