Observera att svaren redovisas kortfattat och hänvisas till kursboken för utförligare svar.

1. **Internets TCP/IP-modell är liksom OSI-modellen baserad på att dela upp kommunikationen i ett antal lager ”layers”. (3p)**

   a) Vilka är de **tre** högre lagren i Internets TCP/IP protokollarkitektur?
   b) Vilka är de välkända **tjänster** och **protokoll** som ingår i varje lager?

   c) Vilken **benämning** används för datamängden (s.k. **P**rotocol **D**ata **U**nit) som bearbetas av protokollet vid **varje** lager i frågan?

   d) Hur skapas ett **PDU** av ett protokoll? Förklara kortfattat vad som händer med data (t.ex från en fil som skall skickas över Internet) när den bearbetas uppifrån och ner i protokollstacken för dessa tre lager (på sändarsidan).

Se avsnitt 1.5.1 resp. 1.5.2 i kursboken

(Layer 5) Applikation tjänster: Web, filöverföring, domännamn, email, ...
protokoll: http, ftp, dns, smtp, ...

(Layer 4) Transport: pålitlig (förbindelseorienterad) transport, TCP
användardatagram (förbindelselös) transport, UDP

(Layer 3) Nätverk: förbindelselös datagram leverans (best effort delivery), IP

(5) Meddelande (message), (4) segment, (3) datagram (packet)

PDU skapas genom att protokollet lägger header till datamängeden som tas emot uppifrån. PDU = header + data

2. **Många av Internets protokoll användar kontrollsumma ”Checksum” för att upptäcka bitfel, medan de flesta länkprotokollen användar CRC (**Cyclic **R**edundancy **C**heck**). (2p)**

   a) Vad är skillnaderna mellan de två metoderna? Jämför deras tillämpning.
   b) Beskriv kortfattat hur bitfel kan upptäckas med varje metod.

Se avsnitt 3.3.2 resp. 5.2.3 i kursboken

Kontrollsumma: 1’s komplement binär addition av 16-bitars ord (från header, datafält eller både och). Mjukvarubaserad. Finns fält för kontrollsumman i header.

CRC: binär division av lång bitström (data+header) med ett CRC-tal (generator). Hårdvarubaserad. Finns fält för FCS (resten av divisionen) i trailer.

I princip görs samma beräkning (dock olika metoder) hos sändaren såsom mottagaren och jämförs mottagarens resultat med vad sändaren har lagt i fältet. Om dessa inte är lika konstateras att det har hänt bitfel.

3. **Grundprincipen för protokollet HTTP är att klienten begär i ett GET-meddelande att hämta ett objekt identifierad med URL på en webb-server. Servern skickar objektets data i respons-meddelande som svar. (3p)**

   Beskriv **tre** viktiga mekanismer som avsevärt förbättrar hämtningen av webbsidor och dess objekt om både webbläsaren och webbservern använder HTTP version 1.1.

   Se avsnitt 2.2.2 resp. 2.2.6 i kursboken

   - Behålla TCP-anslutning öppen (persistent connection), tills alla objekt inhämtade,
   - Parallell hämtning av objekten länkade till samma server (pipelining),
   - Web-caching och villkorligt (conditional) GET.

4. **I nedanstående exempel som liknar en verklig situation, misslyckas en användare av en nystartad PC-dator att ansluta med webbläsaren till** http://www.student.chalmers.se**. Användaren utför följande kommando för att kontrollera datorns IP-konfiguration. (2p)**

```
C:\>ipconfig /all

IP-konfiguration för Windows
        Värddatornamn . . . . . . . . . . . . : chalmers-2116fb
Ethernet-kort nätverksanslutning:

        Anslutningsspecifika DNS-suffix  . . : chalmers.se
        Beskrivning . . . . . . . . . . . . . : Broadcom NetXtreme 57xx
        Fysisk adress . . . . . . . . . . . . : 00-1B-77-D3-20-B9
        DHCP aktiverat . . . . . . . . . . . . : Ja
        IP-adress . . . . . . . . . . . . . . : 129.16.214.119
        Nätmask . . . . . . . . . . . . . . . : 255.255.252.0
        Standard-gateway . . . . . . . . . . . : 129.16.212.23
        DHCP-server . . . . . . . . . . . . . : 129.16.212.24
        DNS-server . . . . . . . . . . . . . . :
```

   Undersök noggrannt den ovanstående konfigurationen.

   a) Vad kan problemet huvudsakligen bero på?
   b) Ge en fullständig förklaring till vad som kan vara orsaken till det.

   Saknas konfigurationsparameter om den lokala DNS-servern. DHCP-servern är inte konfigurerad med denna option. Webbklienten kan inte översätta namnet ”www.student.chalmers.se” till en IP-adress och därmed kan den inte skicka några IP-paket (eller åtminstone starta en ARP-förfråga).

5. Stockningskontroll "congestion control" är en viktig funktion på nätverk för datakommunikation. Redogör för denna kontrolltyp på Internet genom att svara på följande delfrågor. (3p)

a) Förklara hur trippel duplikat ACK kan förekomma i samband med stockning.
b) Vad indikerar trippel duplikat ACK?
c) Hur påverkas tillämpningen av stockningsalgoritmer av trippel duplikat ACK?

Se avsnitt 3.7 i kursboken

Vid en kortvarig stockning på en router (en tillfälligt bildad kö på ett interface) på vägen mellan TCP-sändare och mottagare. Sändaren håller på att sända ett antal segment i följd (från CongWindow) där ett av dem hamnar till den fulla kön och routern kastar bort det, men resterande segment släpps efteråt i vägen och når mottagren som i sin tur skickar ACKen till sändaren som har samma nästa förväntade sekvensnummer (på det förlorarde segmentet). Detta indikerar att nätverket leverar segmenten men endast ett av dem blev förlorat pga av mycket kortvarig stockning. I sådan situation behöver inte sändaren gå till Slow Start (Tahoe), utan går den istället till Congestion Avoidance (Reno) med ny tröskel på halva CongWindow och sedan öka det linjärt.

6. Symmetriska och publika krypteringsnycklar kan kombineras för att på säkert sätt överföra meddelande mellan A och B över Internet. (2p)

Redogör för hur **A** kan skicka ett konfidentiellt meddelande till **B** samtidigt som den autentiserar sig till **B** och dessutom skyddar integriteten av meddelandet.

Se avsnitt 8.3 i kursboken

En lösning kan vara:

Steg 1: **A** använder hash-funktion på meddelandet och resultatet signeras med **A**'s privata nyckel (*sändar-autentisering*). Meddelandet plus det signerade hash-värdet behandlas nu i steg 2.

Steg 2: **A** krypterar (meddelandet + signerad hash) med egen-vald session (symmetrisk) nyckel, samt **A** krypterar själva symmetriska nyckeln med **B**'s publika nyckel och skickar båda de krypterade delarna.

[***B*** *dekrypterar med sin privata nyckel den andra delen för att få fram den symmetriska nyckel för att efteråt dekryptera den första delen och få fram meddelandet+ signerad hash.* ***B*** *använder* ***A****'s publika nyckel att få fram hash-värdet som sedan jämföras med sitt eget hash-resultat (integritet).]*

7. IEEE 802.11 MAC (Media Access Control)

a) Vid kommunikation över trådlösa LAN finns det tre fält för adresser i MAC-header på en dataram. (2p)

- Vilka enheter adresseras med dessa fält?
- Hur kan sändaren av dataramen ta reda på dessa adresser?
- Ge ett exempel med rätt ordning på adresserna i båda riktningar av normal kommunikationen över den trådlösa länken.

Se avsnitt 6.3.3 i kursboken

Det är tre adressfält som finns i header på MAC-ramen för IEEE 802.11. De första två adressfälten används traditionsenligt för mottagarens respektive sändarens MAC-adress på den trådlösa länken (dvs. AP eller STA). En tredje adressfält används antingen för den som slutligen får ramen eller för den som ramen har kommit från. På detta sätt kan AP fungera som mellanhand i kommunikationen mellan stationer på det trådlösa nätet och det trådbundna Ethernet.

En trådlös station STA skickar paket till Internet (via default gateway GW):

Adress1 APs MAC-adress (känd från beacon och associering)
Adress2 STAs MAC-adress (inbränt i ROM)
Adress3 GWs MAC-adress (lärd via ARP)

En trådlös station tar emot paket från Internet (via default gateway):

Adress1 STAs MAC adress (som default gateway lärde via ARP och finns I Ethernet-ramens header som mottagaradress)
Adress2 APs egen MAC-adress
Adress3 GWs MAC-adress (från Ethernet-ramens header som sändaradress)

b) IEEE 802.11 accesskontroll är baserad på att undvika kollisioner snarare än att försöka upptäcka dem. (3p)

- Ange minst två anledningar för varför tekniken att upptäcka kollisioner (”Collision Detection”) inte är lämplig för trådlösa LAN.
- Förklara hur kollisioner verkligen kan undvikas med hjälp av de mekanismer som används enligt IEEE 802.11 standarder i trådlösa LAN, **dels** vid sändning av ramar med normal storlek och **dels** vid sändning av långa ramar.

Se avsnitt 6.3.2 i kursboken

Det är svårt att upptäcka kollisioner på den trådlösa länken därför att radiosignalen från en annan sändare kan försvagas kraftigt pga. dämpning och fading eller kan skymmas totalt av föremål (Hidden Terminal problem – Sändarstationen kan inte upptäcka kollisioner med en annan station som är skymd eller långt ifrån så att dess signal är mycket svag). I praktiken är det också hårdvarumässigt kostsamt (för radiodelen i det trådlösa kortet) att själv sända och samtidigt lyssna på försvagad radiosignal från annan sändare.

I WLAN löser man problemet genom att undvika kollisioner snarare än att försöka upptäcka dem. CSMA/CA mekanismer tillämpas kollektivt så att en STA som vill sända en ram med normal storlek, skall lyssna på radiokanalen och se att det är ledig. Är kanalen ledig, vänta DIFS, sända hela ramen och vänta på ACK (skickas av mottagare efter

kortare väntetid SIFS). Är kanalen upptagen, backar STA och startar nedräkning en slumpmässigt vald tid när kanalen blir ledig.

Om stationen har lång ram att sända kan den välja reservation av kanalen från AP(RTS/CTS). Där RTS är en kort ram som skickas av stationen STA för att begära reservation så att alla närliggande stationer vet om kommande sändning. Om AP svarar med CTS då vet alla associerade stationer att kanalen är reserverad för den tid som CTS innehåller. STA väntar kort tid SIFS efter CTS-mottagande och sänder ramen utan att befara kollision. När AP tar emot ramen bekräftar det efter SIFS med ACK och på så sätt vet alla andra stationer att kanalen är återigen ledig att använda.

8. **Ett IT-företag som har flera avdelningar, har tilldelats ett CIDR adressblock 216.18.212.0/23 för sitt nätverk. Eftersom företaget har olika stora avdelningar skall nätverket bestå av olika stora subnät, nämligen ett större subnät, två mindre subnät och tre små subnät. Ett förslag på uppdelningen av nätverket är redan bearbetat så att det stora subnätet skall ha hälften av de tillgängliga IP-adresserna, de två mindre subnäten skall ha 60 adresser vardera medan varje subnät av de tre små skall ha 30 adresser. Resten av adresserna skall användas för 30-bitars subnät till (point-to-point) länkar mellan nätverkets routrar. (5p)**

Din uppgift är att ange i **decimal beteckning** IP-adress och nätmask för varje subnät i en lösning som du arbetar fram enligt den förslagna uppdelningen. Du kan sammanställa svaret med hjälp av en tabell (subnät #, subnät-adress, subnätmask).

Tredje byte (från vänster) i adressen är 212 decimalt som motsvarar 11010100 binärt där de första sju bitarna tillhör prefixen i adressblocket. Genom att använda den sista biten får man två stycken lika stora subnät med 8 bitar för hostdelen (254 adresser).

Subnäten är som följande:

216.18.212.0/24 är det första subnätet, subnätmask 255.255.255.0 som skall användas för det stora subnätet i frågan.

216.18.213.0/24 är det andra subnätet, subnätmask 255.255.255.0 som skall ytterligare subnättas till fyra lika stora subnät med 6 bitar för hostdelen (62 adresser):

(1) 216.18.213.0/26, subnätmask 255.255.255.192 för det första mindre subnätet

(2) 216.18.213.64/26, subnätmask 255.255.255.192 för det andra mindre subnätet

(3) 216.18.213.128/26, subnätmask 255.255.255.192 subnättas ytterligare till två mindre subnät med 5 bitar för hostdelen (30 adresser) vilket ger:

216.18.213.128/27 subnätmask 255.255.255.224 för det första av de tre små subnäten
216.18.213.160/27 subnätmask 255.255.255.224 för det andra av de tre små subnäten

(4) 216.18.213.192/26, subnätmask 255.255.255.192 subnättas ytterligare till två mindre subnät med 5 bitar för hostdelen (30 adresser) vilket ger:

216.18.213.192/27 subnätmask 255.255.255.224 för det tredje av de tre små subnäten

216.18.213.224/27 subnätmask 255.255.255.224 som subnättas ytterligare till 8 st. 30-bitars subnät med subnätmask 255.255.255.252 vilket ger:

216.18.213.224/30, 216.18.213.228/30, 216.18.213.232/30, 216.18.213.236/30,
216.18.213.240/30, 216.18.213.244/30, 216.18.213.248/30, 216.18.213.252/30,

9. Ett hemnätverk kan ha ett antal datorer med TCP/IP konfiguration. Vanligen har hemnätverket en bredbandig anslutning via en Internet-leverantör. Leverantörerna brukar tilldela bara en global IP-adress till kundens router. (3p)

a) Hur och med vilka adresser kommer hemdatorerna att konfigureras?
b) Beskriv hur hemroutern kan ge hemdatorerna samtidig tillgång (access) till Internet trots att kunden bara får en enda global IP-adress.
c) Vilka tjänster/funktioner använder routern för ändamålen?

Se avsnitt 4.4 i kursboken

Hemroutern agerar som DHCP-server och tilldelar IP-adresser till hemdatorerna från ett privat CIDR adressblock (t.ex. 192.168.0.0). Routern reserverar den första tillgängliga adressen för eget interface mot det lokala nätverket och därmed blir denna adress en intern ”default gateway”.

Hemdatorerna kommunicerar direkt med detta interface för att skicka och ta emot IP-paket till och från Internet. Hemroutern använder sedan NAT funktionen för att ersätta den privata sändaradressen i varje utgående paket med sin globala adress samt ersätta sändarens portnummer med ett annat portnummer. Denna ersättning upprepas för alla paket som kommer från en och samma sändaradress med samma portnummer. NAT-funkionen sparar denna information (sändaradress och sändarportnummer + NAT-portnummer) och skapar en tabell för dessa ersättningar för att användas också i motsats riktning när inkommande paket adresserat till hemroutern (som egentligen skall till datorerna på hemnätverket) omadresseras och vidarebefordras till det lokala nätet.

10. De flesta access-nätverken har *en* router för uppkoppling mot Internet. (2p)

a) Beskriv routingtabellen som en sådan router har för att utföra sin uppgift.
b) Vad är det som menas med “default gateway” i IP-konfigurationen av en värddator i ett sådant nätverk? Vad är det som anges i denna konfigurationsparameter?

Routingtabellen består av två självklara vägar, (dvs. routes). Dels en specifik route till eget IP-nät som är direktansluten till routerns interface mot access-nätverket. Och dels en default route via det interface som routern har uppkopplingen mot Internet.

”Default gateway” är det närmaste router-interface som har direkt länk med värddatorn på samma subnät och som anlitas av denna för vidarebefordran av paket som skall levereras utanför eget subnät. Konfigurationsparametern är IP-adressen för detta router-interface som ligger på samma subnät.

11. Internet är byggt på att paketkoppla data mellan de kommunicerande enheterna med ansträngningen att göra det på bästa sätt. Dock blir det ibland förlust av paket. (5p)

a) Redogör för *hur* och *var* paketförlusten kan inträffa på Internet.
b) Hur påverkar denna förlust de applikationer som litar sig på Internet för att hämta *data* (hemsidor, filer,...) respektive *realtids multimedia* (samtal, videokonferens, ..)?
c) Förklara utförligt de tekniker/mekanismer som används för att ersätta de förlorade paketen i båda fallen (data resp. realtids multimedia).

Se avsnitten 7.3.1 och 7.3.3 i kursboken

Paket som vidarebefordras till ett överbelastat interface på en router, kastas bort om bufferten är full och paketförlusten är ett faktum. Lång fördröjning pga långa köer hos routrarna innebär också paketförlust t.ex. vid uppspelning av realtids multimedia om paket kommer för sent för användning.

Data är förlust-känslig och applikationer litar sig på TCP för att all data kommer fram till mottagaren i rätt ordning och utan glap i bytetrömmen. Applikationer för realtids multimedia tolererar en viss förlust och kan ersätta enstaka delar av multimediaströmmen genom att spela upp kopia av förgående del utan att användaren märker mycket störning.

TCP, ofta för data, tillämpar omsändning av förlorade packet (med hjälp av timeout, ACK, sekvensnummer). För realtids multimedia används RTP tillsammans med UDP. RTP sekvensnumrerar och tidsstämplar multimedia paket vilket hjälper applikationen att bl.a. upptäcka paketförlust. Applikationen kan använda sig av att lägga en redundant del till originella multimediaströmmen enligt en av FEC-metoder (extra kodat block för ett antal multimediablock eller låg-hastighet version som redundant del). Interleaving är också ett sätt att minska effekten av paketförlust på multimediaströmmen.

12. Förklara följande begrepp och termer i sammanhang med deras användning eller förekomst i datakommunikationssystem. Förklaringen skall kunna begripas av vanlig Internet-användare. (5p)

a) **M**aximum **T**ransmission **U**nit

Det maximala antalet byte (vanligen paketets totala längden) som kan inkapslas i en ram (frame) och som det underliggande fysiska nätverket kan hantera över länken, t.ex. Ethernet har MTU på 1500 byte. Paket som är större än MTU måste fragmenteras.

b) **S**ervice **S**et **ID**

Det är namnet (ett eller två ord) på det trådlösa 802.11 nätverket som identifierar AP-tillhörighet vilket underlättar för de trådlösa enheterna att välja bland många tillgängliga trådlösa nätverk inom ett visst område. Information om SSID finns i klartext med i beacon som AP sänder regelbundet.

c) Throughput

Den effektiva (netto) överföringshastigheten som ett kommunikationsprotokoll eller system kan åstakomma vid överföringen av datamängd på en session. Den räknas som den totala antalet överförda användardatabitar delat med den totala tiden tills överföring är fullbordat.

d) Nonce

En slumpgenererat binärt tal som används vid autentisering av en slutanvädare. Talet får användas av autentiseringsprotokollet bara en gång ”once in a life time”. Nonce-användning syftar till att verifiera den som påstår sig vara en pålitlig användare och att den är aktuell (live).

e) Jitter

Det är variationen i fördröjningen som drabbar paket över Internet, så att paket tillhörande samma multimediaströmmen kommer till mediaspelaren hos mottagare olika fördröjda trots att de skickades i konstant takt från sändaren. Fördröjningen är olika pga. olika kötider på routrarna mellan sändaren och mottagren. Effekten blir hackning i t.ex. ljud om mediaspelaren spelar upp paket som de kommer utan att kompensera för jitter.

****

Lycka Till