# Computer Network and the Internet

**ISP** – levererar Internet

**Kant(edge) och kärna(core)** – Kant är mer av datorer, servrar alltså värdar, medan kärna är routrar och switchar som kopplar samman värdarna och använder Store-and-Forward (sparar först och sedan skickar)

**Länk (kommunikationslänk)** – Antagligen kablar och wireless

**Router** – Väljer vägen för paketen t.ex. via IP-adress. Smartare än switchar och hubbar. Den ser till välja den väg med minst trafikbelastning och kan utrustas med brandväggsfunktioner.

**Bandbredd (bandwidth)** – Bithastigheten (?). Bits per second för R, Hertz för W.

**Protokoll** – Program för hur datautrustningen ska fungera under kommunikation.

**Internet/Intranet** – Internet är nätverk av nätverk. Intranet är ett nätverk som är uppbyggt för en specifik grupp och har restriktioner t.ex. så att utanför inte kan komma in och de som redan är i nätverket inte kan komma ut.

**Internet-standarder** – Utvecklat av Internet Engineering Task Force (IETF). Standarddokumentet heter RFC (Request For Comment), RFC XXXX.

**Värd (host, end-system)** – Servrar

**Modeller: klient/server och peer-to-peer** – Kommunikation mellan klient och server, hög säkerhet, miljontals användare, central datastation, dyrare. p2p mellan datorer, mindre säkert, finns ingen styrcentral, billigare.

**Kretskopplade nät och paketförmedlande nät** – Grundläggande nättyper. Circuit Switching (FDM och TDM).

**FDM och TDM** – Frequency-Division Multiplexing, man delar upp begäran jämt över frekvensen. Time-Division Multiplexing, man delar upp begäran på olika tidsintervall på bandbredden. Bestämda vägar för routrar.

**Statistisk multiplexering –** Bandbredden är tilldelade beroende på begäran och har inga bestämda vägar.

**Virtuell tjänst** – (Internet: TCP)

**Tier-1, Tier-2, Tier-3**

**Multi-home** – När en dator är kopplat till mer än en router utport. Inte tier-1

**IXP** – Internet Exchange Point. Gör så att fördelningen av datan blir snabbare.

**Content Provider** – Google. Tier-1.

**Kärna och kant –** (Värdar och klienter)

**Paketförlust –** Paket som droppas vid full inkö och utkö.

**Genomströmning – KOLLA VAD DETTA INNEBÄR**

**Fördröjning sändare-mottagare –**

**RTT -**

**OSI-modellen – Applikation, Presentation, Session, Transport, Network, Datalink, Physical¨**

**Förbindelse-orienterad tjänst i protokoll –** Kopplar upp – meddelanden – kopplar ned. Kvitterar. På internet (TCP)

**Förbindelselös tjänst i protokoll –** Kopplar inte upp/ned innan meddelandeutbyte. Kvittering eller inte. På Internet: UDP (Ingen kvittering)

**Grundläggande primitiver –** Request-Response. Indication-Confirm.

**Kontrollinformation (PCI) –** Protocol Control Information. Skickas med alla förutom fysiska och datalänk-skikten.

**SAP** – Service Access Protocol

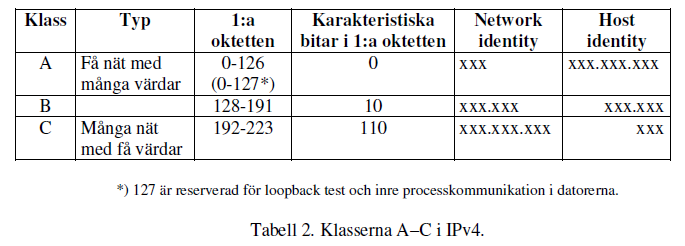
**Sammankopplade enheter:**

* Skikt 1: Hubb
  + Fungerar som förstärkare
* Skikt 1-2: switch
  + MAC = Media Access Control t.ex. Ethernet-adress
* Skikt 1-3: router - (Mot omvärlden: Gateway)
  + Nätverksadress, t.ex. IP-adress
* Skikt 1-7: Gateway (protocol converter)

**Adresser på Internet** –

* IPv4: Address Resolution Protocol
  + (ARP) MAC -> IP
  + (RARP) IP -> MAC
  + Räcker till 2^32 adresser
* IPv6: Neighbor Discovery Protocol
  + (NDP)
  + Räcker till 2^128 adresser
  + Används inte helt idag pga dagens routrar. Många använder fortfarande IPv4 Protokol, kommer att kosta väldigt mycket att byta ut alla.
* URL: Uniform Resource Locator
  + tjänst://värd.subdomän.toppdomän/katalog/filnamn/
  + http
  + ptp
  + ipp
* DNS: Domain Name System
  + URL -> IP-adress

**IPv4-klasser:**



**Delnätmask –** Fördelar med delnätmask – Administrativt skäl, reducerar trafikbelastning.

**CIDR –** Finns i routrar och i Tier-1 och Tier-2. Dem är delnät i routrar i företags/organisationers nät. Med CIDR kan man spara minne i routrarna. IP-delnät och MAC-delnät sammanfaller, då får man det mest effektiva nätet.

# Application Layer

**Applikationsprotokoll –***Definieras*: Typer av utbytta meddelanden, Meddelandesyntax (Vilka fält som finns i meddelanden), Meddelandesemantik (Betydelsen av informationen i fälten) och Regler för när och hur processer skickar och svarar på meddelanden.   
*Utvecklas*: Program som kan köras på olika end systems. Mindre program för routrarna och inte för användarprogram.   
*Adressering av applikationsprocesser*: Värden adresseras med sin IP-adress -> Applikationsprogrammet i värden adresseras med sitt applikationsprotokoll -> Applikationsprotokollet adresseras av sin port (SAP). Porten finns mellan applikationsskiktet och transportskiktet.

**TCP/UDP –** Förbindelseorienterad/Förbindelselös, HTTP/FTP på båda, UDP används om man inte bryr om förlorad data.

**Webbapplikationer -** En webbsida är uppbyggd av en grundläggande HTML-fil som har flera refererade objekt. Varje objekt är adresserbar av URL.

**HTTP**

* STATELESS – SPARAR INTE INFORMATION
* HTTP v1.0
  + Metoder: GET, POST, HEAD – Asks server to leave requested object out of response
  + Non-persistent: Ett objekt per TCP-uppkoppling
    - Requires 2 RTT per object
* HTTP v.1.1
  + Metoder: GET, POST, HEAD, PUT – Uploads file to URL-field, DELETE – Deletes file specified in URL-file
  + Persistent (Default): Flera objekt kan per TCP-uppkoppling
  + With Pipelining (Default): Client sends requests as soon as it encounters a referenced object. Fastest.
    - As little as 1 RTT for ALL objects
  + Without Pipelining: Client issues new request only when previous response has been received.
    - One RTT for each referenced object.
* “In-band” – Send/Receive på samma band

**Cookies –** Används för att spara sidor

* Fyra komponenter:
  + Cookie header line of http response message
  + ---------------“---------------- request message
  + Cookie file kept on user’s host, managed by user’s browser
  + Back-end database at Web site

**Webcache (Proxy server)–** Beter sig både som en klient och en server. Om sidan finns i cache sedan ett visst datum (Kollas med if-conditional-get<date>), hämtar webbläsaren från cachen istället för att få en ny sida från servern.   
Fördelar: Reducera svarstid för begäran från klienten.  
Villkorlig GET-metod: Skicka inte ett objekt om cachen har samma up-to-date version av objektet.

**FTP (File Transfer Protocol) –** Tillståndsorienterad (Sparar information)  
Client to server and back.  
TCP Control Connection : port 21  
TCP Data Connection : port 20  
”Out-of-band” – Send/Receive på olika band

**E-mail –**

* SMTP (Sample Mail Transfer Protocol)
* E-postklient – Skickar epost-server. T.ex. Outlook Express
* E-postserver – Tar emot epost-server
* E-postbox – Innehåller inkommande meddelanden för användaren
* E-brevkö – Kö av utgående epost-meddelanden

**SMTP –** (Simple Mail Transfer Protocol).   
Använder TCP för att överföra email meddelanden från client till server via port 25.  
Överföring från e-postklient till e-postklient med direktöverföring mellan e-postservrar.  
SMTP – Push / HTTP - Pull.   
Meddelandeformat: 7-bitars ASCII.

**MIME (Multimedia Mail Extension) –** Används för att skicka bilder  
 Header-line: Content-Type  
 Content-Transfer-Encoding  
 MIME-version  
 7-bitars ASCII kodning

**POP, IMAP, HTTP –** Från SMTP till mottagande mailserver övergår det till accessprotocol.

* POP – Post-Office-Protocol [RFC 1939]
  + Authorization (agent <-> server) and download
* IMAP – Internet Mail Access Protocol [RFC 1730]
  + More features (More complex)
  + Manipulation of stored messages on server
* HTTP – Gmail, Hotmail, Yahoo!, Mail etc.

**DNS (Domain Name System) –**

* Distribuerad Databas - Decentraliserad för att undvika internets undergång
* Används för att översätta från domänadress till IP-adress (youtube.com -> 192.168.1.56)
* Applikationsprotokoll för klient/server
* DNS-post (4-tuple)
  + (Name, Value, Type, TTL)
  + Type
    - A - Standard för värdnamn
    - NS - Domän och dess auktoritativa DNS-server
    - CNAME - Kanonisk värdnamn (original)
    - MX - Kanonisk värdnamn och alias för epost-servrar
* DNS-hierarkin
  + Root (13st)

     |

Toppdomän (ocg, edu, com och landsdomäner)

     |

Lokala (inkl. auktoritativa)

* Arbetsmetoden för DNS
  + Iterativ och rekursiv  
    **Hög** arbetsbelastning för lokal DNS
  + Rekursiv  
    **Låg** arbetsbelastning för lokal DNS
  + Caching  
    Både i DNS-servrar och värdar
  + Filen Hosts  
    Egendefinierad "DNS"
* Lokal och Auktoritativ

**P2P** –

* Direct Communication. Faster with P2P if many clients than server.
* Kan vara bade vara klient och server.
* **Distributed Hash Table (DHT)**
  + Distributed P2P Database
  + Database has (key, value) pairs:
    - key: ss number; value: **human name**
    - key: content type; value: **IP-adress**
    - **(key, value) = (H(låt) (n-bit), IPv4-adr (n-bit))**
  + Peers query DB with key DB returns values that match the key
  + Peers can also insert (key, value) peers

**Sockets –** Från en process genom en socket ut till transportskiktet via internet till annan dator, som skickar in meddelade in i sin egen socket och skriver ut meddelandet genom en process.

# Transport Layer

**Network Layer** – Kommunikation mellan värder

**Transport Layer** – Kommunikation mellan processer   
 Logisk kommunikation mellan approcesser som körs på olika värdar

**Transportskiktet** – Multiplexering: Samlar datar från olika socketar skickar iväg det med en header som senare kommer till demultiplexering som levererar segmenten till korrekt socket.

**Process** sker innan data skickas ut via **socket**. Data skickas ut och kommer till en annan dator. Där kommer den att sorteras in i korrekt **port**.

Felövervakningskonceptet –

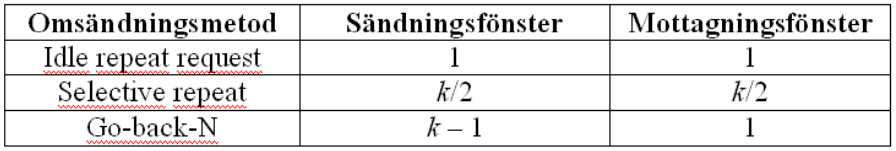
* Felövervakning
  + Sekvensnummer
    - Låt ordlängden för sekvensnummer kallas n, tillhör de positiva naturliga talen (Z^+).
    - Z^n antal sekvensnummer.  
      Ex n=3, 2^3 = 8; 0,1,2,3,4,5,6,7 (0-7dec, 000-111bin)
    - Sekvensnummer utgörs av antal bytes (På Internet)
  + Checksumma
  + Omsändningsmetod
* Auto Repeat Request (ACK, NAK)
  + Manuell
    - Echo Checking
  + Automatisk
    - Automatic Repeat Request, ARQ
    - Upptäcka bitfel (feedback error control)
    - Korrigera bitfel (forward error control)
    - Idle Repeat Request
      * Implicit Retransmission
      * Explicit Request
        + ACK, NAK
    - Continuous Repeat Request
      * Selective Repeat Request
        + Implicit Retransmission
        + Explicit Request
      * Go-back-N

**Piggyback acknowledgement –** Kvittenser inbäddade i nyttomeddelanden  
Onödig trafik reduceras

**Reed-**Solomon – RS(n,k) 2t = n-k  
k = antal data (s-bitars symboler  
n = antal data ink checksummorna  
n – k = Antal checksummor (s-bitars symboler)

**Flödesreglering**:

**Fönsterteknik** – Antal sekvensnummer: k = 2n



**TCP**-segmentets format –   
 Three-way handshake:   
 Connection: ACK, SYN/ACK, ACK. Connection Established.  
 Disconnection: FIN, ACK/FIN, ACK. Connection terminated.

**RTT -**

* EstimatedRTTnew = (1- α)⋅EstimatedRTTold + α⋅SampleRTT
* Följder av TCP-timervärde
  + Too short – premature timeout (unnecessary retransmissions)
  + Too long – Slow reaction time to segment loss
* TimeoutInterval formel: TimeoutInterval = EstimatedRTT + 4⋅ DevRTT

**TCP slow start –** Initial rate is slow but ramps up exponentially fast

# Network Layer

**Transport segment från sändare till mottagare:**

* Sändarens sida enkapsuleras segmenten i datagram
* På mottagarens sida levereras segmenten till transport skiktet
* Finns nätverksskikt-protokoll i varje värd och även routrarna
* Routrarna kollar headern på alla IP-datagram som går igenom dem

**Forwarding –** Move packets from routers input to appropriate router to output

**Routing –** Determine route taken by packets from source to destination with a routing algorithm

**Routerns fyra huvuddelar –**

* Inport
* Routing processor
* Switching fabrics
  + Memory
  + Bus
  + Crossbar
* Utport
* Routingprotokoll
  + (RIP, BGP, OSPF)

**Buffering-recommendation -** Recent recommendation:   
With N flows, buffering equal to B = RTT\*C/sqrt(N)

**Head-of-the-Line (HOL) blocking:** Queued datagram at front of queue prevents others in queue from moving forward

**De tre stora arbetsuppgifterna på nätnivå:**

* Routing Protocol – Forwarding Table
  + Path selection
  + RIP, OSPF, BGP
* IP Protocol
  + Adressing Conventions
  + Datagram format
  + Packet handling conventions
* ICMP Protocol
  + Error reporting
  + Route ”signaling”

**DHCP -** Dynamic Host Configuration Protocol (**DHCP**) is a client/server protocol that automatically provides an Internet Protocol (IP) host with its IP address and other related configuration information such as the subnet mask and default gateway.

**Link-State Routing Algorithm (LS) –**

Djikstras  
Global - Decentralizerad  
Iterativ  
Används av protokollet OSPF

**Distance Vector Algorithm (DV) –**

Bellman-Fords equation (dynamic programming)  
Decentraliserad  
Iterativ  
Asynkron  
Distribuerad  
Används av protokollet RIP

# Security in Computer Networks

Konfidentiella meddelanden (sekretess)  
Autentisering (i meddelanden)  
Meddelandeintegritet   
Operationell säkerhet

Krypteringsalgoritmer

* Symmetriska nycklar
  + Advanced Encryption Standard (AES)
  + Wi-Fi Protected Access (WPA)
  + WPA2