



Università degli Studi di Verona, Dipartimento di Informatica
Programmazione di Rete, A.A. 2016/2017
Appello d'esame del 14 giugno 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 19 giugno 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 20 giugno alle 15:00 in aula L**

I Parte

Esercizio 1 (8 punti)

Implementare un forum tematico. Un utente accede al server con un client a cui passa in linea di comando il tema della discussione può essere "SPORT", "POLITICA", "NATURA"; se digita un tema diverso il programma termina e viene stampato un messaggio di errore. Tutti e soli gli utenti nell'ambito dello stesso tema devono poter comunicare assieme; il server deve premettere a ciascun messaggio inoltrato il nome del mittente seguito da ":". Si chiede di:

- Scrivere il codice Java relativo a client e server
- Motivare la scelta del protocollo di livello trasporto
- Discutere come si potrebbe rendere dinamico l'insieme dei temi di discussione

Domande (2 punti ciascuna)

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

1. Che cosa si può osservare in Wireshark nella prima fase di scambio di messaggi TCP per l'apertura di una connessione? Perché?
2. Per cosa è servito chiamare il comando IPTABLES durante l'esercitazione?
3. Come è strutturato un cavo UTP per Ethernet?

II Parte

Esercizio 2 (7 punti)

Un centro di ricerca è organizzato in 4 laboratori: in ciascun laboratorio sono previste postazioni destinate agli utenti strutturati e postazioni destinate a visitatori. I laboratori sono collocati tutti sullo stesso piano e ciascun laboratorio può ospitare fino a 10 postazioni, metà per gli strutturati e metà per i visitatori. Tutti gli indirizzi dei laboratori sono privati e vi è un router di default che garantisce la connettività verso l'esterno.

Per lo scenario sopra descritto si mostrino

1. Gli apparati di rete utilizzati e l'assegnamento degli indirizzi alle postazioni dei laboratori e al router di default (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 attivare l'assegnazione dinamica degli indirizzi alle postazioni degli utenti strutturati e dei visitatori.

Domande (4 punti ciascuna)

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

1. Si descriva lo schema di crittografia a chiave **asimmetrica** e come esso viene utilizzato nella comunicazione tra due entità.
2. Si descriva il funzionamento del Message Authentication Code (MAC) per l'autenticazione di un messaggio (non è necessario garantire la confidenzialità dei dati).
3. Si illustri, anche attraverso esempi, cosa si intende per politica di tipo "Default deny" adottata da un Firewall.