Università degli Studi di Verona, Dipartimento di Informatica

Programmazione e sicurezza delle reti, A.A. 2016/2017
Appello d'esame del 12 luglio 2017

- 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 ***lunedì 17 luglio dopo le 18:00***
- 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 ***martedì 18 luglio alle 14:30 in aula M***

I Parte

Esercizio 1 (8 punti)

Implementare un sistema distribuito di monitoraggio della temperatura. Ciascun client comunica al server la temperatura rilevata e il luogo (si assuma di avere 10 zone identificate da 0 a 9). Il client conosce la propria zona perché gli viene passata sulla riga di comando. Possono esistere più client per una stessa zona in modo da sopperire all'eventuale perdita di messaggi. Il server mantiene una media delle temperature ricevute per ogni zona; tale media viene comunicata al client in risposta all'invio della temperatura. Si chiede di:

- Scrivere il codice Java relativo a client e server
- Motivare la scelta del protocollo di livello trasporto
- Riportare il codice Java che serve a ritrasmettere la temperatura quando non si riceve la media entro 10 secondi

Domande (2 punti ciascuna)

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

1. A cosa serve e come funziona l'algoritmo/protocollo spanning tree? Esiste uno standard IEEE che lo regola?
2. Che differenza c'è tra un connettore RJ11 e RJ45? Quale dei due è usato da Ethernet? In quali modi può essere configurato?
3. Perché Wireshark ha bisogno di essere eseguito con l'utente Root per fare un'acquisizione live?

II Parte

Esercizio 2 (7 punti)

Gli uffici amministrativi di una grande azienda sono collocati in una palazzina di 3 piani. In ciascun piano vi sono postazioni per tre tipologie di impiegati: i commerciali, i contabili e i tecnici. Ciascun piano può ospitare fino a 20 postazioni di qualsiasi tipologia. L'azienda è collegata ad Internet con un router, che rappresenta il router di default, e gestisce con indirizzi privati gli impiegati all'interno della propria rete.

Per lo scenario sopra descritto si mostrino:

1. Lo schema della rete, indicando gli apparati usati con il loro numero di porte, e gli indirizzi assegnati agli impiegati, considerando che ciascuna tipologia deve essere isolata a livello 2 dalle altre tipologie (la scelta è arbitraria e funzionale al secondo punto; non serve scrivere nessun comando per gli apparati di rete);
2. Per il router di default, i comandi necessari per permettere alle diverse tipologie di comunicare tra di loro.

Domande (4 punti ciascuna)

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

1. Si descriva lo schema di crittografia a chiave simmetrica e come esso viene utilizzato nella comunicazione tra due entità.
2. Si mostri uno schema di firma digitale attraverso l'utilizzo della crittografia asimmetrica.
3. Si spieghi cosa si intende per Access Control List, specificando dove sono memorizzate le informazioni e come vengono utilizzate.