Università degli Studi di Verona, Dipartimento di Informatica

Programmazione di Rete, A.A. 2014/2015
Appello d'esame del 15 Settembre 2015

- L'esame consiste di due parti; ciascuna parte è composta da un esercizio e alcune domande.
- Lo studente svolga Parte I e Parte II su fogli distinti per permetterne la correzione in parallelo.
- Su ciascun foglio scrivere ***nome***, ***cognome*** e ***numero di matricola*** (non è obbligatorio consegnare la brutta copia)
- I risultati verranno pubblicati sugli avvisi della pagina del corso ***24 Settembre dopo le 19:00***
- La correzione dei temi d'esame può essere visionata durante la registrazione o il ricevimento docenti
- ***Orali*** (facoltativi a meno di una richiesta esplicita dei docenti) e ***registrazioni*** si terranno il ***25 Settembre alle 10:30 in Aula L***

I Parte

Esercizio 1 (8 punti)

Implementare un servizio di monitoraggio della temperatura all'interno di un edificio. Ogni sensore di temperatura è dotato di interfaccia WiFi e si comporta da client nei confronti di un'applicazione server che raccoglie i valori su tutto l'edificio per visualizzare dei grafici con l'andamento temporale. Ogni sensore misura ogni 5 secondi la temperatura e la trasmette al server assieme ad un numero progressivo che rappresenta il riferimento temporale e al proprio identificativo univoco (ogni sensore ne ha uno). Se il dato non viene ricevuto dal server, quest'ultimo tiene buono per l'istante di tempo mancante l'ultimo valore ricevuto. Si chiede di:

1) scrivere il codice Java lato client e lato server per implementare tale applicazione;
2) motivare la scelta del protocollo di livello trasporto;
3) discutere modalità alternative di implementazione e relativo impatto sulla probabilità di ricevere le temperature da parte del server.

NOTA: per sospendere un processo per un certo numero di millisecondi+nanosecondi si usa:
static void Thread.sleep(long millis, int nanos) throws InterruptedException

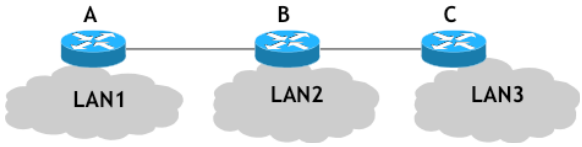
Domande (2 punti ciascuna)

Si risponda in maniera sintetica e concisa (poche frasi per risposta sono sufficienti) alle seguenti domande:

1. Guardando l'implementazione in Java di un client TCP e un client UDP che differenza principale si può notare?
2. Come funzionano i programmi di analisi di rete come Wireshark?
3. Descrivere il ruolo di uno switch/bridge e attraverso quali funzionalità viene svolto.

II Parte

Esercizio 3 (7 punti)



Una rete privata è formata da tre LAN e tre router, come mostrato in figura. Le tre LAN devono contenere 50 utenti ciascuna con un indirizzamento privato (si scelga tra gli intervalli dedicati agli indirizzi privati a piacere). I collegamenti tra i router utilizzano le interfacce seriali e ciascun collegamento deve appartenere ad una sottorete dedicata.

Per lo scenario sopra descritto si mostrino:

1. L'assegnamento degli indirizzi alle LAN e ai collegamenti (la scelta è arbitraria e funzionale al secondo punto; non serve scrivere nessun comando per gli apparati di rete);
2. Per il router B, i comandi necessari per assegnare gli indirizzi alle sue interfacce e per abilitare il routing con il protocollo.

Domande (4 punti ciascuna)

Si risponda, elaborando quanto più possibile, alle seguenti domande:

1. Si dia una breve spiegazione di ciascuno dei tre principali obiettivi della sicurezza (confidenzialità, integrità, disponibilità), anche con l'aiuto di esempi che mostrino come tali proprietà possano essere compromesse.
2. Tra i primi sistemi di crittografia a chiave simmetrica vi è la cifratura monoalfabetica: si spieghi come funziona tale schema e si indichi la dimensione dello spazio delle chiavi.
3. Si illustrino le caratteristiche che le funzioni hash devono possedere per poter essere utilizzate in ambito crittografico.