Cursul 1

Nivelul este un subcapitol de retelistica

**1 Phisical**-se ocupa de mediile de transmisie, adica UTP, cablu coaxial, fibra optica protocoale wireless +bluetooth etc

UTP cca 100 m, coax 500 m

fibra optica - cativa km

**Nivelul 2** Data Link

MAC este o adresa cu urmatoarele caracteristici

-are 48 biti ( 2 \* 24 biti)

-este exprimata hexazecimal

Primul este campul producatorului

ICAN

Al doilea este un camp de 24 biti si contine serialul placii de retea propriu zise

**Nivelul 3** Network

Se ocupa cu adresarea liniara si adresare ierahica

Adresarea ierahica foloseste grupe de cifre care au semnificatii importante in procesul de dirijare a semnalului de la sursa la destinatie

IP = Internet Protocol

32 biti si poate fi binar sau decimal.Are 2 campuri dinamice

Adresa de clasa C

N.N.N.H

N= campul network

H= host

Exemplu :

192.168.8.100

192.168.8

cea cu zero este adresa fara nici un host iar cea cu 1 este adresa de broadcast

Adresa de clasa A

N.H.H.H

Adresa de clasa B ; N.N.H.H 64k noduri

Protocol MAC = adresare liniara, util pt retele cu putine noduri

Protocol IP = adresare ierarhica

Atribuirea IP-urilor

-static ( introducerea de catre utilizator, manual , a IP ului in fiecare nod dintr-o plaja de Ipuri pe care le furnizeaa rooter ul) NU ESTE PRACTIC

-alocare automata DHCP dynamic host configuration protocol >=2

Fiecare nivel are echipamente specific

1-mediile de transmisie

2-switch-are o intrare si mai multe iesiri

Are doua roluri:

-un rol este de a distribui semnalul catre mai multe iesiri din aceasi intrare

-un al rol este de a extinde distanta la care se poate folosi un mediu de transmisie

3-router-functioneaza similar cu sistemele de semafoare

**Nivelul 4-transport**

Ip v4/v6

TCP- transfer control protocol – ajung sigur la destinatie

UTP – user datagram protocol-nu ofera siguranta, dar se repeta cu o frecventa mai mare

**Nivel5 – sesiune**

**Nivel 6 = presentation** – datele de la sursa trebuie sa ajunga in aceeasi forma la destinatie(formatul poate fi interpretat si la destinatie)

Are loc criptarea si arhivarea

Cursul 2- Firewall

Portul este alocararea unui canal de transimtere de date intre noduri caruia se aloca un anumit numar.

Port deschis inseamna ca acel port care a fost asigurat unei activiati este functional -> portul permite traficul de date

Port inchis -> portul nu permite traficul de date

Gestionarea acestor porturi este facuta de un dispozitiv numit FIREWALL.

Firewall permite administrarea unor porturi, traficul prin ele sa fie inchis sau deschis -> instrument de gestiune a securitatii portului respectiv.

Pentru linux folosim un firewall ce poarta numele de FIREWALLD.

Instalarea unui server de aplicatie de tip toolget:

**Systemctl ->**

**-**are un numar de alte componente adaugate si cu care se poate verifica si administra un anumit serviciu intr-o masina linux.

**-**este un ansamblu de comenzi cu care se administreaza un serviciu linux

**Serviciu = functionalitate/aplicatie**

**Systemctl status firewalld**

**IDF = Intermediary Distribution Facility) – echipament de repartizare a traficului dar nu principal adica putem avea mai multe switchuri**

**IDF -> MDF= Main Distribution Facility = switch-ul principal al retelei unde ma aflu**

**IDF -> MDF-> POP ( Point of presence) = locul in care intra reteaua publica in interiorul unei cladiri de unde incepe reteaua locala.**

**ISP = Internet service provider**

**LAN = Local Area Network= reteaua locala care va fi separata de reataua publica prin PoP**

**PoP reprezinta limita retelei noastre.**

**NS(laptop) -> IDF(switch secundar) -> MDF(switch principal) -> PoP(aici s-a terminat retaua locala) -> ISP(furnizorul meu de internet)**

Firewalld

Verificare status

Activare, dezactivare, pornire, oprire, reload FirewallD

Afișare porturi deschise

Verificare un anume port

Adaugarea temporară a unui port pentru un serviciu (cu exemplu):

Adaugarea permanentă a unui port pentru un serviciu (cu exemplu):

Închiderea temporară a portului pentru un serviciu

Închiderea permanentă a portului pentru un serviciu (cu exemplu)

Verificare trafic rețea

Allow a service

Resources

Verificare status

**systemctl** status firewalld

#output

Dacă nu e instalat, se instalează cu yum

**yum install -y firewalld**

Activare, dezactivare, pornire, oprire, reload FirewallD **systemctl enable firewalld**

**systemctl disable firewalld**

**systemclt start firewalld**

**systemctl stop firewalld**

**systemctl restart firewalld**

Afișare porturi deschise

**firewall-cmd --list-ports**

Verificare un anume port

**netstat -na | grep "10311"**

Sau

**netstat -tlnap | grep 61000**

Adaugarea temporară a unui port pentru un serviciu (cu exemplu):

**firewall-cmd –add-port=5672/tcp**

**systemctl restart firewalld**

Adaugarea permanentă a unui port pentru un serviciu (cu  exemplu):

**firewall-cmd --zone=public --permanent --add-port=5672/tcp**

**systemctl restart firewalld**

Închiderea temporară a portului pentru un serviciu **firewall-cmd --remove-port=port-number/port-type**

**systemctl restart firewalld**

Închiderea permanentă a portului pentru un serviciu (cu exemplu) **firewall-cmd --zone=public --permanent --remove-port=10120/tcp**

**systemctl restart firewalld**

Verificare trafic rețea

**netstat -tlnap**

#output

#de la stanga la dreapta a treia coloana e importanta, arata lista de IP-uri+porturi si de acolo se porneste in analiza # doua tipuri de state pentru un port, Listen sau Established

#de revenit mai detaliat

Allow a service

#Deschiderea pentru un serviciu, nu pentru un port

#exemplu pentru postgres

#de aici

https://computingforgeeks.com/how-to-install-postgresql-11-on-centos-7/

#comenzi

**firewall-cmd --add-service=postgresql --permanent**

**firewall-cmd --reload**

#sau

**systemctl restart firewalld**

#output

Resources

https://www.thegeekdiary.com/5-useful-examples-of-firewall-cmd-command/

**Cursul 4**

Conectarea SSH se poate face folosind user+parola sau o cheie.

Tomcat este un sever intermediar care se ocupa cu asigurarea functionalitatii unei aplicatii facute in Java.Codul nu este sufficient ca aplicatia sa functioneze.

Vorbim despre 2categorii diferite de programe:

1)cele de infrastructure:

-servere de aplicatii web, Toomcat, Wildfly, Windows server

-base de date:Oracle, MySQL

AD( Active directory ) este un server are gestioneaza toti utilizatorii dintro retea.

2)APlicatiile propriu-zise

Tomcat.inp.service deschis cu . vim tomcat.inp.service

Java – mediu care permite rularea programelor scrise pt el

Java runtime environment = mediu de executie java

Un VPN este o infrstructura cuprinzand diverse tipuri de noduri de retea care functioneaza ca un tot unitar si care sunt securizate intrun not unitar si sunt accesibile din exterior cu ajutorul unor programre speciale numite client VPN.

**Java -version**

**Vim tomcat.siima-dms.service**

Conceptul de redundanta presupune replicarea functionalitatii unui sistem de catre un sistem complementar astfel incat in caz de ncesitate serviciul furnizat de sistemul principal serviciului respective sa I se asigure continuitate.

**Nmcli** – afiseaza toate datele ce tin de conectivitate pe diverse tipuri de interfete intre masina mea si alte tipuri de masini

Gateway este punctul prin care toate nodurile din retea ies mai departe ( mai expuse).