NTNU
Norges teknisk-naturvitenskapelige universitet
Institutt for telematikk

Contact during exam

Name: Kjersti Moldeklev
Tel: 913 14 517

-

Fall exam

TTM4150 INTERNET NETWORK ARCHITECTURE

TTM4150 NETTARKITEKTUR I INTERNETT

2. December/desember 2011

Kl. 0900 - 1300

No remedies.

Results will be ready within 3 weeks.

E: English	N: Norsk/Norwegian
Glance over all pages before you start answering the exercises. **Take care to share your time between the exercises.** **It is better to answer a little on all the exercises than to answer a lot on a few.**	**Se raskt over hele oppgavesettet før du starter å besvare oppgavene.** **Pass på å fordele tiden mellom oppgavene!** **Det er bedre å svare litt på alle oppgavene enn å svare mye på noen få oppgaver.**
If you feel there is a lack of information to solve an exercise, state the assumptions you make.	**Dersom du føler informasjon mangler for å løse oppgaven, angi de antakelser du gjør deg.**

Ex/Oppg 1 Internet architecture/ Internett arkitektur

(a) **E:** The ethernet network is limited in size by the maximum distance it can span. The Internet architecture, however, allows for global communication between heterogeneous end systems running a diversity of applications, and being attached to different kinds of physical networks.
Give a short description of the internet architecture programming interface, data transmission protocols, addressing, and interconnection of networks.

N: Et ethernet nettverk er begrenset i utstrekning. Internettarkitekturen tillater imidlertid global kommunikasjon mellom heterogene endesystemer som kjører et antall anvendelser, og som er tilkoplet ulike fysiske nettverk.
Gi en kort beskrivelse av internettarkitekturens programmeringsgrensesnitt, data overføringsprotokoller, adressering og sammenkopling av nettverk.

*The **socket application programming interface** provides access to the TCP/IP communication services.*
*The **TCP/IP protocols** run between the user applications and the network driver/interface of a physical network. TCP connection oriented reliable end-to-end. IP is a connectionless best effort protocol based on datagrams.*
*Each host is assigned a **global IP address** to identify location and host.*
***Routers interconnect** the underlying networks, and forward packets from source to destination based on destination IP address and the forwarding/routing table made by the routing protocols.*

(b) **E:** IPv4 and IPv6 are distinct and different communication protocols. IPv6 is not "backward-compatible" with IPv4. Describe what is needed to transition to IPv6.

N: IPv4 og IPv6 er separate og ulike kommunikasjonsprotokoller. IPv6 er ikke bakoverkompatibel med IPv4. Beskriv hva som kreves for en overgang til IPv6.

New address (format and size) requires address translation/change in all protocol and applications utilizing IPv6 addresses – both in end system applications and in network nodes (routers). It is not possible to do the transition globally and complete in a short time. Will run IPv6 and IPv4 in parallel, or use translation protocols.

(c) **E:** One motivation behind multicast was content delivery without known receivers. This may potentially be a weakness today. Comment on why, and describe other motivations for implementing multicast in a network.

N: Et argument for bruk av multikast var leveranse av innhold uten å kjenne mottaker. I dag sees dette på som en svakhet. Kommenter hvorfor, og beskriv andre argumenter for å implementere multikast i et nettverk.

Multicast weakness: if multicast is used for a commercial service we need to know the receiver for authorisation or billing. Arguments for multicast implementation:

- *Better utilization of server capacity, bandwidth/router capacity in core and access network.*
- *Concurrent delivery*
- *Simplified administration*

(d) **E:** 2000 customers are sharing *one* single IP address. Each customer has 20 or so devices. Assume all the customer devices run web-applications.
Why might there be the case that many of the applications will fail?

N: 2000 kunder deler *en* enkelt IP-adresse. Hver kunde har ca. 20 enheter. Anta at alle kundeenhetene kjører web-anvendelser.
Hvorfor kan man oppleve at mange av anvendelsene ikke vil fungere?

Need to use NAT. Maximum port number is 64k (16 bits). Each web-client uses several TCP-connections; not enough port numbers to do all the translations between internal and external address:port.

Ex/Oppg 2 Addressing and routing / Adressering og ruting

(a) **E:** Full-cone NAT (Network Address Translation) is susceptible to port scan attacks. Why is this so, and how can this security be mitigated?

N: Full-cone NAT (Network Address Translation) er sårbar overfor portskanning-angrep. Hvorfor er det slik, og hvordan kan denne sikkerhetstrusselen begrenses?

Full cone NAT: anyone from the public Internet that wants to reach a client behind a NAT need only know the mapping scheme in order to send packets to it. May instead use: Restricted cone NAT: the external address:port pair is only opened up once the internal computer sends out data to a specific destination IP.

(b) **E:** Classless routing protocols pass the subnet mask along in routing updates, classbased protocols do not. Why this difference? Illustrate by an example.

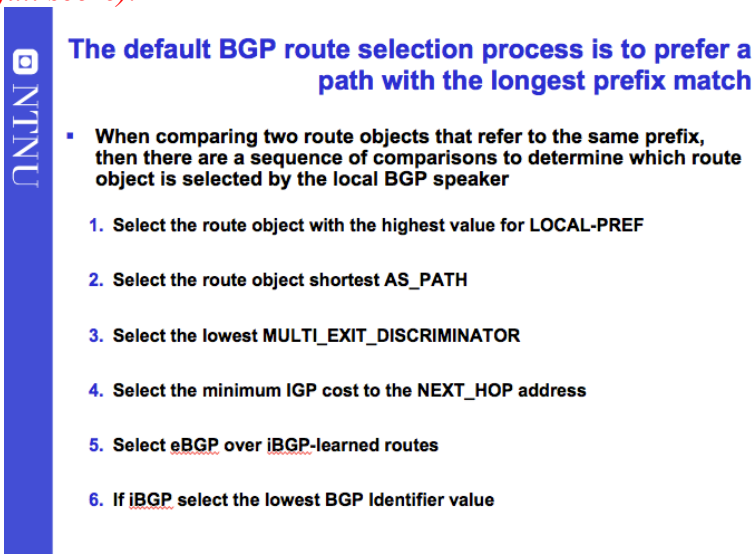
N: ”Classless” rutingsprotokoller sender subnettmasken i ruteoppdateringer, ”classbased” rutingsprotokoller gjør ikke dette. Hvorfor denne forskjellen? Illustrer ved et eksempel.

Subnet mask information clues the router in on how big the block of addresses is/the size of the network part of the address (prefix). That way, the router can tell the difference between 10.50.20.0 /24 and 10.50.20.0 /22. The former is a Class C-sized block of addresses, 256 addresses/3-byte network address. The latter is 4 Class C-sized blocks, or 1024 addresses/22 bit network address.

(c) **E:** BGP (Border Gateway Protocol) is an inter-domain routing protocol. OSPF (Open Shortest Path First) is an intra-domain routing protocol. They both use longest prefix match when choosing the route to use from the forwarding table when forwarding packets. But how does BGP select between routes when there are more routes with the same prefix and length?

N: BGP (Border Gateway protocol) er en inter-domain rutingsprotokoll. OSPF (Open shortest path first) er en intra-domene rutingsprotokoll. De bruker begge ”longest prefix match” for å velge rute fra videresendingstabellen når pakker skal videresendes. Men hvordan velger BGP mellom flere ruter med samme prefix og lengde?

BGP has additional path attributes used to choose among routes of same prefix length. In that way BGP may be more policy-based. (Two of the six below should be mentioned for full score).



(d) **E:** The BGP scalability can be reflected from the routing table size, the rate of BGP updates and routing convergence time. Give two reasons for the increasing routing table size.

N: BGP skalerbarhet reflekteres i rutetabellstørrelsen, BGP rate på ruteoppdateringer og konvergenstid i beregning av ruter. Gi to årsaker til at det stadig blir flere ruteinnslag i rutetabellen.

- *Provider independent addressing*
- *Discrete routing policy being applied to finer address blocks*
- *Multi-homing for increased reliability*
- *Multi-homing for traffic engineering*
- *Countermeasure against prefix hijacking*

Ex/Oppg 3 Congestion and QoS/Metning og QoS

(a) **E:** Give 3 ways end system protocols can use to sense that packets in the network are experiencing congestion.

N: Angi 3 måter som protokoller i et endesystem kan benytte for å oppdage at pakker opplever metning i nettverket.

*Congestion occurs when any user's traffic suffers **increased delay**, **loss** (time out or duplicate acks) or **ECN (Explicit Congestion Notification) marking** as a result of one or more network resources becoming overloaded.*

(b) **E:** Traffic management solutions limit traffic based on either bit-rate or traffic volume. Describe a scheduling algorithm that limits the traffic based on bit-rate.

N: Løsninger for å håndtere trafikk begrenser trafikken enten basert på bit-rate eller på trafikkvolum. Beskriv en "scheduling"-algoritme som begrenser bitraten til trafikken.

For instance, (weighted) fair queuing shares bit-rate when a link is congested.
Fair queuing: Traffic is explicitly separated into flows. Each flow a queue. Round-robin assures that each flow gets fair access to network resources – no flow gets more capacity than an other. (Implemented eg by simulated bit-by-bit fair queuing. Scheduler selects the packet with earliest finish time as next packet for transmission)
Weighted fair queuing: Each flow given a weight of bandwidth independent of packet size. Each flow assigned a weight = number of bits transmitted when the flow is served (FQ weight=1).

(c) **E:** Which performance parameters are the most important for real-time interactive traffic? Which treatment is required in the routers to support such traffic?

N: Hvilke ytelsesparametere er de viktigste for sanntids interaktiv trafikk? Hvilken behandling kreves i ruterne for å støtte slik trafikk?

For real-time interactive traffic low delay and predictable jitter (delay variation) are critical. (Too much loss is also hard to correct.) Such traffic needs specific treatment:

scheduling (priority to reduce the delay/delay variation) and active queue management (packet drop of non real-time traffic).

(d) **E:** Describe the difference between the two traffic condition mechanisms *policing* and *shaping*. Comment on their combination with marking and their application on inbound/outbound direction of a network interface.

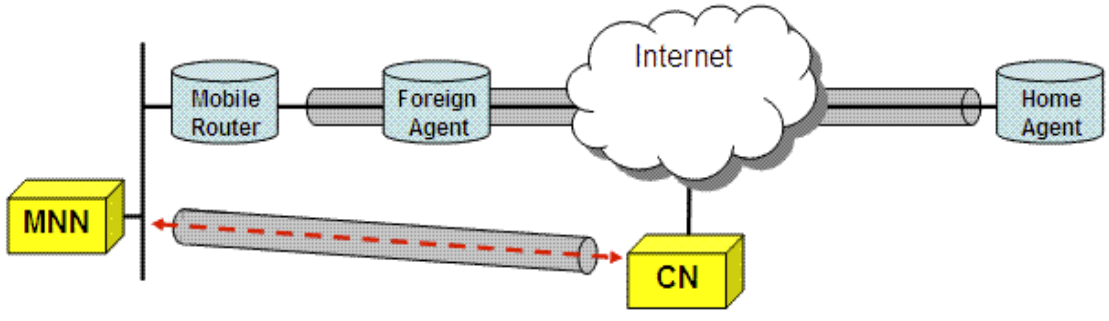
N: Beskriv forskjellen mellom de to trafikkhåndteringsmekanismene ”*policing*” og ”*shaping*”. Kommenter også på kombinasjon av disse med ”marking” og deres anvendelse på inn/ut retningen av nettverksgrensesnittet.

Policing—*Policing typically limits bandwidth by discarding traffic that exceeds a specified rate. Policing can be used to remark traffic that exceeds the specified rate and attempt to send the traffic anyway. Can be used in either inbound or outbound direction.*
Shaping—*Shaping limits excess traffic by buffering not by dropping. This buffering of excess traffic can lead to delay. Unlike policing, shaping cannot remark traffic. Shaping can be applied only in the outbound direction on an interface.*

Ex/Oppg 4 Mobility and ad-hoc networks/ Mobilitet og ad-hoc nettverk

(a) **E:** The figure below illustrates the communication between a MNN (Mobile Network Node) and a CN (Corresponding Node). With your knowledge of mobility in the internet describe what the figures illustrates.

N: Figuren under illustrerer kommunikasjon mellom en MNN (Mobile Network Node) og en CN (Corresponding Node). Med din kunnskap om mobilitet i internett, beskriv hva figuren illustrerer.



As the whole mobile network moves, the MNN can keep its address attached to the mobile router. It does not need to be aware of change of point of attachment. Two addresses: home address (node endpoint identifier) and care of address (point of attachment/routing directive). The network mobility basic protocol:

- *HA: packets routed via HA. Get location update (on a whole prefix) from mobile router (or FA w/MIPv4). (MIPv4 Foreign agent: Allocate care of address)*

- *Tunnel: from HA to MR (FA w/MIPv4) The figure shows IPv6 as tunnel is between home agent (HA) and mobile router (MR).*
- *Traffic from CN via HA to MNN (FA w/MIPv4)*

Route optimization would allow a way for MRs or MMNs to send packets directly to CNs. The Figure illustrates this direct communication between MNN and CN via a tunnel. Mobile IP nodes send Binding Updates with current CoAs to their CNs as they change attachment points to the Internet. Mobile nodes and CNs are then able to directly communicate using the CoA of the mobile node.

(b) **E:** Describe two required network functions to support communication continuity when a device changes topological point of attachment.

N: Beskriv to nødvendige nettverksfunksjonene for å opprettholde kommunikasjon når en enhet bytter topologisk tilknytningssted.

Handover Management: *The most important function needed to support mobility is to keep the ongoing communication alive while a mobile node (MN) moves and changes its point of attachment to the Internet. In order to continue to communicate, handover management is required. Its main objective is to minimize service disruption during handover.*

Location Management: *Another important function needed to support mobility is the reliable and timely notification of the MN's current location to those other nodes that need it. The technique to track the desired MN is called location management. Location management involves identifying the current location of the MN and also keeping track of their location changes as it moves on.*

(c) **E:** Explain the 3 performance metrics that are the most relevant for internet mobility.

N: Forklar de 3 ytelsesparameterne som er viktigst for internett mobilitet.

Handover latency *refers to the elapsed time from the last packet received via the old network to the arrival of the first packet along the new network during a handover.*
Packet loss *is defined as the number of packets lost while maintaining communication during a handover.*
Signalling overhead *is defined as the number of messages for the handover and location procedures.*

(d) **E:** What characterize an ad-hoc network?

N: Hva karakteriserer et ad-hoc nettverk?

No formal structure with core, backbone etc: Any host can play any role, must be able to forward
Host are mobile: Link breaks are part of normal operations
Wireless interconnect: Radio or infrared, not necessarily bi-directional connectivity

(e) **E:** What are channel and topology challenges when implementing ad-hoc networks?

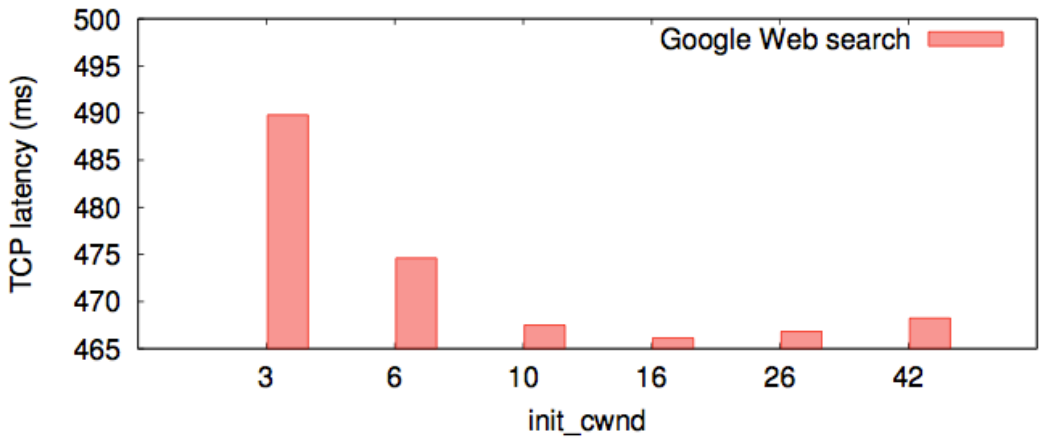
N: Hva er kanal- og topologiutfordringer i implementasjon av ad-hoc nettverk?

- *Nodes share a channel, not a link (Interference, packet collision. Resource allocation not feasible on a per link basis*
- *Interference: Signals from different sources may interfere and cause bit errors.*
- *Bit error rate vary over time (packet loss is normal and not necessarily a sign of congestion)*
- *Trade-off on transmission power. Higher power means: fewer hop to destination (larger number of other terminals are blocked or create interference. Reduced power increase likelihood of partitioning)*
- *Topology: hidden terminal, exposed terminal*

Ex/Oppg 5 Transport protocols/Transportprotokoller

(a) **E:** The figure below shows the TCP latency of Google search for different values of TCP initial congestion window. Give your comments to the figure.

N: Figuren under viser Google søk TCP-forsinkelse for ulike verdier av TCP initialt metningsvindu. Gi dine kommentarer til figuren.



A search request-response transfers a small amount of data. Thus the slow start and its initial congestion window size will have effect on measured latency. Using 6/10 segments improves the average TCP latency compared to using 3 segments. Raising init cwnd to 16 improves latency further. However, much larger values, such as 42, show degradation in latency, likely due to increased packet losses.

(b) **E:** Describe two TCP extensions for higher performance over paths with large bandwidth-delay products.

N: Beskriv to TCP-utvidelser for høyere ytelse over ruter med et stort ”bandwidth-delay” produkt.

Window scaling, timestamps, and protection against wrapped sequence numbers, for efficient and safe operation over paths with large bandwidth-delay products.

“Window scale” option: *Do a shift-operation on advertised window.*
“Round trip time measurement” option: *Store a time stamp in outgoing segments.*
*-**“Sequence number wrap around”:** use a 32-bits time stamp to extend the sequence number space.*
(Selective acknowledgment)

(c) **E:** The Datagram Congestion Control Protocol (DCCP) is for applications with large or long-lived flows of datagrams. The underlying motivation is to avoid congestion collapse. Why is such a protocol requested?

N: The Datagram Congestion Control Protocol (DCCP) er for anvendelser mer store eller langvarige flyt av datagram. Den underliggende motivasjonen er å unngå metningskollaps. Hvorfor er en slik protokoll etterspurt?

There is a changing traffic mix towards long-lived non-congestion-controlled: Audio, internet telephony, multiplayer games.
DCCP supports unreliable datagram delivery with built-in congestion control.