NTNU
Norges teknisk-naturvitenskapelige universitet
Institutt for telematikk

Contact during exam

Name: Kjersti Moldeklev
Tel: 913 14 517

-

Fall exam

TTM4150 INTERNET NETWORK ARCHITECTURE

Wednesday December 5, 2007
Kl. 0900 - 1300

.

No remedies.

Results will be ready before 07.01.08.

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.

Exercise 1 Internet architecture

In a Norwegian newspaper article Google's" chief Internet evangelist" Vinton Cerf is quoted as follows: "*If Internet is to continue its development and stimulation of innovation, it cannot be divided into two. Internet is big, and the point is that nobody owns it. The network shall be open and neutral*".

(a) Comment on this statement, and specifically on the point of view of how internet providers want to use "next generation internetwork" mechanisms to "divide the internet into two".

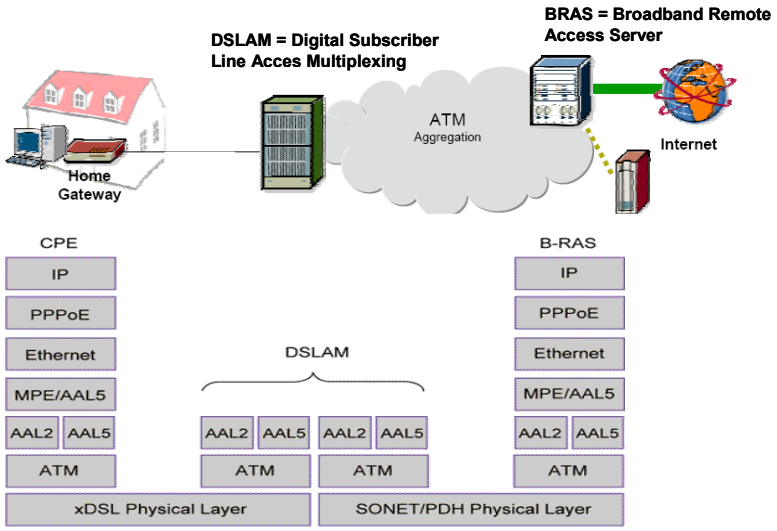
Dividing the internet into two by QoS-mechanisms – one part for paying customers and one for others. Customers may pay for a specific application which traffic is given special treatment by "right of way"/priority etc.

In the Internet best-effort packet-switched network end-to-end congestion control is a major issue for its success. Internet as a multi-service network needs to support the transport of real-time applications.

(b) Describe how quality-of-service and end-to-end congestion control are two of a kind when it comes to supporting real-time application streams to avoid congestion collapse in the Internet. Relate your discussion to the end-to-end argument.

QoS-based networks pre-allocate sufficient resources to satisfy quality of service requirements and avoid congestion. (Resource reservation, router-oriented, rate-based)
End-to-end congestion control as in TCP (end-system, feedback, window-based) aim at finding the rate the sender may send at to avoid congestion.
Resource reservation violates the end-to-end argument, while congestion control (TCP) may be done solely in end systems.

The figure below shows the network architecture and protocol stack for an xDSL-based access network. The public IP-address is handed out by PPPoE (Point-to-point Protocol over Ethernet).



(c) Which challenges do you see to implement the TV component of 3-play (internet access, VoIP, and TV broadcast) in this architecture?

There is a virtual point-to-point link between the BRAS and the home gateway. There can be no IP multicast from BRAS and out and this will give bandwidth and performance challenges. DSLAM should perform IP multicast so only need one stream of same content to the DSLAM.

(d) Routers perform statistical multiplexing. What are tradeoffs related to the size of the buffers of a router performing statistical multiplexing?

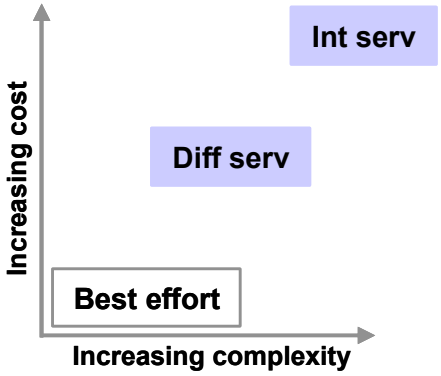
The buffers need to be large enough for traffic bursts, but small enough for the RTT to remain acceptable. This among others to avoid mistakenly retransmission of packets.

Exercise 2 Quality of service

(a) What quality of service parameters can be affected by statistical multiplexing

Bandwidth/Throughput, Delay, Variation in delay (jitter = The change in inter-packet latency within a stream over time), Packet loss – arise from congestion.

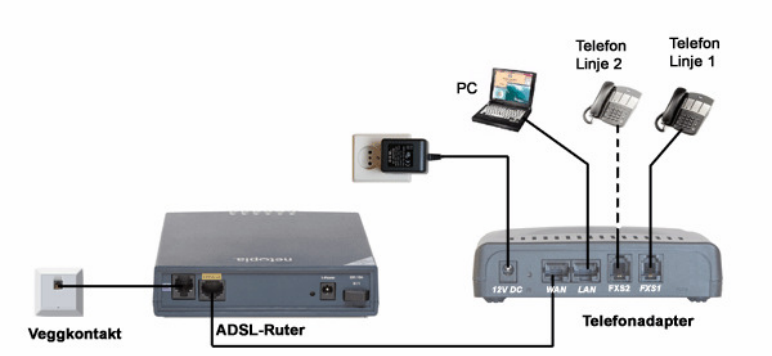
Integrated Services (IntServ) and Differentiated Services (DiffServ) are two architectures for quality of service through bandwidth management:



(b) Compare the IntServ and DiffServ architecture. Use a table.

IntServ	DiffServ
▪ Signaling mechanism ▪ Traffic handling per flow ▪ State information in network nodes ▪ Limited scalability in core due to amount of state information ▪ Better end-to-end guarantees as resources are reserved end-to-end per flow	▪ Priority mechanism ▪ Traffic handling of aggregated flows ▪ No state information ▪ Scale – aggregated flows ▪ End-to-end guarantees requires admission control and adequate dimensioning ▪ Currently, static SLAs give limited flexibility

The figure below is a picture of a voice over IP set-up. The “Telefonadapter” (phone adapter) connects a standard analog telephone to an IP-based network.



(c) How do you think quality of services is assured the application of voice over IP in this set-up?

Voice is given priority in the "Telefonadapter", eg LAN port traffic is forwarded when no voice traffic. In this way upstream QoS can be assured when the whole home network is interconnected behind the Telefonadapter.

(d) There is another set-up that also could provide quality of service to the voice application. Sketch this set-up, and comment on advantages/disadvantages of the two set-ups as seen from a voice service provider.

The home network can be connected directly to the ADSL-router if IP QoS in the ADSL-router is used to give voice traffic priority. The telefonadapter could tag packets by diff serv class, or ADSL-router could give priority to traffic on a specific input port.
The first set up: could be used by overlay voice service provider. The last set-up requires configuration of the ADSL-router, and is thus more a configuration the internet network provider may use.

Exercise 3 Virtual private networks

An IPVPN is an emulation of a private wide area network facility using IP technology.

(a) Give some details to the VPN requirements: opaque packet transport, tunneling mechanism, quality of service, and data security.

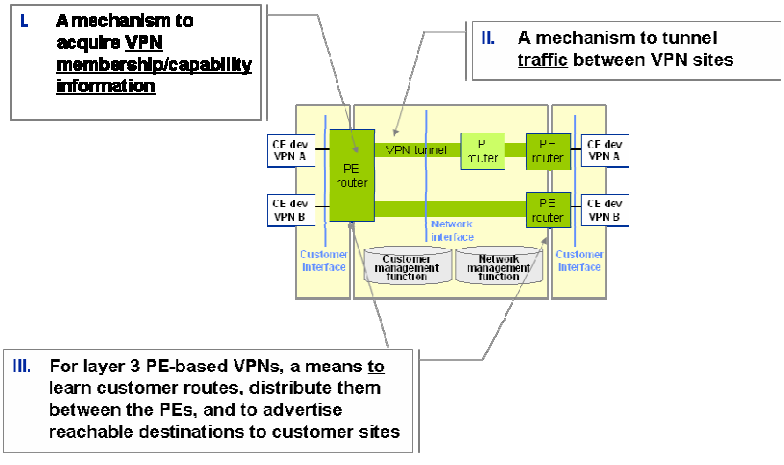
1. Opaque packet transport	• Isolated data forwarding VPN traffic no relation to rest of IP backbone traffic • Isolated routing - VPN may use private IP addresses • VPN-identifier
2. Tunneling mechanisms	• VPN addresses (and packet format) unrelated to IP backbone • Isolation between different customer networks • Per tunnel: possibly multi-protocol support, frame sequencing, specific QoS
3. Quality of service guarantees	• Because leased and dial up lines provides guarantees on bandwidth and latency
4. Data security	• By customer (encryption + firewall) • Secure managed VPN by service provider

(b) What is a provider-provisioned VPN compared to a customer-provisioned VPN? Give an example on each of these VPN types.

Provider provisioned: Provider provisions and remotely manages the customer edge device. In provider-provisioned VPNs the service provider participates in management and provisioning E.g. BGP/MPLS IPVP, Virtual router based VPNs.

Customer provisioned: Customer edge routers managed by private network administrator. In customer-provisioned VPNs all VPN-specific procedures are performed in the CE devices. The shared service provider network is not VPN aware. CE-based VPNs are pure overlays and can be used for both site-to-site and remote access VPNs. Eg. IPSEC tunnels across internet, VPN client in PC

(c) Briefly describe three functional components of a provider-provisioned provider-edge layer 3 VPN of which the reference model is pictured in the figure below.



Exercise 4 Multicast

(a) Why is UDP the preferred transport protocol for multicast?

Reliability has a different semantic in multicast. Reliable protocols are not set up to handle response from multiple receivers. DCCP could be an alternative, but congestion control would then be a challenge due to feedback

(b) Why is there a need for an inter-domain protocol when PIM-SM is deployed? What is the weakness of this protocol (MSDP)?

PIM-SM is an intra-domain protocol since the mapping of RP to group is domain specific. Either the MDSP for announcing sources to other domains is used combine with source specific trees in PIM SM or address allocation with a top RP is used. MSDP weaknesses are scalability - delay and flooding

(c) Describe what is meant by scoping, and how it is done for multicast in IPv4 and IPv6.

Scoping limits the distribution of multicast to a subset of the network, per link, department, organization and so on. In IPv4 it is done by setting the TTL in the multicast packet and use TTL limit on interfaces, i.e a packet with a TTL lower than interface lim will not be distributed on the interface. By setting the limit on the interface on meaningful boundaries can the distribution be limited. There is a limited address range set aside for scoping in IPv4. In IPv6 scoping is part of the address.

(d) Explain the difference between shared and source-specific trees.
Describe why core/RP is a part of most of the shared tree multicast protocols.

A shared tree is common for all sources sending to a group. A source specific tree has a separate distribution tree for each source. The advantages of the latter are: spread of load, shorter delay, no address collision, while the advantages for the former are, lower cost, easier to discover sources, less state in the network.
In a shared tree protocol the leaf router must send a signal that it wants to join a tree. That join message must have a routable address and therefore also a unicast address as the destination. This aiming point is the RP/Core. The multicast address is not routable before the leaf node has joined the shared tree.

Exercise 5 Ad-hoc networks

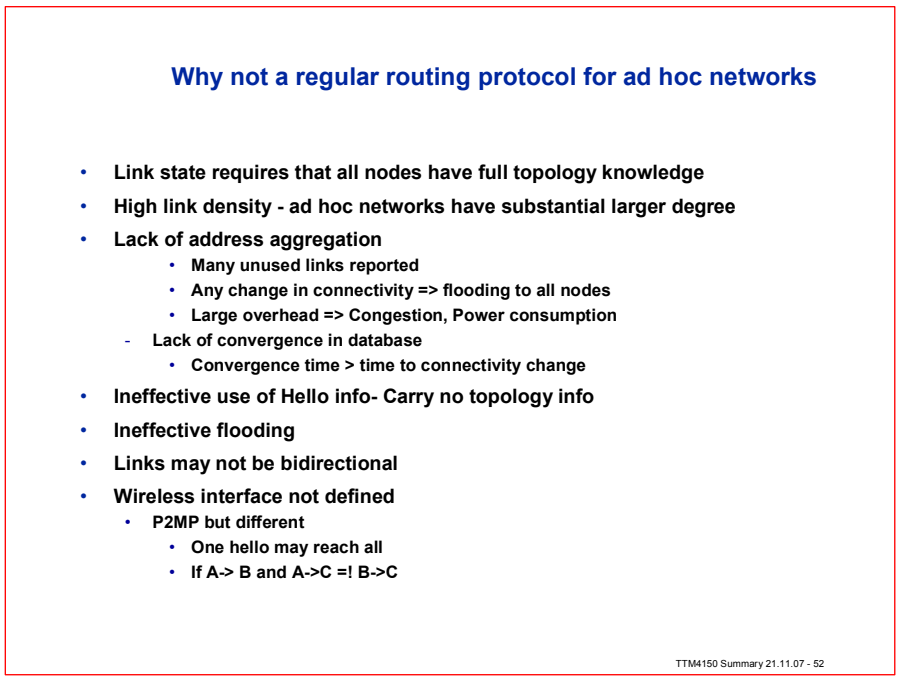
(a) What is the potential performance bottleneck in AODV (Ad-Hoc Distance Vector)?

AODV must broadcast RREQ . All nodes must repeat the broadcast once. It can therefore lead to broadcast storm. It is limited by extended ring search and intermediate nodes answering if they know about a path. 3/4 credit for an answer that include freshness stamp of the RREQ and the RREP. This is a mechanism that avoids stale routes to propagate in the network. They represent a clear inefficiency that could be viewed as a bottleneck.

(b) In geographic unicast routing there are two components. Besides the forwarding component what is the other major component?
Describe a few of the different design choices for this component.

Distribution of location information. Design choices are all to all, all to some, some to all and some to some

(c) If a regular link state routing protocol were used in an ad-hoc network, why wouldn't the solution scale?



Exercise 6 Mobility

(a) Describe two methods SIP (Session Initiation Protocol) can use to handle session mobility.

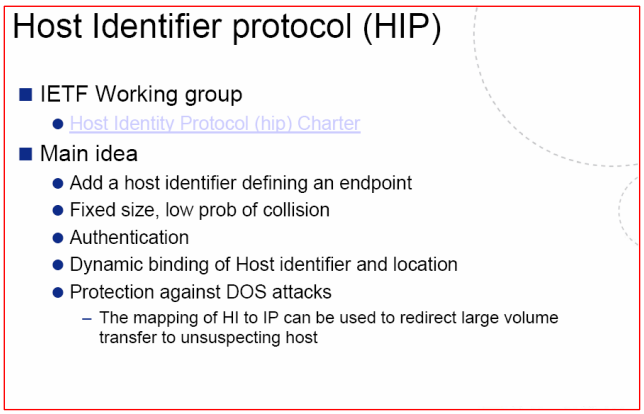
Reinvite/Invite by MN, RTP translator, or proxy that redirect the packets. In addition a sip proxy can redirect the signaling messages for pre-call mobility (partial credit)

(b) Address translation is an important function in mobility systems at the IP level. Are there any limitations on the placement of this function in a network? Describe two examples with different placements.

Must be placed somewhere on the path between source and the home location of the mobile node. In mobile IPv6 after the route optimization address translation is placed at the source, in IPv4 it is placed at the Home agent somewhere in the home location of the mobile node. In the article it is mentioned an experimental system, where it was palced at are router based on snooping for updating. The last alternative was a system at Columbia where the address translation was placed at routers responsible for the subnet allocated to the mobile nodes, i.e the set of routers that had routes to the subnets that all mobile nodes belonged to.

(c) Describe the flaw in the IP addressing model that makes mobility a problem. Why will HIP (Host Identity Protocol) be usable for handling mobility?

Two-tier address: location and end-point identifier. 1) Mobile node point of attachment, used as a routing directive 2) Mobile node end-point identifier, remains static for the lifetime of a mobile node.



(d) What are the two major security problems that mobility handling protocols must concern themselves with? Explain why.

Hijacking of address by signaling that a node has moved to a new address in order to steal the identity

Denial of service attack. By starting a download and then signal that the node has moved to a new location although the node has not moved. The source of the download could then incorrectly swamp the new location with unwanted traffic.