ITIS "A. Monaco" – Classe 5 A Informatica (art. Informatica) – Lab. di Sistemi e Reti - Prof. Sirangelo Daniele

Elenco Esercitazioni per Laboratorio di Sistemi e Reti

Protocollo DNS

1. Dopo un'apposita ricerca su Internet, determinare ed elencare, in un file testo, tutti i "Root NameServer" utilizzati dal protocollo DNS su Internet, per la risoluzione dei nomi di dominio di Primo Livello. Indicare un Server per rigo, riportando l'Ente che lo gestisce e l'indirizzo IP del Server stesso.
2. Dopo un'apposita ricerca su Internet, determinare ed elencare, in un file testo, almeno 10 domini di primo livello di tipo "generic" (gTLD) e almeno 10 domini di primo livello di tipo "contry-code" (ccTLD).
3. Visitando il sito "www.nic.it", gestito dal Consiglio Nazionale delle Ricerche (ossia dall'Ente preposto alla gestione dei domini di secondo livello di tipo ".it"), comprendere: (a) cosa sia un "REGISTRAR"; (b) la procedura necessaria per Registrare un nuovo dominio ".it". Riportare una breve descrizione di quanto appreso, in una pagina web "registrazionedominio.htm"

I SEGUENTI ESERCIZI, SE NON ALTRIMENTI INDICATO, VANNO RISOLTI CREANDO E SIMULANDO, CON IL SOFTWARE **PACKET TRACER**, UNA O PIU' RETI, IL CUI FUNZIONAMENTO RISOLVA LA PROBLEMATICA DESCRITTA NEL TESTO DELL'ESERCIZIO.

Posta Elettronica e Protocolli POP3, SMTP

4. In una LAN privata è presente un Server Mail (SMTP + POP3) che gestisce il dominio di posta "miaScuola.it" con gli account "preside@miaScuola.it", "vicepreside@miaScuola.it", "coordinatore@miaScuola.it" e un Server DNS che risolve il dominio "miaScuola.it". Configurare i 3 PC di Preside, Vicepreside e Coordinatore in modo che, usando i rispettivi Client di Posta, possano scambiarsi messaggi di posta elettronica.
5. Il router con NAT di una rete privata di classe C è connesso al router di una rete pubblica di classe B. Nella rete B sono presenti: un Server Mail (SMTP + POP3), che gestisce il dominio di posta "hopmail.com" e due account di posta "tizio@hopmail.com" e "caio@hopmail.it"; un Server DNS su cui è registrato il dominio "hopmail.com". Nella rete privata, configurare il PC di "tizio" e il Portatile di "caio" (connesso in wi-fi) affinché, usando i rispettivi Client di Posta, possano inviarsi vicendevolmente messaggi di posta elettronica.
6. Tre reti, di classe A, B e C, con almeno 2 PC per rete, sono connesse fra loro tramite i rispettivi router, secondo il classico schema a "triangolo": ogni router è connesso agli altri due. Nella rete A, è presente un Server Mail (SMTP + POP3) registrato sotto il dominio "love.it" su un server DNS presente nella rete B. Nella rete C, in cui è attivo il DHCP, configurare un PC e un Portatile (connesso in wi-fi), che, con i rispettivi Client di Posta, possano inviare/scaricare la posta rispettivamente per gli account "batman@love.it" e "superman@love.it". Infine nella rete B è presente un Server Web "www.supereroi.it" che deve essere raggiungibile da tutti i PC delle varie reti.

VLAN Untagged su Singolo Switch

7. Ad un unico Switch sono connessi 8 hosts configurati per appartenere ad un'unica rete locale privata di classe C. Con una appropriata configurazione dello Switch, suddividere tale rete in due VLAN di 4 hosts ciascuna e verificare che le due VLAN non comunicano fra loro. In particolare, verificare, in simulazione, che un ping da uno degli host all'indirizzo di broadcast, viene trasmesso solo agli host della stessa VLAN e non a tutti e 8 gli host della rete.
8. In una piccola azienda commerciale sono presenti 6 PC fisicamente connessi ad uno stesso Switch. L'azienda opera con 3 aree di lavoro indipendenti (Contabilita', Magazzino, Vendita) ciascuna operante con 2 dei 6 PC presenti. Sfruttando la tecnologia delle VLAN, si configuri la rete in modo da garantire che le 3 aree non possano comunicare fra loro. Verificare, in simulazione, che anche configurando gli indirizzi IP di tutti i PC su una stessa rete di classe C, essi comunicano solo se appartenenti alla stessa area di lavoro.

VLAN Untagged su più Switch

9. 6 host sono fisicamente connessi a 2 switch SW1 e SW2 (3 host per switch). Definire 2 VLAN in modo che, la prima includa 2 host di SW1 e 1 di SW2, la seconda includa 1 host di SW1 e 2 di SW2. Collegare e configurare correttamente i due switch per garantire la comunicazione fra gli host di una stessa VLAN e, al tempo stesso, la "separazione" delle due VLAN. Si utilizzino VLAN Untagged. Verificare in simulazione il tragitto dei frame fra SW1 e SW2.
10. Una società di servizi utilizza 10 pc suddivisi fra le aree Sviluppo, Clienti e Ricerca. La sede è su 3 piani e ogni piano ha un proprio switch. Al Piano 1 sono dislocati 3 PC uno per ciascuna area. Il Piano 2 è organizzato come il Piano 1. Invece, il Piano 3 è interamente dedicato al settore Sviluppo con 4 PC. Configurare e connettere i 3 Switch nel modo più semplice possibile, pur garantendo la separazione fra aree diverse e la comunicazione fra i PC appartenenti a una stessa area. Si utilizzino VLAN Untagged.

VLAN Tagged su più Switch

11. A due Switches sono connessi 6 Hosts, 3 per ogni Switch. Collegare fra loro e configurare i due Switches in modo da realizzare due VLAN e distribuire, su ciascuna di esse, 3 dei 6 Hosts. In simulazione, evidenziare il dettaglio del frame del protocollo 802.1q, che viene generato durante la comunicazione fra gli switches.
12. Un'azienda possiede un'unica infrastruttura di rete distribuita su due piani: su ogni piano è presente uno Switch e 5 Hosts, per un totale di 10 Hosts. Gli uffici dei Reparti "Produzione" (3 Hosts), "Vendita" (4 Hosts), "Amministrazione" (3 Hosts) sono sparsi per i vari piani ed è necessario creare delle VLAN che permettano di separare in modo sicuro gli Hosts di ciascun reparto dagli Hosts degli altri reparti. Collegare correttamente fra loro i due Switches e configurarli in modo da realizzare quanto richiesto.
13. A tre Switches sono connessi 6 Hosts, 2 per Switch, e sono configurate 2 VLAN denominate "Ricerca" e "Contabilita" con 3 Hosts per ciascuna. Connettere alla rete un Router con cui la sola VLAN "Ricerca" può accedere a un'altra rete (una sottorete pubblica 80.10.10.0 di 8 indirizzi) in cui all'indirizzo 80.10.10.3 risponde un server web sul quale solo gli utenti della VLAN "Ricerca" devono poter navigare utilizzando la tecnologia NAT.

Protocollo VTP

14. L'infrastruttura di rete di un'azienda, prevede 4 Personal Computer: Pc1 e Pc2 connessi a uno Switch SW1; Pc3 e Pc4 connessi a uno Switch SW2. Configurare 2 VLAN: Vendita (con Pc1 e Pc3) e Amministrazione (con Pc2 e Pc4) utilizzando un terzo Switch (SWserver) che connetta assieme i due Switches SW1 e SW2 e agisca da Server VTP per distribuire automaticamente agli altri switches la configurazione delle VLAN.
15. In uno dei padiglioni di un quartiere fieristico, l'infrastruttura di rete è distribuita su 3 aree espositive, ciascuna servita da un proprio Switch. Ogni azienda che espone nella fiera (prevedere almeno 4 espositori), è presente con un proprio PC in ciascuna delle 3 aree e desidera che i propri PC risultino connessi in rete fra loro, ma, al tempo stesso, siano assolutamente irraggiungibili dai PC delle altre aziende. Ogni azienda utilizza inoltre un proprio server con funzioni DHCP (per attribuire automaticamente gli IP ai propri PC). I server delle aziende sono tutti dislocati in una 4° area di "servizio" anch'essa servita da un proprio Switch. Tutte le reti utilizzate devono essere sottoreti (max 14 hosts) di un'unica rete privata di classe C. Utilizzare le VLAN per risolvere la problematica, sfruttando il protocollo VTP e, quindi, un ulteriore Switch con funzioni di Server VTP.
16. Come estensione dell'esercizio precedente, si desidera fornire alle aziende espositrici l'accesso ai server web presenti nella rete pubblica di classe A di un ISP. Per far ciò, l'ISP fornisce al quartiere fieristico un proprio router R (con NAT) che, attraverso una opportuna sottorete minima, è connesso al router della rete di classe A dell'ISP contenente i server web. Il quartiere fieristico ha una propria rete privata di classe C che ha come gateway proprio il router R. Ogni espositore, utilizzando un proprio router (con NAT), connette la propria VLAN con la rete privata del quartiere, ottenendo così l'accesso desiderato. Configurare l'intero sistema in modo che sia garantita la navigazione dai PC delle aziende (dislocati nelle varie VLAN) ai server web dell'ISP.

Inter-VLAN Routing

17. Una rete è costituita da 4 host: PcX1, PcY1 connessi a uno Switch SW1 e PcX2 e PY2 connessi a uno Switch SW2. Dopo aver configurato 2 VLAN ("AreaXRicerca" con PcX1 e PcX2 e "AreaYCollaudo" con PcY1 e PcY2) usando due reti private di classe C, configurare e connettere alla rete un Router che, utilizzando la tecnica "Inter-VLAN Tradizionale", garantisca la comunicazione fra le due VLAN.
18. Un'azienda opera in una sede distribuita su due piani di un edificio. Ogni piano ha un suo switch al quale sono connessi tutti gli host del piano. Su uno stesso piano ci sono diversi host (almeno 4 su ogni piano) appartenenti alcuni all'area "Produzione" altri all'area "Marketing". Configurare l'infrastruttura in modo che "Produzione" e "Marketing" siano due VLAN, configurate come due distinte reti private di classe C e utilizzare un Router che, tramite la tecnica "Inter-VLAN Router-on-a-stick", garantisca la comunicazione fra le due reti.
19. Gli uffici di un Comune, sono distribuiti su tre piani di un edificio. Su ogni piano, uno "switch di piano" connette tutti gli host del piano stesso. Gli host degli uffici appartengono a due settori distinti "Tributi" e "Gestione" e sono distribuiti su tutti e tre i piani. Inoltre, nell'edificio, sono presenti 2 Server Web "locali" (di nome "archivio.comune.it" e "vetrina.comune.it"), che costituiscono l'area "Server" e sui quali devono poter navigare tutti gli host (si tratta di una cosiddetta INTRANET). Configurare 3 VLAN distinte per "Tributi", "Gestione" e "Server" utilizzando: un ulteriore switch per centralizzare la tabella delle VLAN; tre sottoreti di una stessa rete privata di classe B per le 3 VLAN; un ulteriore Server come server DNS; un Router che, con la tecnica "Inter-VLAN Router-on-a-stick" garantisca la connettività fra le tre VLAN e, in particolare, la navigazione sui server web locali.

Crittografia: Algoritmi di Cifratura

20. Data un Frase (messaggio) e un valore K compreso fra 1 e 25 (chiave), convertire la frase in lettere maiuscole e criptarla sostituendo ogni sua lettera con quella che, nell'alfabeto, si trova K posti più avanti (Esempio: se Frase è "ABBA" e la chiave K è 3 si ottiene "DEED"). Prevedere anche la possibilità di decriptare la frase così ottenuta, per verificare che si ritorna a quella originale. Lasciare invariati i caratteri che non siano lettere.
21. Data una frase già criptata secondo la tecnica dell'esercizio precedente, visualizzare in una ListBox tutte le frasi che si ottengono decriptando la frase data secondo tutte le possibili chiavi.
22. Data un Frase (messaggio) e una stringa di 26 caratteri contenente tutte le lettere dell'alfabeto in un ordine diverso da quello alfabetico (chiave), convertire la frase in lettere maiuscole e criptarla sostituendo ogni sua lettera con un'altra lettera determinata applicando il seguente criterio: (1) si determina la posizione P della lettera originale nell'alfabeto; (2) si considera la lettera che, nella stringa chiave, si trova nella stessa posizione P (Esempio: se Frase è "CIAO" e la chiave è "QWERTYUIOPLKJHGFDSAZXCVBNM", si ottengono le posizioni 3, 9, 1, 15, per cui si ha "EOQG"). Prevedere anche la possibilità di decriptare la frase così ottenuta, per verificare se si ritorna a quella originale. Lasciare invariati i caratteri che non siano lettere.

Crittografia Simmetrica: AES e 3DES

23. Usando il blocco note, preparare un file A con un testo a piacere di almeno 50 righe, quindi realizzare un'applicazione Windows che offra le seguenti opzioni: (1) generare automaticamente e visualizzare una chiave K e un Vettore di Inizializzazione VI per l'algoritmo AES; (2) Criptare il testo contenuto nel file A, usando l'algoritmo AES e le chiavi precedentemente generate e riversare in un file B il contenuto criptato; (3) Decriptare il file B precedentemente generato e memorizzare il testo decriptato in un file D. (4) Facoltativo: implementare una procedura automatica che confronti i files A e D verificando se sono o no identici.
24. Usando il blocco note, preparare un file A con un testo a piacere di almeno 50 righe. Realizzare una prima applicazione Windows "KEY" che, selezionato il tipo di algoritmo da usare fra AES e 3DES, ne generi automaticamente chiave K e Vettore di Inizializzazione VI, memorizzandoli in un file testo "CHIAVI" la cui prima riga contiene la voce "AES" o "3DES" per memorizzare nel file anche il tipo di algoritmo relativo alle chiavi generate. Realizzare, quindi, una seconda applicazione Windows "CRYPTO" che cripti il file A usando l'algoritmo e le chiavi indicate nel file CHIAVI, scaricando il contenuto criptato in un file B. Realizzare infine una terza applicazione "DECRIPTO" che decripti il file B usando l'algoritmo e le chiavi indicate nel file CHIAVI, scaricando il contenuto decriptato in un file D.

Crittografia: RSA

25. Dati in input le due chiavi RSA pubblica (d,n) e privata (e,n) e una singola lettera maiuscola (messaggio), criptare la lettera con l'algoritmo RSA, utilizzando la chiave pubblica (d,n) e, successivamente, decriptare il messaggio criptato, usando la chiave privata (e,n).
26. Dati in input due chiavi RSA pubblica (d,n) e privata (e,n) e una frase F, criptarla con la chiave pubblica e decriptarla la chiave privata. utilizzando, come "blocchi" da crittografare, i codici ASCII dei singoli caratteri della frase: ogni carattere diventa così un messaggio di dimensione pari a un Byte e con valore compreso fra 0 e 255. E' necessario usare chiavi con n > 255 (o, in alternativa, spezzare ciascun byte in due messaggi distinti da 4 bit ciascuno con valori da 0 a 15).
27. Dati in input le due chiavi RSA pubblica (d,n) e privata (e,n), criptare, usando la chiave privata (d,n), l'intero contenuto di un file testo di nome "Originale.txt" e salvare il testo criptato in un'altro file testo di nome "Criptato.txt". Inoltre, le prime due righe del file criptato devono contenere, in chiaro, i numeri d ed n della chiave pubblica. Scrivere una seconda applicazione che, accedendo al file "Criptato.txt", legga la chiave pubblica e la usi per decriptare il restante testo criptato, scaricandolo in un ulteriore file testo di nome "Decriptato.txt". Verificare che originale e decriptato coincidano.

Crittografia: RSA con Cryptography

28. Usando le classi del namespace Cryptography, generare una coppia di chiavi RSA, (d,n) e (e,n). Quindi chiedere in input un messaggio M di almeno 200 caratteri, criptarlo con le chiavi generate e visualizzare in una ListBox i bytes del messaggio criptato Mc. Con un ulteriore pulsante, decriptare del messaggio criptato Mc, riproducendo e visualizzando il messaggio M originale. Consiglio: criptare suddividendo il messaggio in blocchi di 50 caratteri.

29. Creare un'Applicazione "GENERA" che generi una coppia di chiavi RSA, (d,n) e (e,n) e le memorizzi in un file testo "ChiaviRSA.txt". Creare altre due Applicazioni separate "CRIPTA" e "DECRIPTA": la prima, legge un file testo "Messaggio.txt", lo cripta usando le chiavi presenti in "ChiaviRSA.txt" e memorizza la sequenza di byte risultante in un file testo "MessaggioCriptato.txt" (un byte per riga); la seconda, legge il file testo "MessaggioCriptato.txt", lo decripta usando le chiavi presente in "ChiaveRSA.txt" e memorizza il testo risultante in un file testo "MessaggioDecriptato.txt".
30. Creare un'Applicazione di Rete che consenta la trasmissione sicura di un messaggio fra due PC, tramite l'uso della Crittografia Ibrida (ossia usando la Crittografia Asimmetrica per trasmettere in sicurezza una Chiave Comune, per poi usare la Crittografia Simmetrica per criptare il messaggio).

Crittografia: MD5

31. Considerato il file testo "Documento.txt" generato con l'esempio pilota, verificare che il contenuto del file stesso non sia stato "modificato" dopo la sua generazione. Per far questo, è sufficiente: (1) leggere l'Impronta Digitale contenuta nel documento (i 16 numeri presenti nelle prime 16 righe del file); (2) leggere tutto il testo e porlo in una stringa (usare il metodo FR.ReadToEnd per leggere in un sol colpo tutto il testo rimanente dopo le 16 righe lette); (3) generare l'impronta del testo letto; (4) confrontarlo con l'impronta letta nel file.
32. Implementare una prima applicazione, del tutto simile all'esempio pilota, che memorizzi nel file testo "Documento.txt" l'Impronta Digitale ma "criptata" usando la Chiave Privata del mittente (questo, come è noto, garantisce l'identità del mittente). Implementare una seconda applicazione, del tutto simile all'esercizio precedente, che verifichi l'integrità del documento "decriptando" l'Impronta Digitale presente nel file con l'uso della Chiave Pubblica del mittente.

I SEGUENTI ESERCIZI, SE NON ALTRIMENTI INDICATO, VANNO RISOLTI CREANDO E SIMULANDO, CON IL SOFTWARE **PACKET TRACER**, UNA O PIU' RETI, IL CUI FUNZIONAMENTO RISOLVA LA PROBLEMATICA DESCRITTA NEL TESTO DELL'ESERCIZIO.

NAT e Port Forwarding con WRT300N

33. Un'azienda è disposta su due piani di un edificio. Al primo piano, quello dei "dirigenti", sono presenti 3 PC e un Server Web accessibile solo tramite il suo indirizzo IP (e non tramite nome). Al secondo piano, quello degli "impiegati", sono presenti 4 PC con IP statici e un certo numero (max 3) di Notebook che accedono alla rete in W-Fi con indirizzi dinamici. Utilizzando il dispositivo integrato WRT300N e, quindi, la tecnica NAT, si desidera "proteggere" la rete dei dirigenti, pur garantendo l'accesso degli impiegati al Server Web.
34. La rete degli "impiegati" dell'azienda dell'esercizio precedente è dotata di un secondo Router di tipo WRT300N connesso al Router A di una rete pubblica di classe A. Gli host presenti nella rete A devono poter accedere a un server web di nome "ServerPubblico" posizionato nella rete "impiegati" dell'azienda. Tutti gli host della rete aziendale (dirigenti e impiegati) devono poter accedere in NAT a un Server Web "SitoEsterno" e a un Server DNS che risolve tutti i nomi, posizionati entrambi nella rete A. La rete aziendale, ad esclusione di "ServerPubblico", deve risultare inaccessibile dalla rete A.

Personal Firewall di Packet Tracer

35. In una rete locale privata è presente un host PC0 e due server SRV1 e SRV2. I due server sono entrambi Server Web, mentre solo SRV2 fornisce il servizio DNS. Configurare il Personal Firewall di PC0 in modo che possa navigare, usando il nome, verso il server SRV1 ma non possa navigare verso il server SRV2, neanche utilizzando il solo l'indirizzo IP.
36. In una rete sono presenti 3 host (PC0, PC1 e PC2) e un Router R che è connesso anche a un'altra rete dotata di un server SRV1 con funzioni di Server Web e DNS. Configurare il Personal Firewall di PC0 in modo che PC0 possa navigare (con nome) verso SRV1 e, al tempo stesso, nessun altro host della sua rete (PC1 e PC2) possa connettersi a PC0. Gli host PC1 e PC2 possono anch'essi navigare liberamente sul server.
37. Una rete A include due host PC0 e PC1 e un router RA. Una rete B include due server SRV1 (server web HTTP con nome di dominio "www.pippo.it" e server mail POP3/SMTP "pippo.it" con gli account topolino@pippo.it e "minnie@pippo.it") e SRV2 (server DNS) e un router RB. Connettere i due router in modo che la rete A possa comunicare con la rete B. Configurare il Personal Firewall di PC0 in modo che possa navigare, con nome, su SRV1 e possa solo inviare posta. Configurare il Personal Firewall di PC1 in modo che NON possa navigare su SRV1, neanche tramite indirizzo, e possa solo ricevere posta.

Windows Firewall, Desktop Remoto e Wireshark

38. Agendo su Windows Firewall, filtrare il traffico di rete del proprio PC, per ottenere quanto segue: (a) inibire la navigazione verso il sito dell'ITIS; (b) consentire il funzionamento dell'applicazione di esempio ChatServer solo per richieste di connessioni provenienti da un unico altro PC della rete locale (a tua scelta); (c) impedire l'uso

dell'applicazione di esempio ChatClient (d) bloccare l'uso del comando Ping. Riportare in un documento tutti gli screen-shot (e relativo brevissimo commento) delle finestre che mostrano le configurazioni effettuate e la verifica del loro corretto funzionamento.

39. Utilizzando Wireshark, isolare il traffico di rete di una breve connessione ChatClient - ChatServer (entrambi operanti sul tuo stesso PC) e riportare in un documento tutti gli screen-shot (e relativo brevissimo commento) delle finestre che mostrano la breve chat effettuata con ChatClient/ChatServer e il contenuto dei frames, individuati e ispezionati con Wireshark, che riportano le medesime frasi chattate.
40. Sul proprio PC attivare Desktop Remoto e limitarne l'accesso solo da un unico altro PC della rete locale (a tua scelta). Con Wireshark individuare il traffico di rete relativo ad una connessione in desktop remoto verso il proprio PC ed evidenziarne i soli frames che "aprono" la relativa connessione TCP. Impedire al proprio PC di controllare altri PC in Desktop Remoto. Riportare in un documento tutti gli screen-shot (e relativo brevissimo commento) delle finestre che mostrano le configurazioni effettuate, la verifica del loro corretto funzionamento e i frames individuati con Wireshark.

Application Proxy e software CCProxy

41. Utilizzando il software CCProxy in "locale" (ossia configurando il Browser per accedere alla rete attraverso di esso), configurare opportunamente gli Utenti nel Proxy e verificare le seguenti funzionalità: (a) accesso al web e richiesta di autenticazione; (b) blocco di siti tramite filtro web su Dominio, su Url e su contenuto; (c) limite di banda. Riportare in un documento tutti gli screen-shot (e relativo brevissimo commento) delle finestre che mostrano le configurazioni effettuate e la verifica del loro corretto funzionamento.

GLI ESERCIZI SEGUENTI VANNO RISOLTI CREANDO E SIMULANDO, CON IL SOFTWARE **PACKET TRACER**, UNA O PIU' RETI IL CUI FUNZIONAMENTO RISOLVA LA PROBLEMATICA DESCRITTA NEL TESTO DELL'ESERCIZIO.

VPN Lan-to-Lan

42. Una rete L1 (pubblica di classe C, con due host) è dotata di un Router R1 e una seconda rete L2 (anch'essa pubblica di classe C, con tre host) è dotata di un Router R2. I due routers R1 e R2 sono connessi fra loro da una terza rete che rappresenta Internet. Instaurare fra L1 e L2 una VPN di tipo Lan-to-Lan che cripti e autentichi tutto il traffico fra le due reti. Si configuri ISAKMP con chiave condivisa, AES e MD5 e IPSec con 3DES e MD5. Si riportino, in caselle di testo, le sequenze di comandi CLI per la configurazione di R1 e di R2 e si invii lo screenshot che evidenzia, in sumulazione, l'azione di criptazione e incapsulamento del pacchetto originale.
43. Tre reti pubbliche di classe C (L1, L2 ed L3) sono connesse fra loro tramite i rispettivi routers (R1, R2 ed R3) collegati in cascata (R1---R2---R3). Instaurare una VPN che si limiti a garantire l'autenticazione (e non la crittografia) per tutto il traffico fra L1 ed L3. Si configuri ISAKMP con chiave condivisa, 3DES e SHA e IPSec con SHA. Si riportino, in caselle di testo, le sequenze di comandi CLI per la configurazione di R1 e di R2 e si invii lo screenshot che evidenzia, in simulazione, l'incapsulamento del pacchetto originale.

VPN Host-to-Net

44. Riprodurre con Packet Tracer l'infrastruttura di rete dell'esempio "VPN Host-To-Net", utilizzando, per configurare la VPN, dei nomi diversi da quelli dell'esempio per tutte le definizioni necessarie.

GLI ESERCIZI SEGUENTI SONO REALI **PROVE D'ESAME** O **SIMULAZIONI MINISTERIALI** UFFICIALI.
IL **TESTO COMPLETO** DI CIASCUNA DI ESSE È SCARICABILE DAL **SITO DI SUPPORTO**.

80. Sviluppare, limitatamente ai punti inerenti la materia Sistemi e Reti, la Prova d'Esame 2015 sessione Ordinaria (materia Informatica - "Web Community")
81. Sviluppare, limitatamente ai punti inerenti la materia Sistemi e Reti, la Prova d'Esame 2016 sessione Ordinaria (materia Sistemi e Reti - "Rete Scuola")
82. Sviluppare, limitatamente ai punti inerenti la materia Sistemi e Reti, la Prova d'Esame 2016 sessione Suppletiva (materia Sistemi e Reti - "Compagnia Taxi")
83. Sviluppare, limitatamente ai punti inerenti la materia Sistemi e Reti, la Prova d'Esame 2016 sessione Straordinaria (materia Sistemi e Reti - "Sorveglianza Sanitaria")
84. Sviluppare, limitatamente ai punti inerenti la materia Sistemi e Reti, la Prima Simulazione Ministeriale 2016 (materia Sistemi e Reti - "Flotta Mezzi")
85. Sviluppare, limitatamente ai punti inerenti la materia Sistemi e Reti, la Seconda Simulazione Ministeriale 2016 (materia Sistemi e Reti - "Giornale Locale")

86. Sviluppare, limitatamente ai punti inerenti la materia Sistemi e Reti, la Prova d'Esame 2017 sessione Ordinaria (materia Informatica - "Car Pooling")
87. Sviluppare, limitatamente ai punti inerenti la materia Sistemi e Reti, la Prova d'Esame 2017 sessione Suppletiva (materia Informatica - "Assenze Studenti")
88. Sviluppare, limitatamente ai punti inerenti la materia Sistemi e Reti, la Prova d'Esame 2017 sessione Straordinaria (materia Informatica - "Associazione Culturale")
89. Sviluppare, limitatamente ai punti inerenti la materia Sistemi e Reti, la Prova d'Esame 2018 sessione Ordinaria (materia Sistemi e Reti - "Spedizione Pacchi")
90. Sviluppare, limitatamente ai punti inerenti la materia Sistemi e Reti, la Prova d'Esame 2018 sessione Suppletiva (materia Sistemi e Reti - "Rete StartUp")
91. Sviluppare, limitatamente ai punti inerenti la materia Sistemi e Reti, la Prima Simulazione Ministeriale 2019 (materie Informatica + Sistemi e Reti - "Noleggio Bici")
92. Sviluppare, limitatamente ai punti inerenti la materia Sistemi e Reti, la Seconda Simulazione Ministeriale 2019 (materia Informatica + Sistemi e Reti - "Compagnia Ferroviaria")
93. Sviluppare, limitatamente ai punti inerenti la materia Sistemi e Reti, la Prova d'Esame 2019 sessione Ordinaria (materie Informatica + Sistemi e Reti - "Assessorato al Turismo")