Nätverk

Hur de fungerar och Cybersäkerhet

Uttryck att känna till 1

- Hosts

Alla enheter som är kopplade till ett nätverk och har en IP-adress är en host. Dessa har i uppgift att erbjuda eller ta emot resurser och tjänster inom ett nätverk. Kan jämföras med vad ”vardagligt” folk anser att en server är. Din telefon eller dator kan även agera host i vissa situationer.

- Client

Client är de som skickar förfrågningar på olika sätt och begär data. När man surfar internet med en webbläsare agerar din enhet och dess webbläsare som client när den efterfrågar olika information. Saker som vanligtvis ses som clients är mobiltelefoner, datorer, smartklockor och internetskrivare.

Alla hosts kan agera som en client men alla clients kan inte agera som en host

- Server

En host (kan även agera client) som lagrar information på något sätt. Finns flera olika sorter av servrar med olika syften. En server kan även ha flera olika syften. Kan jämföras med uppslagsverk som din client vill läsa i för att få information.

- Gateway

Vägen ut till internet. Sitter oftast ihop med hemmaroutrar men på skola eller i organisationsnät kan man ha olika gateways till olika delar av nätet. Den kan även sitta någon helt annan stans än i eller vid routern.

Uttryck att känna till 2

- IP – Internet protocol

Internet protocol enkapsulerar och förflyttar data mellan två platser över internet. Detta behöver inte innebära att det bara är två hosts. Eftersom samma meddelande kan skickas till flera hosts (via broadcast & multicast).

- Ip- address

Det finns två olika versioner av IP-adresser, IPv6 och Ipv4.

IPv4 består av 0 och ettor på en 32 bits rad presenterad på binär form. Men så som man brukar läsa dem är de i numerisk form exempelvis: 192.57.28.10.

IPv6 är 128 bits lång och presenteras på hexadecimalform översatt från binär form. Exempelvis: 2001:0df2::06ee:0000:0f11 .Dropping leading zero betyder att man tar bort de inledande 0:orna i bitarna, saknas därför information förutsätter datorn att det ska in en 0:a, är det bara 0:or i följd kan man ersätta detta med :: men kan bara göras en gång i adressen (zero compression).

- TCP - Transmission Control Protocol

Protokoll som upprätthåller en transportväg mellan hosts, kontrollerar att all data flyttats och utgör en så kallad trevägshandskakning. TCP kan kontrollera att all data förflyttats och inte skadats på vägen. Används i de flesta fallen. Arbetar på lager 4 i OSI modellen.

- UDP - User Datagram Protocol

Protokoll som nästan alltid används när TCP inte används, om TCP kan ses som att den bygger en väg och sen låter all data åka på vägen så är UDP som ett maskingevär skjuter all data åt alla håll och hoppas att måltavlan träffas. Snabbare vid överföring av data men saknar möjlighet att kontrollera om all data flyttats över och om den skadats eller förändrats under vägen till mottagaren.

- MAC Adress

Fysisk adress som alla hosts har och är unik, tillskillnad från IP-adress som kan ändras så är alltid MAC-adressen den samma. 48 bits lång kan se ut på följande sätt: A1:B4:F6:CC:DD:23. (Hexadecimal Form).

Uttryck att känna till 3

- **HTTP – Hypertext Transfer Protocol**

HTTP är det grundläggande protokollet som används för att överföra data på webben. Det är det som gör att webbsidor kan laddas i din webbläsare när du skriver in en URL eller klickar på en länk. Grundtanken var att överföra HTML sidor till hosts. Allt som använder http för att överföra information skickar den i plaintext. Det vill säga vanlig text som inte är skyddad alls.

- **HTTPS - Hypertext Transfer Protocol Secure**

Togs fram när man insåg bristerna i http som gör det användbart för kriminella att utläsa information som är konfidentiell. HTTPS är samma process som http men det som skickas med https är ”secure”. Om man läser ut ett https paket så skulle det kunna stå: ” jksf sda#9ew0 +\ ?783 ” istället för: ” Mitt lösenord är lätt ” Det vill säga att innehållet är krypterat.

Hur text krypteras är komplicerat men bygger på att samma text inte översätts till samma sak varje gång man skickar saker, det gör att krypteringen är säkrare.

- **FTP – File Transfer Protocol**

Är ett nätverksprotokoll som används för att överföra filer mellan en dator (klient) och en server via internet. Det kan användas både för att ladda ner filer från en server till en dator och för att ladda upp filer från en dator till en server. När en fil laddas ner skapas en kopia på din dator medan originalet finns kvar på servern. FTP används ofta för att ladda ner stora filer som spel, program eller uppdateringar. För bättre säkerhet används varianter som SFTP (Secure FTP) och FTPS (FTP Secure) som krypterar datan vid överföring.

- **NAT – Network Translation Protocol**

Gör att en router kan översätta privata IP adresser på sitt eget nätverk till publika IP adresser som den använder för att sköta kommunikation med internet.

- **ICMP – Internet Control Message Protocol**

Protokoll som hjälper till med felsökning av nätverksenheter och dess konfigurering. Om man skickar data som ej kommer fram rapporteras det till avsändaren och genom kända kommandot ping kan man se om man har en öppen väg till destinationen man söker.

Uttryck att känna till 4

- LAN - Local Area Network

Ett Local Area Network är ett nätverk som kopplar ihop enheter inom ett begränsat geografiskt område. Exempelvis, hemnätverk och skola. Traditionellt är ett LAN fysiskt kopplat med nätverkskablar men kan även innehålla trådlösa delar. En fysisk koppling mellan enheter erbjuder hög prestanda och låg latens samt bra översikt och kontroll över nätverket.

- WLAN- Wireless LAN

Trådlös del/version av LAN, där man inte behöver ha en fysisk koppling för att använda. I stället Wi-Fi teknik för att skicka data mellan host och clients istället för fysiska kopplingar. WLAN är mer flexibelt men har oftast lägre prestanda än en fysisk koppling.

- WAN- Wide Area Network

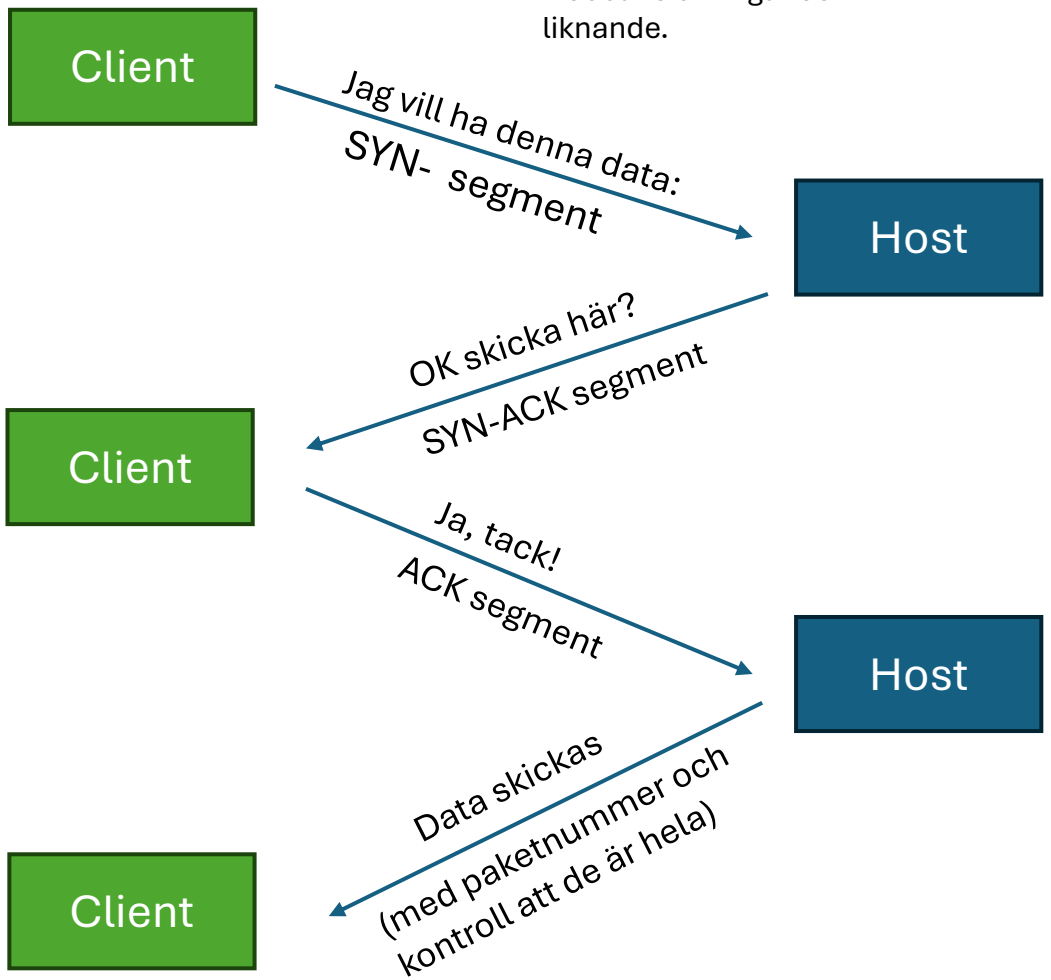
Ett WAN är ett nätverk som täcker ett betydligt större geografiskt område än ett LAN. Det består av flera sammanlänkade LAN som kommunicerar och samarbetar på olika sätt. Exempel på WAN är kommunnätverk och skolnätverk, där användare kan ansluta sina enheter på olika platser inom en stad och få tillgång till samma nätverk även om de byter geografisk placering. WAN (och subnetting) är anledningen till att de olika kommun nätverken kan kommunicera med varandra på ett effektivt sätt.

- DNS – Domain Name Server

Databaser som är centrum för tekniken som gör att du slipper skriva in IP adresser när du ska besöka olika hemsidor. Databasen innehåller tabeller där man jämför hemsidor och deras IP adresser åt båda håll. Skriver du in Google.com kommer DNS servern översätta det till Googles IP adress till exempel 8.8.8.8. och vice versa. Finns en säkrare version som är standard att använda idag. DNSSEC där kryptering och samarbeten mellan servrar försäkrar om att någon inte ändrat på innehållet i servrarna och skickar folk till fler platser.

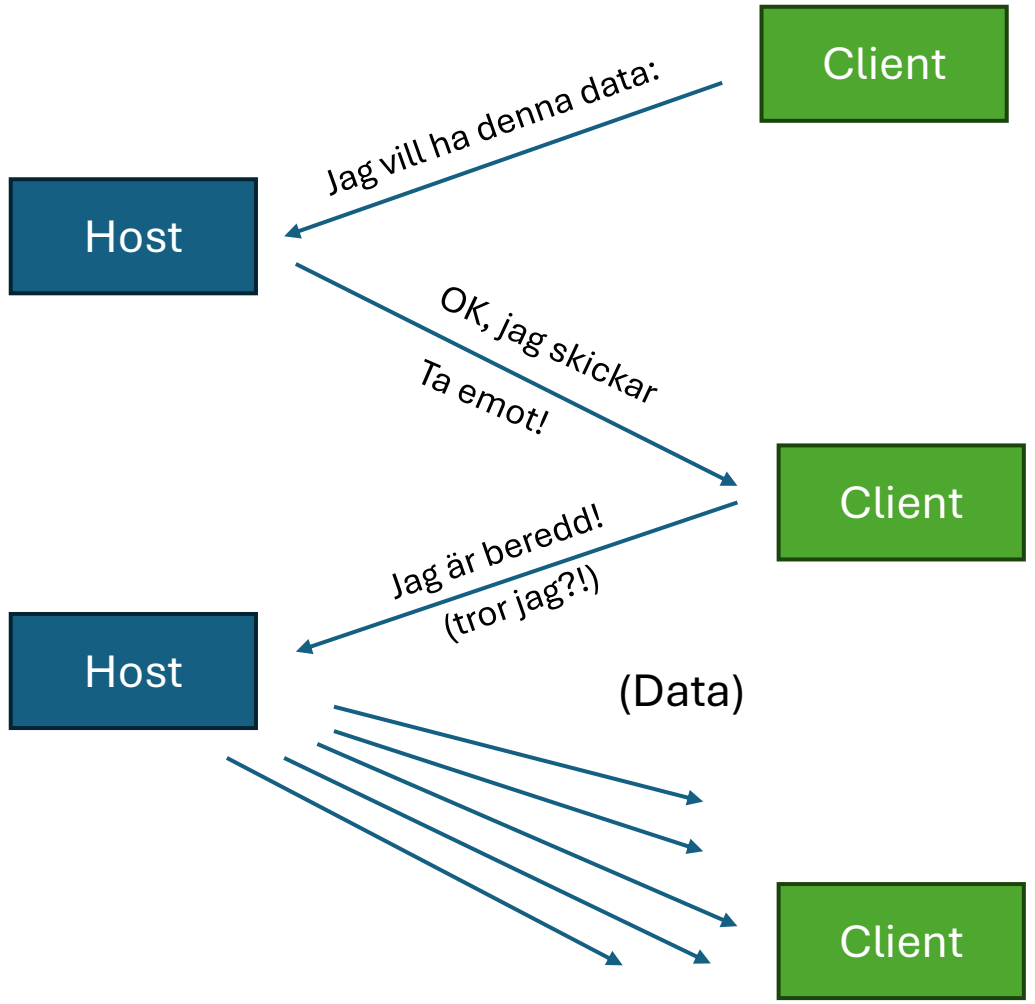
TCP

TCP tar tid men kan kontrollera att data som tas emot är hel och att den flyttas på ett korrekt sätt, kan ses som en konversation där mottagare och sändare, används ofta vid webbanslutningar och liknande.



UDP

UDP är snabbt men kan inte kontrollera om all data är hel eller tas emot. Används ofta vid streaming av ljud och bild, om data förloras börjar det buffra.



OSI (Open System Interconnect) – Modellen (enkel)

- 7 lager som förklarar och kartlägger data som skickas över nätverk, räknar nedifrån och upp.
- Beroende på applikation och typ av förfrågan kan flera av lagren vara sammanhängande och att ett protokoll tar hand om flera processer i OSI - modellen.
- **Lager 5-7.**

Data är uppdelat i 3 lager (Viktigaste delen eftersom den innehåller all information du vill ha) den brukar vara sammanhängande men kan även vara uppdelad i vilken session den tillhör, hur den ska presenteras och vilken applikation som ska användas.

- **Lager 4**

Segment är transportmetoder ex TCP & UDP

- **Lager 3**

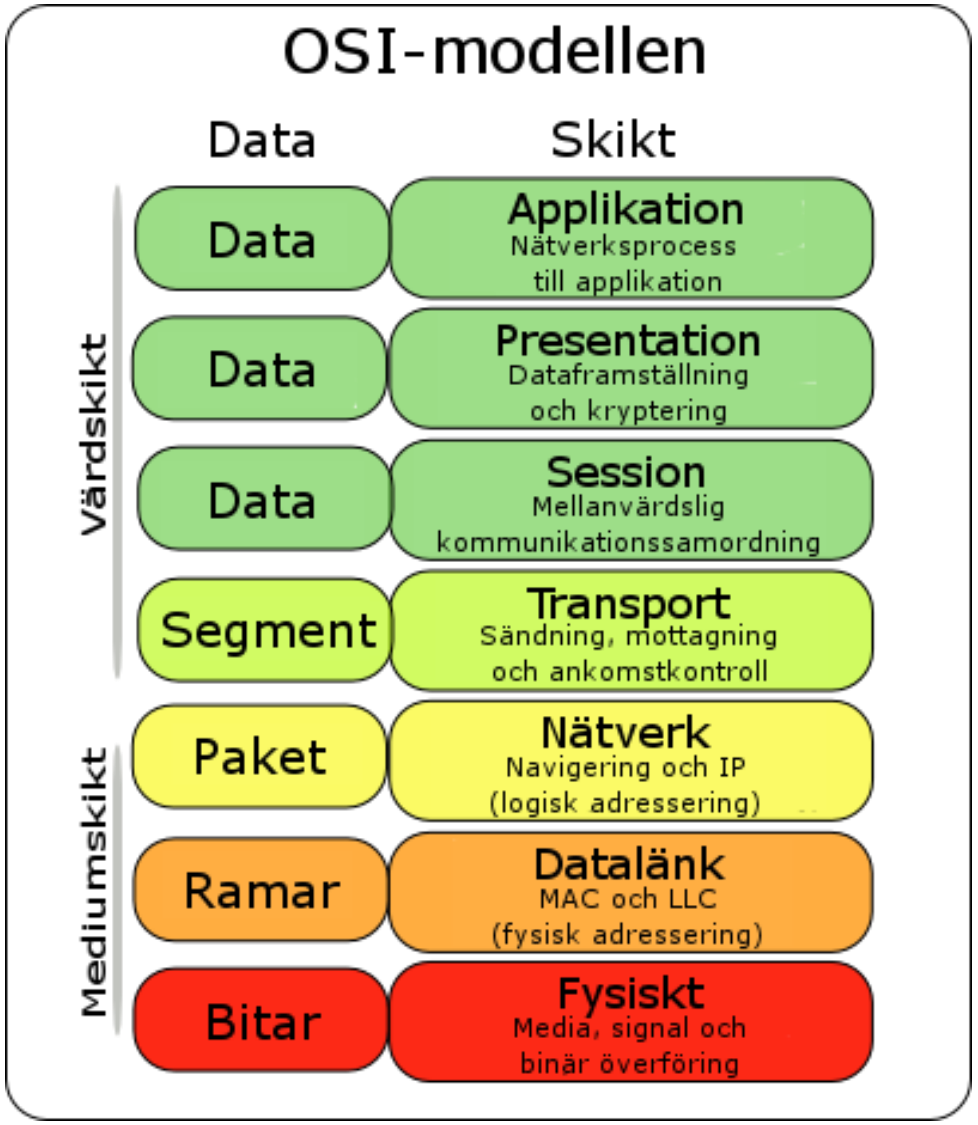
Paketen är den logiska adressering med navigering och IP- adress

- **Lager 2**

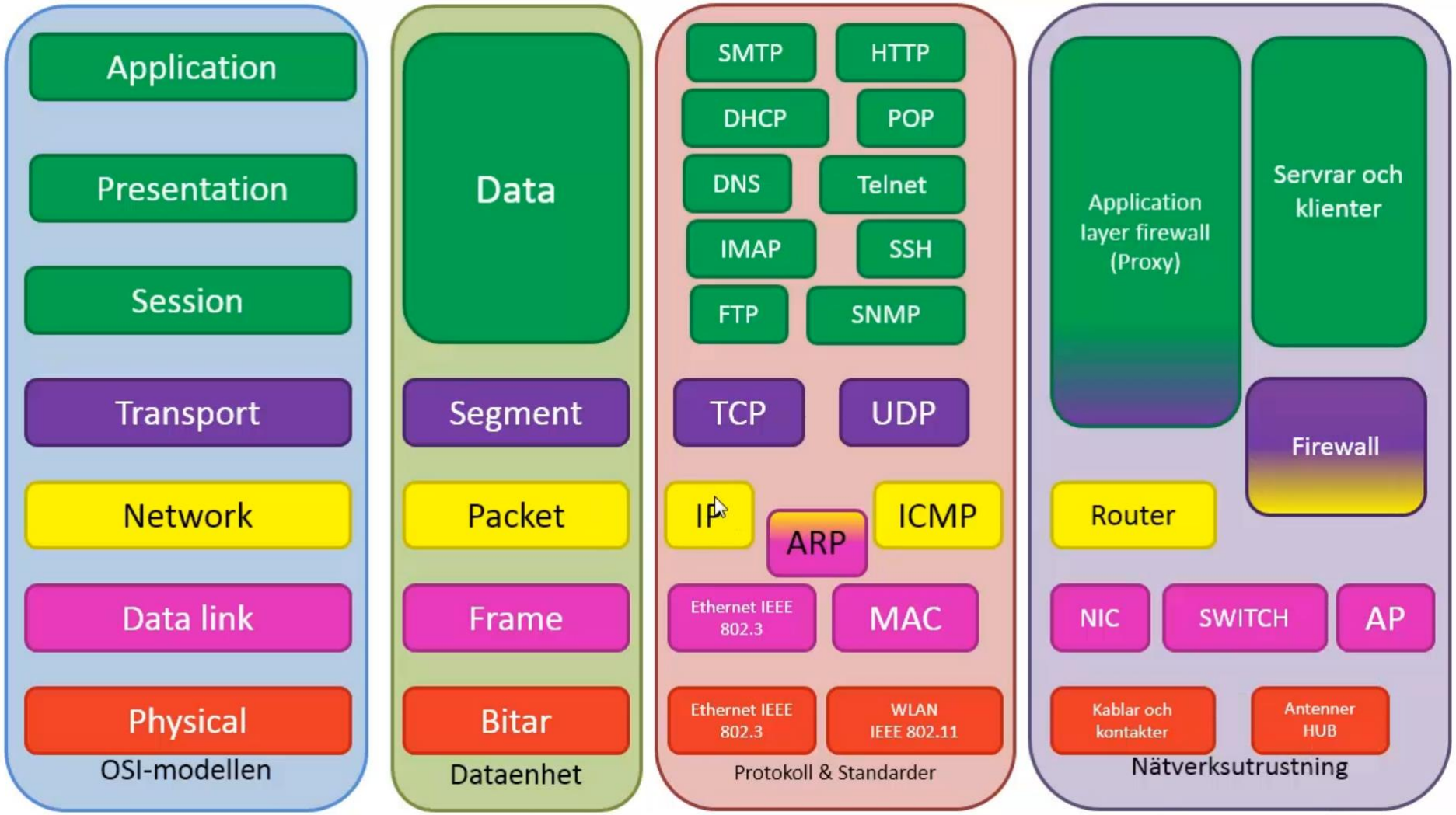
Datalänken är Fysisk adressering, vem data tillhör. Oftast används MAC-adress

- **Lager 1**

Fysisk koppling, exempel är Ethernet, WLAN (Wi-fi) & Bluetooth.



Exempel på processer och lager i OSI-modellen



Vad är ett nätverk och hur ser de ut?

- **Vilken utrustning används/krävs?**
- **Router**

Har i uppgift att föra all kommunikation med internet vidare åt dig. När man frågar om information eller ska ge ut information på internet pratar man viskleken med routern som senare skickar meddelandet vidare och tar emot meddelanden. Eftersom den oftast används som Default Gateway.Se bild .

- **Accesspunkter**

Enheter som skapar trådlösa signaler till nätverket. För att köra ett WLAN(Wi-fi nätverk) krävs accesspunkter för att ge dig signaler. En hemmarouter fungerar som router och accesspunkt i ett.

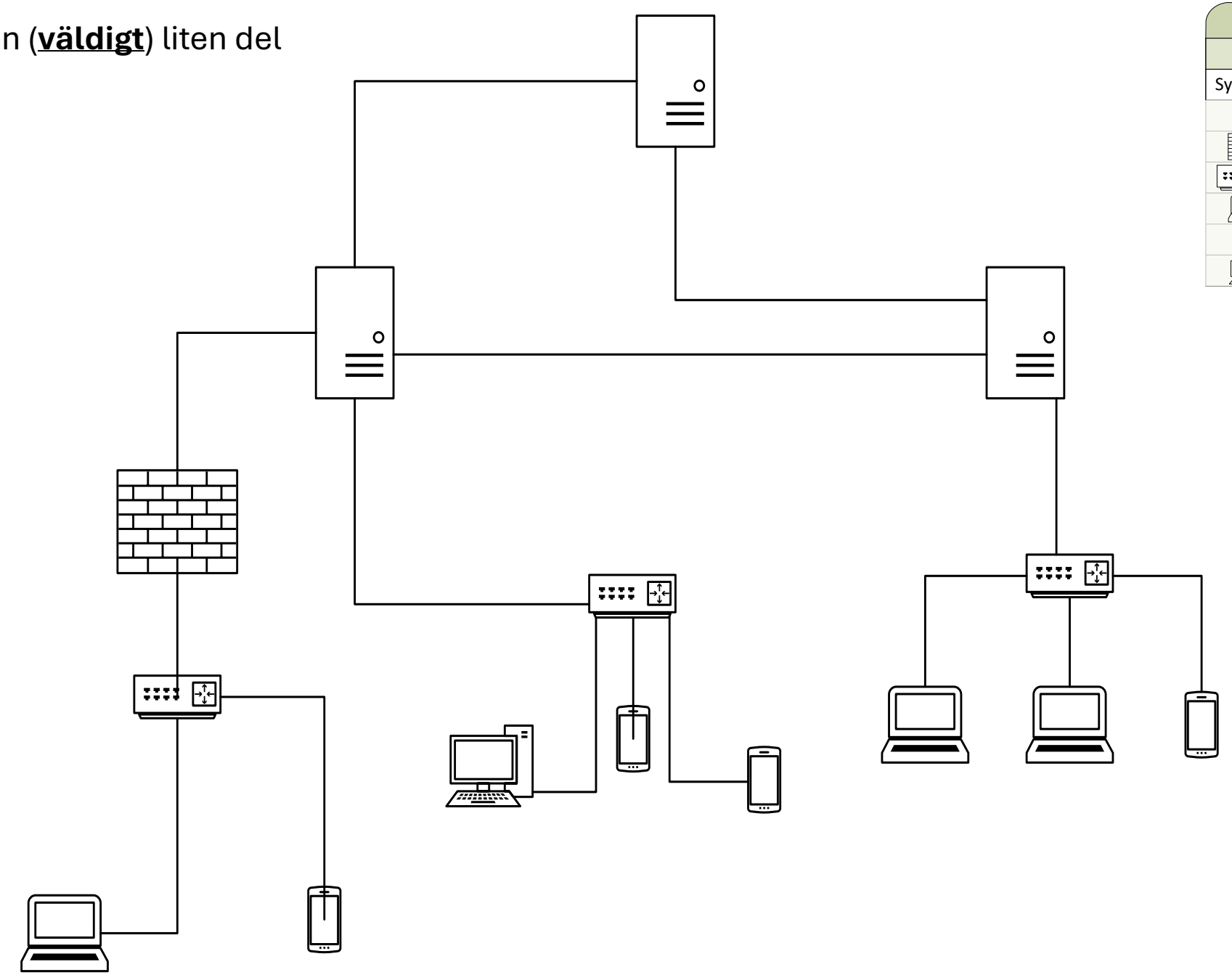
- **Switchar**

Boxar som används för att koppla ihop enheter i ett nätverk. Förlänger det trådade nätverket och ökar antalet enheter som kan kopplas till det. Väldigt smarta och kan hålla ordning på MAC-adresser och dela ut olika IP adresser till alla som ansluter via den.

- **Ethernetkablar**

Finns många olika modeller med olika standarder. Nätverkskablarna in i ditt Playstation, Xbox eller dator är av formen Ethernet. Nätverkskabel som är standard för kommunikation mellan hosts och router eller switch. För kopplingar högre upp i nätverksträdet används speciella ethernetkablar eller fiberkablar av olika sorter.

Förenklad bild av en (**väldigt**) liten del av Internet



Förklaring		
Underrubrik till förklaring		
Symbol	Antal	Beskrivning
	3	Server
	1	Brandvägg
	3	Router
	3	bärbar dator
	4	Smartphone
	1	PC

Default Gateway och Router Ex

(Helhetsbild)

Förenklat exempel på när dator A efterfrågar information på internet

(Tilldelar Session nummer x & sparar informationen om förfrågningen)

Jag (dator A) vill ha denna info {}

Jag (router session x) vill ha denna info {}

Internet

Jag (dator A) vill ha denna info {}

Jag (router session x) vill ha denna info {}

Här är info dator A vill ha {}

(Användning av data och loopen startar om)

Default Gateway (Router)

Här är info router (session x) vill ha {}

Dator A

Jag (dator A) vill ha denna info {}

Här är info dator A vill ha {}

Här är info router (session x) vill ha {}

(Letar efter host som frågade om info med session x i historik och hittar dator A)

(flödet börjar här)

Förenklat exempel på när dator A efterfrågar information på internet

(Tilldelar Session nummer x & sparar informationen om förfrågningen)

(Efterfrågan)

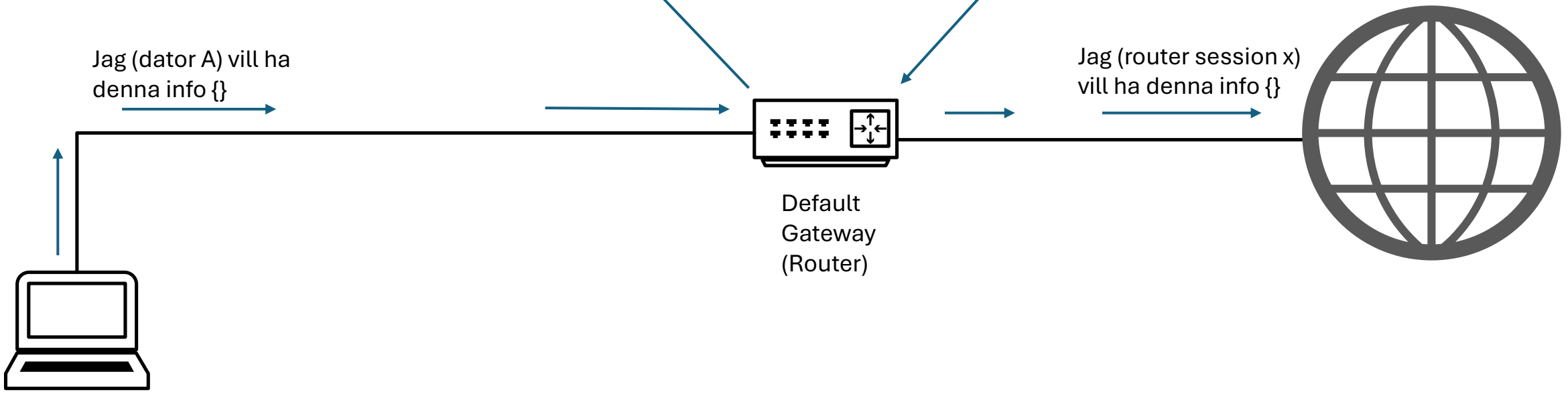
Jag (router session x) vill ha denna info {}

Jag (dator A) vill ha denna info {}

Internet

Jag (dator A) vill ha denna info {}

Jag (router session x) vill ha denna info {}



Default Gateway (Router)

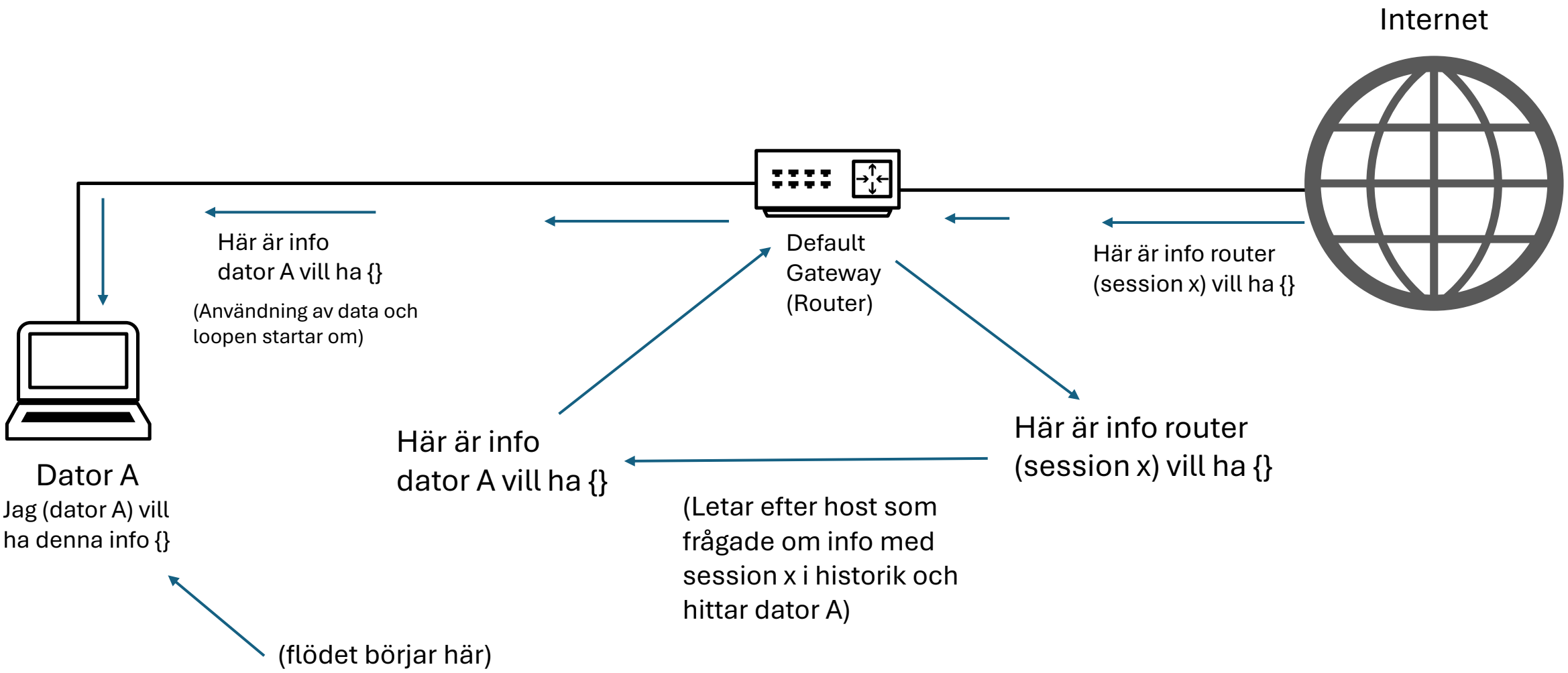
Dator A

Jag (dator A) vill ha denna info {}

(Flödet börjar här)

Förenklat exempel på när dator A efterfrågar information på internet

(Svar)



Hur kommunicerar man via nätverket?

- **TCP & UDP**

Används vid kommunikation runt på nätverk eller internet. För att bestämma hur data ska skickas. Se begrepp för mer information.

Typer av meddelanden:

- **Broadcast (Alla enheter)**

Ett meddelande in i ett nätverk som skickas ut till alla enheter i ett nätverk. I signalen står det vem den är menad för och alla som inte ska ta emot den avböjer signalen.

- **Multicast (Flera men inte alla enheter)**

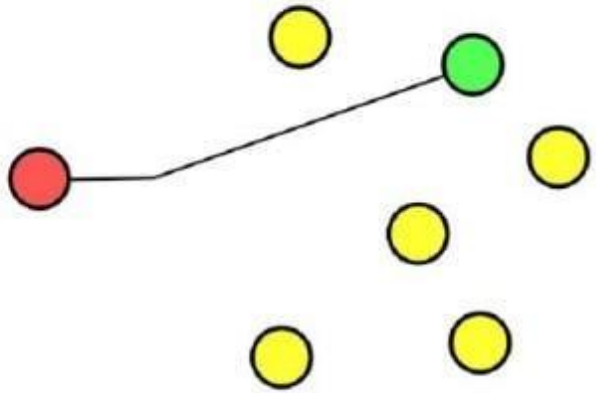
Meddelande som skickas till en viss grupp på ett nätverk och tas emot av alla som är med i gruppen.

- **Unicast (En specifik enhet)**

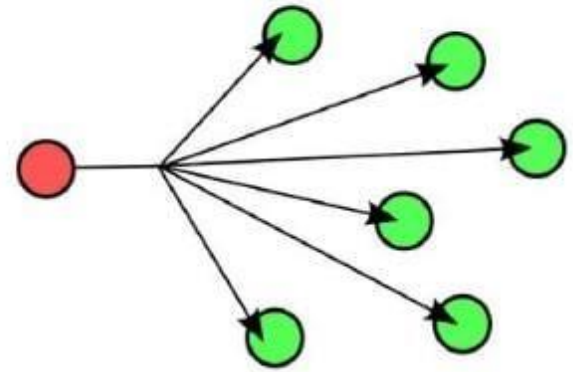
Meddelande som skickas till en specificerad enhet och tas emot av bara den enheten.

- **Anycast (Vilken enhets som helst)**

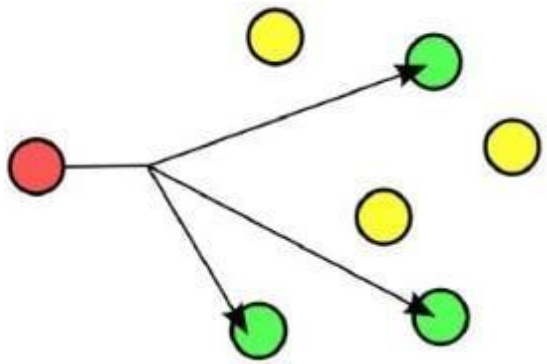
Meddelande in i ett nätverk som skickas in med avsikt att någon i nätverket ska ta emot den.



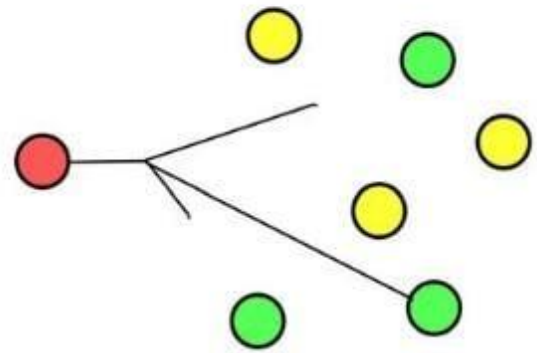
Unicast



Broadcast



Multicast



Anycast

Skillnad nätverk & Internet

- **Nätverken är lokala**

Ett LAN & WAN enskilt eller ihopkopplade är nätverk som man kommunicerar inom. Detta innebär att det kan finnas en fysisk skillnad på vart man befinner sig men beroende på hur nätverket är kopplat så är ni logiskt kopplade (det vill säga kopplade direkt mellan varandra på något sätt).

- **Internet**

Internet är en samling av sammankopplade nätverk där enheter kommunicerar via olika protokoll. Applikationer och hosts kan tillhöra det publika nätverket, vilket kan möjliggöra direkt kommunikation mellan client och host, ofta används brandväggar, proxyservrar eller andra mellanhandstjänster för säkerhet och lastbalansering. När man kommunicerar med enheter på privata nätverk, t.ex. ett hemmanätverk, sker kommunikationen oftast via en mellanhand i form av en tjänst eller genom att clienten egentligen kommunicerar med routern, som vidarebefordrar trafiken till den avsedda mottagaren.

Hur sker förflyttning av data över internet?

- **Sammanfattning:**

Förflyttning av data över internet sker genom ett nätverk av sammankopplade datorer och servrar. Data delas upp i små paket (Enkapsulering), som skickas från en avsändare till en mottagare. Dessa paket reser genom olika routrar och nätverk via den mest effektiva rutten. Protokoll som TCP/IP styr hur paketen skickas, tas emot och sätts ihop igen för att skapa den ursprungliga informationen.

- **Protokoll:**

Protokoll bestämmer hur något ska skickas, hur man ska hitta vägen dit och vad för något som skickas. Protokollen bestämmer reglerna som datorn ska följa för att möjliggöra kommunikation. (IP, TCP, UDP, HTTPS, FTP är alla olika protokoll)

- **Ports:**

De olika tjänsterna använder olika portar för att datorn ska kunna identifiera trafiken och nyttja den på ett effektivt sätt. Portar kan ses som dörrar och de olika tjänsterna (ex HTTP ,HTTPS, FTP & SSH) har varsin nyckel till sin egna dörr. Med hjälp av detta kan man analysera trafik och söka efter fel eller skadlig trafik. (Om en dörr står öppen utan att en applikation använt en nyckel kan man se det som att någon okänd kan gå ut och in ur dörren till datorn som den vill)

Hur sker förflyttning av data över internet? 2

- **Frames:**

När data skickas över internet delas den upp i mindre enheter som kallas **paket**. På nätverkslagret (Layer 3) adresseras paketen med IP-adresser, och på datalänklagret (Layer 2) paketeras de i **frames**, som innehåller MAC-adresser och felkontroll. Frames används inom det lokala nätverket, till exempel mellan din dator och din router. Routern packar upp framen, läser IP-adressen och skapar en ny frame för nästa hopp. Denna process upprepas genom hela nätverket tills paketet når sin destination. De tillägg som görs i varje lager följer OSI-modellens protokoll, vilket säkerställer att kommunikationen fungerar korrekt.

- **Enkapsulering**

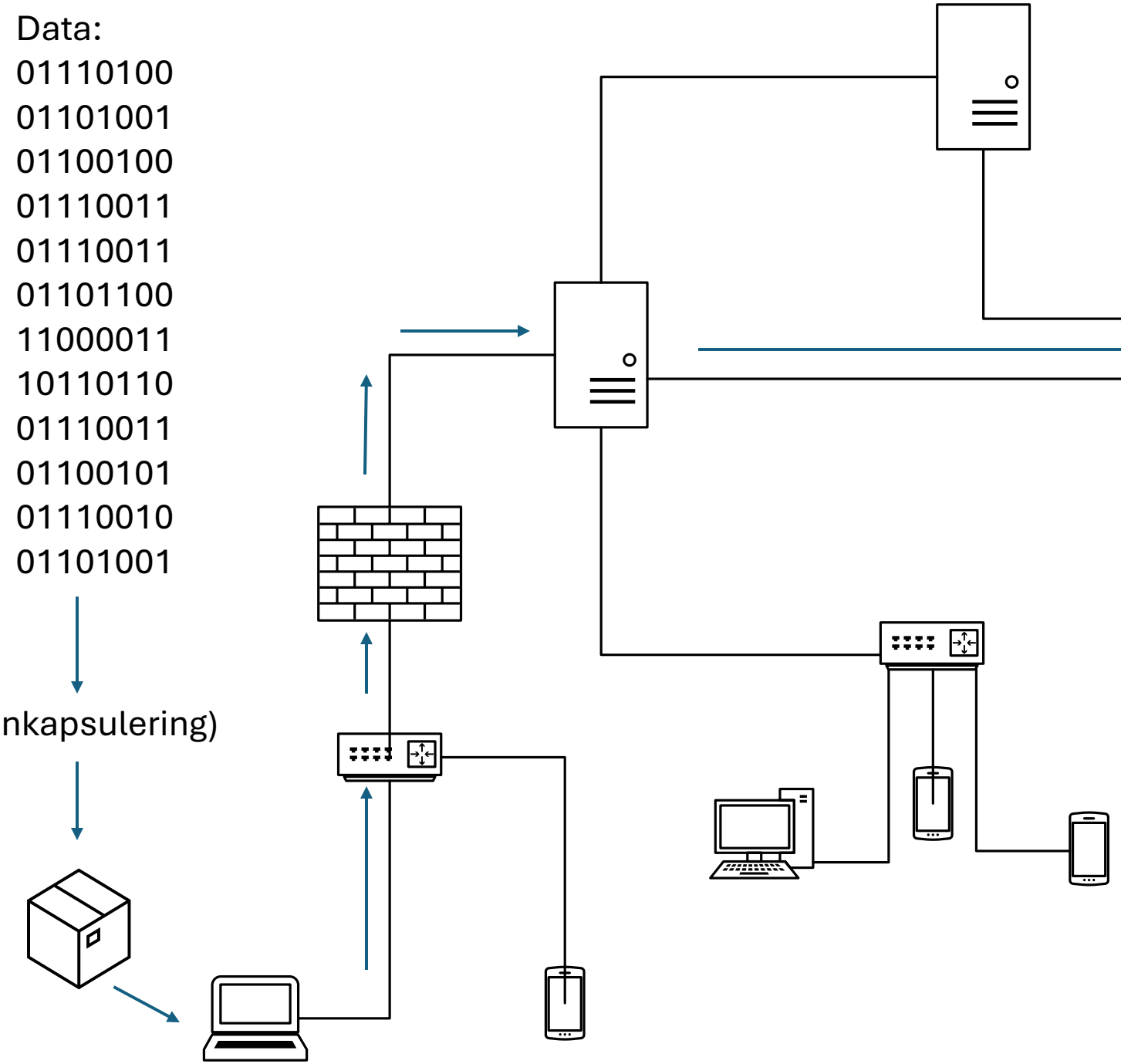
Process där data delas upp och packas ner med information i olika lager med de olika protokollens identifieringar och nödvändig information. Detta så att mottagaren kan packa upp paketet i omvänd ordning och förstå hur datan ska hanteras när den är mottagen. Kan jämföras med en julklapp inslagen i flera lager där varje lager presentpapper är instruktioner hur du ska bygga innehållet.

- **DNS / DNSSEC:**

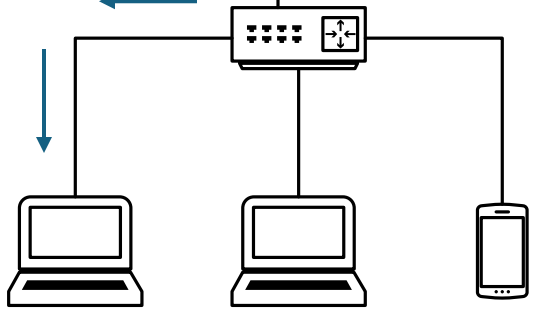
När du frågar om information på infomedia.orebro.se så frågar datorn första DNS servern ”Vart hittar jag den här hemsidan?”. DNS servern söker igenom sin lagring för att se om den vet vart den givna hemsidan finns. Om den inte finns skickar den upp i lager till nästa server i hierarkin som letar efter adressen. Hierarkin delas upp i root servrar som är högst upp och har koll på hur man tar sig till de olika second level servrarna. Second level är servrar som tillhandahåller .com .net .se med flera. Third och lower level är de som har specifika domännamn. En domän vid namn infomedia.orebro.se har .se i top level, orebro.se i second level och senare infomedia.orebro.se i third eller lower DNS.

Data:
01110100
01101001
01100100
01110011
01110011
01101100
11000011
10110110
01110011
01100101
01110010
01101001

(Enkapsulering)

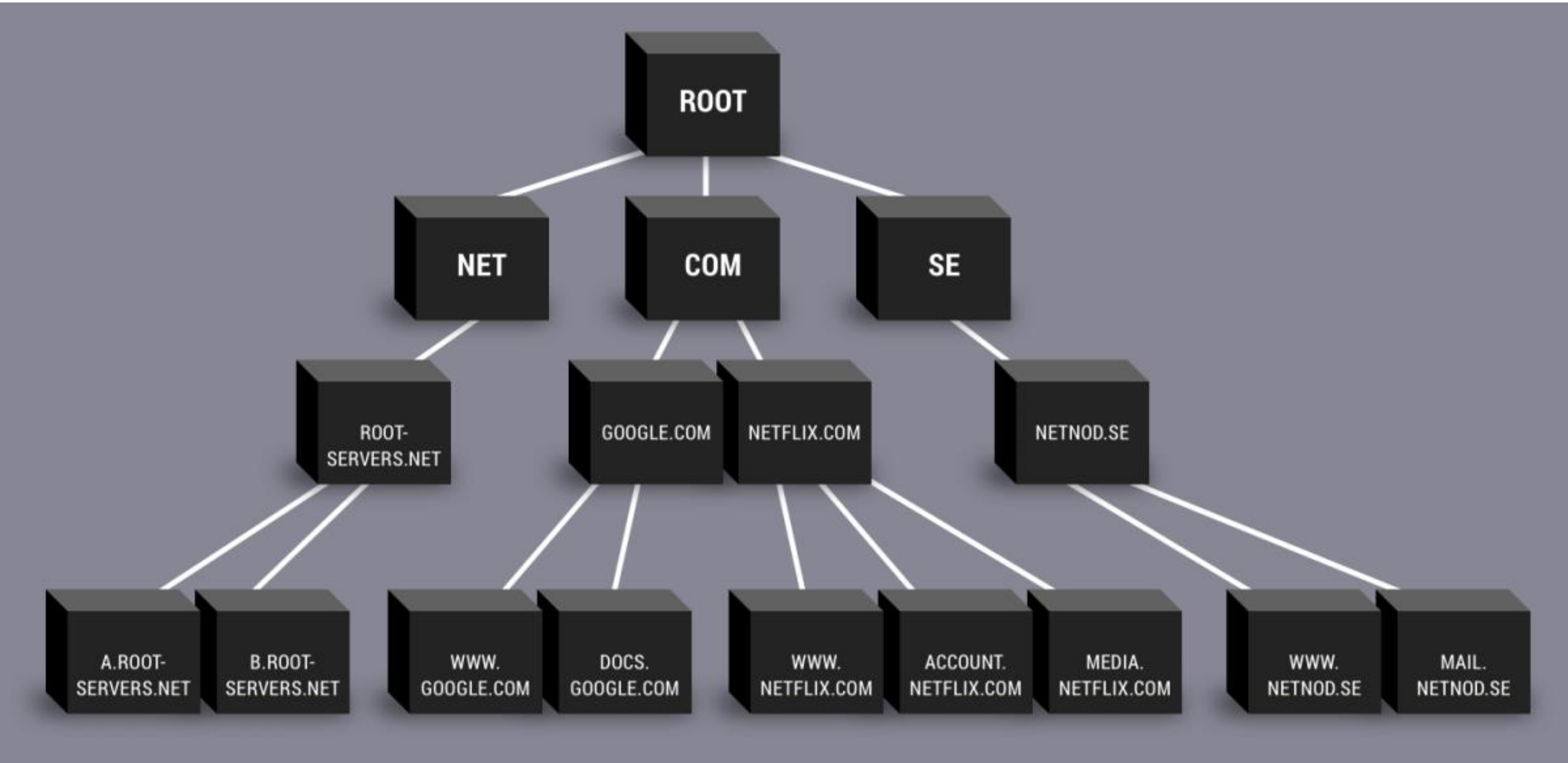


Förklaring		
Underrubrik till förklaring		
Symbol	Antal	Beskrivning
	3	Server
	1	Brandvägg
	3	Router
	3	bärbar dator
	4	Smartphone
	1	PC



(Uppackning och användning)

DNS/DNSSEC Hierarki



Cybersäkerhet

- Grundtankar CIA
- **Confidentiality**

Data ska vara konfidentiell och skyddas från obehörig åtkomst genom kryptering, åtkomstkontroller och autentisering.

- **Integrity**

Data ska ha integritet och vara säkerställt att den inte manipulerats eller öppnats innan. Görs ofta via checksum och hashfunktioner.

- **Availability**

Data ska vara tillgängligt till den mån som krävs. Se till att information och system är tillgängliga för behöriga användare när de behövs, genom redundans, säkerhetskopiering och skydd mot attacker (t.ex. DDoS).

Cybersäkerhet

Vanliga Attacker

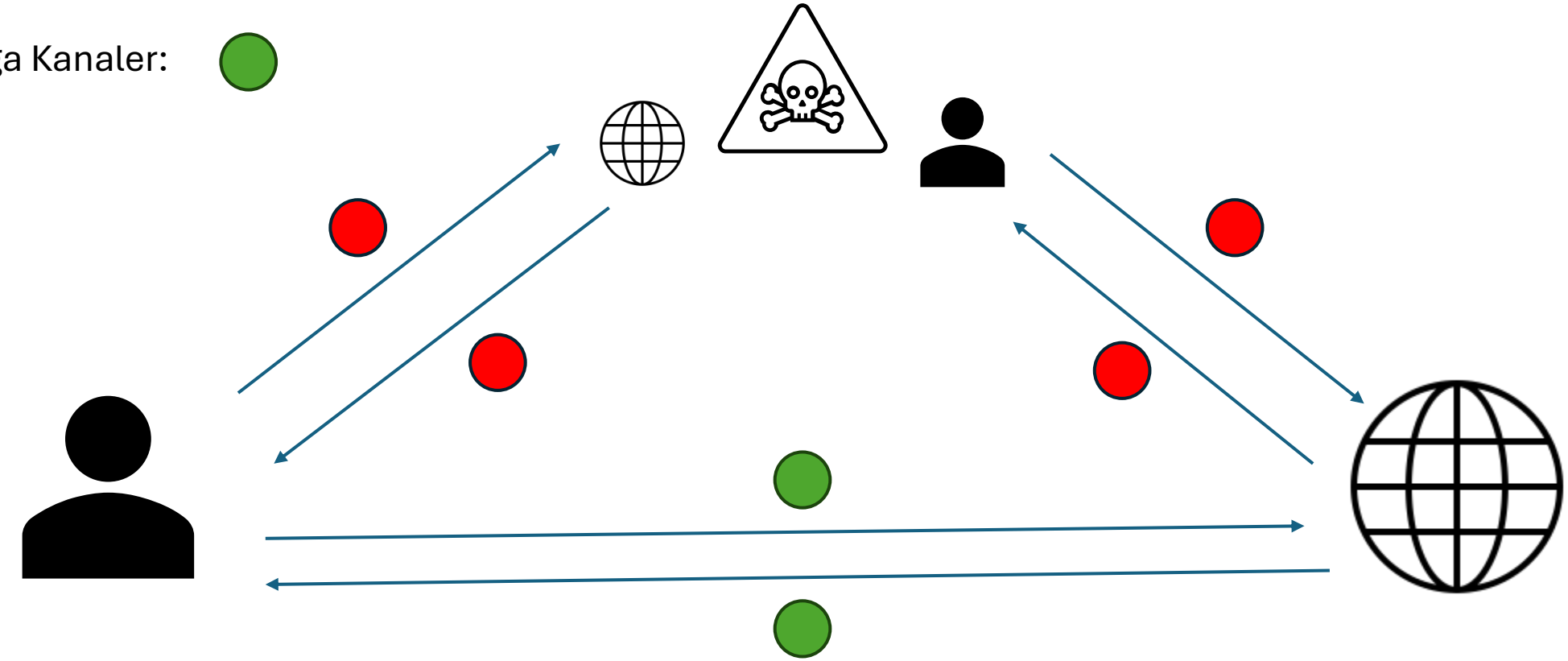
- **Trojan horse:** Attack där ett fejkprogram är maskerat som ett riktigt. När användaren laddar ner eller använder programmet startas ett virus eller annan skadlig kod som är gömd och tar över datorn.
- **Ransomware:** Attack där ett skadligt program injekteras in i ett system och attackeraren begär en lösensumma för att inte läcka känslig data eller avstå från att fortsätta attacken.
- **DDOS:** Denial of service attack är en attack där man har som mål att få normal verksamhet att stanna eller sluta fungera. Oftast att man överbelastar ett system för att få det att sluta fungera. Principen innebär att du skickar så mycket till en mottagare att den inte kan hantera det och då får problem att upprätthålla alla tjänster.
- **Phishing:** Har du fått ett konstigt mail från fake facebook, steam eller instagram någon gång? Då har du utsatts för en phishing attack. Phishing är namnet på attacker där man försöker få tag på folks inloggningsuppgifter eller annan känslig information genom att utge sig för att vara den verkliga mottagaren.
- **Man In the middle:** En attack där en attackerare upprätthåller en kanal och avlyssnar din kommunikation med internet. Genom att allt det du gör skickas till attackeraren och senare vidare så kan attackeraren även injecera skadlig kod i och manipulera svaren du tar emot.

Man In the Middle

Fejkade kanaler:

Riktiga Kanaler:

Genom att låtsats vara sändare och mottagare samt upprätthålla fejkade kanaler kan en tredje part avlyssna trafik och även påverka trafik mellan två parter.



DDOS

Betala XXXXXX kr så kommer er server fungera igen

Ägare

Botnet
(virusinfekterade datorer under hotets kontroll)

En form av överbelastningsattack där ett botnet av något slag blir beordrade att skicka förfrågningar till samma ”plats”. På så sätt sakta ner eller slå ut mottagaren som ska ge svar. Där server eller annan form av mottagare antingen används som gisslan mot en lösensumma eller slås ut för att förstöra delar av nätet som kan öppna upp andra svagheter.

Phishing

Försök till att få någon att ange sina inloggningsuppgifter på en sida som inte är den riktiga. Hotet får ta del av de riktiga uppgifterna och kan använda dem