

Çözümler

1. (5p)

- a) Kablosuz linkin başlıca özellikleri nelerdir?
 - b) Bir ortamı paylaşmanın (aynı ortamı birden çok kullanıcının aynı anda kullanımı) yöntemleri nelerdir?
 - c) CDMA'in temel prensibi neye dayanır?
- a) **decreased signal strength, interference, multipath propagation.**
 - b) **TDMA, FDMA, CDMA**
 - c) **allows multiple users to "coexist" and transmit simultaneously with minimal interference (if codes are "orthogonal")**

2(7p). Varolan ağ altyapısını kullanarak çoğulortamlı iletişimi sağlamaya yönelik geliştirilen yaklaşımları sıralayınız.

use UDP to avoid TCP congestion control (delays) for time-sensitive traffic
client-side adaptive playout delay: to compensate for delay
server side matches stream bandwidth to available client-to-server path bandwidth
chose among pre-encoded stream rates
dynamic server encoding rate
error recovery (on top of UDP)
FEC, interleaving, error concealment
retransmissions, time permitting
CDN: bring content closer to clients

3. (5p) a) ISO tarafından tanımlanmış ağ yönetim alanları hangileridir?

Performance management, fault management, configuration management, accounting management, security management.

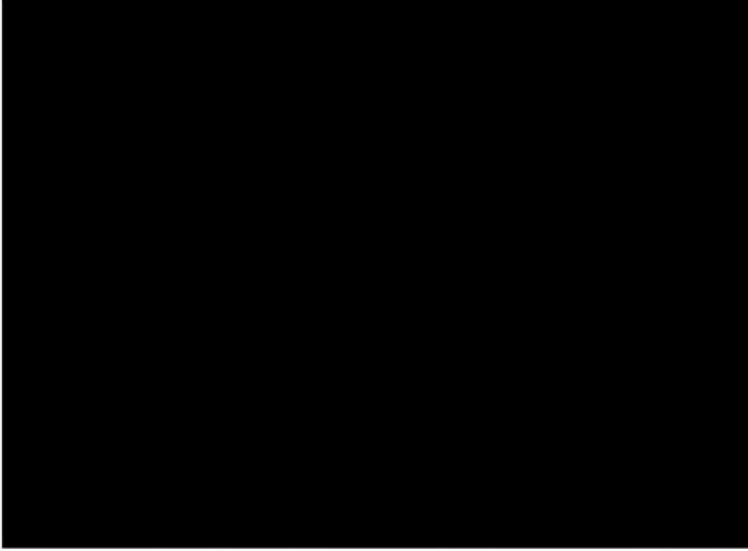
b) Ağ yönetim altyapısını oluşturan bileşenleri tanımlayınız.

- **Managing entity:** control the collection, processing, analysis, display of network management information, and is used by the network manager to control the devices in the network.
- **Managed device:** a piece of network equipment that is under the control of the managing entity.
- **Management agent:** a software process running on a managed device that communicated with the managing entity and takes action on the managed device under the control of the managing entity.
- **MIB:** pieces of information associated with all of the managed objects in a device.
- **Network management protocol:** runs between the managing entity of the management agents on the managed devices, allowing the agents to alert the managing entity to potential problems, and allowing the managing entity to send commands to the management agents.

c) SNMP'de *request-response* ile *trap* mesajları arasındaki önemli fark nedir?

The trap message is sent by the management agent to the managing entity (and requires no response from the managing entity). A request-response message is sent by the managing entity, with the response coming back from the management agent.

4. (8p) Sırdışlık, mesaj tamlığı ve kimlik doğrulama özelliklerinin bulunduğu güvenli e-mail gönderme nasıl gerçekleştirilir, bütün detayları ile blok diyagram olarak gösteriniz.



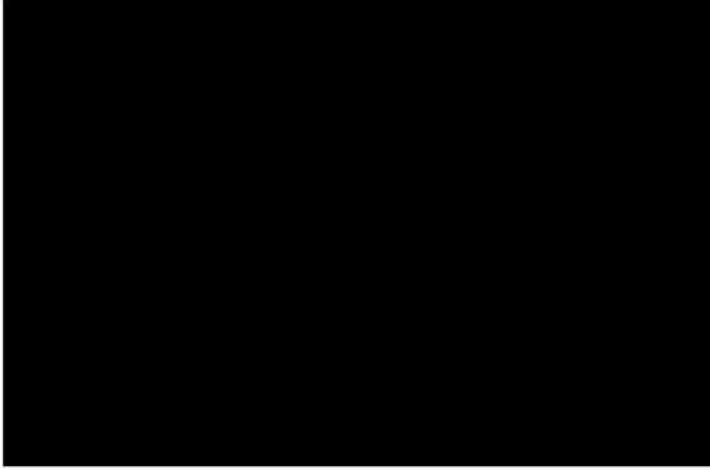
5. (4p) Kamusal anahtar şifrelemesi, sırdışlık, mesaj tamlığı ve kimlik doğrulama gibi alanların hepsinde başarı ile kullanılabilmesinin nedenini matematiksel olarak açıklayınız.

$$(m^e)^d \bmod n = (m^d)^e \bmod n$$

6.(6p) a)En güvenilir kimlik doğrulama protokolünü (ap.5.0) açıklayınız.

b) Man (woman) in the middle saldırısı ne demektir?

a)



b) Man (woman) in the middle attack: Trudy poses as Alice (to Bob) and as Bob (to Alice)

7.(5p) Üstel dağılıma sahip sürekli rasgele değişken X 'in olasılık yoğunluk fonksiyonu (pdf) aşağıda verilmektedir. X 'in beklenen değerini bulunuz, $\lambda > 0$.

$$f(x) = \begin{cases} \lambda e^{-\lambda x}, & x \geq 0 \\ 0, & x < 0 \end{cases}$$

8.(10p) Poisson sürecine uygun şekilde bir yönlendiriciye paketler ortalama 500 paket/sn hızında gelmektedirler. Yönlendiricinin hizmet süresi üstel dağılmakta ve ortalama 1 milisaniye'dir.

- a) Gelen paketin yönlendiriciyi boş bulma olasılığını bulunuz.
- b) Yönlendiricideki ortalama paket sayısını bulunuz.
- c) Ortalama bekleme süresini bulunuz.
- d) Paketin kuyrukta geçirdiği süreyi bulunuz.

a) $\lambda = 500$, $\mu = 1000$, $\rho = 0.5$

$P_0 = 1 - \rho = 0.5$

b) $E[n] = \rho / (1 - \rho) = 1$ paket

c) $E[T] = E[n] / \lambda = 1 / 500$ saniye

d) $E[w] = E[T] - 1 / \mu = 1 / 500 - 1 / 1000 = 1 \text{ ms}$