INTRO 4.0

NETWORK COMMUNICATION

EuroProfis

edit value
apoio à gestão

@nced
ASOCIACIÓN NACIONAL DE CENTROS DE e-LEARNING Y DISTANCIA

bit schulungscenter
member of bit group

Co-funded by the Erasmus+ Programme of the European Union

Associate partner:

udima
UNIVERSIDAD A DISTANCIA DE MADRID

INTRODUCTION TO THE INDUSTRIAL REVOLUTION 4.0

These didactical materials, which have been developed in the framework of the European project 'Industry 4.0 - INTRO 4.0', funded by the European Commission aims to come up with an overview of what has been done in the European Industry in terms of Industry 4.0.

The content of these didactical materials provides the most relevant and useful information on Industry 4.0 to a target group that includes: adults, educators (VET & Higher Education), teachers, trainers, coaches, employers, employees, the general public, and suppliers of innovative solutions.

This information is rooted within the report 'Current Status Of The Industry 4.0' and the report 'Summary Report of the expert interviews/questionnaires and the specific research on the field of manufacturing companies", both developed by the partners of this project.

INDEX

THIS CONTENT MAY BE OF GREATER INTEREST TO THE COMPANIES

THIS CONTENT MAY BE OF GREATER INTEREST TO THE GENERAL PUBLIC

LEARNING OBJECTIVES

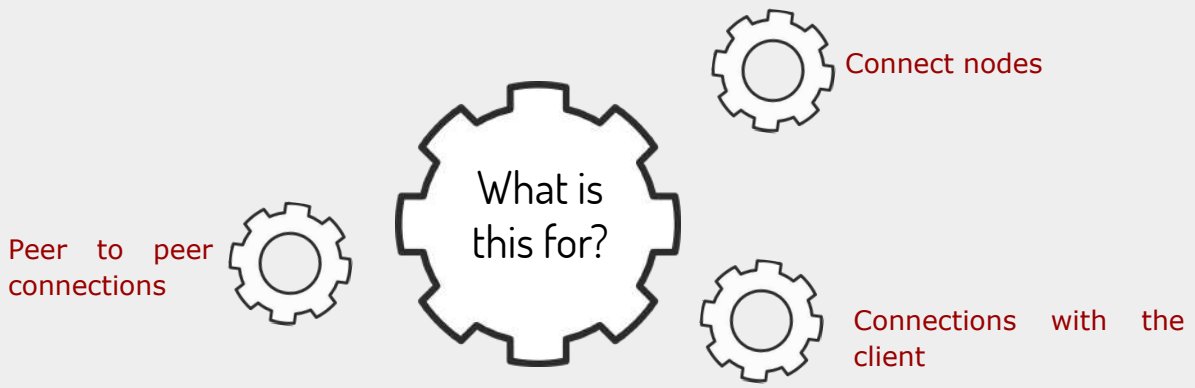
- Understand the fundamentals of Network Communication
- Identify the different types of Network
- Know the importance of IoT
- Estimate the benefits that Network Communication can have for companies
- Recognize future applications

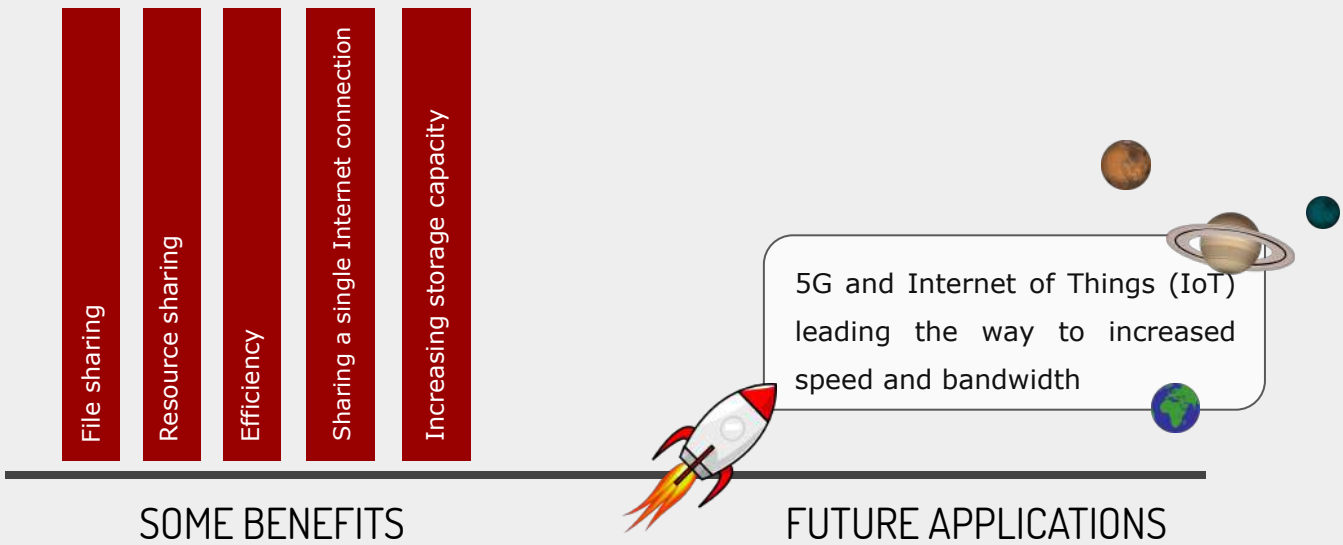
INTRODUCTION

Network Communication is a network of a group of devices comprising hardware and software connected together.

Learning Objectives

- Understand the fundamentals of Network Communication
- Identify the different types of Network
- Know the importance of IoT
- Estimate the benefits that Network Communication can have for companies
- Recognize future applications

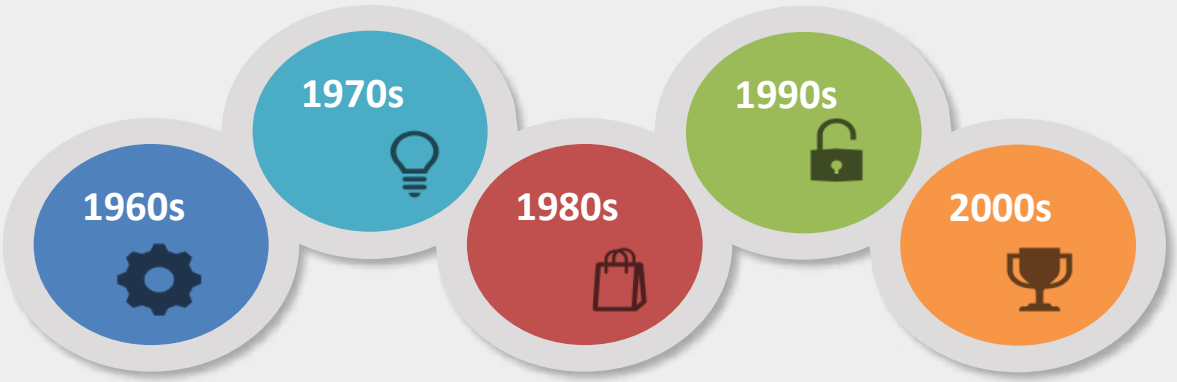




WHAT IS IT?

Communication networks are at the bedrock of our society. A communication network is a network of a group of devices comprising hardware and software connected together, whether in the same geographical location or globally to facilitate communication and information sharing. So you name it: ultra sound machines, cell phones, Internet communications, banking transactions, e-learning, border security, transport networks, satellite imaging and the list goes on, are all made possible only through communication networks. This modern society we live in cannot do without it.

Modern communication network consist of servers, clients, transmission media, data, operating systems, switches, routers, cables, printers and various peripheral devices extending communication between devices from local area network to globally covered networks.



In 1962, MIT computer scientist J.C.R. Licklider comes up with the idea for a global computer network.

In 1973, Robert Kahn and Vinton Cerf collaborate to develop a protocol for linking multiple networks together. This later becomes the Transmission Control Protocol/Internet Protocol (TCP/IP)

In 1981, Metcalfe's company 3Com announces Ethernet products for both computer workstations and personal computers; this allows for the establishment of local area networks (LANs)

CERN develop hypertext markup language (HTML) and the uniform resource locator (URL), giving birth to the first incarnation of the World Wide Web.

The rise and proliferation of Wi-Fi as well as mobile Internet devices like smartphones and, in 2005, the first-ever Internet cat video.

WHAT IS IT?

Networking Types and Structures

Networks can be wired or wireless with most networks being a mixture of both.

Wired vs Wireless Networks

Early (pre 2008) networks were predominately wired. Today however most networks will use a mixture of wired and wireless network.

Wired networks use Ethernet as the data link protocol. This is unlikely to change with the IoT, as IoT devices will be predominantly wireless.

Wired networks have the following advantages/disadvantages:

Advantages

- Ethernet ports are found on almost all laptops/PCs and netbooks even on those 8 years old.
- Wired networks are faster than Wireless. Data rates were periodically increased from the original 10 megabits per second, to 1 gigabyte per second. Most home networks use 10-100 Mbps.
- More secure than Wireless

Ethernet is a family of computer networking technologies commonly used in local area networks (LAN), metropolitan area networks (MAN) and wide area networks (WAN).

WHAT IS IT?

Disadvantages

- Need to Use cable which can be unsightly, difficult to run and expensive.
- Can't be used easily between buildings (planning etc).
- Note a new technology that uses mains cable overcomes many of these disadvantages. Powerline networking is common on home/small office networks
- Not supported on Mobile phones and tablets.

Wireless Networks – Advantages and Disadvantages

Wireless networks use Wi-fi as the data link protocol. However other wireless options are being developed for the IoT (Internet of Things). See Wireless networking Technologies for the IoT

Wireless Networks have the following advantages/disadvantages:

Advantages

- Generally easier to set up.
- Can be used both on home and public networks
- No cables required.
- Can be used with mobile phones and tablets.

Wireless Networks Disadvantages

- Generally Slower than wired networks.
- Limited by range.
- Open to eavesdropping.
- Not as secure depending on set up.

WHAT IS THIS FOR?

Networking Topologies and Layout

There are many different ways network nodes can be connected together. This isn't normally a consideration in small networks but has networks get larger it becomes more important. There are many different ways network nodes can be connected together.

Common connection technologies like Wi-Fi, Bluetooth etc are designed to work using a particular network topology. When designing networks and choosing connection protocols having an understanding of these topologies is important.

Common are: Bus, Ring, Mesh, Star, Hybrid

Early Ethernet networks used a bus structure, modern Ethernet networks and Wi-Fi Networks use a star bus (hybrid) structure.

Networking Topology- Physical vs Logical

How the nodes on a network communicate with each other can be very different to how they are physically interconnected. Most home and small office networks use a physical bus topology. Common logical typologies are Peer to Peer and Client Server. The web (WWW) is a client server network at the logical level.
In a peer to peer network all nodes are equal and any node can talk to any other node. No node has any special role. This was the original networking model of windows networking. (Windows for Workgroups).

WHAT IS THIS FOR?

Peer to Peer Networking Model

Advantages

- Easier to setup
- Not dependent on a single node
- More resilient
- Better distribution of network traffic
- No central administration required
- Less expensive hardware required

Disadvantages

- Less secure and more difficult to secure
- More difficult to administer
- More difficult to backup
- More difficult to locate information.

This was the original networking model used in early Windows networks (Windows for Workgroups)

A Modern example of Peer to Peer networking is BitTorrent.

Although this networking model isn't currently popular it could become more popular with the Internet of Things (IOT).

WHAT IS THIS FOR?

Client Server

In a Client Server network a server has a special role e.g file server, domain controller, web server etc. A client connects to a server to use the appropriate services.

This is the networking model used on the web and the Internet and on modern large Windows networks.

Advantages

- Easy to find resources as they are on a dedicated node i.e. A server
- Easy to secure
- Easy to administer
- Easy to backup

Disadvantages

- Servers are a single point of failure
- Expensive hardware required
- Network traffic get concentrated

A Modern example of Client Server networking is the Web. Facebook, Twitter, Google search and many other web services use this networking model.

WHAT IS THIS FOR?

Network Size

Networks vary considerably in size. The following are commonly used terms:

- PAN -Personal Area Network – Linking local devices e,g, PC to printer
- LAN – Local Area network- links devices in an office or offices
- MAN – Metropolitan Area network – links devices across multiple buildings like a campus
- WAN – Wide area network – links devices across a country/countries.

Networking Levels and Layers and Protocols

A protocol defines a set of rules that govern how computers talk to each other.

Ethernet and Wi-Fi are Data link protocols that are responsible for framing data on the media (cable or wireless).

Ethernet and Wi-Fi use a physical level address know as the MAC address which is 48 bits.

EUI 64 addresses are MAC addresses with 64 bits will replace MAC addresses on IPV6, 6LoWPAN, ZigBeeand other new network protocols.

You can divide networking into distinct levels or layers. Each level or layer is responsible for a particular function.

The OSI uses a 7 layer model and TCP/IP networks use a 4 layer model.

WHAT IS THIS FOR?

Because TCP/IP (TPC = Transmission Control Protocol, IP = Internet protocol) networks are the most common, the TCP/IP model is the most important one to understand. The levels are:

- Data link level – e.g. Ethernet, Wi-Fi
- Networking e.g. IP, – IPv4 Address classes and subnetting and IPv6 Explained for Beginners.
- Transport level e.g.TCP, UDP – See TCP vs UDP
- Application level – e.g. HTTP -See HTTP for beginners

Network Addressing

What is an IP Address?

Every device attached to a network, and the Internet has an IP address.

> An Internet Protocol address (IP address) is a numerical label assigned to each device (e.g., computer, printer) participating in a computer network that uses the Internet Protocol for communication

There are two versions of IP, they are IPv4 and IPv6.

IPv4 has been in use since the start of the Internet, and is deployed across the Internet, and home/corporate networks.

IPv4 uses 32 bits for addressing, however due to the rapid growth of the Internet, all IPv4 addresses have been allocated (as of 2013).

WHAT IS THIS FOR?

Techniques like NAT (network Address Translation) have extended the life of IPv4 by allowing the use of private IP addresses inside networks.

However IPv4 will eventually be replaced by IPV6 which uses 128 bits for the address, and so can accommodate many more hosts (computers/devices)

The roll out of IPv6 across the Internet is happening slowly, and IPv4 will be with us for many years to come especially in home and small office networks.

As IP6 rolls out they will also be a need to operate with two addresses until migration is complete, and IP4 is discontinued.

IP addresses are logical addresses, and are assigned by a network administrator or can be auto assigned (using DHCP).

The important thing to note is that the IP address of a device isn't fixed.

Public and Private IP Addresses

Both IPv4 and IPV6 have both public and private address ranges.

The private addresses are used for home/business networks and the addresses aren't routeable on the Internet i.e. they don't travel across the Internet.

For IP4 the private addresses starts with 10.x.x.x or 192.168.x.x or 172.16.x.x

Public addresses are reachable from anywhere on the Internet and are routeable.

WHAT IS THIS FOR?

IP Address Assignment

Most modern networks use automatic IP address assignment via DHCP with manual assignment only being done in special cases.

For home networks the Internet router or hub usually provides DHCP services for the network.

For larger networks a dedicated DHCP server is normally used.

Most windows machines will auto assign their own address if they fail to find a DHCP server.

This can cause problems see troubleshooting Internet connections.

IP Addresses and Domain Names

Computers use numbers (IP addresses) but people use names as they are much easier to remember.

When you type in a domain name into your web browser the name is translated into an IP address by a DNS server usually located on the Internet.

WHAT IS THIS FOR?

TOP 8 NETWORK COMMUNICATION SKILLS FOR WORKERS

Figure 1. Top 5 Network Communication skills for workers
Source: self made

Computer network professionals manage the day-to-day operation of computer networks. Demand for these skilled information technology workers is expected to grow as more companies invest in newer, faster technology. A successful computer network professional will have a variety of skills they use to support an organization's computer systems, including:

WHAT IS THIS FOR?

Analytical skills

Learn to evaluate network and system performance and detect and monitor changes to computer systems.

Computer skills

Work with a variety of technologies, including local area networks, wide area networks, network segments, intranets, hardware and software. Administrators up-to-date in cloud computing and mobile technology will be especially in high-demand.

Communication skills

Provide IT support and communicate problems and solutions to administrators and less tech-savvy employees.

Problem-solving skills

Learn to quickly resolve problems that arise with computer networks.

Multitasking skills

Manage multiple problems and projects at once for an organization.

WHAT IS THIS FOR?

Researchers estimate that within two years from now, a whopping 20.4 billion Internet of Things (IoT) devices will be connected. This surge in the number of IoT devices in use will translate into a significant increase in the number of IoT jobs as well. Clearly, a job in IoT can pay well because of the rising demand, but candidates will require a combination of skills to ensure a promising IoT career.

Broad-based skills for an IoT career

1. Business intelligence
2. Data security
3. Application design
4. Mobile applications
5. IoT hardware
6. Networks
7. Sensors
8. Embedded chips
9. Cloud computing
10. Troubleshooting IoT

GOOD PRACTICES

Wearable Technology

Magoo Project

Magoo is a wearable device specifically designed for the visually impaired that is accessible, easy-to-use and fashionable in a way that it doesn't make the blind feel like they stand out negatively. This device provides two basic functions: obstacle detection and navigation assistance, both via haptic feedback

In obstacle detection, the user wears a necklace that contains an ultrasonic sensor, which provides vibration (haptic feedback) on the neck if the user is within 2 meters range of a barrier in front of them.

The second piece is an arm-length glove which houses the actuators and wifi component and features a beautiful, tactile design on the top. The user inputs his/her destination using a voice command and the integrated circuit on the glove commutes with the GPS to find the optimal route to this destination piece wise (every 0.1 miles) by finding a direction vector. The user can swing his/her arm to track the right direction. As the user's arm falls in the region of 'correct direction vector' (as indicated by GPS), the user gets a haptic feedback which points them in the right direction. This not only helps the blind in convenient navigation, but also prevents them from getting lost. .

GOOD PRACTICES

Best Practices of the University of Mary Washington (Google Glass)

The University of Mary Washington was part of the Google Glass Explorer Program. This program is now moving to its next phase of development.
Google Glass is a portable technology similar to your smartphone. It fits an eye-glass frame and has a camera mounted on the head and a screen placed over the right eye. To communicate with this mini laptop, you can use your voice using the command, ok glass or you can use touch. As with your smartphone, download applications that provide functionality to the device.

Glass in an Educational Setting:

Students:
First person perspective, record interactions, processes, role plays, public speaking activities, group work, problem solving strategies, tutorials, and field trips, head and body movements in sports. Take notes. Simple Google Searches. Augmented reality via QR Codes to view content (video, text, images). Real time language translation. Accessibility for visual, auditory, and physical handicaps.

GOOD PRACTICES

Teachers:

Document student learning during lecture, demonstrations, hands-on experiences activities, field trips in real time from teacher point of view. Record lessons from teacher perspective and combine with student perspective for a reflection. Tutorial lessons to help clarify misperceptions or answer student questions. Take notes. Receive questions from students during lectures. Poll students. View slide notes during presentation. Wear during intern evaluations or have intern wear and record from their point of view. Connect through Google Hangouts. Create content videos. Display student information to tailor lessons to students needs. Display various types of information for easy access. Send and receive messages.

General Uses:

Create video guides (first person tour in real time). Create documentaries to enhance storytelling. Capture everyday life. Connect with others through Google Hangout. Transfer content from Glass to Google+ computer for easy access. Personalized searches. Design and build Apps. Closed captioning.

The Internet of Things (IoT)

University of Wisconsin–Madison

At the IoT lab of this university researchers with the colaboration of industrial collaborators are developing many devices such as a digital home message center, a health monitoring bracalet or gadgets connected to bikes to warn about proximities to vehicles..

In this place students with great ideas can teaming up to advance their technology and business sense.

GOOD PRACTICES

IoT Lab

IoT Lab is a research platform exploring the potential of crowdsourcing and Internet of Things for multidisciplinary research with more end-user interactions. It gives the power to the crowd to be at the core of the research and innovation process. It gives you the power to change the world and the way we understand it.

IoT in Medical Education

This article describes IoTFlip or IoT Flipped Learning Platform that uses the IoT devices , IoT data and CBL (Case Based Learning) to create a platform based on flipped learning for medical education.

Some leading companies:

XILINX®

Google

INGENU simply genius

ARM

CISCO

IBM

BOSCH

R-Style Lab

BENEFITS FOR THE COMPANY

Setting up a computer network is a fast and reliable way of sharing information and resources within a business. It can help you make the most of your IT systems and equipment.

Main benefits of networks include:

File sharing
You can easily share data between different users, or access it remotely if you keep it on other connected devices.

Resource sharing
Using network-connected peripheral devices like printers, scanners and copiers, or sharing software between multiple users, saves money.

Sharing a single Internet connection
It is cost-efficient and can help protect your systems if you properly secure the network.

Increasing storage capacity
You can access files and multimedia, such as images and music, which you store remotely on other machines or network-attached storage devices.

Networking computers can also help you improve communication, so that:

- staff, suppliers and customers can share information and get in touch more easily
- your business can become more efficient - eg networked access to a common database can avoid the same data being keyed multiple times, saving time and preventing errors
- staff can deal with queries and deliver a better standard of service as a result of sharing customer data

BENEFITS FOR THE COMPANY

Cost benefits of computer networking

Storing information in one centralised database can also help you reduce costs and drive efficiency. For example:

Staff can deal with more customers in less time since they have shared access to customer and product databases

You can cut costs through sharing of peripherals and Internet access

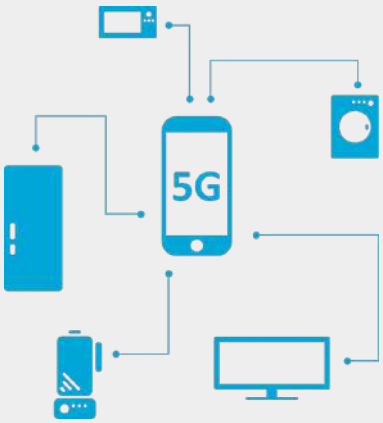
You can centralise network administration, meaning less IT support is required

You can reduce errors and improve consistency by having all staff work from a single source of information. This way, you can make standard versions of manuals and directories available to them, and back up data from a single point on a scheduled basis, ensuring consistency.

FUTURE APPLICATIONS

Securing the Communications Networks of Tomorrow

5G and other next-gen telecom technology are keeping IT and security managers on their toes. Learn what needs to be done to secure these new services.



Global IT is changing faster than ever with technologies such as 5G and Internet of Things (IoT) leading the way to increased speed and bandwidth, but also increased connectivity complexity. Through these ongoing changes and migrations to the next generation of telecommunications networks, communications service providers (CSPs) are dealing not only with new technology but also the security requirements that come with it.

Facing these challenges on the frontline are enterprise and provider IT and security managers, who will be charged respectively with overseeing the deployment and maintenance of new advanced networks and the related security issues.

Even though 5G may still seem several years from becoming ubiquitous, now is the time for IT managers, security managers, and their staff to learn about the issues and prepare themselves for what's coming.

FUTURE APPLICATIONS

Sharing the security responsibility

As the global IT ecosystem undergoes a rapid evolution, it will be critical for IT departments to have a strong understanding of the new network architecture, security implementation, and ultimately who will be responsible for what. Once 5G, and by extension its enabling services and technologies – such as IoT, IPv6, and machine-to-machine (M2M) – become the de facto standard within the communications landscape, operators and their IT departments and security managers will need to face, understand, and overcome a whole new set of security challenges that will be more complex than anything that's come before.

Some of the challenges that are specific to internal departments include:

Since IT departments at telcos will need to overcome these issues while running a 5G-enabled, and eventually a 5G-ready network, they will need help from a trusted partner that understands the network layer, the customer layer, and the security layer. This help must encompass proven expertise in various data types, such as customer data, transaction data, and network data, to ensure that sensitive information is compartmentalized and safe from a variety of threats. Good skills in security architecture can buttress effective security through a number of techniques, including segmentation.

FUTURE APPLICATIONS

Securing 5G networks becomes even more complex when network slicing, the ability to create multiple simultaneous mini-networks that operate under different sets of security and service requirements, enters the picture. This ability to invoke a 5G instance quickly for a specific period of time, in a specific place, will make security an even higher priority and that's much more of a challenge for IT and security managers, who will be the ones tasked with securing these various data types.

Their customers will turn to them in the event of a problem, and operators will be tasked with resolving any issues, which will require significant levels of knowledge and proficiency around security issues. For these reasons, most operators will not be able to go it alone successfully when it comes to overcoming the security hurdles of 5G and other shifts in communications networks. Rather, they will need to work with trusted partners that have the expertise, track record, and experience to ensure data integrity, customer privacy, and compliance with any mandates or orders. This approach can include:

FUTURE APPLICATIONS

Having these policies and framework in place is critical for vendors working with operators as they roll out next-generation networks, but in addition, there must exist the solid experience and knowledge to back it up.

Implementing an enhanced security plan

Operators need to ensure subscriber and other data is secure within the confines of their network as well as when data traverses public or private clouds. By implementing an enhanced security plan, operators can protect sensitive data, as well as the software and services used to store and process that data and to apply it to their needs.

This strategy would incorporate the principles of the shared model of responsibility outlined above and go further through alignment with industry security frameworks and standards in order to bring the highest levels of assurance to customers.

This strategic approach includes providing industry-leading secure services and solutions designed to ensure the confidentiality, integrity, and availability of our own data and our customers' data and systems, against the fast-evolving threats of cyber criminals, hackers and other forms of intrusion and disruption.

Security should never be an afterthought and teaming up with a partner that's serious about security and has been delivering a strong solution to its customers is critical for operators as they move into the world of 5G and beyond.

ADVANCED CONTENT

Transmission Efficiency (Data Communications and Networking)

One objective of a data communication network is to move the highest possible volume of accurate information through the network. The higher the volume, the greater the resulting network's efficiency and the lower the cost. Network efficiency is affected by characteristics of the circuits such as error rates and maximum transmission speed, as well as by the speed of transmitting and receiving equipment, the error-detection and control methodology, and the protocol used by the data link layer.

Each protocol we discussed uses some bits or bytes to delineate the start and end of each message and to control error. These bits and bytes are necessary for the transmission to occur, but they are not part of the message. They add no value to the user, but they count against the total number of bits that can be transmitted.

Each communication protocol has both information bits and overhead bits. Information bits are those used to convey the user's meaning. Overhead bits are used for purposes such as error checking and marking the start and end of characters and packets. A parity bit used for error checking is an overhead bit because it is not used to send the user's data; if you did not care about errors, the overhead error checking bit could be omitted and the users could still understand the message.

ADVANCED CONTENT

Transmission efficiency is defined as the total number of information bits (i.e., bits in the message sent by the user) divided by the total bits in transmission (i.e., information bits plus overhead bits). For example, let's calculate the transmission efficiency of asynchronous transmission. Assume we are using 7-bit ASCII. We have 1 bit for parity, plus 1 start bit and 1 stop bit. Therefore, there are 7 bits of information in each letter, but the total bits per letter is 10 (7 + 3). The efficiency of the asynchronous transmission system is 7 bits of information divided by 10 total bits, or 70 percent.

In other words, with asynchronous transmission, only 70 percent of the data rate is available for the user; 30 percent is used by the transmission protocol. If we have a communication circuit using a dial-up modem receiving 56 Kbps, the user sees an effective data rate (or throughput) of 39.2 Kbps. This is very inefficient.

We can improve efficiency by reducing the number of overhead bits in each message or by increasing the number of information bits. For example, if we remove the stop bits from asynchronous transmission, efficiency increases to 7/9, or 77.8 percent. The throughput of a dial-up modem at 56 Kbps would increase 43.6 Kbps, which is not great but is at least a little better.

ADVANCED CONTENT

The same basic formula can be used to calculate the efficiency of synchronous transmission. For example, suppose we are using SDLC. The number of information bits is calculated by determining how many information characters are in the message. If the message portion of the frame contains 100 information characters and we are using an 8-bit code, then there are 100 x 8 = 800 bits of information. The total number of bits is the 800 information bits plus the overhead bits that are inserted for delineation and error control. Figure 4.9 shows that SDLC has a beginning flag (8 bits), an address (8 bits), a control field (8 bits), a frame check sequence (assume we use a CRC-32 with 32 bits), and an ending flag (8 bits). This is a total of 64 overhead bits; thus, efficiency is 800/(800 + 64) = 92.6 percent. If the circuit provides a data rate of 56 Kbps, then the effective data rate available to the user is about 51.9 Kbps.

This example shows that synchronous networks usually are more efficient than asynchronous networks and some protocols are more efficient than others. The longer the message (1,000 characters as opposed to 100), the more efficient the protocol. For example, suppose the message in the SDLC example were 1,000 bytes. The efficiency here would be 99.2 percent, or 8,000/(8000 + 64), giving an effective data rate of about 55.6 Kbps.

The general rule is that the larger the message field, the more efficient the protocol. So why not have 10,000-byte or even 100,000-byte packets to really increase efficiency? The answer is that anytime a frame is received containing an error, the entire frame must be retransmitted. Thus, if an entire file is sent as one large packet (e.g., 100K) and 1 bit is received in error, all 100,000 bytes must be sent again. Clearly, this is a waste of capacity. Furthermore, the probability that a frame contains an error increases with the size of the frame; larger frames are more likely to contain errors than are smaller ones, simply due to the laws of probability.

ADVANCED CONTENT

Thus, in designing a protocol, there is a trade-off between large and small frames. Small frames are less efficient but are less likely to contain errors and cost less (in terms of circuit capacity) to retransmit if there is an error.

Throughput is the total number of information bits received per second, after taking into account the overhead bits and the need to retransmit frames containing errors. Generally speaking, small frames provide better throughput for circuits with more errors, whereas larger frames provide better throughput in less-error-prone networks. Fortunately, in most real networks, the curve shown in Figure 4.12 is very flat on top, meaning that there is a range of frame sizes that provide almost optimum performance. Frame sizes vary greatly among different networks, but the ideal frame size tends to be between 2,000 and 10,000 bytes.

What is IoT?

https://www.youtube.com/watch?v=LIhmzVL5bm8

IoT Tool kits

http://iotservicekit.com/

http://tilestoolkit.io/

EDUCATION

IoT security checklist:

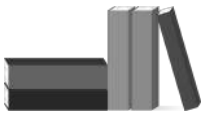
https://www.enisa.europa.eu/news/enisa-news/your-must-have-iot-security-checklist-enisas-online-tool-for-iot-and-smart-infrastructures-security

MOOCS:

- Introduction to Computer Networking - Standford University
- Fundamentals of Network Communication - Coursera
- Smart Device & Mobile Emerging Technologies - Coursera

EXTERNAL MANUALS FOR MORE INFORMATION:

- Networking Fundamentals - Cisco
- Network-based communication for Industrie 4.0 - Plattform Industrie 4.0
- Computer networking fundamentals - Study
- Communication Networks - Samson



BIBLIOGRAPHY

- *Importance of Communication Networks*. Retrieved from https://study.com/academy/lesson/importance-of-communication-networks.html
- *Networking Fundamentals*. (2006). Retrieved from https://www.cisco.com/c/dam/global/fi_fi/assets/docs/SMB_University_120307_Networking_Fundamentals.pdf
- *Benefits of computer networks.* Retrieved from https://www.nibusinessinfo.co.uk/content/benefits-computer-networks
- Cope, S. (2018). *Basic Networking Concepts-Beginners Guide*. Retrieved from http://www.steves-internet-guide.com/networking/
- *Top 5 Computer Networking Skills You Need to Learn Today* [Updated 2019]. (2019). Retrieved from https://potomac.edu/the-top-5-skills-needed-to-become-a-computer-network-professional/
- *Top 10 skills you need for a high-paying IoT career.* (2018). Retrieved from http://techgenix.com/iot-career-skills/

SELF APPRAISAL

- ★ After reading this text, do I have a clear idea of what Network Communication is?
- ★ What skills should I improve in my work?

- ★ Do I know the benefits that Network communication can bring to my company?
- ★ How could I detect any training need for my team?