# Dugga 4

**Beskriv Link State (LS) på bästa sätt.**

* **Dijkstras algoritm**
* **Global** - information om hela delnätet krävs
* **Decentraliserad** - Varje router ställer upp sin egen routingtabell
* **Iterativ metod**
* Beskrivs med matematiska uttryck, tabeller eller grafer
* Grunden för **OSPF** (Open Shortest Path First)

**Jämför Link state (LS) och Distance Vector (DV)**

* Både LS och DV kräver ett stort antal routermeddelanden
* Fel fortplantas **snabbt** i de båda
* Snabba, stora förändringar av länkkostnader medför långa konvergeringstider i DV och speciell åtgärd kallad "poisoned reverse", kan behövas för att motverka **ping-pong-effekt**

**Beskriv ATM.**

* "Central station" sätter upp Virtual Paths (VP, "**vägar**") och Virtual Circuits (VC, "**filer på vägar**").
* VP/VC meddelas till ATM-nätets **switchar** och routrar.
* Varje ATM-nät har **gränsroutrar** som kapslar in IP-paket

**Beskriv växelstrukturen "switching via memory".**

* Den **första** generationens routrar som byggdes upp av traditionella datorer, där växlingen gjordes av **processorn**.
* Inkommande paket skrevs in i arbetsminnet, RAM, i väntan på tabellslagning och vidarebefordran till bestämd utport.
* Relativt stor fördröjning som orsakades av transport över systembussen **2** ggr.
* Portarna utgjordes av **nätverkskort**.

**Vilka är de tre huvuddelarna i Internet-skiktet (nätverksskiktet)?**

* Internet Protocol (IP)
* Routingprotokoll och routingtabell
* ICMP (Internet Control Message Protocol)

**Vad är typiskt för Distance Vector (DV)?**

* **Bellman-Fords algoritm** och även **Dynamisk programmering**
* Distribuerad eftersom varje router beräknar sin DV som de närmaste grannarna får ta del av
* **Decentraliserad** eftersom varje router ställer upp sin egen routingtabell
* **Iterativ metod**
* **Asynkron** eftersom uppdateringar nödvändigtvis inte görs i samma takt som andra routrar
* Beskrivs med matematiska uttryck, nodtabeller eller grafer
* Grunden för **RIP**

**Vilka är de nya fälten i IPv6 jämfört med IPv4?**

* Payload length
* Flowlabel

**Vad hanterar IP-protokollet?**

1. Adresser
2. Adressering
3. Paketformat

**Vilka fält i IPv6 motsvarar tidigare fält i IPv4?**

* IPv4 - IPv6  
  Type of Service (TOS) - Traffic class  
  Upper-layer-protocol - Next header  
  TTL - Hop limit

**Vilken tumregel gäller för dimensionering av utbuffertar hos routrara? Hur har den förbättrats enligt nya rekommendationer?**

* Tumregel: Utbuffertstorlek = RTT\*C, där RTT är Round-Trip Time (**s**) och C är bandbredden (**bps**).
* Förbättring: Utbuffertstorlek = , där N är antal **pågående TCP-strömmar**.

**Vilka routingprotokoll används för olika situationer?**

**Vad innebär begreppen forward och routing?**

**Forwarding**: Varje router skickar ett IP-paket vidare genom respektive bestämd **utport**.

**Routing**: Att välja "**bästa väg**" från sändande värd till mottagande. Val av **utport** görs i varje router längs vägen.

**Vad är korrekt beträffande flaggor/fält för fragmentering?**

* Om flaggan Don't Fragment (DF) är satt, kan paketet **inte delas upp**.
* Om flaggan More Fragments (MF) är satt, är det fråga om ett paket som innehåller en del av ett uppdelat paket, men dock inte det sista i sekvensen.
* Fragment offset anger **relativt** bytenummer i en sekvens av paket för ett uppdelat paket. Paketen i sekvensen innehåller alltid heltalsmultiplar av **8** byte, med reservation för det sista.
* Ordlängden för Fragment offset är **13** bitar vilket ger **8192** **relativa** sekvensnummer.

# Dugga 5

**Vilka är tjänstetyperna i Logical Link Control (LLC, 802.2)?**

* Förbindelselös tjänst utan kvittering
* Förbindelselös tjänst med kvittering
* Förbindelseorienterad tjänst
* Obtain reply

**Hur ställer switchar och bryggor upp sina tabeller (routingtabeller)?**

* De lär sig av **inkommande ramar** som skickas för både begäran och svar (respons). Principen kallas att enheterna är **självlärande**. Om port är okänd för en MAC-adress, tillämpas **flooding**, dvs. **inkommande ram** skickas ut på **samtliga portar** utom på **inporten**. När väl en post har lagts in i tabellen, finns den kvar på **bestämd tid. Sedan tas den bort.**

**Vad skiljer praktisk Ethernet (Ethernet II) från standardiserad Ethernet (802.3)?**

* **Ethernet II** används inte ihop med LLC
* Följande fält i ramarna är olika eller används på olika sätt:
  + **Preamble** i Ethernet II och **Preamble med Start-of-Frame** I 802.3
  + **Type** i Ethernet II och **Length Indicator** i 802.3

**Vad är Controller Area Network (CAN)?**

* Utvecklades av **Bosch** för att ersätta kabelsystem i fordon.
* CAN används i Volvofordon och kallas **Volcano.**
* CAN används i ABB:s robotar och kallas **DeviceNet.**
* CAN används i Atlas Copcos **gruvmaskiner.**
* Bussen består av ett par ledare, CAN\_L och CAN\_H.
* Mottagen signal är differensen **CAN\_L – CAN\_H** som omvandlas för att matcha övrig elektronik

**Hur beräknas Slot time för en Ethernetversion?**

* Slot time = **2**\*utbredningstiden + säkerhetsmarginal där utbredningstiden bestäms för den **längsta** nättypen för Ethernetversionen. Ett exempel är utbredningstiden över 5\*500 = 2500 **m tjock koaxialkabel (RG11)** för versionen med bithastigheten 10 Mbps. Multiplikationen med **2** innebär att Slot time beräknas för "tur och retur", tur för dataramen och retur av jam. Detta ger Slot time **= 51,2 μs.**

**Förklara kabelbeteckningen för Ethernet: [max. bithastighet] BASE/BROAD -Y [max. segmentlängd]**

* [max. bithastighet] ges i **Mbps**
* BASE är **basband**, dvs. utan FDM
* BROAD är **bredband**, dvs. med FDM
* Y anger transmissionsmediet om inte **koaxialkabel** används
* [max. segmentlängd] ges i hundratals **meter**

**Varför görs bit stuffing i CAN och hur går det till?**

* För att skydda mot förväxling mellan dataramar och felramar. De senare innehåller felflaggor av typen **aktiv** (000000) eller **passiv** (111111).
* För att förbättra **synkroniseringen hos mottagarna**.
* Efter fem lika bitar insätts en extra bit med **motsatt värde** till de fem lika. Mottagarna räknar antal lika bitar och efter fem lika kastas den sjätte biten. (Den sjätte biten räknas förstås in i nästa sekvens av eventuellt lika bitar.)

**Beskriv hur noder styrs på fältbussar**

* Masters styr slaves
* En passiv master kallas **monomastersystem**
* Två eller flera inaktiva masters kallas **multimastersystem**
* Masters kan utgöras av PC och PLC:er (på cellnivå)
* Slaves är typiskt I/O-enheter (för givare och ställdon) och PLC:er (på fältnivå)

|  |
| --- |
| **Vilken typ av kodning visar figuren? Vad kallas accessmetoden för Ethernet som använder denna? Varför används koden? I vilka Ethernetversioner används denna accessmetod?**  E:\Users\Özgun\Downloads\kod.png |

* Kod: **Manchester**
* Accesmetod: **CSMA/CD (802.3)**
* Syfte: Generera fler växlingar än utan koden för att bättre **synkronisera mottagarna**
* Ethernetversioner: 10 Mbps (**802.3**) och **halv duplex-versionen** av Fast Ethernet (**100 Mbps**)

**Vilka är de fyra egenskaperna för åtkomst med ett idealt flerpunktsprotokoll (Mutliple Access Protocol)?**

1. Om endast en nod har data att sända, ger noden bitflödet **R** bps.
2. Om M noder har data att sända, kommer varje nod att ge ett medelbitflöde av **R/M** bps.
3. Protokollet är **decentraliserat**, dvs. inga masternoder kan fela och ta ned hela nätet.
4. Protokollet är **enkelt** så att det blir billigt att **implementera**.

# Dugga 6

**Beskriv indirekt routing för åtkomst av värd med permanent IP-adress. När kan tekniken vara användbar?**

1. En dator med **egen IP-adress** finns tillfälligt i ett annat nät. Datorn registreras hos både den främmande agent och hemagenten.
2. En korrespondent skickar ett paket till datorns **permanenta IP-adress**.
3. Hemagenten kapslar in paketet i ett yttre paket och vidarebefordrar det till datorns**C/O-adress (COA)**
4. Den främmande agenten packar upp det yttre paketet och skickar det inre vidare till datorn. Korrespondentens **avsändaradress** finns i det inre paketet.
5. Datorn svarar genom att skicka paket direkt till korrespondenten (givetvis via **den främmande agenten**).

På detta sätt kan datorn alltid nås, även om den inte befinner sig i sitt hemnät.

(Svar från Jack:)

”Din fråga gäller värdar, exempelvis datorer, som behåller sina egna (privata, permanenta) IP-adresser trots att de flyttas. Detta blir möjligt om värdarna i de besökta näten också får var sin C/O-adress. Det finns redan protokoll för hur denna tillfälliga C/O-adress delas ut och meddelas "hemroutern".  
  
En värd (B) som vill kommunicera med en värd (A) som har flyttats och tilldelats även en C/O-adress, skickar som vanligt paket till mottagarens permanenta IP-adress. Beroende på metod händer följande:  
  
1. Om indirekt metod  
"Hemroutern" vidarebefordrar paket från B till A genom att lägga in paketen i nya paket som förses med C/O-adressen. A svarar direkt till B.  
  
2. Om direkt metod  
"Hemroutern" ger B den nya tillfälliga C/O-adressen att använda. B får du adressera om paketen med den nya tillfälliga C/O-adressen. A svarar direkt till B.  
  
CIDR-teknik används av routrar på Internets kärna, inte av nätens standard gateways. Omdirigering med hjälp av C/O-adress görs av "hemroutern" (standard gateway) och den främmande routern (det besökta nätets standard gateway). ”

**Vad kännetecknar IEEE 802.11 och i synnerhet versionerna a, b, g och n?**

* Kallas WiFi eller "**trådlöst Ethernet**"
* Är **WLAN**
* 802.11a, b, g och n använder **CSMA/CA för multiple access**
* finns med moderna (nätversionerna) **basstation** och **ad-hoc**

**Vad innehåller fältet Payload Type i ett RTP-huvud? I vilket fält finns identifieraren SSRC? Vilken ordlängd har SSRC? Vad identifierar SSRC?**

* Payload Type innehåller **audio- och videoformat**, **samplingsfrekvens** och**bithastighet (kodningshastighet)**.
* SSRC finns i fältet som kallas **Synchronization Source Identifierer**. SSRC har ordlängden **32 bitar** och utgör **identifieringsnummer för mediet som avspelas**.

**Vilka är de tre versionerna av Profibus vad kännetecknar respektive?**

* Profibus-FMS (Field Message Specification)  
  **Universell** fältbuss på **nivåerna fält och cell**.
* Profibus-DP (Decentral Peripheral)  
  **Snabb** fältbuss på **fältnivå**.
* Profibus-PA (**Process Automation**)  
  Ger egensäkert område, exempelvis inom kemisk och petrokemisk industri. På **fältnivå**.

**Beskriv HTTP-strömmar. Vilka är fördelarna?**

* HTTP-strömmar använder **GET-metoden**. Först hämtas länken (URL:en) till mediefilen. Denna länk överlämnas till **mediespelaren** som hämtar filen chunk för chunk. Med headerline **HTTP byte-range** meddelar mottagaren vilken del av mediet som önskas härnäst. På så sätt kan mottagaren indexera i filen. Med prefetching kan mediefilen snabbt överföras till mottagaren. Hur mycket som kan överföras beror på **mottagarbuffertens storlek**.
* Fördelar: Säkrare överföring än med UDP. **Få brandväggar spärrar** TCP-segment. Ingen **RTSP-server** behövs.

**Vilka skikt ger Quality-of-Service (QoS)? Vilket skikt kan förbättra QoS? Vad innebär Best-effort Service?**

* QoS bestäms av skikten **värd-till-nät (fysiskt och länk)** och **Internet-skiktet (nätverksskiktet)**. QoS kan förbättras i **transportskiktet**,**exempelvis genom att välja TCP istället för UDP**.
* Best-effort Service innebär att **routrarna distribuerar paket så snabbt som möjligt** och detta i kombination med att använda **det snabba UDP**. Best-effort Service ger **ingen garanti för tidsfördröjning och jitter**.

**Beskriv förslaget Per-connection QoS Quarantess, även kallat Integrated Services (Intserv).**

* **Mottagaren** gör call setup  
  **Mottagaren** begär att de valda routrarna längs vägen från servern till klienten ska reservera resurser, Rspec, för den kommande sessionen. Rspec handlar om **buffertstorlek och bandbredd**. En annan parameter är Tspec som står för **antingen trafiken från servern eller till klienten**.
* Om en router inte kan reservera tillräckligt med resurser för sessionen, **väljs en annan väg**.
* **ReServation Protocol (RSVP)** används för call setup

**Beskriv förslaget Differentiated Services (Diffserv).**

* **Paketklassificiering** och **uppsättning av trafikvillkor** i kanten  
  Information skrivs in i paketens huvuden av en **diffservkapabel värd** eller **den första diffservroutern längs vägen**.
* Vidarebefordran **enligt paketklassens "per-hop behavior"** i kärnans routrar

**Vad kännetecknar IEEE 802.15?**

* Beskriver ett **PAN**.
* Standarden utvecklats från **Ericssons Bluetooth V1.0**.
* Kallas **piconet**.
* **Ad-hoc**
* Består av maximalt**8 aktiva**enheter: **en master och resten slavar**.
* Det får finnas **parkerade (inaktiva)** enheter. (Upp till 255 st.)
* Syftet är att ersätta **kablar**, exempelvis **musens sladd till systemenheten**

**Vilka är de tre typerna av multimedia över nät, enligt kursboken? Beskriv dessa**

* Streaming Stored Audio and Video
* Conversational Voice- and Video-over-IP
* Streaming Live Audio and Video

*Streaming*: Strömmande multimedia börjar avspelning typiskt inom några **sekunder** efter det att mediet har kommit fram.

*Stored*: Lagrat innebär att mediet har spelats in innan det ska visas.

*Conversational*: Att konversera i ljud och bild handlar om telefoni och konferenser. Ljudfördröjningar **< 150 ms uppfattas inte, 150-400 ms kan accepteras, och > 400 ms tolereras inte**.

*Live*: Är samma som direktsändning, där det kan vara flera mottagare. **P2P-nät och CDN:er** har visat sig vara effektiva för distribution av direktsändningar. Fördröjningar upp till omkring **10 s** tolereras.

# Dugga 7

**Vilka nycklar behövs för att kryptera och skicka ett meddelande och att på mottagarsidan dekryptera meddelandet. Utöver det krypterade meddelandet finns ett certifikat som ska användas. Sändaren kallas A, mottagaren kallas B och utfärdaren av certifikatet kallas CA.**

1. För att kryptera meddelandet används **KA+**.
2. För att dekryptera certifikatet används **KCA-**.
3. Inne i certifiktatet finns **KA-** som används för att dekryptera meddelandet

FEL

**Hur kontrolleras meddelandeintegriteten?**

1. Sändaren beräknar H(m), där m är meddelandet och H(.) är **hashfunktionen**.
2. Sändaren skickar m + H(m), där + är **konkatenering**.
3. Mottagaren **separerar** inkommande meddelande (m') från **hashkoden**.
4. Mottagaren beräknar H(m').
5. Mottagaren testar om **H(m') = H(m)**

**Förklara Krypteringsmodellen**

Hos sändaren:

1. Indata till krypteringen är det som ska krypteras (m) och en nyckel (KA).  
   Nycklar kan vara **symmetriska, KA = KB, där KB används för dekryptering**.  
   Alternativet är **asymmetriska nycklar, KA != KB**.
2. Utdata från krypteringen kallas **chiffer (c)**.

Hos mottagaren:

1. Indata till dekrypteringen är det som ska dekrypteras (**c**) och en nyckel (KB).
2. Utdata från dekrypteringen är **m**.

**Beskriv en Application Gateway.**

* Filtrerar trafiken in/ut med avseende på speciell **applikation**.
* Applikationen kan exempelvis vara TELNET och då kan filtret ange tillåtna IP-adresser för TELNET-sessioner och kräva inloggning.

**Vilka är de 3 VPN-tillstånden och vilket protokoll ligger bakom Virtual Private Network (VPN)?**

1. Transport  
   **VPN mellan värdar utan inblandning av routrarna i Internets kärna. (Routrarna inverkar inte på VPN).**
2. Tunnel, typ 1  
   **VPN mellan en värd och en router i Internets kärna.**
3. Tunnel, typ 2  
   VPN mellan en närliggande router och en annan värd.

Bakomliggande protokoll kallas **IP security (IPsec)**.

**Vilka nycklar ingår då PGP används?**

* Hos sändaren:
  + Sändarens **privata**nyckel  
    Används för att kryptera hashfunktionen av meddelandet.
  + En **symmetrisk** nyckel  
    Denna nyckel är okänd för mottagaren då meddelandet skickas. Används för kryptering av meddelandet konkatenerat med krypterad hashkod.
  + Mottagarens **publika** nyckel  
    Används för att kryptera **den symmetriska** nyckeln.
* Hos mottagaren:
  + Mottagarens **privata** nyckel  
    Används för att dekryptera **den symmetriska** nyckeln.
  + **Den symmetriska** nyckeln  
    Används för att dekryptera meddelandet konkatenerat med hashkoden.
  + Sändarens **publika** nyckel  
    Används för att dekryptera hashkoden.

**Förklara begreppen meddelandeintegritet, autenticitet och driftsäkerhet.**

* ***Meddelandeintegritet:***  
  Parterna i ett meddelandeutbyte ska kunna **upptäcka förändringar av texten**. Detta säkerställs genom **hashkodning**.
* ***Autenticitet:***  
  Parterna i ett meddelandeutbyte ska kunna **identifiera varandra**. Detta kan göras med hjälp av **kryptering med asymmetriska nycklar**. (Det kan också handla om att logga in med bestämd användare och lösenord.)
* ***Driftsäkerhet:***  
  Användaren ska ha åtkomst till tjänster som förstås ska vara tillgängliga, men naturligtvis inte för obehöriga. Därför behövs **åtkomst- och behörighetskontroll**.

**Var placeras SSL i en Internet-stack? Vad ger SSL? Vad kallas SSLv3?**

* Eftersom SSL är en **socket**placeras den mellan **applikationsskiktet och transportskiktet**.
* SSL ger **krypterad kommunikation** exempelvis för e-handel och bankärenden.
* **Transport Layer Security (TLS) = SSLv3**

**Förklara TLV encoding i Basic Encoding Rules (BER), enligt Abstract Syntax Notation (ASN.1) i ISO X.680. Varför görs TVL-kodning?**

T = **Type**   
L = Length (bytes)  
V = Value

Istället för att enbart skicka **V**, skickas TLV för att upplysa mottagaren om exakt **datatyp** och storlek för att få korrekt **behandling** av data.

**Beskriv informationsflödet med Simple Network Management (SNMP).**

**Request/response** **mode**:

Liknar kommunikationen mellan klient och server.**Managing entity** begär att få insamlad information och **agenten** svara med denna.

**Trap mode**:

**Agenten** skickar insamlad information till **managing entity** allt eftersom det kommer in sådan.