NTNU
Norges teknisk-naturvitenskapelige universitet
Institutt for telematikk

Kontakt ved eksamen/Contact during exam

Name: Kjersti Moldeklev
Tel: 913 14 517

-

TTM4150 NETTARKITEKTUR I INTERNETT

TTM4150 INTERNET NETWORK ARCHITECTURE

December 15, 2008
Kl. 0900 - 1300

.

No remedies/Ingen hjelpemidler.

Results will be ready before 190109.
Sensuren faller innen 190109.

E: English
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.

If you feel there is a lack of information to solve an exercise, state the assumptions you make.

N: Norsk/Norwegian
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.

Dersom du føler informasjon mangler for å løse oppgaven, angi de antakelser du gjør deg.

Exercise 1 Internet architecture/ Internett arkitektur

(a) **E:** A network architecture is a set of high-level design principles that guide the technical design of the network, especially the engineering of its protocols and algorithms.
What was the top-level goal of the original Internet architecture?

N: En nettverksarkitektur er et sett av høynivå designprinsipper som gir retningslinjer for design av nettverket, spesielt konstruksjon av protokoller og algoritmer.
Hva var det primære målet til Internett-arkitekturen?

Top level goal was effective interconnection

- *an effective technique for multiplexed utilization of existing interconnected networks using packet switching as a fundamental component for multiplexing*
- *interconnected by routers: store-and-forward forwarding of variable length packets*

(b) **E:** One of the second level goals is that "The Internet must support multiple types of communications service."
How does the original internet architecture satisfy this goal?

N: Ett av de sekundære målene var "The Internet must support multiple types of communications service."
Hvordan tilfredsstiller den originale internettarkitekturen dette målet?

Dumb network with intelligence at the edge

- *End-to-end service in the transport layer and above*
- *Different end-to-end transport protocols offer different service*

(c) **E:** To assign a primary IP address and a network mask to a network interface, the following command may be used: "IP <IP address>/mask".
When and why is the mask attribute needed?

N: For å tilordne en primær IP-adresse og en nettverksmaske til et nettverks-grensesnitt kan den følgende kommandoen benyttes: "IP <IP address>/mask". Når og hvorfor trengs "mask" attributtet?

A mask identifies the bits that denote the network number in an IP address. When you use the mask to subnet a network, the mask is then referred to as a subnet mask. It is necessary when classless addressing is used.

(d) **E:** First-in, first-out (FIFO) queuing is an example of which service model?
N: First-in, first-out (FIFO) køing er eksempel på hvilken tjenestemodell?

A. Differentiated Service
B. Traffic engineering Service
C. Integrated Service
D. Best-Effort Service

Answer: Best Effort Service

Exercise 2 Forwarding and routing/ Videresending og ruting

(a) **E:** Describe three of the operations a router performs when forwarding a unicast packet in a router without any QoS (quality of service) processing.

N: Beskriv 3 operasjoner som en ruter utfører når den videresender en unicast pakke uten QoS (quality of service) prosessering.

Validate the IP header, decrement TTL, longest prefix matching, CRC calculation, possible check for fragmentation.

(b) **E:** Describe the interrelationship between congestion in a router and end-to-end jitter?
N: Beskriv sammenhengen mellom metning i en ruter og ende-til-ende jitter.

Jitter is defined as a variation in the delay of received packets. At the sending side, if packets are sent in a continuous stream with the packets spaced evenly apart, due to congestion and thereby varying queuing delay, the delay between each arriving packet can vary instead of remaining constant.

(c) **E:** Suppose we choose a larger buffer for a queue in a congested router. Which of the below results A-D is correct?
N: Anta at vi velger et større buffer for en kø i en ruter i metning. Hvilke av resultatene A-D under er korrekt?

A. Longer end-to-end delay, less packet loss
B. Longer end-to-end delay, higher packet loss
C. Shorter end-to-end delay, less packet loss
D. Shorter end-to-end delay, higher packet loss

Answer: A

(d) **E:** A DiffServ core router distinguishes between packet flows in implementing different Per-Hop Behaviors (PHBs) by using which of the statements A – E below?

N: En DiffServ kjerneruter skiller mellom pakkeflyt når den implementerer ulike Per-Hop Behaviors (PHBs) ved å benytte hvilke av punktene A-E under?

A. Source IP address, destination IP address, and packet markings
B. Source and destination IP addresses
C. Source and/or destination port numbers
D. Packet markings alone
E. None of the above

Answer: D

(e) **E:** IPVPN is a virtual private network based on internet technology.
Briefly describe two different ways of assuring private exchange of routing information between provider edge routers within a layer 3 provider-provisioned IPVPN.

N: *IPVPN er et virtuell privat nettverk basert på internetteknologi.*
Beskriv kort to ulike måter å sikre privat utveksling av rutinginformasjon mellom operatørens kantrutere i et lag 3 "provider-provisioned" IPVPN.

Per-VPN routing/Virtual routers: Intra-domain routing protocol between virtual routers of the actual VPN. Multiple virtual routers within a single physical provider edge router. Each logical router maintains its own entirely separate routing protocol instance of reachability information. Routing protocol packets for each VPN tunneled between provider edge routers.
Aggregated routing (BGP/MPLS): Routing information for multiple different VPNs is aggregated into a single inter-domain routing protocol running between provider edge routers in the VPN. Provider edge devices maintain separate routing and forwarding tables per VPN. The Internet topology has changed from core and stubs to a large number of peer routing autonomous domains.

Exercise 3 Mobility / Mobilitet

(a) **E:** Why is the DNS (domain name system) not suited as a location database in a mobility scheme?

N: Hvorfor er DNS (domain name system) ikke egnet til å være lokasjonsdatabase for mobilitet?

DNS relies on caching to scale. Several servers may therefore contain the mapping from logical name to IP address.

(b) **E:** How is DNS used in some mobility schemes, for example in HIP (host identity protocol)? Describe why this is a workable solution.

N: Hvordan er DNS benyttet i noen mobilitetsløsninger, for eksempel i HIP (host identity protocol)? Beskriv hvorfor dette er en løsning som fungerer.

DNS is used at pointer to the mobility location database. The name of the location server varies with the scheme. The IP address of the location server changes seldom. It is the mapping between Host id and location that changes.

(c) **E:** An enterprise is multi-homed between two different ISP. Both accesses are active and carry traffic. The enterprise runs mobile IP v4. One of the ISP offers to run the enterprise's Mobile IP home agent (HA) in its network.
What is your recommendation? Describe why.

N: Et selskap er multi-homed mellom to ulike ISPer. Begge aksessene er aktive og bærer trafikk. Selskapet benytter mobil IPv4. En av ISPene tilbyr å kjøre selskapets mobil IP hjemmeagent (HA) i sitt nettverk.
Hva er din anbefaling? Beskriv hvorfor.

The HA (home agent) must be on the path between any corresponding node and the mobile node. With multi-homing the HA cannot be located in one of the ISPs. Recommendation should be a strong no

(d) **E:** Describe the two major security threats that must be considered when evaluating a mobility scheme, and how these are addressed in mobile IPv4.

N: Beskriv de to primære sikkerhetstruslene som må vurderes ved evaluering av en mobilitetsløsning, og hvordan disse håndteres i mobil IPv4.

Address hijacking and DOS attacks. MIPv4 uses authentication between MB and HA to count against address hijacking. DOS attacks are not an issue. A MN can start a download from a server and then update its location to the intended victim. The corresponding node is unaware of the movement and cannot use a four-way handshake. However, the victim

will be bombarded with tunneled packets from the HA. The result is as trackable and preventable as any DOS attack from a known address. The advantage is that the HA will presumably be better managed than any user terminal.

Exercise 4 Multicast / Multikast

(a) **E:** What are the deployment issues regarding multicast addressing in IPv4? Are these the same for deployment of multicast IPv6 addresses?

N: Hvilke utfordringer representerer multikast IPv4 adresser i forhold til bruk av multikast i nettverk? Er disse de samme for bruk av multikast IPv6 adresser?

Flat multicast address space from 224 to 239.255.255.255. Addresses a session. Most are temporary addresses. Temporary addresses without authentication are vulnerable against address collision, address hijacking and so on. Few addresses allocated to know protocols, one address range with AS id in byte 2 and 3.
In IPv6 half the address space is permanent, and the issues can be avoided.

(b) **E:** Given that PIM-SM is used, what are the arguments against placing the processing of multicast packets in the router's critical path.

N: Gitt at PIM-SM benyttes, hvilke argumentene taler mot å plassere prosessering av multikastpakker i ruterens kritiske sti?

There are two forwarding mibs (S,G) and (,G). If neither of these exists, the packet must be tested against whether it originated from a src that the router is leaf router to. In addition RPF check. Short version of answer: multicast processing contains several tests for various conditions. Not suited for the fast processing on the critical path.*

(c) **E:** Justify the number of RP's (rendezvous points) in a domain running PIM-SM (protocol independent multicast - sparse mode).

N: Rettferdiggjør antallet RPer (rendezvous point) i et domene som benytter PIM-SM (protocol independent multicast - sparse mode).

In principle only one, since the RP is the aiming point for building the distribution tree. However, there can be multiple RP if they run a source distribution protocol like MSDP between them. (Either answer should give full score.)

Exercise 5 Ad-hoc network protocols / Ad-hoc nettverksprotokoller

(a) **E:** In the reactive protocol AODV (ad-hoc on-demand distance vector) there is a seqno for each route request (RREQ). In addition there is a need for a sequence number in the RREQ associated with the destination. Explain why?

N: I den reaktive protokollen AODV (ad-hoc on-demand distance vector) er der et sekvensnummer for hver ruteforespørsel (RREQ). I tillegg er der behov for et sekvensnummer i RREQ assosiert med destinasjonen. Forklar hvorfor.

Each request is to be broadcasted once, the sequence number is used to enforce this. Stale routes are when an intermediate route reports a path to dst that is no longer valid, i.e an old route. When a src floods a RREQ it contains a seq no. The intermediate nodes must have a path with a higher or equal seq no in order to respond to the request. Whenever a path is invalidated, the src increases the seq no before it sends out a new RREQ. Only the dst can then respond. The dst will put the highest seq in the RRESP message to ensure that all nodes with a valid path has the same seq no.

(b) **E:** What are the most advantageous usage scenarios for geographic routing? Justify your answer and give a separate answer for unicast and for multicast.

N: Hva er det mest fordelaktige bruksscenario for geografisk ruting? Begrunn svaret og bruk separate beskrivelser for unicast og for multicast.

Geographic routing unicast consists of location updating/finding and the routing. The longer the lifetime of a location, the less impact will location updating have on the performance. The most advantageous usage scenarios are therefore when the nodes have minimal movement.
For multicast, geographic routing is most useful when information is sent to nodes within a limited geographic area, like around a famous building.

(c) **E:** What role does the MRP (multi relay point) have in the proactive routing protocol OLSR (optimized link state routing), and how does this role impact the overhead of the routing protocol?

N: Hvilken rolle har MRP (multi relay point) i den proaktivte rutingprotokollen OLSR (optimized link state routing), og hvordan påvirker denne rollen rutingsprotokollens ”overhead”?

The MPR generates and relays the topology information from other nodes and only links between MPR and leaf nodes are reported (recommended option). The first implies a more efficient flooding of information. The latter results in smaller packets.

Exercise 6 Congestion control/ Metningskontroll

(a) **E:** What indicates that a network interface in a router experiences congestion?

N: Hva indikerer at et nettverksgrensesnitt i en ruter opplever metning?

An interface experiences congestion when it is presented with more traffic than it can handle: Buffers get filled, and packets dropped.

(b) **E:** DCCP (datagram congestion control protocol) is a transport protocol for unreliable flows, with the application being able to specify either TCP-like or TFRC (TCP friendly rate control) congestion control. DCCP also supports ECN (explicit congestion notification).
Describe how ECN works.

N: DCCP (datagram congestion control protocol) er en transportprotokoll for upålitelige flyt hvor applikasjonen kan spesifisere enten TCP-liknende eller TFRC (TCP friendly rate control) metningskontroll. DCCP støtter også ECN (explicit congestion notification).
Beskriv kort hvordan ECN virker.

Explicit congestion notification (ECN) responds to congestion by marking packets in routers. Experienced (CE) bit set in IP TOS byte by routers when congestion is experienced.
A single packet with the CE code point set in an IP packet causes the transport layer to respond, in terms of congestion control, as it would to a packet drop.

(c) **E:** Random Early Detection (RED) is a congestion avoidance mechanism that takes advantage of TCP's congestion control.
Describe the RED mechanism.

N: Random Early Detection (RED) er en mekanisme for "congestion avoidance" som drar fordel av TCP sin metningskontroll.
Beskriv RED mekanismen.

RED (Random Early Detection) monitors average queue length and drops before buffer is full.
Drop packets with a drop probability when the queue is longer than a given drop level.
Configurable drop profile for the packet discard process
*Compute average queue length (AvgLen=(1-Weight)*AvgLen+Weight*SampleLen)*
SampleLen is the queue length each time a packet arrives
Two queue length thresholds, MinThreshold & MaxThreshold

- *If AvgLen <= MinThreshold queue packet*

- *If MinThreshold <= AvgLen < MaxThreshold compute probability P and drop arrive packet with this probability*
- *If MaxThreshold <= AvgLen drop arriving packet*

E: Which of A-E below describe benefits of the scheduling discipline WFQ (weighted fair queuing)?

N: Hvilke av A-E under beskriver fordelene med købetjeningsdisiplinen WFQ (weighted fair queuing)?

A. WFQ is very easy to configure, and no manual traffic classification is necessary.

B. WFQ can provide fixed-bandwidth and fixed-delay guarantees.

C. WFQ alone can provide fixed-bandwidth guarantees.

D. WFQ can provide fixed-delay guarantees.

E. WFQ prevents the large-volume flows with large packet size from starving out the low-volume flows with small packet size.

F. Based on DSCP, WFQ allows weighted, random dropping of packets when the WFQ system is full.

Answer: AE