NTNU
Norges teknisk-naturvitenskapelige universitet
Institutt for telematikk

Kontakt ved eksamen/Contact during exam

Name: Kjersti Moldeklev
Tel: 91314517

TTM4150 NETTARKITEKTUR I INTERNETT

TTM4150 INTERNET NETWORK ARCHITECTURE

Desember/December 7, 2009
0900 - 1300

Ingen hjelpemidler/No remedies.

Sensuren faller innen 4 uker/Results will be ready within 4 weeks.

N: Norsk/Norwegian
Se raskt over hele oppgavesettet før du starter å besvare oppgavene.
Pass på å fordele tiden mellom oppgavene!
Noen av svarene krever en dypere analyse enn for eksamensoppgaver fra tidligere år. For hver oppgave er det angitt maksimal poengsum **(p)** som reflekterer forventet arbeidsbelastning.

E: English
Glance over all pages before you start answering the exercises.
Take care to share your time between the exercises.
Some of the questions in this exam require a more in-depth analysis. For each question, there is a max score **(p)** assigned to reflect the expected amount of work.

Oppgave/Exercise 1 Arkitektur/Architecture

(a) **(4p)**

N: Det viktigste målet for Internett-arkitekturen var å utvikle en effektiv teknikk for å multiplexe trafikk over eksisterende nettverk. Beskriv kort lagene i internettarkitekturen.

E: The top level goal for the Internet architecture was to develop an effective technique for multiplexed utilization of existing networks. Shortly describe the layers of the Internet architecture.

Non-integrated, layered architecture, horizontal layering, clear separation between data transport and applications:
Application: The program that communicates across the network.
Transport: This layer should support a variety of types of service. Different types of service are distinguished by differing requirements for such things as speed, latency and reliability.The traditional type of service: bidirctional virtual circuit (TCP). UCP was created to provide a applicationlevel interface to the basic datagram service of Internet
Interworking: The layer for interconnecting existing networks for efficient multiplexed utiliztion. Basic building block: datagram (connectionless packetswitching)
Network interface: (Interface to) the underlying existing networks

(b) **(4p)**

N: Hva er en “IP address mask”, og hvordan brukes den?

E: What is an IP address netmask, and how is it used?

The netmask indicate the length of the IP-address that is be used in routing protocols and packet forwarding. A bitwise AND between the IP-address and the netmask gives the network part of the address.

(c) **(8p)**

N: Internettarkitekturen er i utvikling. Den er ikke lenger en ren lagdelt arkitektur med isolerte lag. Beskriv kort to tilfeller hvor det er kommunikasjon/informasjonsutveksling mellom transportprotokollen og ett av lagene under.

E: The Internet architecture has evolved and is not a pure layered architecture with isolated layers. Shortly describe two cases where there is inter-layer communication/information exchange between the transport protocol and one of the layers below.

Path MTU (maximum transmission unit) discovery: to find smallest MTU of networks between two communicating end systems for optimal TCP byte stream segmentation: -Send IP datagram with DF ”don't fragment” bit
-Router returns ICMP message ”unreachable” if datagram too big
-ICMP message returns MTU of next hop
-ICMP-message received and TCP reduces MSS and retransmits

(About every 10 minutes, try a larger MSS. But, TCP implementation often use the default MSS of 536 to non-local hosts)

ECN (explicit congestion notification): Explicit congestion notification (ECN) responds to congestion by marking packets in routers. Motivation: As opposed to solely relying on implicit TCP congestion notification (packet drop).
Destination TCP host sends explicit notification to source TCP host dependent on value of ECN bit in the IP header.

(d) **(4p)**

N: Som en del av utviklingen av ruterarkitektur har ruteoppslag og videresending blitt flyttet fra en sentral CPU til egne CPUer på nettverksgrensesnittkortene. Hva er fordeler og ulemper med dette?

E: In the evolution of router architecture routing lookup and forwarding were moved from a central CPU to CPUs at the network interface cards. What are the advantages and disadvantages?

The interface cpu has a routing table cache and a mac header cache. It moved the packet directly to the outgoing interface. This implies less traffic on the bus (a packet traverse the bus once) and an offloading of the central cpu. The disadvantages are the delay to fill the route cache for the first packet and the need for cache invalidation. The potential for load sharing is limited

Oppgave/Exercise 2 Ruting/Routing

(a) **(4p)**

N: Hva er forskjellene mellom multikast-videresending av pakker i en ruter i et trådbasert nettverk og i en ruter i et trådløst nettverk?

E: What is the difference between multicast packet forwarding in a router in a wired network and in a router in a wireless network?

In a wired mulitcast router there needs to be a forwarding table given the interfaces a packet must be sent over. Depending on the protocol used, the forwarding table can be by src, group. In wireless environment the router only needs to determine whether to retransmit or not. Another major difference is that in wired routers a multicast packet is never forwarded on the interface it was received on, while in wireless environment they always are (given one antenna nodes)

(b) **(20p)**

N: Hva er det fundamentale problemet ved å håndtere sesjonsmobilitet i Internett? Skisser en generisk løsning og elementene som inngår i en slik løsning. Til slutt, diskuter hvordan mobilitetshåndtering kan implementeres på ulike nivåer i protokollhierakiet. Kommenter på likheten og de viktigste forskjellene mellom løsningene.

E: For session mobility in the Internet, discuss the fundamental problem. Outline the generic solution and the elements in such a solution. Finally, discuss how mobility can be implemented at different layers in the protocol hierarchy. What is the commonality between the solutions and what are the major differences?

Need to discuss location and end point identity of IP addresses. How to map one into the other. Elements in the solution are address translation, location directory and, location update. Network layer MIPv4 tunnel , mipv6 tunnel + address translation in src, link6 network prefix substitution to a prefix reserved for mobility, networklayer +, hip with a location end point address mapped to a locator address by a rendezvous server(RVS). First packet by RVS, rest by src.
Trnsport by separate protocol like Mobile Stream Control Transmission Protocol (MSCTP) where new endpoint and src can be added to a bundle, TCP and DCCP extensions where transport endpoint is mapped to new IP addresses, or proxy that hides the mobility and new or extended protocols between proxy and mobile node. General problem with transport solutions is to find the mobile host to initiate the flow. At application layer sip with location directory and reinvite is an example. IP sec can also be discussed since IPsec is tunneling, but it is only done for certain applications or usage scenarios.
Commonality is the mapping and the for network and network + and sip the location directory in the the location of the mobile node.
Difference is given by the specifics of the solution.

(c) **(10p)**

N: Beskriv de ulike fasene eller elementene i PIM-SM (protocol independent multicast – sparse mode) samt de korresponderende protokollmekanismene. Et eksempel på et element er etablering av et "shared" tre. Hva er motivasjonen for disse elementene og for valget av protokollmekanismer?

E: Describe the different phases or elements in the PIM-SM (protocol independent multicast – sparse mode) and the corresponding protocol mechanisms. One example of an element is the establishment of a shared tree.

What is the motivation for these elements and for the selection of the corresponding protocol mechanisms?

Etablering av shared tree, receiver sends join towards the rendvous point. Establish a common distribution tree to discover src and rec information efficient distribution mechanisms, but with unnecessary delay. Rec initiated since the the assumption is that only a few nodes are interested.
Src sends packet to the RP by tunnel until the RP establish a tree towards src SRc and rec are not coordinated and src has no knowledge of receivers. Must be tunneled to a known location MC address cannot be used to forward a packet before a tree is established
RP estabklish a source specific tree to src by sending join motivated by avoiding tunneling
Rec establish a source specific tree towards src (optional) Potentially a faster distribution tree
If this is the case rec decouples from the shared tree for this particular src by sending leave message to RP.

(d) **(4p)**

N: Beskriv kravet til "opaque packet transport" i VPN (virtual private network), og hvordan dette er hensyntatt i "provider-edge based layer 3 VPNs"?

E: Describe the VPN (virtual private network) requirement "opaque packet transport", and how this is reflected in provider-edge based layer 3 VPNs.

Opaque packet transport:
Isolated routing - VPN may use private IP addresses: VPN addresses may overlap with addresses of other VPNs (within an VPN addresses must be unique)
Isolated data forwarding - VPN traffic no relation to rest of IP backbone traffic.

Tunneling and vpn-identifier: Identifies the "scope" of a private IP address and the VPN to which the packet belongs. PE devices maintain tunnels and per-VPN state including virtual forwarding instance. The VFI is a logical entity that contains the routing and the forwarding table for a single VPN.

Oppgave/Exercise 3 Metning og tjenestekvalitet/ Congestion and quality of service

(a) **(4p)**

N: Definer "congestion" og "congestion collapse".

E: Define congestion and congestion collapse.

Congestion: when data must be discarded due to: - A router receiving data faster than it can be forwarded - A receiver with more data than it can handle (handled by e2e flow control)
Congestion collapse gives small effective throughput - Bandwidth is wasted by delivering packets through the network that are dropped before reaching their destination -Primarily due to open-loop applications not using end-to-end congestion control

(b) **(10p)**

N: Beskriv "best-effort congestion control" i TCP. Hvordan er det mulig å øke ytelsen til forbindelser med kort levetid?

E: Describe the TCP best-effort congestion control. How is it possible to increase the performance of short-lived connections?

Internet (TCP) best-effort congestion control objective: adapt to change in available capacity -Challenge: What is available network capacity? End-system oriented, feedback-based, window-based. CongestionWindow is changed by

(1) Additive Increase: Increment CongestionWindow with one segment per RTT (additive increase) Multiplicative Decrease: Decrease CongestionWindow when congestion increases. Divide CongestionWindow by 2 at timeout.
(2) Slow Start: Slow start increases congestion window exponentially. Objective: To faster decide available capacity in network. Start by setting CongestionWindow = 1 MSS. Double CongestionWindow each RTT (increment with 1 MSS for each acknowledgement)
(3) Fast Retransmit, Fast Recovery: Problem: TCP time-out interval is coarse and give periods without data flow.
"Fast retransmit": Use (3) acknowledgment duplicates to trigger retransmission. Receiver sends acknowledgement for packets received out of order. "Fast recovery": Remove slow-start phase; go directly to half the previous successful congestion window. Slow start only at start and with T.O. (not when "fast retransmit").

Short-lived connection can get a higher performance through a larger initial window size. Small transfers can finish within 1 RTT

*(Increase initial window from one or two segment(s) to roughly 4K bytes. "The upper bound for the initial window is min (4*MSS, max (2*MSS, 4380 bytes))"*

(c) **(4p)**

N: IP tale- og videotelefoni tilbys privatkunder både av nettverksoperatører og av 3. parts "overlay" operatører uten et eget IP-nettverk. Beskriv *tjenestekravene* som stilles av tale- og videotelefoniapplikasjoner.

E: IP voice and video telephony services are offered to residential users by both network operators and by 3rd party overlay service operators without an IP network. Describe *service requirements* related to voice and video telephony applications.

Real-time video, voice telephony/conference service requirements: Low jitter and delay, low loss rate. Video requires sufficient bandwidth.

(d) **(14p)**

N: Diskuter ulike tjenestekvalitetsmekanismer tilgjengelig for henholdsvis en nettverksoperatør og en 3. parts "overlay" operatør uten eget nettverk for å oppfylle tjenestekvalitetskravene over.

E: Discuss quality of service mechanisms available to a network operator, respectively a 3. party overlay operator without its own IP-network, for fulfilling the requirements above.

NETWORK OPERATOR	***3rd PARTY OVERLAY SERVICE PROVIDER***
Can utilize machanisms both in network provider and customer equipment.	*Can only utilize mechanisms in customer equipment and application servers.*
Service specification – SLS (Service Level Specification):	
-Traffic specification – what does the traffic look like? Bandwidth, delay and jitter, burst size	
- Service guarantees: Guaranteed mean time between failure (MTBF). Bandwidth, delay, jitter, packet loss	*- Serice guarantees: Guaranteed mean time between failure (MTBF) – not as strict as no control over internetwork.*
-Service level monitoring: Traffic Conditioning Agreement (TCA) - Assure, control, monitor traffic flow.	*-Service level monitoring only at the endpoints!*
Operator vs customer: Pricing and billing procedures. Consequence of breach of contract.	*Operator vs customer: Pricing and billing procedures. Consequence of breach of contract.*
Admission control:	
Decide if a "connection/flow" is accepted or rejected into the network	*Decide if a "connection/flow" is accepted or rejected depends on the total load of the input link and application servers, not the IP-network per se.*
***Traffic monitoring**:*	
Network nodes collect and store statistics about traffic. Eg. per service class – metering	*Only at endpoints.*
***Packet classification**:*	
Each packet associated with a corresponding reservation/traffic class for the packet to be treated correctly -Source and destination address and port (IPv4) -Traffic class (in IPv4 TOS field), flow identification (IPv6)	*Only within end points – eg upstream in customer telephone adapter*

Packet marking *based on classification criteria. Packets which do not comply with the agreed traffic contract are marked as best-effort or dropped*	
Traffic conditioning includes metering, marking, shaping, policing *Monitor traffic and take actions if traffic not according to agreement* *-E.g. dropped or (re)marked* *Policing different from admission control.* *Policing checks compliance, shaping changes/delays the packet flow to be in accordance with traffic specification (leaky bucket, token bucket)*	*Only within end points*
Scheduling and active queue management *In all nodes end-to-end.* *Eg priority queueing for voice*	*Only at end-points*
Resource reservation and congestion control *In all nodes end-to-end*	*Only at end-points*