Università degli Studi di Verona, Dipartimento di Informatica

Programmazione e Sicurezza delle Reti, A.A. 2016/2017

Appello d'esame del 26 settembre 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 ***mercoledì 27 settembre 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 ***giovedì 28 settembre alle 15:30 in aula M***

I Parte

Esercizio 1 (8 punti)

Implementare il telecontrollo di un drone. La stazione a terra e il drone sono entrambi collegati ad Internet attraverso una rete wireless. La stazione a terra inizializza la comunicazione e poi impartisce comandi di navigazione al drone (ad es. SU, GIU, DX, SX). Indipendentemente da questi, il drone invia a terra periodicamente le immagini (nello svolgimento è sufficiente mandare un numero o una stringa qualsiasi che viene stampata a video dal programma di terra). Seguendo l'ordine delle domande, si chiede di: ***1)*** discutere la scelta del protocollo di livello trasporto; ***2)*** discutere qual è il client e il server tra la stazione a terra e il drone e perché; ***3)*** definire quali sono i thread necessari lato client e lato server e perché; ***4)*** scrivere la porzione di codice Java lato client e lato server per implementare tale sistema.

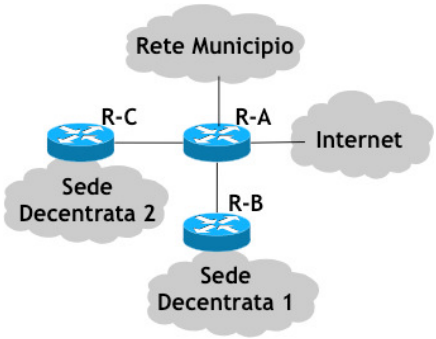
Domande (2 punti ciascuna)

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

1. Spiegare come funziona uno bridge/switch.
2. Che cos'è, come funziona e a cosa serve una Virtual LAN?
3. Perché in laboratorio è stata usata una virtual machine per l'esercitazione "UDP vs. TCP"?

II Parte

Esercizio 2 (7 punti)



Il router R-A di un Municipio è collegato ad Internet attraverso un cavo seriale: a tale interfaccia è stato assegnato l'indirizzo 90.112.77.42/30. Le altre interfacce (tutte Fast Ethernet) del router sono collegate ad altri due router (che garantiscono la connettività verso le sedi decentrate del Municipio) e ad una rete interna del Municipio stesso (si veda la figura a fianco). Tutti gli indirizzi all'interno del Municipio e delle sedi decentrate sono privati.

Per lo scenario sopra descritto si mostrino:

1. L'assegnamento degli indirizzi alla rete interna del Municipio, alle reti delle sedi decentrate, e ai collegamenti tra il router R-A e gli altri router (la scelta è arbitraria e funzionale al secondo punto; non serve scrivere nessun comando per gli apparati di rete);
2. Per il router R-A, i comandi necessari per assegnare gli indirizzi alle sue interfacce e per abilitare il routing con il protocollo RIP.

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. Si illustrino le caratteristiche che le funzioni hash devono possedere per poter essere utilizzate in ambito crittografico.
3. Un sistema di rilevamento delle intrusioni (IDS, Intrusion Detection System) si può basare su diversi modelli: rilevamento della anomalie, oppure rilevamento di uso malevolo, oppure rilevamento in base a specifiche. Si spieghi il principio di funzionamento di **uno** tra questi modelli, anche attraverso esempi.