Università degli Studi di Camerino

Scuola di Scienze e Tecnologie

Corso di Laurea in Informatica (Classe L-31)

Studio e Realizzazione di moduli ed esami personalizzati per *Cisco Packet Tracer*

Laureando
Francesco Cremona
Matricola 093206

Relatore
Prof.Fausto Marcantoni

Correlatore
Dott.Marco Maccari

A.A. 2016/2017

Abstract

Negli ultimi anni, lo sviluppo di reti complesse ha richiesto nuove conoscenze in ambito networking. A tal fine la società Cisco nelle sue certificazioni, propone moduli di esame per la verifica dell'apprendimento dei candidati. Tale verifica necessita l'introduzione costante di nuovi moduli. Per raggiungere tale scopo, ho analizzato i più diffusi simulatori di rete tra i quali: GNS3, Virl, BosonNetSim e Packet Tracer. Nella tesi, ho utilizzato Packet Tracer per la sua estensione Activity Wizard, la quale permette la creazione di esami personalizzati. Questo lavoro introduce un miglioramento nella verifica delle conoscenze individuali da parte degli esaminatori Cisco.

La sfida non deve essere come 'usare' bene la rete, come spesso si crede, ma come 'vivere' bene al tempo della rete.

Antonio Spadaro

Indice

Elenco delle Figure

Elenco delle Tabelle

1. Introduzione

1.1 Background

Internet è un insieme di reti private e pubbliche interconnesse, capaci di: raccogliere, elaborare e scambiare informazioni. Molte tecnologie elettroniche sono state progettate per aiutare questo processo di scambio in modo efficiente. Originariamente, queste tecnologie esistevano e operavano indipendentemente, servendo i propri scopi, non fino a poco tempo fa queste meraviglie tecnologiche sembrano convergere, ed è un fatto ben noto che una rete di comunicazione informatica è il risultato di questa convergenza. Una rete è composta da dispositivi come workstation, server, router, punti di estensione wireless, ecc) e dei loro collegamenti(fisici o logici), che attraverso cavi in rame, fibra cavi ottici e collegamenti microonde/satellite/radio, consentono lo scambio di informazioni o piuttosto la condivisione dei dati tra più utenti. [1]
Esistono diverse tipologie di rete, quelle più importanti sono sostanzialmente due:

- le **LAN (Local Area Network)**, ovvero quelle reti realizzate all'interno di un'area piuttosto circoscritta, ad esempio, in una casa. Il collegamento esistente tra le varie componenti hardware di una LAN può avvenire solitamente o mediante l'utilizzo di speciali cavi, chiamati in gergo cavi Ethernet, oppure in maniera del tutto wireless. In quest'ultimo caso, tuttavia, piuttosto che di LAN si parla di *WLAN* (Wireless Local Area Network), cioè di una rete Wi-Fi che non corrisponde altro che ad una speciale LAN protetta da un'opportuna password.
- le **WAN (Wide Area Network)**, non sono altro che delle reti appartenenti ad un'area geografica molto più grande rispetto alle comuni LAN, ad esempio, tra nazioni. Tra tutte le WAN esistenti, quella più grande e, al tempo stesso la più importante, prende il nome di Internet.

Lo sviluppo delle reti, non più circoscritte alle singole organizzazioni, ha portato radicali cambiamenti principalmente nelle realtà lavorative, aumentando sensibilmente il grado di interoperabilità tra di esse. Questa crescita di necessità di comunicazione sempre più istantanea e allo stesso tempo sicura, non ha fatto altro che inizialmente far nascere, e successivamente sviluppare, all'interno delle organizzazioni aziendali, la figura del *Network System Administrator*. All'amministratore di rete è dunque indispensabile uno strumento che gli permetta di controllare, gestire, amministrare la rete, riducendo in questo modo possibili problemi relativi alla sicurezza e allo stato dei servizi di rete.

I simulatori di rete forniscono un metodo conveniente per:

- Validazione della progettazione di rete per aziende / centri dati / reti di sensori, ecc.
- R&S di rete (più del 70 % di tutti i documenti di ricerca di rete fanno riferimento a un simulatore di rete.)
- Istruzione - Sperimentazione di laboratorio. La maggior parte delle università utilizza una simulazione di rete per insegnare/sperimentare sul networking poiché è troppo costoso per acquistare apparecchiature hardware.

I simulatori di rete inoltre, sono degli strumenti di apprendimento utilizzati per acquisire competenze e capire la complessità delle tecnologie dell'informazione e della comunicazione (ICT). In questa tesi si spiega cosa è una simulazione, cosa sono i simulatori di rete ed in particolare si andrà in dettaglio con Packet Tracer.

Cisco Packet Tracer. Cisco è il leader mondiale nel networking per Internet. Tra i vari prodotti che offre vi è il simulatore di rete: Packet Tracer il quale è un software didattico distribuito liberamente agli studenti ed istruttori del programma Cisco Networking Academy. Esso è usato per la simulazione di reti, per facilitare e migliorare l'apprendimento del Networking, consentendo di creare delle topologie composte da dispositivi di rete generici oppure dispositivi Cisco. Inoltre permette di simulare l'interfaccia a riga di commando CLI (Command Line Interface) del Sistema operativo Cisco IOS presente in tutti i dispositivi Cisco, oppure configurare gli apparati di rete usando la semplice GUI (Grafic User Interface). Tra le funzioni più importanti del software c'è quella di ispezionare in real-time lo stato di tutti i dispositivi utilizzati nella rete e il formato di ciascun pacchetto inviato sulla rete.

1.2 Obiettivo

La tesi ha l'obiettivo di supportare Cisco-Packet Tracer, in particolare, si vuole garantire non solo agli studenti, ma più in generale, a coloro che vogliono sostenere l'esame, di godere a pieno delle funzionalità che offre Packet Tracer, fornendo guide, spiegazioni ed esempi. Nella seconda parte della tesi, si spiega come realizzare nuovi moduli di esami personalizzati con l'activity wizard.

La tesi è strutturata nel modo seguente: il Capitolo 1 introduce il lavoro svolto e riporta le motivazioni e l'obiettivo della tesi. Il Capitolo 2 spiega cosa sono i Simulatori/Emulatori di Rete, riportando alcuni di quelli più diffusi. Nel Capitolo 3 si entra in dettaglio con Packet Tracer. Inoltre verrà spiegato come creare una prima e semplice topologia di rete. Il Capitolo 4 riporta vari comandi per le configurazioni per esempio il routing tra reti IPv6, accedere all'interfaccia della riga di comando e infine si spiega come utilizzare i dispositivi per creare VLAN. Il Capitolo 5 spiega come creare delle valutazioni con Packet Tracer per testare l'apprendimento degli utenti. Alla fine di questo capitolo verrano mostrate due nuove topologie di esame per CCNA1 e CCNA2 e si introdurranno sezioni più complesse dell'activity wizard come per esempio " Using variables". Il Capitolo 6 riporta le conclusioni, le competenze acquisite e i possibili sviluppi futuri.

2. Network-Simulator

In informatica i simulatori di rete sono dei particolari programmi in cui si simulano i comportamenti di una rete osservando le interazioni tra le varie entità (router, switch, nodi, punti di accesso, collegamenti ecc.); in questo modo il comportamento della rete ed i vari servizi che può offrire , possono essere osservati in ambiente di laboratorio ed è possibile cambiare o settare dei parametri per controllare come reagisce la rete. Gli amministratori di sistema non possono sempre sapere come funzioneranno le cose nella vita reale, specialmente quando è coinvolto un numero elevato di computer. I rischi che qualcosa possa andare storto sono molto alti e i costi sono troppo grandi. È qui che le simulazioni sono utili, infatti permettono agli sviluppatori di replicare i modelli che si aspettano di vedere nel mondo reale. Gli sviluppatori possono quindi analizzare questi risultati e utilizzarli durante il processo di sviluppo. In generale, si parla di simulazione sia nel caso in cui viene utilizzato un modello concreto, sia nel caso in cui viene utilizzato un modello astratto che riproduce la realtà mediante l'uso del computer. Per simulare il comportamento di un sistema è necessario costruire un modello di simulazione. Il modello dovrà essere sufficientemente complesso da rispondere alle esigenze dal caso, ma deve comunque rimanere il più semplice possibile. Devono inotre essere chiari i limiti di utilizzo del modello stesso.

I motivi che spingono all'approccio simulativo sono diversi:[2]

- Lo studio e la sperimentazione delle interazioni interne di un sistema complesso; una migliore conoscenza del sistema reale come conseguenza della creazione del modello di simulazione.
- Lo studio dell'impatto sui risultati dei diversi parametri del modello di simulazione.
- La valutazione del funzionamento e delle prestazioni di un sistema prima della costruzione del prototipo.
- La possibilità di valutare eventi e condizioni rare o rischiose.
- L'identificazione dei punti deboli del sistema.
- La valutazione what-if senza interrompere il funzionamento del sistema.

Per l'organizzazione di uno studio di simulazione sono necessarie varie fasi :

Fase iniziale: bisogna formulare il problema, definendo gli obiettivi e pianificando lo studio.

Costruzione del modello e acquisizione dei dati: si deve progettare il modello, acquisire

i dati di input ed output dal sistema reale, implementare il modello, verificarlo e validarlo.
Simulazioni: bisogna definire le varianti da studiare, progettare le sessioni di simulazione e analizzare i risultati, ed eventualmente pianificare nuove sessioni di simulazione.
Documentazione e presentazione dei dati: si deve documentare il modello e le diverse sessioni di simulazione, e infine mostrare i risultati dello studio.

Classificazione dei Modelli di Simulazione. I modelli di simulazione si possono classificare in base a diversi criteri[3]:

- Modelli continui, in cui le variabili variano con continuità.
- Modelli discreti, in cui il valore delle variabili cambia in ben definiti istanti di tempo.
- Modelli statici, che rappresentano un sistema in un particolare istante ditempo.
- Modelli dinamici, che rappresentano un sistema in evoluzione nel tempo.
- Modelli deterministici, che non contengono componenti probabilistici.
- Modelli stocastici, che presentano elementi soggetti ad aleatorietà.

2.1 Simulatori-Emulatori di Rete

La simulazione di rete viene spesso confusa con l'emulazione di rete, che potrebbero sembrare la stessa cosa perchè un emulatore ha le stesse proprietà di un simulatore, ma mentre un simulatore di rete ha solo dei dispositivi virtuali , quindi che fisicamente non esistono, usando un emulatore di rete è possibile collegare dei dispositivi reali alla rete virtuale in modo tale da simulare una rete attiva. **Un simulatore di rete** è un software che predice il comportamento di una rete di computer. Poiché le reti di comunicazione sono diventate troppo complesse per i metodi analitici tradizionali per fornire una comprensione accurata del comportamento del sistema, vengono utilizzati i simulatori di rete. Nei simulatori, la rete di computer è modellata con dispositivi, collegamenti, applicazioni, e vengono analizzate le prestazioni. I simulatori sono dotati di supporto per le più diffuse tecnologie e reti oggi in uso, quali LAN wireless, reti mobili Adhoc, reti di sensori wireless, reti veicolari ad hoc, reti cognitive radio, LTE/LTE-5G, Internet of things (IOT), ecc. A livello base, un simulatore di rete utilizza formule matematiche per creare un modello teorico e interamente virtuale di una rete. I simulatori sono soluzioni software e sono disponibili diversi tipi per diverse applicazioni. Pur essendo utilizzati principalmente per scopi di ricerca e didattici, possono anche fungere da strumenti di test cruciali per la progettazione e lo sviluppo di una rete.
I simulatori, come ns-3, vengono utilizzati per simulare i protocolli di rete e routing. OPNET, ha fornito anche un ambiente di simulazione autonomo. Entrambi questi simulatori di rete utilizzano una simulazione di eventi discreti [1] che, in ordine cronologico,

[1]La maggior parte dei simulatori di rete utilizza la simulazione di eventi discreti, in cui è archiviato un elenco di eventi in sospeso e tali eventi vengono elaborati in ordine, con alcuni eventi che attivano eventi futuri, come l'evento dell'arrivo di un pacchetto in un nodo che attiva il evento dell'arrivo di quel pacchetto in un nodo downstream.

accoda ed elabora eventi come il flusso di dati. Ciò consente a un architetto o ingegnere di rete di costruire e valutare un modello sperimentale di una rete, compresa la sua topologia e il flusso di applicazioni. Poiché una varietà di scenari teorici può essere introdotta in una rete in cui qualsiasi cosa può essere costruita e applicata, le prestazioni possono essere ipotizzate prima che la rete stessa sia stata persino implementata nel mondo reale. I simulatori di rete creano modelli in cui le operazioni di un sistema agiranno come una sequenza di eventi e, man mano che il tempo cambia, anche lo stato del sistema si modificherà. Anche se testare una rete in questo modo può far risparmiare tempo e denaro, i simulatori di rete non sono privi di limiti. Queste operazioni altamente complesse richiedono un livello di esperienza e formazione per configurare correttamente al fine di ottenere risultati affidabili. La maggior parte dei simulatori commerciali sono guidati dalla GUI, mentre alcuni simulatori di rete sono guidati dalla CLI. Il modello/configurazione di rete descrive la rete (nodi, router, switch, collegamenti) e gli eventi (trasmissioni di dati, errore di pacchetto ecc.).

Altri simulatori possono anche fungere da emulatori. Ciò significa che è possibile connetterli a una rete attiva. Dopo che un simulatore è stato collegato a una rete in tempo reale, riceverà informazioni dal traffico di rete in entrata e consentirà allo specialista di analizzarlo in dettaglio. **L'emulazione di rete** consente agli utenti di introdurre dispositivi e applicazioni reali in una rete di test (simulata) che altera il flusso dei pacchetti in modo tale da imitare il comportamento di una rete attiva. Il traffico in tempo reale può passare attraverso il simulatore e essere influenzato da oggetti all'interno della simulazione. La metodologia tipica è che i pacchetti reali da un'applicazione live vengono inviati al server di emulazione (dove viene simulata la rete virtuale). Il pacchetto reale viene "modulato" in un pacchetto di simulazione. Il pacchetto di simulazione viene demodulato in un pacchetto reale dopo aver sperimentato effetti di perdita, errori, ritardo, ecc., Trasferendo in tal modo questi effetti di rete nel pacchetto reale. Così è come se il vero pacchetto fluisse attraverso una rete reale ma in realtà fluisse attraverso la rete simulata. L'emulazione è ampiamente utilizzata nella fase di progettazione per la convalida delle reti di comunicazione prima della distribuzione. Gli emulatori di rete vengono utilizzati dalle organizzazioni che devono verificare le prestazioni delle applicazioni in un ambiente che replica in modo accurato le reti reali, mentre i simulatori di rete sono generalmente utilizzati per scopi accademici o di ricerca. Non è possibile eseguire il traffico di rete reale tramite un simulatore di rete, ma è possibile tramite un emulatore di rete.
In sintesi si può dire che, entrambi sono strumenti utili e necessari e ciascuno di essi ha il proprio scopo distinto. Un simulatore di rete aiuta a progettare una rete da zero senza la necessità di dispositivi fisici. Una volta che la rete è stata progettata e costruita, un emulatore di rete aiuterà a testare e convalidare le prestazioni delle applicazioni, a risolvere i problemi e a fornire proof-of-concept. [2]

2.2 Software più diffusi per le reti

Ci sono una vasta gamma di simulatori di rete, che vanno dal molto semplice al molto complesso, ognuno ha le proprie peculiarità e si differenziano l'un dall'altro. Esistono sul mercato molte implementazioni e applicativi che si basano sulle simulazioni/monitorag-

[2]Dimostrazione pratica dei funzionamenti di base di un applicativo o intero sistema integrandolo all'interno di un ambiente già esistente.

gio delle reti. Ci sono prodotti che si concentrano sul monitoraggio dell'infrastruttura di rete ed offrono un supporto elevato per i protocolli, altri applicativi invece sono stati sviluppati con il solo compito di controllare particolari componenti, sia hardware che software, di una rete, o a raggiungere determinati obiettivi, altri software lavorano su specifiche piattaforme, quali Linux, Windows, MacOS ecc.., e che si rendono utili per un controllo quanto più completo di tutta l'infrastruttura web.
In minima parte, un simulatore di rete deve abilitare un utente a:

- Modellare la topologia di rete specificando i nodi sulla rete e i collegamenti tra tali nodi.
- Modellare il flusso dell'applicazione (traffico) tra i nodi.
- Fornire le metriche delle prestazioni di rete come output.
- Visualizzazione del flusso di pacchetti.
- Valutazione della tecnologia / protocollo e design dei dispositivi.
- Registrazione di pacchetti / eventi per analisi drill down / debugging.
- Creazione di topologie per nuove attività di laboratorio.

Negli ultimi anni, la tecnologia di virtualizzazione è avanzata al punto che quasi tutto può essere virtualizzato. Avviato da virtualizzazioni server e storage, a Software Defined Networking (SDN), l'intera tecnologia datacenter tende a spostarsi dall'infrastruttura fisica. Se la rete di produzione diventa virtuale, per gli ingegneri di rete, gli studenti di certificazione e i trainer di Cisco Academy, non c'è motivo di utilizzare dispositivi fisici per i test di laboratorio e per scopi di apprendimento. I simulatori di rete sono una grande risorsa per la simulazione di determinati scenari, l'apprendimento, le certificazioni e il semplice test: "cosa succederà se faccio questo nella rete?". Ci sono una varietà di simulatori disponibili in natura per l'uso, tuttavia, i tre principali per motivi diversi sono *GNS3, VIRL, Packet Tracer e BosonNetSim.* Alla domanda quale di questi è il migliore da usare, non vi è una risposta chiara, poiché ognuno di essi ha determinati punti di forza e punti deboli che portano in tavola e molto dipende dalle preferenze personali.

2.2.1 GNS3

GNS3 è utilizzato da centinaia di migliaia di ingegneri di rete in tutto il mondo per emulare, configurare, testare e risolvere i problemi di reti virtuali e reali. GNS3 consente di eseguire una piccola topologia composta da pochi dispositivi sul laptop, a quelli con più dispositivi ospitati su più server o addirittura ospitati nel cloud. GNS3 non supporta solo i dispositivi Cisco. Cisco viene spesso discusso perché è ciò a cui la maggior parte degli ingegneri di rete è interessata a conoscere. Tuttavia, molti altri fornitori commerciali e open source sono supportati oggi in GNS3. Ora si è in grado di testare l'interoperabilità tra molti fornitori e persino provare configurazioni esoteriche usando tecnologie di rete con SDN, NFV, Linux e Docker. GNS3 consiste di due componenti software: il software GNS3 all-in-one (GUI) e la macchina virtuale GNS3 (VM). Quando si creano le topologie in GNS3 utilizzando il client della GUI del software All-in-One, i dispositivi creati devono essere ospitati ed eseguiti da un processo del server: *Local GNS3 server, Local GNS3 VM e Remote GNS3 VM.* È possibile utilizzare

GNS3 senza utilizzare VM GNS3. Questo è un buon modo per iniziare inizialmente, ma questa configurazione è limitata e non fornisce tante scelte riguardo alle dimensioni della topologia e ai dispositivi supportati. Se si desidera creare più topologie GNS3 avanzate o si desidera includere dispositivi come i dispositivi Cisco VIRL (IOSvL2, IOSvL3, ASAv) o altri dispositivi che richiedono Qemu, si consiglia la GNS3 VM.
GNS3 ha ironicamente simulatore nel suo acronimo, ma simula intere reti, non solo i sistemi operativi di rete, infatti oltre ad essere definito come simulatore di rete grafico, ha anche le proprietà di un emulatore. EmulationGNS3 imita o emula l'hardware di un dispositivo ed esegue immagini reali sul dispositivo virtuale. Ad esempio, è possibile copiare Cisco IOS da un router Cisco reale e fisico ed eseguirlo su un router Cisco virtuale emulato in GNS3. Esso può essere utilizzato per simulare una rete composta esclusivamente da virtualBox e/o macchine virtuali Qemu, che eseguono software open source. GNS3 funziona su hardware PC tradizionale e può essere utilizzato su più sistemi operativi, inclusi Windows, Linux e MacOS X, al momento l'ultima versione di GNS3 è la versione 2.1.4.
Una volta installato, verranno installati anche altri software a supporto che servono ad analizzare i pacchetti in entrata ed uscita, applicando quello che comunemente è definito Sniffing , cioè l'attività d' intercettazione passiva dei dati che transitano in una rete per valutare il comportamento di un protocollo di rete come: NpCap, SolarWinds Response TimeViewer, WinPcap e WireShark (fig.2.1)[6] . Il simulatore di rete GNS3 facilita agli utenti l'acquisizione e la visualizzazione dei dati che passano attraverso le interfacce dei dispositivi in esecuzione, in una simulazione di rete GNS3.

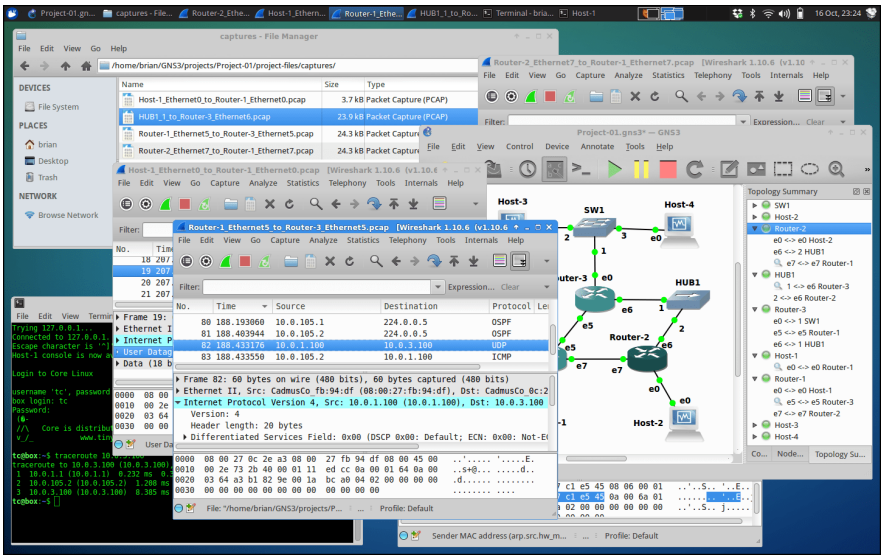


Figura 2.1: Wireshark in GNS3

GNS3 ha molti vantaggi come il supporto nativo per Linux senza la necessità di ulteriori software di virtualizzazione, supporta sia hypervisor gratuiti che a pagamento (Virtualbox, workstation VMware, lettore VMware, ESXi, Fusion), non vi è nessun costo di licenza mensile o annuale ed ha una comunità grande e attiva. Inoltre con GNS3 si può:

- Connettere un dispositivo reale (emulazione).
- Con l'intuitiva interfaccia grafica, gli utenti possono connettere perfettamente

tutti i tipi di interfacce virtuali a una rappresentazione reale delle reti.

- Ciò che distingue GNS3 dagli altri simulatori, è la sua capacità di EMULARE il routing e il switching, nonché di incorporare macchine virtuali REALI e di collegarle tra loro tramite un sistema di tunneling logico (overlay network).
- Inserire online una rete virtuale ed accedervi remotamente.
- Testare prodotti e simulare la rete reale per i test di pre-distribuzione, senza la necessità di hardware di rete

Svantaggi GNS3

- Non possiede la licenza per i prodotti Cisco. Le immagini Cisco devono essere fornite dall'utente (scaricare da Cisco.com, acquistare la licenza VIRL o copiare dal dispositivo fisico).
- Dato che GNS3 è concesso in licenza con GPLv3, ci sono alcune condizioni sull'uso del software come parte di un prodotto commerciale. Ad esempio, non è possibile creare un prodotto alternativo da GNS3, apportando modifiche al codice e quindi vendere il lavoro risultante. È inoltre necessario rendere le modifiche apportate al codice sorgente GNS3 disponibili a tutti i destinatari della versione modificata e devono essere concesse in licenza secondo i termini di GPL.
- Alcune caratteristiche, funzionalità di GNS3 possono essere sfruttate solo nel kernel di Linux, che aumentano le prestazioni e la stabilità, ad esempio KVM (infrastruttura di virtualizzazione, che dà la possibilità di astrarre le componenti hardware/fisiche degli elaboratori, al fine di renderle disponibili al software in forma di risorsa virtuale). Tramite questo processo è quindi possibile installare sistemi operativi su hardware virtuale; l'insieme delle componenti hardware virtuali (Disco fisso, RAM, CPU, Scheda di rete) prende il nome di macchina virtuale e su di esse può essere installato il software come, appunto, i sistemi operativi e relative applicazioni.
- Il processore della macchina fisica che si va ad utilizzare è sottoposto ad un oneroso overhead, ovvero quella parte di banda di trasmissione che viene utilizzata per spedire, anziché informazione utile, dati aggiuntivi necessari per il particolare protocollo di rete utilizzato. Per questo motivo bisogna installare una distribuzione Linux: *GNS3 VM*.
- Con gns3 è possibile avere un throughput al massimo di 1000 pachetti al secondo, mentre nella realtà un router è capace di gestire un throughput anche mille volte superiore.

2.2.2 VIRL

Cisco Virtual Internet Routing Lab (VIRL) è uno strumento software sviluppato da Cisco, il quale sta mettendo molto peso dietro a questo prodotto, rendendolo come il suo software preferito di test e simulazione in futuro. Questa infatti è una soluzione molto più potente rispetto a Cisco Packet Tracer e consente non solo l'apprendimento, ma la simulazione di reti reali. Cisco VIRL è un prodotto più vicino rispetto a GNS3 che consente agli ingegneri di rete di simulare le reti del mondo reale oltre all'apprendimento

delle tecnologie Cisco. È possibile installare un VIRL su un'infrastruttura server di livello aziendale, un computer desktop, un laptop o anche sul cloud. È possibile eseguirlo come macchina virtuale su VMware ESXi, VMware Workstation, Player o VMware Fusion per Mac OS. A differenza dell'esecuzione su un hypervisor, alcuni scelgono di costruire VIRL su un computer bare metal per ottenere il massimo delle prestazioni. Una volta installato e in esecuzione, il laboratorio VIRL è un laboratorio di networking virtuale all-in-one senza fili e cavi collegati. Quando lo si esegue come una macchina virtuale, è possibile ridimensionare, migrare e implementare la disponibilità elevata (HA) sfruttando le funzionalità offerte dall'infrastruttura VMware.

Funzionalità. VIRL ha certamente una quantità enorme di funzionalità. AutoNetkit, che viene fornito con VIRL, può assegnare automaticamente gli indirizzi IP ai nodi al momento dell'avvio e imposta anche alcuni protocolli di routing di base. La configurazione di bootstrap offre una rete completamente convergente non appena vengono avviati e si può andare direttamente alle funzionalità e concentrarsi su ciò che si vuole testare. Questa è una funzione interessante per i tecnici di rete che desiderano configurare un ambiente temporaneo unico per cercare comandi e testare alcune funzionalità. Inoltre, fornisce alcune delle più recenti versioni sui router ed appliance di IOS che è possibile ottenere. Consente di lavorare con le più recenti e ufficiale immagini di molti prodotti Cisco e per questo motivo non vi è nessuna preoccupazione per problemi legali o di licenza software e si possono creare ed eseguire simulazioni di rete senza la necessità di hardware fisico.
VIRL è completamente descritto (per la maggior parte) in entrambe le capacità di commutazione di livello 3 e di livello 2, che è qualcosa che in particolare manca a GNS3, a meno che non si riescano a mettere le mani su immagini di IOU incrinate.
VIRL è una piattaforma basata su OpenStack ed è pronto per SDN. Se si è interessati a conoscere Software Defined Network, VIRL ha l'integrazione diretta con OpenDaylight. Offre un ambiente di progettazione e simulazione di rete scalabile ed estensibile utilizzando il frontend di VM Maestro e ha anche un'ampia capacità di integrazione con macchine virtuali di fornitori di terze parti come Juniper, Palo Alto Networks, Fortinet, F5 BigIP, Extreme Networks, Arista, Alcatel, Citrix VIRL AutoNetkit.[4]

Svantaggi VIRL

- Non adatto ai neofiti della rete, l'installazione e la manutenzione di VIRL sono molto complesse, installarlo è un'impresa, vi sono molti step da eseguire per configurarlo e risolvere i problemi ancor di più .

- VIRL è disponibile in due diverse versioni: Personal Edition e Academic Edition. Quest'ultimo costa 79,99 $ all'anno, mentre la versione Personal Edition costa 199,99 $ all'anno. VIRL ha un limite di licenza per simulare fino a 20 nodi Cisco alla volta. Si può pagare un extra di 100,00 $ per l'aggiornamento a 30 nodi Cisco, massimo. Per qualificarsi per l'acquisto dell'Academic Edition, bisogna essere docente, staff e studenti di qualsiasi istituzione pubblica o privata K-12 o istituto di istruzione superiore.Cisco VIRL è supportato dalla comunità ed è progettato per singoli utenti. Per gli utenti aziendali che desiderano supporto TAC, documentazione approfondita, formazione e altro ancora, c'è Cisco Model-

ing Labs (CML), una versione aziendale di VIRL. Ovviamente la versione CML costa molto di più.

- Se si sta cercando risultati soddisfacenti, semplicemente non lo si otterà se lo si mette su una macchina debole o una macchina multiuso che viene utilizzata per altre cose. VIRL ha bisogno del proprio hardware dedicato per funzionare correttamente. Requisito hardware minimo per VIRL è un computer basato su Intel con quattro core CPU e con almeno 12 GB di memoria. Ogni nodo Cisco IOS-XRv richiede 3 GB di memoria da avviare, quindi bisogna assicurarsi che il computer abbia abbastanza slot vuoti per installare memoria aggiuntiva.

- Nessun supporto multivendor - supporta solo i dispositivi di rete Cisco.

GNS3 vs Virl vs Packet Tracer

- GNS3 esegue IOS reale, è più avanzato, consente di utilizzare IOS completo e connettere dispositivi reali alla rete per un maggiore divertimento. Il rovescio della medaglia è che bisogna mettere le mani su file IOS e non supporta nativamente il passaggio.

- VIRL è lo strumento ufficiale di Cisco, dà accesso a vari dispositivi Cisco e supporta il routing e la commutazione, anche se alcune funzionalità di commutazione come la SPAN non funzionano in questo momento. Il rovescio della medaglia è che non è gratuito, richiede un server decente per funzionare, ed è più avanzato di GNS3.

- PT è uno strumento semplice e gratuito che simula il comportamento dell'IOS. Cisco Packet Tracer è una rete multi-tasking, un software di simulazione per eseguire e analizzare vari attività di rete come: l'implementazione di diverse topologie, selezionare il percorso ottimale in base ai vari percorsi degli algoritmi, creare server DNS e DHCP, creare sottoreti, analizzare varie configurazioni di rete e comandi di risoluzione dei problemi. È abbastanza buono per la maggior parte del CCNA, ma non è così utile al di fuori degli argomenti Router e Switching di CCNA. Inoltre, si limita a "simulare" le ios. Questo vuol dire che non tutti i comandi che esistono su un apparato reale sono configurabili, giusto quelli che ricadono nel CCNA e qualche comando aggiuntivo per la parte security. In sintesi, i suoi vantaggi sono: facile da configurare, supporta le simulazioni di router, switch e PC Cisco, ottimo per gli studi CCNA, simula più dispositivi e protocolli (router, switch, wireless, RADIUS, SNMP). I suoi svantaggi invece: disponibile solo per gli studenti Cisco Academy, software non libero (è necessario aderire a Cisco Academy), codice proprietario - non open source, simula solo i dispositivi Cisco (non esegue vere immagini Cisco, ma solo una simulazione) nessun supporto multivendor, impossibile integrare con dispositivi fisici reali, nessun supporto per Mac OS

La scelta tra uno di questi 3 software varia in larga misura su ciò che si sta cercando di realizzare. Lavorando con moderne immagini e dispositivi IOS, VIRL è ottimo, GNS3 ha simili funzionalità, con molte risorse ma più intuitivo, invece Packet Tracer è un altro piccolo strumento che può essere utilizzato efficacemente nei test e negli scenari rapidi.(fig.2.2)

2.2.3 Boson NetSim

Boson NetSim Network Simulator è un'applicazione che simula l'hardware e il software di rete di Cisco Systems ed è progettata per aiutare l'utente ad apprendere la struttura dei comandi Cisco IOS. Promette di essere il software di simulazione di rete Cisco più potente e versatile disponibile per i professionisti IT che cercano la certificazione CCNA.
NetSim utilizza le tecnologie proprietarie di Simulatore di rete, Router Simulator® ed EROUTER® di Boson, insieme al motore della tecnologia Virtual Packet di Boson, per creare singoli pacchetti. Questi pacchetti vengono instradati e commutati attraverso la rete simulata, consentendo a NetSim di creare una tabella di routing virtuale appropriata e simulare reti reali. Altri prodotti di simulazione sul mercato non supportano questo livello di funzionalità.
Boson offre un simulatore di rete CCENT NetSim, CCNA Network Simulator e CCNP Network Simulator. Ciascuno supporta le tecnologie e le competenze necessarie per la relativa certificazione. Boson NetSim offre più versatilità e supporto di qualsiasi altro software di simulazione di rete sul mercato. Il software NetSim include anche un menu di laboratorio completo che contiene lezioni e laboratori che coprono protocolli di routing, dispositivi Cisco, switching, progettazione topologica e molto altro [7]. Lo strumento simula effettivamente il traffico di rete di una rete reale, in una rete simulata che gli utenti possono progettare autonomamente. Le sue caratteristiche principali sono:

1. Può avere fino a 200 dispositivi per rete. Consente di progettare e configurare una rete con 42 diversi modelli di router e 5 diversi modelli di switch.

2. Lo strumento offre la tecnologia Virtual Packet: pacchetti creati dal software che vengono instradati e commutati attraverso la rete simulata.

3. Fornisce una modalità Telnet che consente di configurare i dispositivi nella topologia simulata utilizzando il programma Windows Telnet.

4. Offre la possibilità di caricare e salvare le configurazioni di rete e la capacità di incollare le impostazioni reali del router nei dispositivi.

5. È anche possibile configurare le proprie mappature degli switch ISDN e Frame Relay.

6. I componenti di simulazione di router, switch e stazioni di NetSim contenuti nel software sono i più avanzati del settore.

7. All'interno di NetSim, la simulazione di router, switch e PC è inclusa in un pacchetto di simulazione di rete drag-and-drop completamente personalizzabile.

2.2.4 Cisco IOS

L'internetwork di un'organizzazione deve avere la capacità di aumentare la produttività complessiva delle sue persone e risorse. Per fare questo, può massimizzare la disponibilità delle applicazioni mentre riduce al minimo il costo totale di proprietà, ciò significa, fornire agli utenti un accesso continuo a una rete flessibile e affidabile e tenere sotto controllo le spese che un'organizzazione deve assorbire nel tempo per sviluppare e mantenere i suoi sistemi e servizi di informazione. Più di ogni altra cosa, Cisco deve la

Network Tools	Packet Tracer	GNS3	VIRL	Boson NetSim
Type	Simulatore	Simulatore/Emulatore	Simulatore	Simulatore
Open Source	✗	✓	✗	✗
Free	✓	✓	✗	✗
Licence Cisco	✓	✗	✓	✓
Requisiti Minimi Hardware	✗	✓	✓	✓
Support Multivendor	✗	✓	✗	✓
Activity Wizard	✓	✗	✗	✗
Virtualization Software	✗	✓	✗	✓
Licence Cisco	✓	✗	✓	✓
Software supported(Wireshark,Np Cap, SolarWinds..)	✗	✓	✓	✓

Figura 2.2: Confronto Simulatori

sua posizione di leadership all'Internetwork Operating System® (IOS) unico e robusto di Cisco. Cisco IOS è un software a valore aggiunto che risiede nel cuore di tutte le soluzioni di internetworking Cisco. Cisco IOS è la chiave di Cisco per aiutare a rendere più produttive le aziende ad alta intensità di informazioni in tutto il mondo. E in definitiva, questo è il più grande vantaggio che qualsiasi rete possa fornire. Esso è un'altra opzione per l'esecuzione di router Cisco in un ambiente virtuale.
Proprio come le imprese che investono in sistemi operativi di rete LAN in grado di evolversi con l'introduzione di nuovi hardware e applicazioni, Cisco IOS è un investimento strategico che consente alle organizzazioni di salvaguardare il futuro delle proprie reti. Cisco IOS supporta cambiamenti e migrazioni inevitabili grazie alla sua capacità di integrare tutte le classi in evoluzione delle piattaforme di rete. Ciò include router, switch ATM, switch LAN e WAN, file server, hub intelligenti, personal computer e qualsiasi altro dispositivo che abbia un impatto strategico sull'internetwork di un'organizzazione. Alimentando le piattaforme Cisco e quelle fornite dai partner tecnologici che incorporano Cisco IOS nei loro prodotti, Cisco IOS consente alle aziende di costruire e migliorare un'infrastruttura dei sistemi informativi unica, integrata ed economica. Cisco IOS è il principale elemento di differenziazione che separa le soluzioni di internetworking di Cisco da altre alternative nel settore. La sua intelligenza a valore aggiunto supporta utenti e applicazioni nell'intera azienda e fornisce sicurezza e integrità dei dati per l'internetwork. L'IOS gestisce in modo efficace le risorse controllando e unificando l'intelligenza di rete complessa e distribuita. Inoltre, funziona come un veicolo flessibile che può aggiungere nuovi servizi, funzionalità e applicazioni all'internetwork. Nell'ambito del supporto delle applicazioni, Cisco IOS fornisce l'interoperabilità con interfacce di protocollo fisiche e logiche basate su standard più di qualsiasi altro fornitore di reti nel settore. Dal doppino alla fibra ottica, dalla LAN al campus fino ai media WAN, da UNIX a Novell NetWare fino all'SNA IBM, nessun'altra architettura di rete può eguagliare il supporto del protocollo ad ampio raggio dell'IOS. [5] È una versione pienamente funzionante di IOS che viene eseguita come processo UNIX in modalità utente (Solaris). IOU è stato creato come immagine Solaris nativa e funziona come qualsiasi altro programma. Uno dei principali vantaggi di Cisco IOU è che non richiede quasi tutte le risorse richieste da GNS3 e VIRL.
Se non si è un dipendente Cisco autorizzato o un partner fidato, l'utilizzo di IOU Cisco è potenzialmente un'area grigia legale. A causa della mancanza di pubblicità e disponibilità per gli studenti di certificazione media e gli ingegneri di rete, le risorse online sono limitate e l'impostazione di una rete richiede molto più impegno. Inoltre, a causa delle funzionalità mancanti e dei ritardi nel supporto delle recenti versioni di immagini

Cisco, Cisco non le consiglia a ingegneri e studenti.

2.3 Software-Defined Networking (SDN)

Il Software Defined Networking è un nuovo modo di concepire le reti, verso il quale si sta concentrando un interesse senza precedenti nella storia di Internet. Una SDN (Software Defined Networking) usa il software anziché dispositivi specializzati per eseguire il provisioning [3] e gestire servizi di rete e applicativi, consentendo una mobilità e un rilascio di applicazioni programmabile, scalabile e on demand. Secondo McKeown [9] l'obiettivo principale di SDN è ristrutturare l'architettura di networking, introducendo opportuni livelli di astrazione in grado di operare una trasformazione simile a quanto gi'a avvenuto nel campo delle architetture elaborative. Nell'ambito del computing, infatti, ormai da molto tempo i programmatori sono in grado di implementare sistemi complessi senza dovere gestire le tecnicit'a dei singoli dispositivi coinvolti o senza interagire in linguaggio macchina, il tutto grazie all'introduzione di opportuni livelli di astrazione nell'architettura. I sistemi SDN centralizzati automatizzano la configurazione e il provisioning dell'intera struttura di rete senza essere limitati dai vincoli dell'hardware. La SDN monitora la rete in modo intelligente e la adatta automaticamente per una gestione ottimale delle condizioni attuali. Rete software-defined consente una gestione centralizzata e strategica della rete. Protegge la rete, garantisce la scorrevolezza e la fluidità del traffico, risolve immediatamente i problemi, accelera il rilascio di applicazioni, abbatte i costi e incrementa la flessibilità delle risorse, da un unico dashboard, senza mai toccare uno switch. Contribuisce inoltre all'innovazione di nuove applicazioni, di servizi e di flussi di ricavi e a ridurre l'esigenza di hardware realizzato appositamente, dei relativi costi e limiti consentendo nel contempo modelli di pagamento a consumo. Molti servizi in tempo reale, come le conversazioni voce e video, sono stati adattati per il trasporto su reti Ethernet e Internet Protocol. La crescita di questi servizi ha comportato configurazioni ancor più complicate e inflessibili sul piano di controllo del routing e della commutazione hardware e sono richieste elevate esigenze sulla disponibilità dell'infrastruttura di rete. Il problema principale è rappresentato dalla staticità dell'architettura attuale che si contrappone ai bisogni degli utilizzatori, i quali richiedono una gestione dinamica, veloce e sicura della rete. Una soluzione a questo problema, l'ha proposta la Open Networking Foundation (ONF) con il Software-Defined Networking (SDN), che sembra costituire una vera svolta per la crescita e l' evoluzione dell'attuale rete di intercomunicazione. Il paradigma Software Defined Network è stato progettato per astrarre le risorse di rete disponibili e controllarle da un'autorità intelligente e centralizzata con l'obiettivo di ottimizzare i flussi di traffico in modo flessibile.
Nei dispositivi che compongono la rete tradizionale, il data plane e il control plane coesistono all'interno dello stesso sistema. SDN suggerisce di centralizzare l'intelligenza di rete in un componente separato, disassociando il processo di forwarding dei pacchetti (Data Plane) [4] da quello di routing (Control Plane.)[5]

[3]Nelle telecomunicazioni, il provisioning implica il processo di preparazione e dotazione di una rete per consentirgli di fornire nuovi servizi ai propri utenti.

[4]Il data plane, anche conosciuto con il nome di forwarding plane, 'e l'hardware specializzato per l'inoltro dei pacchetti. Questo livello si occupa di inoltrare i pacchetti in arrivo verso il next hop, attraverso il percorso selezionato dalla logica del control plane.

[5]Il control plane contiene le funzioni di instradamento o routing. La funzione di routing è quella parte che si occupa di calcolare e determinare il percorso dei pacchetti, ovvero quale direzione deve

Caratteristiche principali

- Direttamente programmabile: il controllo di rete è programmabile in modo diretto perchè è disgiunto dalle funzioni di forwarding.
- Gestione centralizzata: a livello logico, l'intelligenza di rete è centralizzata in controller SDN basati su software che mantengono una visione globale della rete, che alle applicazioni e ai motori di policy appare come un singolo switch logico.
- Agilità: la separazione delle funzioni di control e forwarding consente agli amministratori di regolare dinamicamente il flusso del traffico su tutta la rete per soddisfare le esigenze al loro variare.
- Programmazione configurata: SDN consente ai responsabili di rete di configurare, gestire, proteggere e ottimizzare le risorse di rete molto rapidamente tramite programmi SDN automatici e dinamici, che i responsabili possono scrivere in modo autonomo perchè i programmi non dipendono da software proprietari.
- Standard aperti e non vincolati dai fornitori: se implementato attraverso standard aperti, SDN semplifica la progettazione e il funzionamento della rete perchè le istruzioni sono fornite dai controller SDN invece che dai molteplici dispositivi e protocolli con specifiche diverse per ciascun fornitore. [10]

2.3.1 OpenFlow

Lo standard OpenFlow, si è imposto come base per lo sviluppo di questa architettura di rete definita da SDN. Il protocollo OpenFlow è l'attuale interfaccia di comunicazione standard definita tra il controller e i dispositivi di inoltro che specifica come uno switch sia gestito da un unico dispositivo di controllo. [11]. Il protocollo OpenFlow definisce un modello di nodo generale e unificato da presentare alle applicazioni esterne, rendendo così gli strati più alti dell'architettura di rete SDN indipendenti dall'implementazione del particolare vendor e dalle tecnologie impiegate nel piano di forwarding. In questo modo è possibile monitorare e gestire il traffico della rete secondo determinate necessità. Inoltre OpenFlow utilizza il concetto di flusso per la re-direzione dei pacchetti. In questo contesto, per flusso si intende una sequenza unidirezionale di pacchetti aventi caratteristiche comuni, che attraversa il nodo entro un intervallo temporale, avendo sorgente e destinazioni fisse.
L'idea di base di OpenFlow è quella di rendere possibile la gestione di più switch attraverso il collegamento al controller, il quale semplifica la gestione dei flussi. In questo modo si introduce la possibilità di controllare la rete a livello atomico e permette, in maniera semplificata e potenzialmente più efficiente, la gestione dell'intera infrastruttura, la definizione delle politiche, la gestione del tipo di traffico e sopratutto di ottenere una reattività alle modifiche da parte dell'utente in tempo reale.
Il principio di funzionamento alla base di OpenFlow è quindi la separazione del software di controllo del traffico dai dispositivi di rete fisici. Attraverso il protocollo viene definita la comunicazione tra il controller e i dispositivi di rete mediante un set di regole primitive che consentono l'accesso diretto alle flow table dei dispositivi di rete per la

seguire un pacchetto attraverso la rete per raggiungere la sua destinazione. Tale parte è costituita da algoritmi di routing che calcolano il percorso a seconda della conoscenza della topologia della rete, dai protocolli di routing che si scambiano le informazioni sulla topologia della rete con i nodi vicini e da funzioni di routing che generano le tabelle di routing con le informazioni a disposizione.

gestione del forwarding plane. Questo protocollo di rete utilizza un insieme ben definito di regole di comunicazione per classificare il traffico di rete in flussi. Per flusso si intende una sequenza di pacchetti identificabili da uno o più etichette comuni (quali ad esempio: l'indirizzo IP, l'indirizzo MAC, il numero di porta, ecc.). OpenFlow utilizza il concetto di flusso per determinare e gestire il traffico di rete. Infatti, questo concetto permette al protocollo di identificare specifiche porzioni di traffico con delle regole impostate in precedenza e immagazzinate in flow table in modo da far intraprendere azioni personalizzate.

Perchè OpenFlow? OpenFlow si rivela fin da subito un ottimo strumento per la facilità con cui si possono ideare e anche testare il funzionamento di nuovi protocolli. In poco tempo si riesce a raccogliere i risultati e le criticità di una determinata rete, e si può agire su di essa con modifiche strutturali che nelle reti tradizionali richiederebbero operazioni molto più laboriose mentre nel caso di OpenFlow sarà sufficiente modificare a livello software il controller. Si hanno così molteplici vantaggi:[12]

- Aumento di velocità delle reti.
- Maggiore dinamicità e agevolazione nella personalizzazione della rete.
- Maggiore sicurezza e ottimizzazione del sistema.
- OpenFlow permette un uso flessibile della rete, nasconde la complessità delle singole parti dei dispositivi di rete e ne centralizza il controllo in modo virtualizzato, semplificando quindi notevolmente la gestione della rete.

2.3.2 Mininet

Mininet è un emulatore di rete che gestisce una raccolta di host finali, switch, router e collegamenti su un singolo kernel Linux. Utilizza la virtualizzazione leggera per rendere un singolo sistema simile a una rete completa, con lo stesso kernel, sistema e codice utente. Un host Mininet si comporta come una vera macchina. I programmi che si eseguono possono inviare pacchetti attraverso quello che sembra una vera interfaccia Ethernet , con una data velocità di collegamento e ritardo. I pacchetti vengono elaborati da ciò che sembra un vero switch, router o middlebox Ethernet, con una determinata quantità di accodamento. Quando due programmi, come un client e un server iperf, comunicano tramite Mininet, le prestazioni misurate devono corrispondere a quelle di due (più lente) macchine native. In breve, gli host, gli switch, i collegamenti e i controller virtuali di Mininet sono la cosa reale: vengono creati solo utilizzando software anziché hardware, e per la maggior parte il loro comportamento è simile a elementi hardware discreti. In genere è possibile creare una rete Mininet simile a una rete hardware o una rete hardware simile a una rete Mininet e eseguire lo stesso codice binario e le stesse applicazioni su entrambe le piattaforme.
L'emulatore di rete Mininet, è capace di creare rapidamente, efficientemente e con risorse limitate una rete virtuale basata sul concetto di SDN. L'emulatore Mininet è in grado di simulare un'intera rete grazie ad una virtualizzazione leggera avvalendosi di tecnologie implementate nel kernel linux e soprattutto dei network namespaces3 consentendo l'avvio di interfacce virtuali, connesse da cavi virtuali, nell'ambito dell'esecuzione di un singolo sistema operativo. L'emulatore consente di creare reti anche molto complesse e di effettuare numerosi test su di esse. Tutto ciò in un ambiente virtuale,

permettendo lo sviluppo di nuovi sistemi di reti e la verifica della loro funzionalità, all'interno di una singola macchina.[14]

Vantaggi:

- Velocità: l'avvio di una semplice rete richiede solo alcuni istanti, a seconda dell'hardware della macchina su cui viene eseguito.
- È possibile eseguire programmi reali: tutto ciò che viene eseguito su Linux è disponibile per l'esecuzione, dai server Web agli strumenti di monitoraggio delle finestre TCP a Wireshark.
- Possibilità di creare topologie personalizzate: unico switch, topologie più ampie simili a internet, un data center, ecc.
- Si può eseguire Mininet sul laptop, su un server, su una VM, su una Linux box nativa (Mininet è incluso con Ubuntu 12.10+!), O nel cloud (ad esempio Amazon EC2.)
- Personalizzazione ed inoltro di pacchetti: gli switch di Mininet utilizzano il protocollo OpenFlow e quindi sono programmabili.
- Codice open-source: si può esaminare e modificare il codice sorgente.

Limitazioni

- Limitazioni nell'eseguire una rete su un unico sistema: le risorse dovranno essere bilanciate tra gli host della rete.
- Di default tutti gli host Mininet condividono il file system host e lo spazio PID; questo significa che potrebbe essere necessario prestare attenzione se si stanno eseguendo daemon che richiedono la configurazione in / etc, e bisogna stare attenti a non uccidere i processi sbagliati per errore.
- Mininet utilizza un unico kernel linux per tutti gli host virtuali: non è possibile eseguire software dipendente da kernel differenti.
- Mininet non crea il controller: se si necessita di un controller personalizzato bisognerà implementarlo per poi poterlo utilizzarlo.
- Mininet non ha una nozione forte di tempo virtuale: questo significa che le misure temporali saranno basate sul tempo reale e che emularle con maggiore velocità non sarà semplice.

3. Cisco-PacketTracer

CISCO SYSTEMS INC. è il leader mondiale nel networking per Internet. La società è stata fondata nel 1984 da due scienziati informatici della Stanford University, che cercarono un modo più semplice per collegare diversi tipi di sistemi informatici.
Oggi i router Cisco sono conosciuti e utilizzati in tutto il mondo per la loro qualità costruttiva e per le loro prestazioni.

Figura 3.1: Logo CISCO

Prodotti e Servizi I prodotti e i servizi Cisco si concentrano su tre segmenti di mercato: impresa e fornitore di servizi, piccola impresa e casa.

Certificazioni Cisco Systems sponsorizza anche una linea di certificazioni IT professionali per i prodotti Cisco. Esistono cinque livelli di certificazione:

- **Entry** (CCENT, CCT).
- **Associate** (CCDA, CCNA Routing and Switching, CCNA Data Center, CCNA Security, CCNA Service Provider, CCNA Cloud, CCNA Collaboration, CCNA Industrial, CCNA Wireless).
- **Professional** (CCDP, CCNP Routing and Switching, CCNP Data Center, CCNP Security, CCNP Service Provider, CCNP Cloud, CCNP Collaboration, CCNP Wireless).
- **Esperto** (CCDE, CCIE Collaboration, CCIE Data Center, CCIE Routing and Switching, CCIE Security, CCIE Service Provider, CCIE Wireless).
- **Architect**,(CCAr).

Cisco offre formazione per queste certificazioni tramite un portale chiamato **Cisco Networking Academy**. Le scuole idonee possono diventare membri della Cisco Networking Academy e quindi fornire corsi CCNA o di altro livello. Gli istruttori Cisco Academy devono essere certificati CCNA per essere un istruttore certificato CCAI.[15]

3.1 Packet Tracer

Secondo indicazione di Cisco, l'apprendimento efficace delle attività di laboratorio riguardo le reti, passa anche attraverso Packet Tracer. Per questa ragione, Cisco da 12 anni continua a investire e aggiornare continuamente il software impiegando risorse economiche e i migliori esperti di ingegneria e didattica.
Packet Tracer non sostituisce l'indispensabile pratica su apparati reali, ma fornisce un setting didattico individualizzato impossibile da creare in un laboratorio reale, favorendo, strutturando e allenando capacità indispensabili nel troubleshooting come:(Problem Solving;Gestione del tempo;Pensiero critico e creativo; Simulazione; Visuale; Autovalutazione;Pratica individuale e collaborativa).

Il software consente agli utenti di creare topologie di rete, simulare la configurazione di router e switch Cisco utilizzando un'interfaccia a linea di comando simulata. Packet Tracer utilizza un'interfaccia utente *drag and drop*, che consente agli utenti di aggiungere e rimuovere dispositivi di rete simulati come meglio credono. Il software è principalmente rivolto agli studenti certificati Cisco Network Associate Academy come strumento educativo per aiutarli ad apprendere i concetti fondamentali di CCNA. Da agosto 2017 con la versione 7.1 il software è gratuito per tutti, in precedenza solo gli studenti che si erano iscritti a un programma CCNA Academy potevano liberamente scaricare e utilizzare lo strumento gratuitamente per uso didattico.

Nato da un team di programmatori, istruttori ed ex studenti del programma sotto la guida di Dennis Frezzo di Cisco Systems, PT è un ottimo strumento per la simulazione di rete progettato per facilitare e migliorare l'apprendimento del Networking. Esso è considerato da molti una vera rivoluzione nella didattica del Cisco Networking Academy Program. Tutti coloro che hanno avuto esperienza di insegnare corsi di reti, concorderanno che alcuni concetti teorici, il meccanismo di funzionamento di alcuni protocolli o la sequenza di passi per lo svolgimento di una configurazione di un dispositivo, necessitano di "essere visti" per poter essere compresi a fondo.
PT consente questo e molto altro al punto da poter essere considerato per i futuri professionisti del Networking IP una vera palestra formativa dove mettere alla prova le proprie conoscenze teoriche e apprendere per scoperta nuovi aspetti.

Glossario. Prima di andare nello specifico di Packet Tracer sono stati raggruppati nel seguente glossario (tab.3.1), alcuni termini che saranno utitli per questa tesi.

Termine	Significato
Router	Dispositivo elettronico che, in una rete informatica a commutazione di pacchetto, si occupa di instradare i dati, suddivisi in pacchetti, fra reti diverse.
Switch	Dispositivo di comunicazione situato al livello data link (livello 2) dell'OSI Model che inoltra il traffico su una LAN basandosi sull'indirizzo MAC.
AccessPoint	Ricetrasmettitore che usa onde radio per connettere reti cablate con dispositivi wireless o reti esclisivamente wireless.
EDGE ROUTER	Router interfacciato con una rete ATM.
FIREWALL	Software usato per proteggere un server da attacchi pervenuti via rete locale o via Internet. Consente il passaggio solamente di determinati tipi di dati, da determinati terminali e determinati utenti.
GATEWAY	Punto di collegamento tra due o più reti differenti, che quindi fa da ingresso. In Internet un gateway indirizza i datagram sulle numerose reti collegate. Nelle reti aziendali il gateway è un computer che spesso viene usato anche come firewall e proxy server.
GIGABIT ETHERNET	Termine generico utilizzato per descrivere le varie tecnologie che implementano la velocità nominale di una rete Ethernet fino a 1 gigabit per secondo. Viene supportata sia dai cavi in fibra ottica che dai cavi twisted pair.
HOST	Ospite. Computer della rete che ospita risorse e servizi disponibili ad altri sistemi.
KB/SEC	Unità di misura standard della quantità di dati trasferiti nell'unità di tempo su una rete. Equivale a circa 1.000 bit al secondo.
LAN	Nel campo dell'informatica LAN è l'acronimo del termine inglese Local Area Network, in italiano rete locale.Identifica una rete costituita da computer collegati tra loro, dalle interconnessioni e dalle periferiche condivise in un ambito fisico delimitato. Le LAN tradizionali lavorano tra 10 Mbps e 100 Mbps, hanno bassi ritardi e pochissimi errori.
SCREENSHOT	Il risultato della cattura di una immagine dello schermo effettuato con diverse metodologie la cui più semplice risulta tramite il tasto "Stampa schermo". Si può catturare sia lo schermo intero che una parte di esso.
TERMINALE	Programma di "basso livello", di solito una CLI, che consente di controllare il funzionamento di un computer o di una qualunque apparecchiatura remota (tramite una connessione Telnet) oppure di accedere, localmente, ad una periferica che sia collegata ad una porta seriale (un modem, ad esempio) ed in grado di interpretare le stringhe di comando digitate dall'operatore.
CLI	La CLI è un'interfaccia di tipo testuale: la comunicazione tra il sistema (Host) e l'utilizzatore avviene infatti attraverso sequenze (stringhe) di caratteri. Grazie ad un "interprete", la macchina Host riconosce i comandi impartiti dall'utilizzatore ed esegue i programmi corrispondenti: come per esempio visualizzare l'elenco dei file contenuti in una directory, o come la configurare delle interfacce di rete.

BRIDGE	Dispositivo di rete che collega diversi segmenti di rete al livello due dell'OSI Model e separa due collision domain svolgendo le stesse operazioni di uno switch. Non a caso infatti lo switch è detto "bridge multiporta". I bridge filtrano il traffico leggendo gli indirizzi MAC e memorizzando solo quelli che si trovano sul loro lato che saranno poi quelli ai quali verranno consegnati i pacchetti.
HUB	Dispositivo nel quale convergono i dati provenienti da molti computer collegati in rete, e dal quale i dati vengono inviati verso una o più destinazioni (server, altri computer, periferiche...). Spesso i dispositivi comprendono hub e switch: hub è la parte che riceve i dati da più direzioni, switch è la parte che determina dove e come i dati vengono inviati. Nell'insieme del suo funzionamento, un hub non può essere utilizzato e considerato come un router in quanto essendo un dispositivo di livello 1 (fisico) non riconosce il destinatario ed effettua un broadcast a tutti i devices della rete anche se solo il destinatario riceverà il pacchetto.
MODEM	Componente del computer che si occupa di modulare i segnali digitali, trasformandoli in analogici, in modo tale che possano essere trasportati dalle convenzionali linee telefoniche, e di eseguire il processo inverso per i segnali in entrata dalla linea telefonica verso il computer.

Tabella 3.1: Glossario

3.1.1 Perchè utilizzare Packet Tracer?

Packet Tracer è considerato da molti una vera rivoluzione nella didattica del Cisco Networking Academy Program, infatti viene considerato come una vera palestra formativa dove mettere alla prova le proprie conoscenze teoriche e apprendere nuovi aspetti. Si possono creare delle topologie composte da dispositivi generici da dispositivi Cisco, simulare l'interfaccia utente a riga di comando CLI (Command Line Interface) del sistema operativo Cisco IOS presente e svolgere delle analisi di tipo "what if" creando scenari di traffico.
Il software di e-learning Tracer è stato progettato per aiutare le persone più facilmente a sviluppare le competenze della tecnologia di rete in un ambiente in rapida evoluzione offrendo nuove opportunità per l'apprendimento sociale, la sperimentazione e la collaborazione. Cisco Packet Tracer è un simulatore di rete che può essere utilizzato non solo dagli studenti ma anche da istruttori e amministratori di rete. Questo software fornisce una vasta gamma di switch e router Cisco in esecuzione su IOS , dispositivi wireless di Linksys e diversi dispositivi terminali come PC e server con una riga di comando. È più di un semplice simulatore, fornisce una simulazione fisica e uno strumento di valutazione. Lo strumento di valutazione può essere utilizzato per creare domande pratiche sul networking con un modello di punteggio.

Packet Tracer semplifica, migliora e finalizza l'apprendimento nei corsi Cisco in quanto:

- Consente un'esperienza e gestione panoramica della rete da parte del singolo utente.
- Propone laboratori preconfigurati appositamente disegnati da Cisco con obiettivi didattici coerenti con gli obiettivi di certificazione con feedback automatico degli step raggiunti e monitoraggio del tempo.
- Fornisce un ambiente di apprendimento sia individuale che collaborativo.
- Si possono creare delle topologie composte da dispositivi generici e/o da dispositivi Cisco.
- Si può simulare l'interfaccia utente a riga di comando del sistema operativo Cisco IOS presente sui dispositivi Cisco.
- Si può ispezionare dinamicamente lo stato di ciascun dispositivo e il formato di ciascun pacchetto attivo sulla topologia di rete.
- Grazie all'aiuto di un wizard, si possono creare delle PT Activity, un tipo speciale di file che include una topologia iniziale, delle istruzioni e una serie di obbiettivi finali da raggiungere. Nell'esecuzione dell'Activity lo studente è costantemente valutato in maniera automatica dal software che lo guida nella risoluzione dell'esercizio dandogli indicazioni sul grado di completamento dello stesso.

3.2 Interfaccia

Essendo un programma di sviluppo, molti di quelli che iniziano a cimentarsi nel mondo di Packet Tracer, trovano molte difficoltà. Tuttavia, il layout di Packet Tracer risulterà semplice ed intuitivo. Una volta installato il programma per il proprio sistema operativo, la schermata iniziale sarà come in (fig.3.2) e i componenti dell'interfaccia Packet Tracer sono i seguenti:

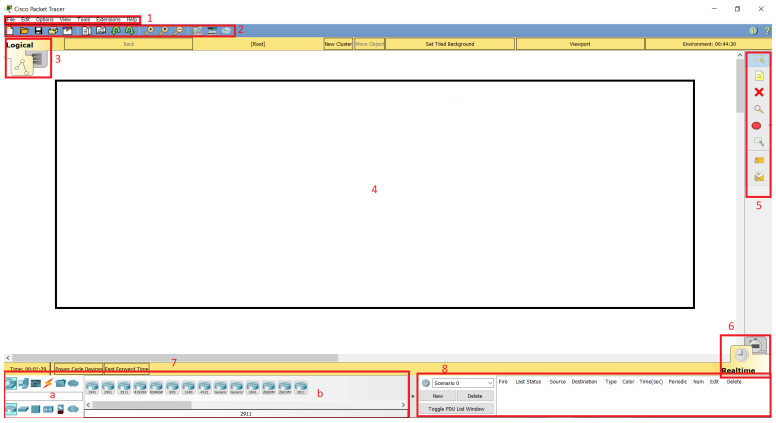


Figura 3.2: interfaccia

- **Area 1: Barra dei menu** - Questo è un menu comune che si trova in tutte le applicazioni software. Tramite la voce *File* si può creare/aprire/salvare/stampare

un progetto; con *Edit* si effettuano le tradizionali operazioni di copia e incolla e di annulla operazione; con la voce *Options*, si possono visualizzare le preferenze e gestirle, come l´user profile. Per visualizzare o no la barra di tool di destra e la Bottom Toolbar, gestire lo zoom, basta selezionare l´apposita voce da *View*. Dalla voce *Tools* si possono settare le impostazioni di disegno. Da *Extensions* si può avviare l'Activity Wizard che aiuterà a creare gli scenari di lavoro. Infine tramite la voce *Help* si può ottenere aiuto per l'utilizzo dell´intero ambiente di lavoro.

- **Area 2: Barra degli strumenti principale** - Questa barra fornisce icone di collegamento alle opzioni di menu a cui si accede comunemente, come open, save, zoom, undo e redo, invece sul lato destro si trova l'icona per inserire le informazioni di rete per la rete attuale.
- **Area 3: Schede dello spazio di lavoro logico / fisico** - Queste schede consentono di passare tra le aree di lavoro logiche e fisiche.
- **Area 4: Area di lavoro** - Questa è l'area in cui vengono create le topologie e le simulazioni.
- **Area 5: Barra degli strumenti comuni** - Questa barra degli strumenti fornisce i controlli per la manipolazione topologie, come selezionare, spostare il layout, inserire note, eliminare, ispezionare, ridimensionare forma e aggiungere PDU semplici / complesse.
- **Area 6: Schede Realtime / Simulation** - Queste schede vengono utilizzate per alternare le modalità reali e di simulazione. Sono inoltre disponibili pulsanti per il controllo di tempo e per catturare i pacchetti.
- **Area 7 : Scatola del componente di rete** - Questo componente contiene tutto il dispositivi di rete e finali disponibili con Packet Tracer, ed è ulteriormente diviso in due aree:
- **Area 7a: Casella di selezione del tipo di dispositivo** - Questa area contiene il dispositivo categorie.
- **Area 7b: Casella di selezione specifica per dispositivo** - Quando una categoria di dispositivo è selezionato, questa casella di selezione visualizza i diversi modelli di dispositivo all'interno di quella categoria.
- **Area 8: Casella pacchetto creata dall'utente** - Gli utenti possono creare una soluzione altamente personalizzata dei pacchetti per testare la loro topologia da quest'area e vengono visualizzati i risultati come una lista.

3.3 Prima Topologia di Rete

La topologia di rete è la rappresentazione geometrica di relazione di tutti i collegamenti che collegano i dispositivi o i nodi. La topologia di rete si rappresenta in due modi: una topologia fisica, che definisce il modo in cui una rete è disposta fisicamente e l'altra è una topologia logica, che definisce come i dati effettivamente fluiscono attraverso la rete. E' possibile utilizzare una topologia di riferimento esistente oppure crearne una nuova da zero.

3.3.1 Dispositivi in Packet Tracer

La rete funziona collegando computer e periferiche tramite switch, router e punti di accesso. Questi dispositivi sono le basi essenziali di networking, che consentono ai vari dispositivi collegati alla rete di comunicare tra loro, così come con altre reti. Router, switch e access point eseguono funzioni molto diverse in una rete. Selezionando Switch o Router dalla casella di selezione del tipo di dispositivo, sono elencati sia i dispositivi Cisco sia alcuni dispositivi etichettati come *"Generic"*. [17]

- **Router**: fornisce connettività tra due reti logiche. I router, vengono utilizzati per connettere più reti. Ad esempio, si utilizzerà un router per connettere i computer in rete a Internet e quindi condividere una connessione Internet tra molti utenti. Il router agirà come un dispatcher, scegliendo il percorso migliore per le informazioni per viaggiare in modo da riceverlo rapidamente.
  Ogni router in Packet Tracer può essere acceso o spento utilizzando il pulsante di alimentazione fornito. L'interruttore di accensione è necessario per fare in modo che un dispositivo simuli la sua controparte reale. I moduli possono essere aggiunti o rimossi solo dopo aver spento il dispositivo. Se la configurazione in esecuzione non viene salvata, spegnendo e riaccendendo un dispositivo si perderà la sua configurazione. Su packet tracer si possono scegliere i seguenti tipi di router: Cisco(1841,1941,2620XM,,2621XM,2811,2901,2911) e Generic Router-PT(fig. 3.3)

Figura 3.3: Vari Router In PT

- **Switches**: uno switch, chiamato anche "ponte multiporta", collega più di due dispositivi finali insieme. Ogni porta dello switch è un dominio di collisione. Gli switch vengono utilizzati per connettere più dispositivi sulla stessa rete all'interno di un edificio o di un campus. Ad esempio, uno switch fungendo da controller, può connettere computer, stampanti e server, consentendo ai vari dispositivi di condividere informazioni e comunicare tra loro. Tra i vari switches disponibili in PT ci sono: Cisco(2950-24, 2950T-24, 2960-24TT, 3560-24PS), Bridge PT e Generic Switch PT. (fig. 3.4)

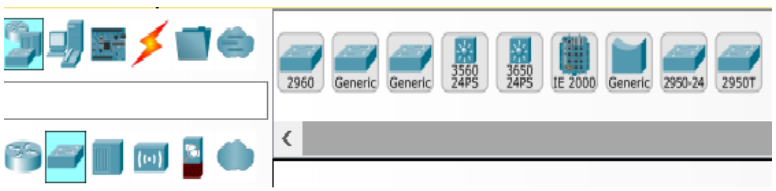


Figura 3.4: Switch In PT

Emulazione di WAN. Per introdurre più scenari di vita reale, Packet Tracer dispone di dispositivi che emulano una WAN. Facendo clic sull'icona della nuvola di emulazione

WAN dalla casella di selezione del tipo di dispositivo si elencano i seguenti dispositivi:

- *Cloud-PT*: questo dispositivo si presenta come una nuvola nella barra degli strumenti, ma sotto la finestra di configurazione sembra più un router con più slot.
- *DSL-Modem-PT*: questo è un modem con un'interfaccia Ethernet e un Interfaccia RJ11. L'interfaccia Ethernet può essere commutata tra Ethernet,FastEthernet e GigibitEthernet. Questo dispositivo non ne ha opzioni di configurazione.
- *Cable-Modem-PT*: questo modem è simile al precedente, tranne il fatto che supporta una porta coassiale.

Figura 3.5: WAN Emulation In PT

Dispositivi IOT. Oltre ai classici dispositivi di rete come router e switch disponibili nelle versioni precedenti, Packet Tracer 7.0 Network Component Box ora contiene un'ampia varietà di Smart Things. Le cose intelligenti sono oggetti fisici che possono connettersi a Registration Server o Home Gateway tramite un'interfaccia di rete. Sono suddivisi in 4 sottocategorie: Home, Smart City, Industrial e Power Grid. I componenti sono oggetti fisici che si connettono al microcontrollore (MCU-PT) o ai computer a scheda singola (SBC-PT). In genere non dispongono di un'interfaccia di rete e si basano su MCU-PT o SBC-PT per l'accesso alla rete. Si tratta di dispositivi semplici che comunicano solo attraverso le loro slot analogiche o digitali. Esistono tre sottocategorie per i componenti:

- Schede: microcontrollori (MCU-PT), computer a scheda singola (SBC-PT) e uno speciale dispositivo chiamato Thing che vengono utilizzati per creare oggetti fisici autonomi come macchine per il caffè o allarmi antifumo.
- Attuatori: questi componenti manipolano l'Ambiente, loro stessi o l'area circostante.
- Sensori: questi componenti percepiscono l'ambiente (rilevatori foto, sensore di temperatura), l'area circostante (RFID, sensore metallico) o le interazioni (potenziometro, pulsante).

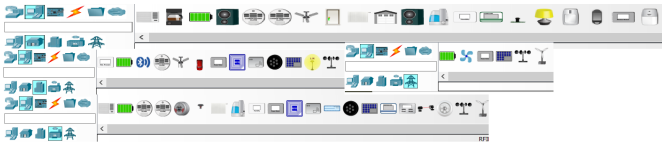


Figura 3.6: Dispositivi IOT

Personalizzazione dispostitivi con moduli. Un modulo dispositivo è un componente hardware che contiene diverse interfacce di dispositivo. Ad esempio, un modulo HWIC-4ESW contiene quattro porte Ethernet (10 MBps). Simile a un router / switch reale, il dispositivo deve essere spento per aggiungere o rimuovere i moduli.
L'interruttore di alimentazione si trova sul lato destro di ciascun dispositivo, con un LED verde che indica lo stato se è acceso. Per aggiungere un modulo, bisogna spegnere il dispositivo, trascinare uno dei moduli elencati su uno slot vuoto. Se un modulo non si adatta a quello slot, lo fa ritornare automaticamente alla lista dei moduli.(fig.3.7)

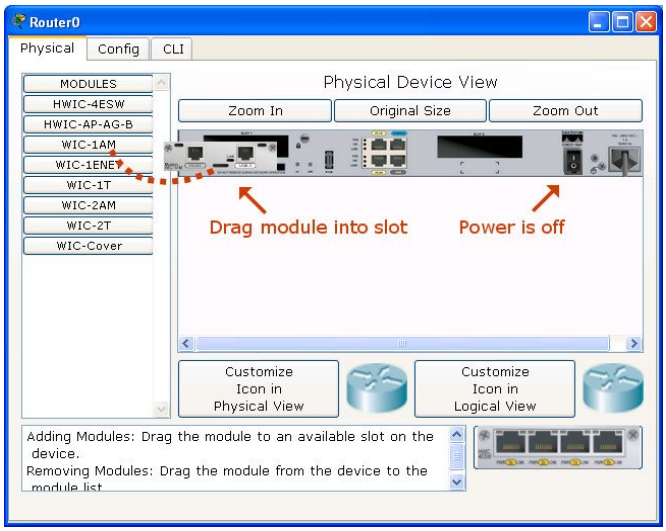


Figura 3.7: Modules In PT

Convenzioni di Nomi Ogni router ha più di una dozzina di moduli, ma l'interfaccia che offrono può essere identificata dai loro nomi.

- **Copper Ethernet Interface:**: questa è la normale interfaccia LAN, che richiede in un connettore RJ-45 aggraffato a un cavo di rame. In base alla velocità, le interfacce possono essere denominate come Ethernet (10 MBps), FastEthernet (100 MBps) e GigabitEthernet (1000 MBps). I moduli con interfacce Ethernet possono essere identificate con un numero seguito da E, FE, CE, CFE o CGE.

  1. HWIC-4ESW (quattro porte di commutazione Ethernet)
  2. WIC-1ENET (porta Ethernet singola)
  3. NM-1E (porta Ethernet singola)
  4. NM-1FE-TX (singola porta Fast Ethernet)
  5. NM-4E (quattro porte Ethernet)
  6. NM-ESW-161 (16 porte di commutazione Ethernet)
  7. PT-ROUTER-NM-1CE, PT-ROUTER-NM-1CFE, PT-ROUTER -NM-1CGE (moduli personalizzati Packet Tracer)

- **Fiber Ethernet Interface**: questo è simile all'interfaccia precedente, tranne il fatto che usa un cavo in fibra. Questi moduli sono identificati in base alla lettera F.

1. NM-1FE-FX (single Fast Ethernet fiber media)
2. PT-ROUTER-NM-1FFE, PT-ROUTER-NM-1FGE(Packet Tracer moduli personalizzati)

- **Serial Interface**: i moduli con interfacce seriali hanno la lettera T o la stringa A / S. La differenza è che quelli con T sono sincroni mentre i moduli A / S sono asincroni. Questa differenza in un simulatore non fa differenza.

  1. WIC-1T, WIC-2T (una porta seriale sincrona singola o doppia)
  2. NM-4A/S, NM-8A/S(quattro o otto asincroni / sincroni porte seriali)
  3. PT-ROUTER-NM-1S, PT-ROUTER-NM-1SS(Packet Tracer moduli personalizzati)

- **Modem Interface**: I moduli con questa interfaccia hanno porte RJ11 per analogico cavi telefonici. Sono identificati avendo le lettere AM presenti dopo un numero come mostrato nel seguente elenco:

  1. WIC-1AM (doppie porte RJ11 per telefono e modem).
  2. WIC-2AM, WIC-8AM (due o otto porte RJ11)
  3. PT-ROUTER-NM-1AM

- **WICs within NMs**: Alcuni moduli di rete (NM) non occupano tutto lo spazio di uno slot, quindi forniscono slot WIC al loro interno per ospitare schede più piccole. Tali moduli possono essere riconosciuti dalla lettera W alla fine del loro nome.

  1. NM-1E2W, NM-1FE2W (una singola porta Ethernet / Fast Ethernet e due slot WIC).
  2. NM-2E2W, NM-2FE2W (due porte Ethernet / Fast Ethernet e due slot WIC)
  3. NM-2W (nessuna interfaccia, solo due slot WIC)

- **Slot Covers**: Packet Tracer fornisce anche coperture per slot vuoti.

  1. NM-Cover copre uno slot per modulo di rete.
  2. WIC-Cover copre uno slot WIC

- **HWIC-8A**: Questo modulo è nuovo di Packet Tracer. Ne fornisce otto connessioni EIA-232 asincrone alle porte della console. Un router può essere usato come un server di accesso se questo modulo è collegato.

  1. NM-Cover copre uno slot per modulo di rete.
  2. WIC-Cover copre uno slot WIC

Creazione di un dispositivo personalizzato Se si ha bisogno di un router con un particolare set di moduli, potrebbe essere un compito arduo trascinare i moduli ogni volta prima di creare una topologia. Quindi Packet Tracer offre una funzione per salvare un dispositivo che hai personalizzato come dispositivo personalizzato. Effettuare, eseguire i seguenti passaggi per creare un dispositivo personalizzato.

1. Trascinare e rilasciare un dispositivo di rete nell'area di lavoro. Per questo esempio, si userà uno Switch.

2. Fare clic sullo switch per aprire la relativa finestra di dialogo di configurazione e ruotare il dispositivo spento.

3. Aggiungere i moduli più usati per questo Switch.

4. Passare a Strumenti — Finestra di dialogo dei dispositivi personalizzati o premere Ctrl + E.

5. Fare clic sul pulsante Seleziona, quindi fare clic sullo switch che è stato personalizzato.

6. Fornire un nome e una descrizione, quindi fare clic su Aggiungi e Salva.

Questo dispositivo personalizzato viene salvato con estensione .ptd in % USERPROFILE %-Cisco Packet Tracer 7.0.1-templates; per rendere questo dispositivo personalizzato disponibile per tutti gli utenti, bisogna copiare % PT5HOME % -templates.

3.3.2 Collegamento dei dispositivi

Scegliendo l'icona Connections dalla casella di selezione del tipo di dispositivo, sono elencati diversi cavi, che possono essere utilizzati per collegare i dispositivi (fig.**??**). I più utilizzati sono:

- *Console*: questo è un cavo console che viene utilizzato per visualizzare la console del dispositivo di rete da un PC / laptop. Un'estremità del cavo si collega alla console porta di un dispositivo di rete mentre l'altro si collega alla porta RS-232 su un PC / laptop.

- *Copper straight-through*: questo è un cavo Ethernet standard che viene utilizzato per collegare due dispositivi che operano in diversi livelli del modello OSI (come hub per router e passare al PC). Può essere utilizzato con Ethernet,Tipi di porte Fast Ethernet e Gigabit Ethernet.

- *Copper cross-over*: questo cavo Ethernet collega i dispositivi che operano in lo stesso livello OSI (come da hub a hub, da PC a PC, da PC a router e PC a stampante). Questo cavo può essere utilizzato anche con Ethernet, Fast Ethernet e tipi di porte Gigabit Ethernet.

- *Serial DCE and DTE*: i cavi seriali collegano i router e si connettono router al cloud. La fine del DCE (apparecchiature per la terminazione del circuito dati)ha un simbolo di orologio su di esso. La sincronizzazione deve essere abilitata a questo scopo usando la frequenza di clock "300-4000000" comando per attivare il protocollo di linea. Se come seriale viene scelto DTE (Data Terminal Equipment), il primo dispositivo collegato con questo cavo sarà il terminale DTE e il dispositivo successivo sarà il terminale DCE. Per il Cavo seriale DCE, questo è esattamente l'opposto.

- *Automatically choose connection type*: se si è confusi riguardo al cavo da usare, scegliendo questa opzione si connettono automaticamente due dispositivi.

Figura 3.8: Connections

Un cavo ethernet incrociato o crossover è un tipo di cavo di rete usato per connettere assieme due dispositivi di rete dello stesso livello ISO/OSI: hub con hub (livello 1), switch con switch (livello 2), router con router (livello 3). Con il **cavo Straight-trough** si possono collegare gli host ai dispositivi di rete. Come prima cosa dopo aver collegato i dispositivi insieme, si noterà una luce a ciascuna estremità del cavo; questo indica lo stato della connessione.

- *Verde acceso* : indica che il collegamento fisico è attivo, ma non indica lo stato del protocollo di linea.
- *Verde lampeggiante*: indica l'attività di collegamento.
- *Rosso*: indica che il collegamento fisico è inattivo. Questo può essere causato da cavi errati o da una porta che viene arrestata amministrativamente.
- *Ambra*: appare solo sugli interruttori e indica che la porta è in esecuzione l'algoritmo STP (Spanning Tree Protocol) per rilevare loop di livello 2.

Un semplice esempio di una topologia di rete, si può creare effettuando le seguenti operazioni:

- Dalla casella del componente di rete, si seleziona "End Devices" e si trascina un'icona del PC generico e un'icona del computer portatile generico nell'area di lavoro. Poi per collegarli bisogna andare su "Connections" selezionare "Copper Cross-Over" da PC0 al Laptop0 e si seleziona "FastEthernet". Successivamente, bisogna fare clic su Laptop0 e selezionare FastEthernet. Il LED di stato del collegamento dovrebbe apparire in verde, a indicare che il collegamento è attivo. (fig. 3.9)

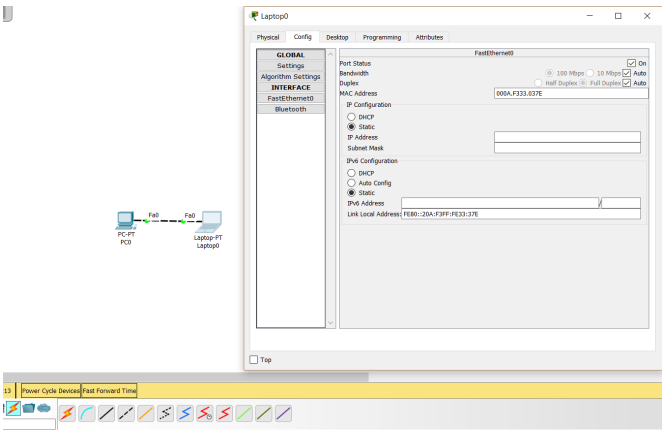


Figura 3.9: Collegamento

Tecnologia	**Protocolli**
LAN	Ethernet (including CSMA/CD*), 802.11 a/b/g/n wireless*, and PPPOE.
Switching	VLANs, 802.1q, trunking, VTP, DTP, STP*, RSTP*, multilayer switching*, EtherChannel, LACP, and PAgP.
TCP/IP	HTTP, HTTPS, DHCP, DHCPv6, Telnet, SSH, TFTP, DNS, TCP*, UDP, IPv4*, IPv6*, ICMP, ICMPv6, ARP, IPv6 ND, FTP, SMTP, POP3, and VOIP(H.323) .
Routing	Static, default, RIPv1, RIPv2, EIGRP, single area OSPF, multiarea OSPF, BGP, inter-VLAN routing, and redistribution.
WAN	HDLC, SLARP, PPP*, and Frame Relay*
Security	IPsec, GRE, ISAKMP, NTP, AAA, RADIUS, TACACS, SNMP, SSH, Syslog, CBAC, Zone-Based Policy Firewall, and IPS.
QoS	Layer 2 QoS, Layer3 DiffServ QoS, FIFO Hardware queues, Priority Queuing, Custom Queuing, Weighted Fair Queuing, MQC, and NBAR* .
Miscellaneous	ACLs (standard, extended, and named), CDP, NAT (static, dynamic, inside/ outside, and overload), and NATv6.

Tabella 3.2: Protocolli

- Una volta verificato che il collegamento sia attivo, si configurano gli indirizzi IP(non esistente) e le Subnet Mask, cliccando i vari PC, accedendo alla scheda Desktop e infine su Configurazione IP. Bisogna assicurarsi che entrambi gli indirizzi IP si trovino nella stessa subnet.

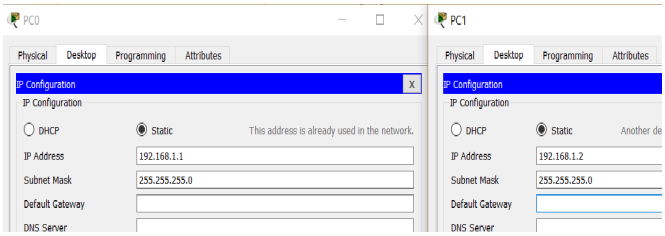


Figura 3.10: IP Configuration

- Per salvare questa topologia, accedere a File — Salva come e scegliere una posizione.

3.4 Protocolli supportati da Packet Tracer

Ogni volta che si vuole configurare, provare una nuova tecnologia, bisogna assicurarsi che i protocolli siano pienamente supportati da Packet Tracer, prima di andare avanti. **Un protocollo** è lo speciale insieme di regole che i punti finali di una connessione di telecomunicazione usano quando comunicano, specificano le interazioni tra le entità comunicanti. Un simulatore, come suggerisce il nome, simula i dispositivi di rete e il suo ambiente, quindi i protocolli in Packet Tracer sono codificati per funzionare e comportarsi allo stesso modo di come lo farebbero su hardware reale.
La tabella(3.2)mostra i protocolli supportati di Packet Tracer.

3.5 Configurazione Router-Switch

Packet Tracer fornisce una scheda *Config* che contiene opzioni GUI per le configurazioni più comuni per i router e gli switches.

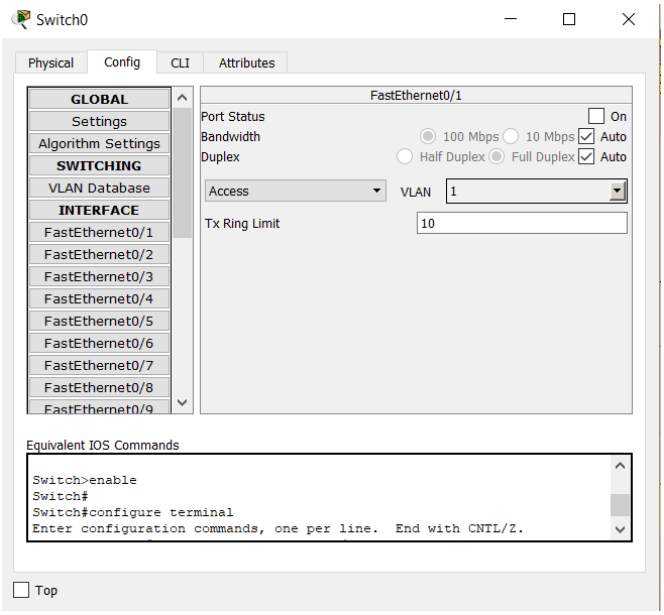


Figura 3.11: scheda config GUI

È possibile accedere all'interfaccia della riga di comando di un dispositivo in Packet Tracer in due modi: **la scheda CLI**, (il modo più semplice per accedere all'interfaccia della riga di comando di un dispositivo) e la **porta della console**, qui non c'è differenza tra ciò che è visto e controllato in questo metodo; la porta della console può essere utilizzata per rendere l'aspetto della topologia simile al mondo reale. Sebbene sia possibile accedere a un dispositivo tramite SSH o Telnet, questi sono metodi di Cisco e non sono esclusivi di Packet Tracer.

3.6 Real-time e Simulation mode

Una delle parti più interessanti di PT sono le due modalità: Realtime e Simulation, infatti una volta creata una topologia, è possibile testare la connettività tra i dispositivi utilizzando PDU semplici o complessi. La modalità di default all'avvio del software è in **Realtime**, nella quale qualunque cosa fatta avviene in tempo reale, ovvero, tutti i dispositivi risponderanno in tempo reale a tutte le richieste che si fanno, come ad esempio quando si effettua una richiesta di ping da linea di comando. Il commando ping genera un pacchetto IP con all'interno incapsulato un messaggio di tipo ICMP EchoRequest [1]. È lo strumento normalmente usato per svolgere troublshooting a livello 2 e 3 del modello OSI. .La maggior parte dei sistemi operativi invia un numero multiplo di richieste ICMP Echo Request. Il dispositivo che riceve un messaggio di Echo Request risponde al mittente con un messaggio di ICMP EchoReply. Packet Tracer consente sia

[1] L'Internet Control Message Protocol (ICMP) si occupa di trasmettere informazioni riguardanti malfunzionamenti (causati dai primi 8 byte del datagramma IP), informazioni di controllo o messaggi tra i vari componenti di una rete di calcolatori

di digitare il comando direttamente dal PC, sia di usare lo strumento Add SimplePDU. Con la CLI per verificare la connettività, bisogna aprire il prompt dei comandi ed eseguire il ping dell'indirizzo IP del dispositivo (fig.3.12). Per visualizzare i comandi

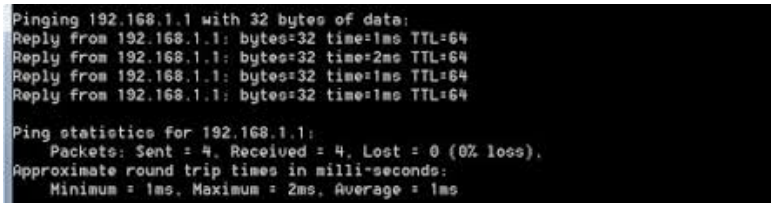


Figura 3.12: Ping Ip

del sistema operativo Cisco IOS presente sui dispositivi Cisco si può digitare help oppure il simbolo "?" per esempio con l'uso del comando arp si ha la possibilità di visualizzare i MAC address corrispondenti agli indirizzi IP pingati. Sebbene sia possibile testare la connettività eseguendo il ping dei dispositivi dall'interfaccia della riga di comando, utilizzando l'opzione PDU, è più veloce per le grandi topologie e vengono differenziate in semplici PDU e PDU complesse.
L'altra modalità, la **Simulation**, è molto utile per lo studio delle reti. Infatti grazie a questa modalità possiamo vedere nel dettaglio qual è il percorso dei pacchetti e come vengono processati in modo dettagliato. Accedendo a questa modalità, appare un nuovo riquadro, il *Simulation Panel*, dove in questo pannello si possono vedere la lista degli eventi, che si andrà a riempire ogni volta che il pacchetto si sposerà da un punto all'altro, possiamo selezionare da uno a più di 30 protocolli da visualizzare. La modalità di simulazione ha una sezione **Play Controls** che funziona in modo simile ai controlli di un lettore multimediale ed è il seguente:

- *Back*: questo pulsante sposta il processo indietro di un passo ogni volta che viene cliccato.
- *Auto Capture / Play*: premendo questo pulsante si ottiene tutto il traffico di rete (scelto sotto i filtri evento) viene continuamente catturato fino a quando lo si riprema.
- *Capture/Forward*: questo deve essere premuto ogni volta per spostare il pacchetto da un posto all'altro.

In modalità "tempo reale", l'unica indicazione del traffico è lo stato del collegamento lampeggiante in verde, invece con la modalità di simulazione, si possono vedere i pacchetti che fluiscono da un nodo all'altro e si può anche fare clic su un pacchetto per vedere informazioni dettagliate suddivise per livelli OSI. In real-time mode la rete si comporta esattamente come fanno apparati reali con risposta immediata di questi ad ogni attività o modifica apportata, in simulation mode l'utente può vedere e controllare la rete, sezionando intervalli temporali, analizzando il funzionamento interno del data transfer ed il processo di propagazione dei dati attraverso la rete. Il tutto permette un'accelerazione nella comprensione dei concetti fondamentali sottostanti il funzionamento della rete impossibile su apparati reali.

Si utilizza la scheda realtime / simulazione per passare alla modalità di simulazione. Andare sul pulsante Auto Capture / Play per iniziare l'acquisizione dei pacchetti. Se si prova una semplice PDU(cliccare sul pulsante Add Simple PDUnella sezione tool box

cioè sulla busta chiusa con il simbolo "+" sovrapposto, e poi in sequenza cliccare sul dispositivo di partenza e quello di destinazione del Ping), l'elenco degli eventi verrà popolato con tre voci, che indicano la creazione di un pacchetto ICMP, echo ICMP inviato e ICMP risposta ricevuta. La finestra Event List mostra sia dove si trova ad un dato istante il Pacchetto (colonna At Device) sia dove si trovava in un passo di simulazione precedente (colonna Last Device). Nella colonna Type è indicato il protocollo incapsulato nel frame Ethernet [16] (fig.3.13). Se si fa clic su un pacchetto,

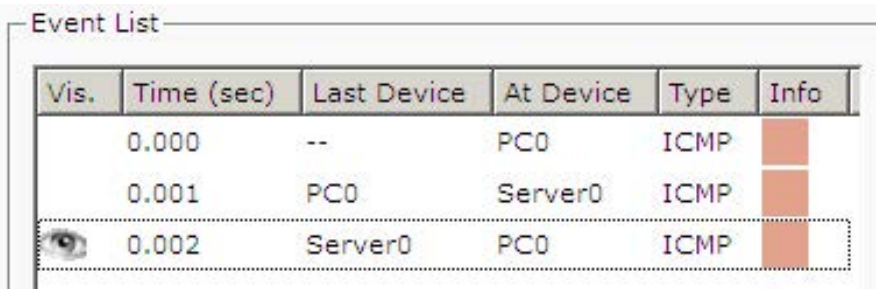


Figura 3.13: Simulation Mode

esso verrà presentato con informazioni categorizzate secondo i livelli OSI.(fig.3.14)

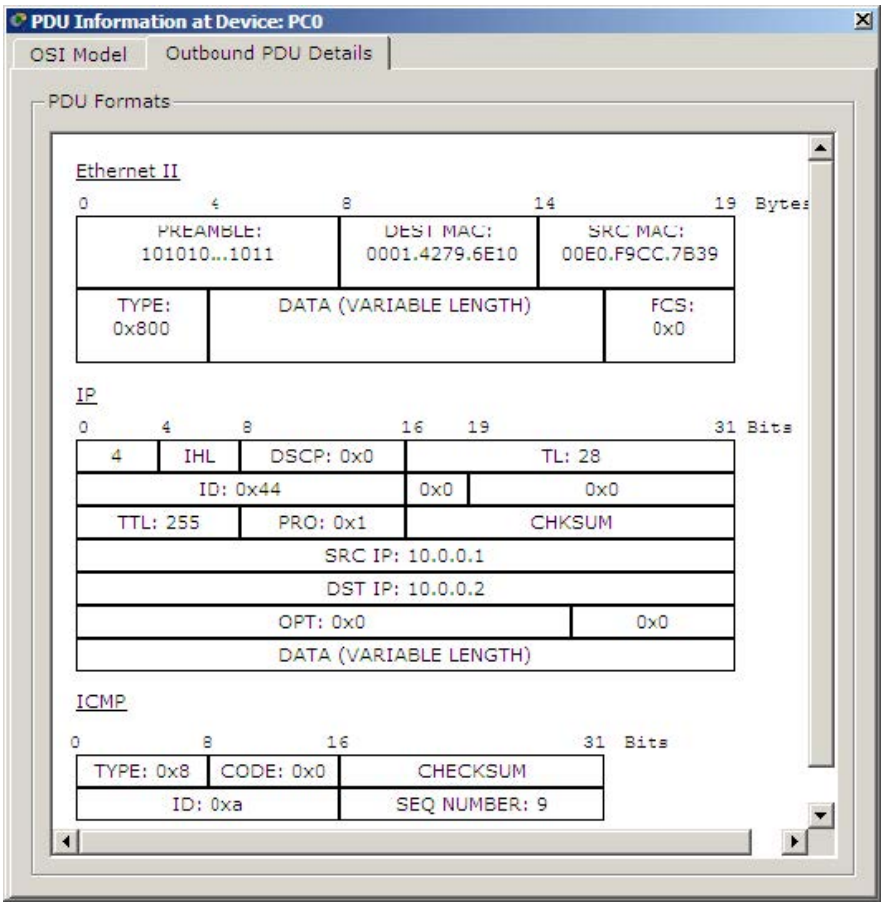


Figura 3.14: infocategorizzate

4. Packet Tracer Assessments

In questo capitolo si creeranno delle valutazioni con Packet Tracer per testare quanto hanno imparato gli utenti. Oltre ad essere un simulatore, Packet Tracer combina le funzionalità di uno strumento di valutazione con un grande potenziale. Ciò che è interessante è che ogni PT Activity può essere modificata e estesa da ciascun istruttore con unosforzo minimo e che un insieme di più PT Activity possono essere integrate a formare un caso di studiocomplesso. Tutto ciò consente agli istruttori di agire sia come produttori che come consumatori deicontenuti, creando quel meccanismo virtuoso di "user generated content" oggi molto popolare e il cuieffetto dirompente è dimostrato siti come l'enciclopedia on-line Wikipedia.

4.1 Comandi base CCNA1-CCNA2

Prima di andare a scoprire come si crea un esame CCNA verranno di seguito mostrati i comandi più utilizzati per gli esami CCNA1-CCNA2 per Packet Tracer.

Comando	Significato
enable	Ingresso modalità EXEC privileged.
configure terminal	Entrare in modalità configurazione.
hostname S1	Assegnare nome allo switch.
no ip domain-lookup	Evitare le ricerche DNS indesiderate.
banner motd # solo acceso AUTORIZADO#	Inserire messaggio del giorno di inizio sessione.
copy running-config startup-config	Salva la configurazione in esecuzione nel file home della memoria ad accesso casuale non volatile.
show running-config	Mostra configurazione attuale.
service password encryption	Crittografare le password di testo in chiaro.
traceroute "..."	Verifica percorso seguito dai pacchetti.
ping "..."	Testa connettività alle apparecchiature remote.
crypto key generate rsa modulus 1024	Creare coppia di chiavi rsa.
username admin privilege 15 secret adminpass	Creare utente con privilegi di abilitazione e protezione da password.
security passwords min-length 10	Abilita minimo 10 caratteri per tutte le password.

ip default-gateway "..."	Configurare il gateway predefinito sullo switch.
copy running-config tftp	Backup file di esecuzione su un server TFTP.
Comando	**Significato**
interface vlan 1 **ip address "..."**	Configurazione indirizzo ip per consentire la gestione degli switch remoti.
enable secret class **line con 0** **password cisco** **login** **exit**	Protezione per console.Configurazione accesso locale.
no shut **exit**	Serve per sollevare le interfacce.
line vty 0 4 **password cisco** **login** **end**	Configurazione linea terminale virtuale in modo che lo switch consenta l'accesso tramite telnet.
int g0/0 **description Connection to PC-B** **ip address 192.168.0.1 255.255.255.0** **no shut**	Configurazione IPv4,descrivere e generare interfaccia.
transport input telnet ssh **login local** **end**	Abilita ssh e l'accesso al database locale.
interface range f0/11-24 **switchport mode access** **switchport access vlan 10 end**	Configurare un intervallo di interfacce come accesso e associarle a una VLAN.
interfaces f0/1 **switchport mode trunk**	Configurare manualmente l'interfaccia come un trunk.
interfaces g0/1.1	Creazione di sottointerfacce.
encapsulation dot1q 1	Incapsulamento della sottointerfaccia,si associa alla VLAN corrispondente con il numero della VLAN.
router ospf 1 **network ".." ".." area 0**	Ingresso alla configurazione ospf.Dichiarazione delle reti con il loro jolly corrispondente
ip access-list standard BRANCH-OFFICE-POlICY **permit host".."** **permit ".." ".."**	Crea l'acl standard denominato. Consente un singolo host. Permette una rete completa.

4.2 Creazione Packet Tracer Assessments

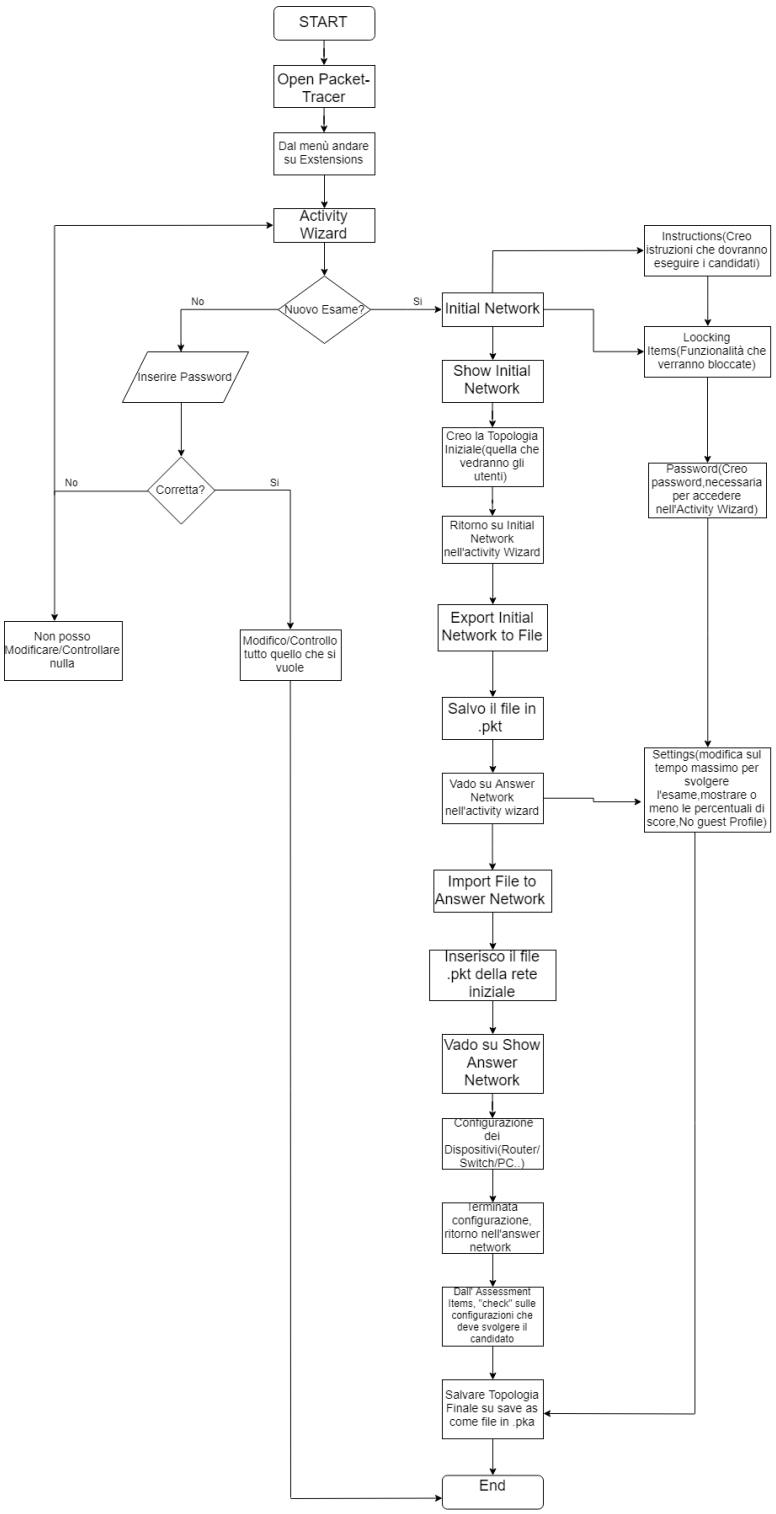


Figura 4.1: Diagramma Di Flusso

L'Activity Wizard in Packet Tracer consente all'utente di creare attività complete di istruzioni, un criterio per determinare la completezza dell'attività, e fornire un feedback all'utente dell'attività. Questo è un ottimo strumento per dare agli utenti ulteriore pratica sulla configurazione dei dispositivi e risoluzione dei problemi della progettazione della rete. È un ottimo strumento per valutare le abilità dell'utente. L'Activity Wizard è reso accessibile navigando su Extensions — Activity Wizard o premendo Alt + W.

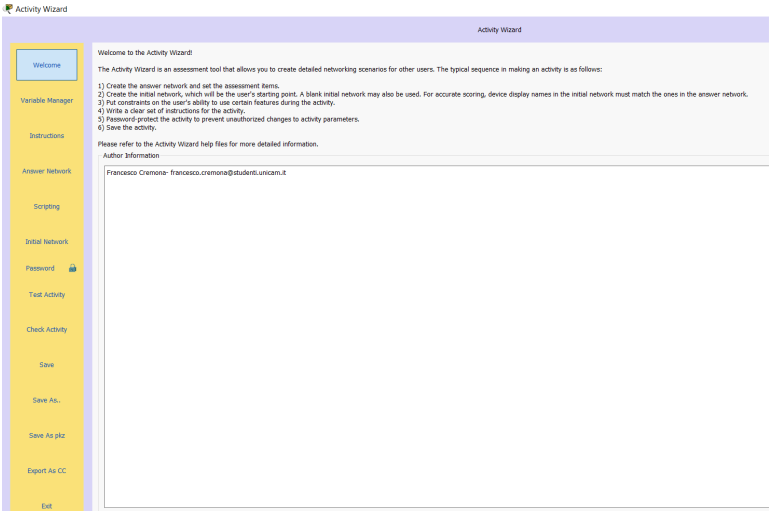


Figura 4.2: ActivityWizard

4.2.1 Welcome-Instructions

La schermata *Welcome* consente di inserire le informazioni dell'autore (nome dell'autore e Commenti).
La sezione *Instruction* (fig.4.3) è dove si inseriscono domande e obiettivi per l'utente. Questa sezione utilizza la sintassi HTML per formattare le istruzioni. Se sono fissate restrizioni rigorose per l'attività, è necessario menzionare anche i metodi previsti per raggiungere gli obiettivi in modo da non confondere gli studenti con le funzioni bloccate. Il riferimento per il supporto dei tag HTML è disponibile su `http://doc.qt.io/archives/qt-4.8/qtwebkit-guide.html`. Tuttavia, bisogna tener presente che se si decide di utilizzare i tag HTML, si deve formattare manualmente ogni aspetto del testo, comprese le interruzioni di riga e i tag di paragrafo. In alternativa, è possibile importare le istruzioni dai file * .htm utilizzando Import Page o Import All e allo stesso modo, è anche possibile esportare le istruzioni in file * .htm. Si utilizza il pulsante Preview as HTML per vedere come apparirà il testo con la formattazione HTML applicata. Inoltre, è possibile separare le istruzioni in più pagine per ridurre il disordine o per dividere i contenuti all'interno dell'attività. Nel nostro caso, si sono scritte tutte le istruzioni in word ed il file è stato salvato in "html", poi una volta aperta la pagina con il proprio browser, si è copiato il codice sorgente nella sezione Instructions dell'activity wizard.

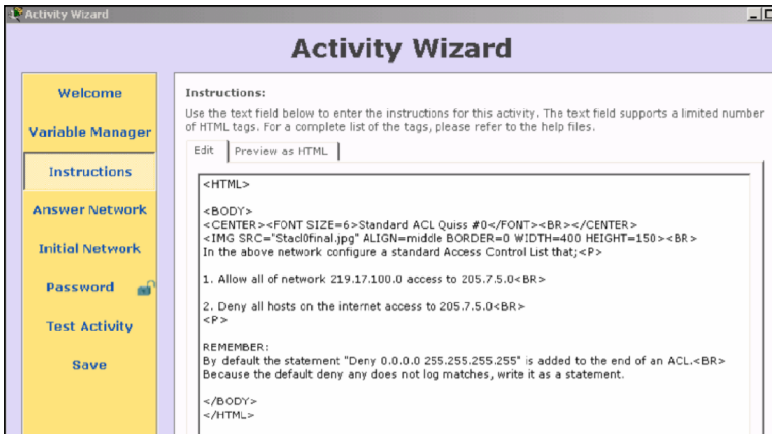


Figura 4.3: IstruzioniHTML

4.2.2 Initial Network

La (fig.4.4) è ciò che vedrà il candidato quando aprirà il file di valutazione. Facendo clic sull'opzione Mostra rete iniziale si arriva alla logica spazio di lavoro, da cui si dovranno aggiungere i dispositivi.

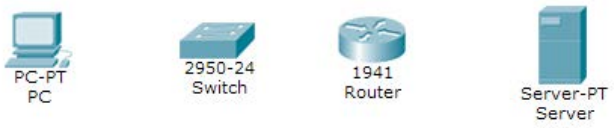


Figura 4.4: reteIniziale

Per collegare nel modo corretto i dispositivi basta seguire le regole definite nel 3° capitolo riguardo i dispositivi. Oltre la scelta del cavo è essenziale, che quando si clicca sul dispositivo di interesse, bisogna scegliere la corretta porta di connessione. Per fermare la creazione della rete iniziale, bisogna cliccare sul "cappello e sull'icona della bacchetta magica" nell'angolo in basso a sinistra per tornare alla procedura guidata. Salvare questa topologia facendo clic su Esporta rete iniziale su file. Questo file verrà usato sulla rete di risposta. Il Locking Tree è una sezione dell' Initial Network che viene

Figura 4.5: Icona Cappello

utilizzata per bloccare le funzioni alle quali non si desidera che lo studente abbia accesso. Ad esempio, è possibile impedire allo studente di passare allo spazio di lavoro fisico. Le restrizioni possono essere molto più specifiche, ad esempio impedire le modifiche al tipo di interfaccia su una porta specifica su un dispositivo specifico. Bisogna fare attenzione a quali funzioni si bloccano perché determinate restrizioni potrebbero impedire allo

studente di terminare l'attività. Per scegliere le *funzionalità* che verranno bloccate nell'interfaccia principale, in modo che gli utenti non prendano aiuto dai vari strumenti di Packet Tracer, bisogna andare su "Locking Items". La seguente schermata mostra per esempio gli *items* da verificare sotto l'opzione "Interfaccia". Se si vuole togliere la possibilità di non far rimuovere i devices ai candidati, si metterà il check su Remove Devices e via dicendo (fig.4.6). Per impostazione predefinita, un'attività utilizza i valori

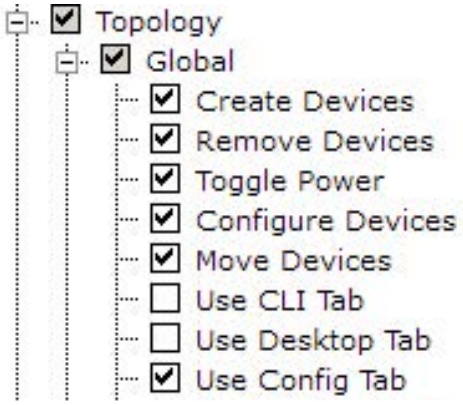


Figura 4.6: opzioneTopologia

definiti nella Rete iniziale. La struttura nella scheda Initial Network Setup consente di definire valori iniziali alternativi per alcuni Items. Ad esempio, un server può avere il gateway predefinito impostato su 192.168.1.1 nella rete iniziale ma si può modificare il valore su 192.168.4.1, e il server in seguito avrebbe il gateway predefinito impostato su 192.168.4.1 anziché 192.168.1.1.

Object Locations. È possibile creare alcuni set di posizioni per i dispositivi nella rete di risposta. A tale scopo, si possono creare una serie di posizioni degli oggetti dello spazio di lavoro logico. Quindi si fa clic su Aggiungi posizioni correnti per creare un set di località. È possibile creare più insiemi di località e aggiungerli a questo elenco. Per sovrascrivere, caricare o eliminare quel set di località, inserire un numero nel campo di testo Modifica set. Immettere un valore nel campo di testo Variabile indice per utilizzare una variabile per determinare il set di ubicazione del dispositivo da cui scegliere quando viene avviata un'attività o si riposa. Se si lascia il campo vuoto, verrà selezionato uno casuale all'avvio dell'attività (fig. 4.7).

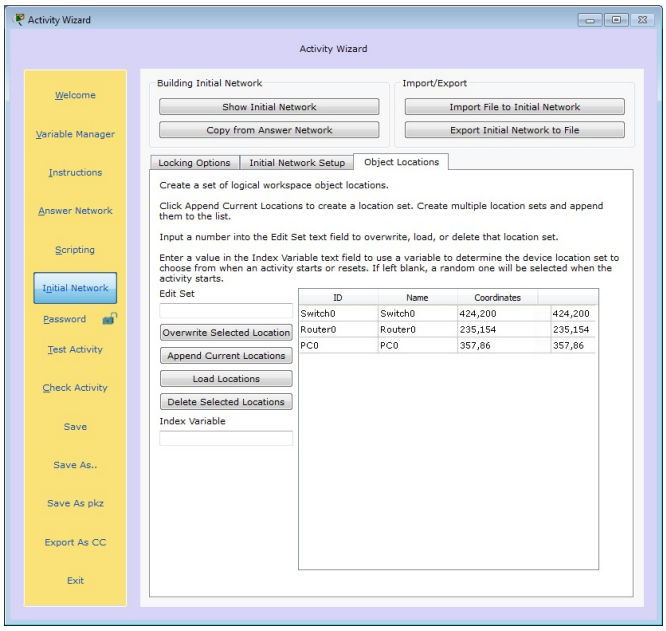


Figura 4.7: Object Locations

4.2.3 Answer Network

Si passa ora alla creazione della rete di risposta. Si apre la sezione della rete di risposta e si importa il file che precedentemente è stato salvato. Se si va su Show—Answer Network, si avrà la vista logica con gli stessi quattro dispositivi di prima. La rete finita sarà simile alla figura (4.8). Un Assessment Item è una funzionalità nella configurazione

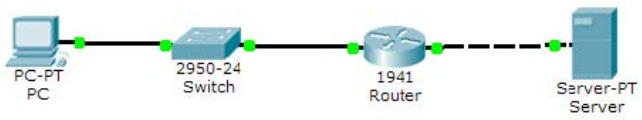


Figura 4.8: reteDiRisposta

dello studente che deve corrispondere alla configurazione di tale funzionalità nella rete di risposta. Qui si scelgono le opzioni di valutazione controllando gli elementi nell'albero espandibile. Si possono controllare caratteristiche specifiche o intere categorie. Ad esempio, è possibile controllare solo l'indirizzo IP di una porta di un determinato router o fare clic sulla categoria Porte per verificare tutte le impostazioni di tutte le porte sul router. Un controllo regolare indica una caratteristica specifica o un'intera categoria è valutata. Una casella di controllo grigia indica che vengono valutate solo alcune delle funzioni della categoria. In generale, è meglio controllare caratteristiche specifiche piuttosto che controllare intere categorie. Per praticità, è possibile mostrare solo determinati componenti nell'albero utilizzando il filtro di visualizzazione. Ad esempio, inserendo la parola chiave "Ip" si nasconderanno elementi di valutazione che non si trovano sotto il componente "Ip". Inoltre, selezionando Show Checked Only, verranno visualizzati solo gli elementi di valutazione che sono stati controllati.
Inoltre, è possibile impostare manualmente la quantità di punti che vale un particolare elemento di valutazione e classificare i componenti a cui appartiene l'elemento di valutazione. Si possono impostare feedback degli elementi per valutazione, che forniscono

suggerimenti agli studenti se il loro item valutato non è corretto. Il feedback degli elementi per valutazione viene visualizzato nella scheda Assessment Items tab nella sezione Check Results solo per elementi di valutazione errati.
Quindi dopo che si configurano i vari dispositivi, si selezionano tutti gli elementi che saranno presi in considerazione nella valutazione, si valutano gli indirizzi IP di PC, server e router, le connessioni tra tutti i dispositivi e la connettività tra PC e server.
Il test di connettività è un altro metodo di valutazione e consente di classificare l'attività in base alle funzionalità e alle prestazioni della rete anziché corrispondere ai parametri di configurazione statici. A differenza degli elementi di valutazione, che cercano la configurazione di rete dello studente e la confrontano con la configurazione della rete di risposta, i test di connettività si basano su PDU in tempo reale inviati quando l'utente fa clic su Controlla risultati. Per ciascuna PDU, è possibile impostare la condizione di test su Non testare, eseguire correttamente o Fail. Non appena clicchiamo l'icona della busta e definiamo la sorgente e la destinazione, automaticamente nell'activity wizard su Answer Network, verranno aggiunte queste connettività (fig.4.9).

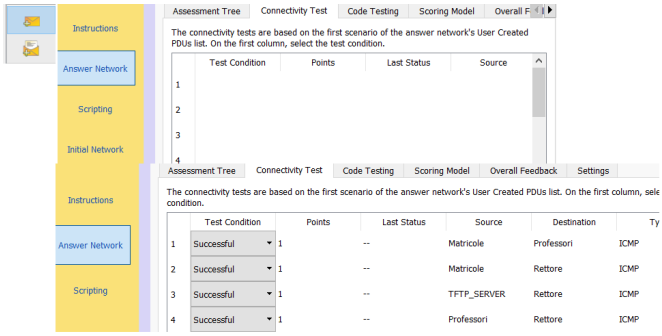


Figura 4.9: Connectivity Test

La schermata *Answer Network* consente anche di controllare gli Assessment Item, ovvero quelle istruzioni che devono eseguire i candidati e che quindi sono valutate. Ad ogni Assessment Items si può assegnare un punteggio (fig.4.10).

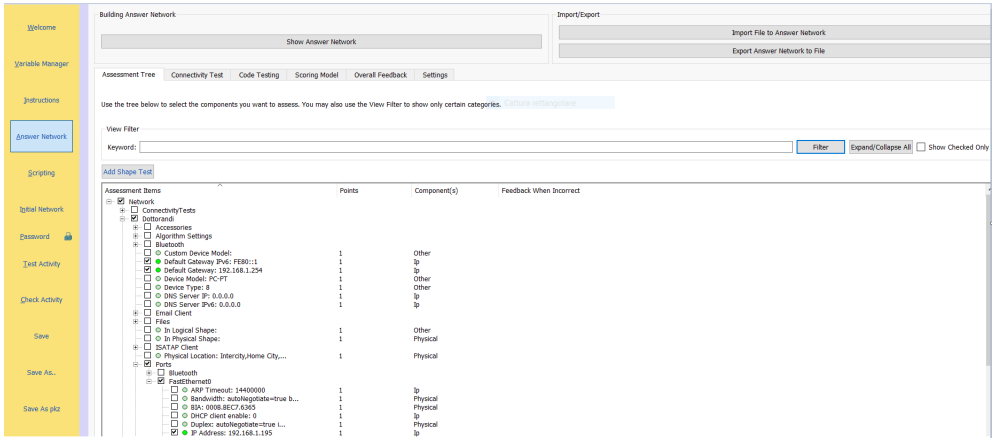


Figura 4.10: ControlloAssessmentItem

L' *Overall Feedback* consente di impostare messaggi di feedback personalizzati per attività completate e incomplete. Il messaggio Feedback completato viene visualizzato

quando l'attività è completa al 100%. In caso contrario, viene visualizzato il messaggio di Feedback incompleto. C'è anche il supporto per un sottoinsieme di tag HTML, come con le istruzioni.
Nella scheda *Settings*, è possibile cronometrare l'attività (tenere traccia del tempo trascorso mentre gli studenti lavorano sull'attività con l'opzione Tempo trascorso) o impostare un limite di tempo (con l'opzione Conto alla rovescia). È anche possibile impostare le impostazioni di feedback che valuteranno la rete dell'utente rispetto all'albero di valutazione ogni pochi secondi. Si è notato che le attività di grandi dimensioni possono ridurre le prestazioni del sistema. Si hanno queste opzioni per il feedback dinamico: No Dynamic Feedback, Show Score, Show Item Count Percentage, Show Item Count and Show Score Percentage (fig.4.11).
Per impedire agli studenti di modificare il proprio profilo utente durante un'attività, è possibile abilitare il blocco del profilo utente. Se viene effettuato un tentativo di modifica del profilo utente mentre un'attività è in esecuzione, viene visualizzata una finestra di dialogo che avverte che l'attività verrà ripristinata se le informazioni dell'utente vengono modificate. Facoltativamente, è possibile impostare la quantità di tempo (in ms) per inoltrare la rete di risposta utilizzando l'opzione Convergenza rete risposta. Un tipico caso d'uso di Answer Network Convergence si ha quando si controllano i risultati dell'attività dopo aver caricato un'attività, i risultati possono mostrare che l'attività è incompleta in quanto la rete di risposta non è convergente nel tempo. Impostando un tempo arbitrario per inoltrare la rete di risposta, questo problema verrebbe risolto.

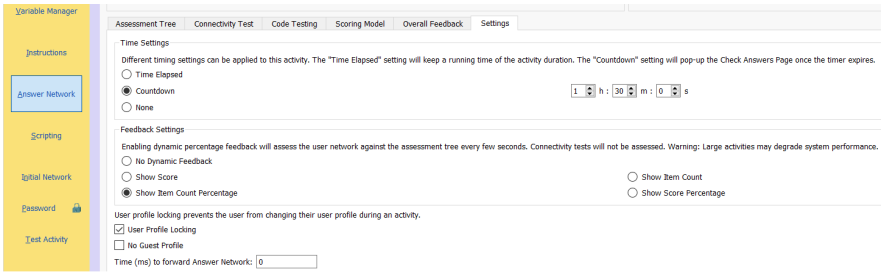


Figura 4.11: Setting

4.2.4 Password

In questa schermata si crea una password che è necessaria per entrare nell'attività guidata. Se non è impostata alcuna password, chiunque apra il file di attività può accedere all'Active Wizard e modificarne i parametri. Il sistema di password protegge l'esclusiva capacità dell'autore di modificare un'attività, la password è case sensitive.

Figura 4.12: Password

4.2.5 Test activity and save

Dopo che è stata preparata la valutazione, dovrà essere testata e vedere se funziona come dovrebbe. Fare clic sul pulsante Attività di test, completare la valutazione e vedere come aumenta la percentuale di completamento. Una volta che si è soddisfatti del risultato, bisogna tornare alla procedura guidata di attività e salvarlo. Attraverso in menu File si possono caricare due tipologie di file:

1. i file con estensione **.PKT**, contengono le informazioni relative ad una topologia di rete ed eventualmente a degli "scenari" di traffico reimpostati.

2. i file con estensione **.PKA** sono invece i file delle "Activity" : esercitazioni guidate con sistema di autovalutazione.

Il file di valutazione da solo verrà salvato con un'estensione .pka. Questo file può essere distribuito a chiunque debba prendere la valutazione. Se l'utente finale tenta di aprire la procedura dell'attività guidata, verrà visualizzata una richiesta di password (fig. 4.13). Infine si verifica che la rete di risposta è stata testata e si torna nell'Activity

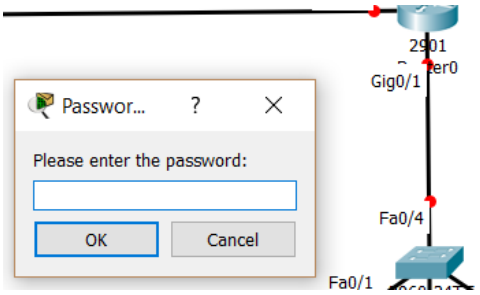


Figura 4.13: Richiesta Password

Wizard per salvare il file finito in .pka.

4.2.6 CCNA-1

Il corso CCNA – Cisco Certified Network Associate – tra i corsi Cisco sulle reti informatiche, è il primo e più diffuso percorso formativo richiesto a Network Administrators e System o Field Engineers ovvero Sistemisti di rete e Sistemisti IT.
Il corso CCNA in modalità distribuita Cisco Academy è costituito da quattro moduli – CCNA1 — CCNA2 — CCNA3 — CCNA4. Il CCNA1 (Introduction to Networks) introduce le architetture, la struttura, le funzioni, i componenti e i modelli di Internet e delle altre reti di computer. Vengono presentati anche i principi e la struttura degli indirizzi IP e i concetti fondamentali, i "media" e il funzionamento di Ethernet. I candidati alla parte pratica di Packet Tracer dovranno essere capaci di effettuare la configurazione di base dei router e degli switch, e di implementare schemi di indirizzamento IP. Gli obiettivi principale sono:

- Comprendere e descrivere gli apparati e i servizi usati per supportare le comunicazioni delle reti dati e di Internet.

- Comprendere e descrivere il ruolo dei livelli protocollari nelle reti dati.

- Comprendere e descrivere l'importanza degli schemi di indirizzamento e di denominazione degli apparati, ai vari livelli delle reti dati, in ambiente IPv4 e IPv6.

- Progettare, calcolare ed applicare gli indirizzi e le subnet mask per soddisfare certi requisiti delle reti IPv4 e IPv6.
- Costruire una semplice rete Ethernet usando router e switch. Usare i comandi CLI-Command Line Interface per configurare in modo base i router e gli switch secondo quanto previsto nel livello Cisco CCNA.
- Utilizzare le comuni "utilities" di rete per verificare il funzionamento di una rete semplice, e analizzarne il traffico, con particolare riferimento all'analisi delle rotte (traceroute esteso)

Per il CCNA-1 si è creato il nuovo esame con questa topologia:

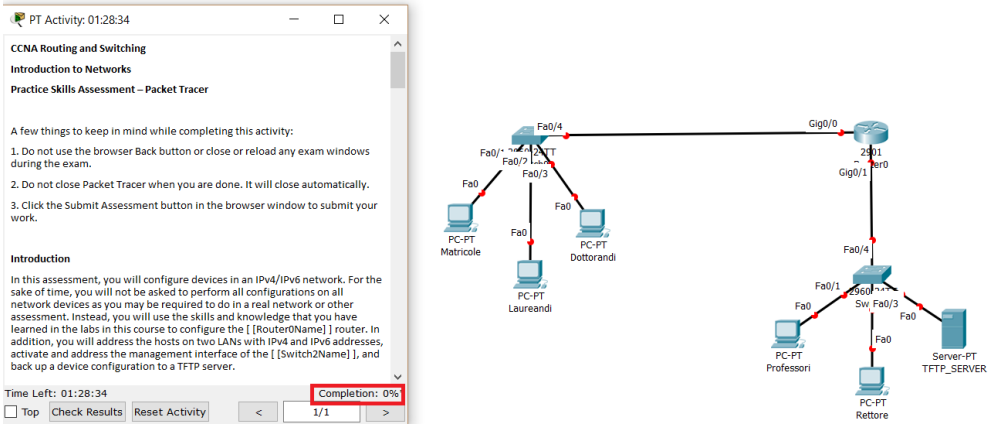


Figura 4.14: topologia Esame

Le istruzioni che i candidati devono svolgere e completare per questo esame sono:

Step 1: Determine the IP Addressing Scheme.

Subnet Number	Beginning Address	Ending Address	Mask	Assignment
1	192.168.1.0			
2				
3				
4				[[LAN1Name]] Subnet
5				
6				[[LAN2Name]] Subnet

Design an IPv4 addressing scheme and complete the Addressing Table based on the following requirements. Use the table to help you organize your work.

a. Subnet the 192.168.1.0/24 network to provide 35 host addresses per subnet while wasting the fewest addresses.

b. Assign the fourth subnet to the [[LAN1Name]].

c. Assign the last network host address (the highest) in this subnet to the G0/0 interface on [[Router0Name]].

d. Starting with the fifth subnet, subnet the network again so that the new subnets will provide 14 host addresses per subnet while wasting the fewest addresses.

e. Assign the second of these new 14-host subnets to the [[LAN2Name]].

f. Assign the last network host address (the highest) in the [[LAN2Name]] subnet to the G0/1 interface of the [[Router0Name]] router.

g. Assign the second to the last address (the second highest) in this subnet to the VLAN 1 interface of the [[Switch2Name]].

h. Configure addresses on the hosts using any of the remaining addresses in their respective subnets.

Step 2: Configure the [[Router0Name]] Router.

a. Configure the [[Router0Name]] router with all initial configurations that you have learned in the course so far:

- Configure the router hostname: **University**
- Protect device configurations from unauthorized access with the encrypted privileged exec password.
- Secure all access lines into the router using methods covered in the course and labs.
- Require newly-entered passwords must have a minimum length of 12 characters.
- Prevent all passwords from being viewed in clear text in device configuration files.
- Configure the router to only accept in-band management connections over the protocol that is more secure than Telnet, as was done in the labs. Use the value **1024** for encryption key strength.
- Configure local user authentication for in-band management connections. Create a user with the name **admin** and a secret password of **ciscocourses**. Give the user the highest administrative privileges. Your answer must match these values exactly.

b. Configure the two Gigabit Ethernet interfaces using the IPv4 addressing values you calculated and the IPv6 values provided in the addressing table.

- Reconfigure the link local addresses to the value shown in the table.
- Document the interfaces in the configuration file.

Step 3: Configure the [[Switch2Name]].

Configure [[Switch2Name]] for remote management over Telnet.

Step 4: Configure and Verify Host Addressing.

a. Use the IPv4 addressing from Step 1 and the IPv6 addressing values provided in the addressing table to configure all host PCs with the correct addressing.

b. Use the router interface link-local address as the IPv6 default gateways on the hosts.

Step 5: Backup the Configuration of the [[Router0Name]] Router to TFTP.

a. Complete the configuration of the TFTP server using the IPv4 addressing values from Step 1 and the values in the addressing table.

b. Backup the running configuration of [[Router0Name]] to the TFTP Server. Use the default file name.

Figura 4.15: Istruzioni CCNA1

Quando si inizia l'esame, il completation della schermata Istruzioni sarà al 0 % (fig. 4.14).Eseguite le prime istruzioni, si aggiorna automaticamente il completation (fig. 4.16) e l'activity results (fig. 4.17): se i comandi sono corretti, gli **Assessment Items** avranno un segno "v" di color verde, altrimenti rimarranno con il segno "x" di color rosso.

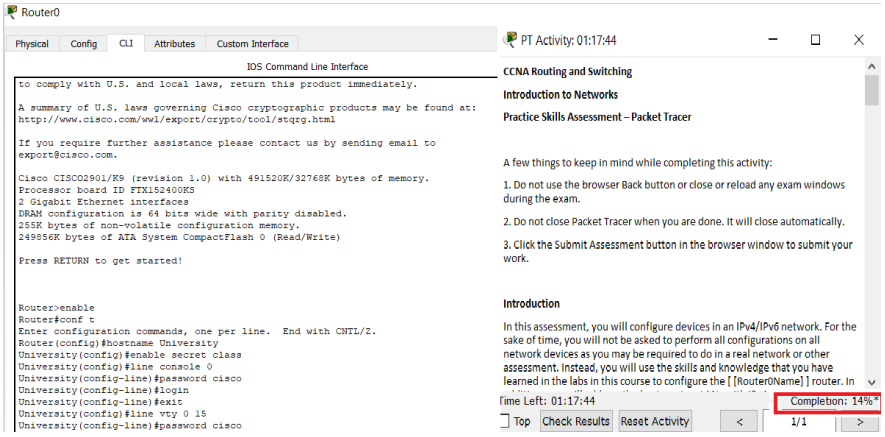


Figura 4.16: Prime Istruzioni

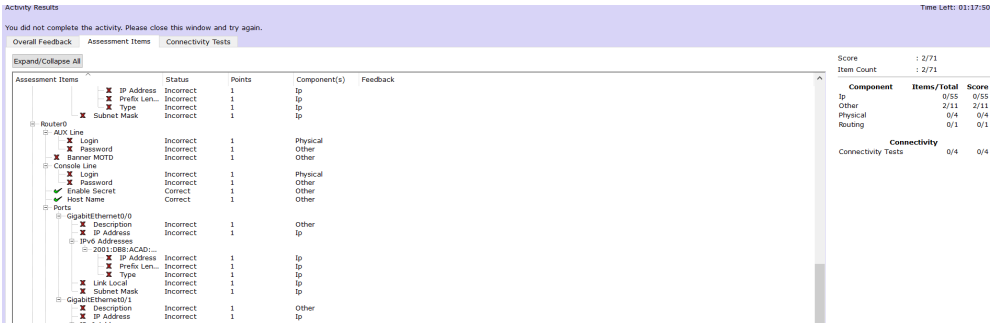


Figura 4.17: Activity Results

Di seguito verranno mostrate le soluzioni per completare l'esame. Completate tutte le

Device	Interface	IPv4 Address	Subnet Mask	IPv4 Default Gateway
		IPv6 Address/Prefix		IPv6 Default Gateway
Router0	G0/0	192.168.1.254	255.255.255.192	N/A
		2001:DB8:ACAD:A::1/64		N/A
	G0/1	192.168.2.30	255.255.255.240	N/A
		2001:DB8:ACAD:B::1/64		N/A
	Link Local	FE80::1		N/A
LAN 2 Switch	Vlan 1	192.168.2.29	255.255.255.240	
		N/A		N/A
Matricole	NIC	192.168.1.193	255.255.255.192	192.168.1.254
		2001:DB8:ACAD:A::FF		FE80::1
Laureandi	NIC	192.168.1.194	255.255.255.192	192.168.1.254
		2001:DB8:ACAD:A::15		FE80::1
Dottorandi	NIC	192.168.1.195	255.255.255.192	192.168.1.254
		2001:DB8:ACAD:B::CC		FE80::1
Professori	NIC	192.168.2.17	255.255.255.240	192.168.2.30
		2001:DB8:ACAD:B::FF		FE80::1
Rettore	NIC	192.168.2.18	255.255.255.240	192.168.2.30
		2001:DB8:ACAD:B::15		FE80::1
TFTP Server	NIC	192.168.2.19	255.255.255.240	192.168.2.30
		2001:DB8:ACAD:B::CC		FE80::1

Router

→ enable →conf t→,hostname University→enable secret class→ line console 0→password cisco→login→exit→line vty 0 15→password cisco-→login→exit→security passwords min-length 12→service password-encryption→ip domain-name cisco.com→crypto key generate rsa…→1024-->line vty 0 15→transport input all→transport input ssh→login local→exit-→username admin privilege 15 secret ciscocourses→int g0/0→description LAN 1→ip address 192.168.1.254 255.255.255.192→ipv6 address 2001:DB8:ACAD:A::1/64-->ipv6 address fe80::1 link-local→no shutdown→ int g0/1→description LAN 2→ip address 192.168.2.30 255.255.255.240→ipv6 address 2001:DB8:ACAD:B::1/64-->ipv6 address fe80::1 link-local→no shutdown

Switch

enable→conf t→int vlan1→ip address 192.168.2.29 255.255.255.240→no shutdown-→exit→ip default-gateway 192.168.2.30→line vty 0 15→password cisco→login

Matricole terminal cisco--- cisco(pass) enable→ class(pass)—>copy running-config tftp→ ip 192.168.2.19→enter

Infine verifico i vari ping

Figura 4.18: SoluzioniCCNA1

istruzioni il completation dovrà essere al 100 % e gli Assessment Item tutti completati.

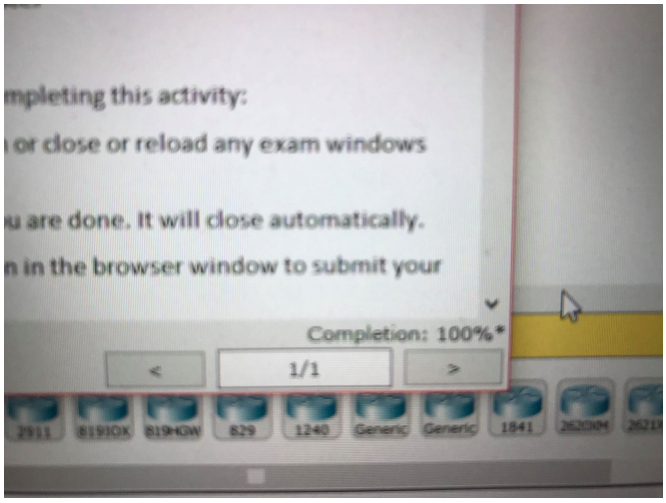


Figura 4.19: Completetion

Una volta completato l'esame, cliccando su *Submit Assessment*, si otterrà il punteggio ottenuto come nella seguente figura:

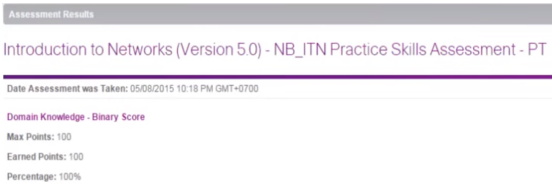


Figura 4.20: Assessment Results

4.2.7 CCNA-2

Il CCNA2(Routing and Switching Essentials) descrive le architetture, i componenti e il funzionamento dei router e degli switch in una piccola rete. Qui si apprenderanno come configurare un router e uno switch per il suo funzionamento di base. Alla fine del presente modulo Cisco CCNA 2, i candidati saranno capaci di configurare e correggere il funzionamento di router e switch, e di risolvere i problemi comuni relativi a RIP, RIPng, OSFP single-area, VLAN-Virtual LAN e instradamento tra le VLAN, sia in reti IPv4, sia in reti IPv6. Gli obiettivi principale sono:

- Comprendere e descrivere i concetti di base dello switching, e il funzionamento degli switch Cisco
- Comprendere e descrivere lo scopo, la natura e il funzionamento di un router, le tabelle di routing, e il processo di ricerca di una rotta (route lookup)
- Comprendere e descrivere come le VLAN creano reti logicamente separate tra loro, e come avviene l'instradamento tra esse
- Comprendere e descrivere i protocolli per il routing dinamico, i protocolli di routing "distance vector" e quelli "link state"
- Configurare e correggere il funzionamento del routing statico e della rotta di default (RIP e RIPng)
- Comprendere, configurare e correggere il funzionamento delle ACL-Access Control List in reti IPv4 e IPv6
- Comprendere, configurare e correggere il funzionamento del DHCP-Dynamic Host Configuration Protocol in reti IPv4 e IPv6

Per il CCNA-2 invece, si è creato l'esame con la seguente topologia:

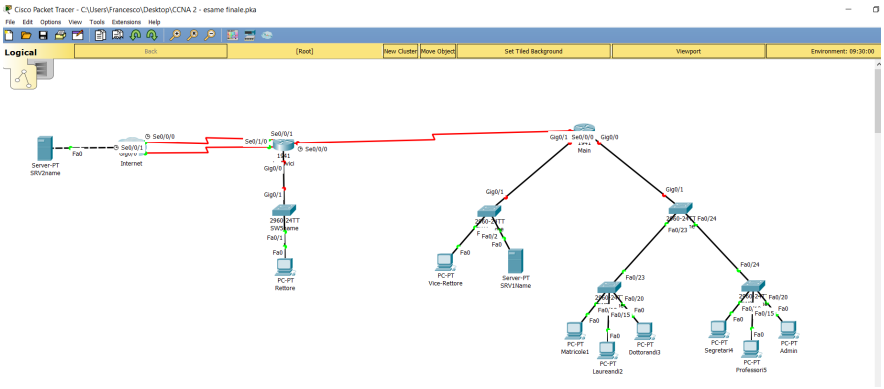


Figura 4.21: CCNA-2

Le istruzioni per questo esame sono:

Instructions

Step 1: Determine Addressing

Determine the IP addresses that you will use for the required interfaces on the three switch SVIs, and the eight LAN hosts. Use the information in the Addressing Table.

- Select the switch SVI addresses.
- The interfaces on the **[[Main]]** router that are used to route the VLANs should be addressed with the last usable IP address in the subnet.
- Assign valid host addresses to the LAN hosts according to the Addressing Table and VLAN assignment.

Step2: Basic Device Configuration

Complete a basic device configuration on the **[[Main]]** router. Perform the following tasks:

a. Disable DNS lookup.
b. Configure the device with the name shown in the addressing table.
c. Configure password encryption.
d. Assign the encrypted type of privileged EXEC password.
e. Configure a MOTD banner to warn users that unauthorized access is prohibited.
f. Configure the console line so that router status messages will not interrupt command line input.
g. Configure the console to require a password for access.
h. Configure the VTY ports to only accept connections over SSH. Use the following values:

Domain Name: **cisco.com**
Local Username: **admin**
User Password: **class**
Modulus: **1024**
Version: **2**

The values for your SSH configuration must match these values exactly in order for you to receive credit for your configuration.

Step 3: Interface Addressing [[R1name]]

Activate and configure the **G0/1** and **S0/0/0** interfaces of the **[[R1name]]** router with the IP addresses given in the Addressing Table. The G0/0 interface will be configured later in the assessment. **Configure descriptions for these interfaces**.

Step 4: VLANs and Trunking

Configure the **[[SW1name]]**, **[[SW2name]]**, and **[[SW3name]]** switches with VLANs and trunking according to the values in the VLAN table.

a. Add the VLANs to the switches.
b. Name the VLANs exactly as shown in the VLAN table.
c. Configure the links between the [[SW1name]], [[SW2name]], and [[SW3name]] switches as trunks. Configure the link between [[SW1name]] and [[R1name]] as a trunk. All trunking interfaces should be statically configured as trunks.
d. Assign the appropriate ports to the VLANs.

Step 5: Routing Between VLANs

Configure routing between VLANs on the **[[R1name]]** router. Use the information in the addressing and VLAN tables.

Figura 4.22: Istruzioni per CCNA2

Step 6: Access Control List Configuration

Configure a named standard ACL that meets the following requirements:

a. The list should be named **INT-WEB**. The name must match this value exactly in order for you to receive credit for your work.
b. Prevent any host with an address on the **VLAN20** subnetwork from accessing the **VLAN10** subnetwork.
c. All other hosts should be permitted
d. The list should have two statements. One statement for each requirement in steps 5b and 5c.

Step 7: Switch Virtual Interface (SVI) Configuration

Configure the switch virtual management interfaces on **[[SW1name]]**, **[[SW2name]]**, and **[[SW3name]]**. Use the information in the addressing and VLAN tables for your configuration. All switches should be reachable from hosts on other networks for the purpose of this assessment.

Step 8: Switch Port Security Configuration

Improve network security by configuring the **[[SW2name]]** switch with the following. You are only required to configure these settings on this one switch for this assessment.

a. Disable ALL unused switch ports.
b. Activate port security on all ports that have hosts connected.
c. Allow only a maximum of two MAC addresses to access the active switch ports.
d. Configure the switch ports to automatically learn the two allowed MAC addresses and record the addresses in the running configuration.
e. Configure the switch ports so that, if the maximum number of addresses for each port is exceeded, packets with unknown source addresses are dropped until a sufficient number of secure MAC addresses are removed.

Step 9: Dynamic Routing

Configure RIPv2 routing on **[[Main]]** and **[[Lodovici]]**.

a. Configure RIPv2 on [[Main]] and [[Lodovici]] so that all networks are reachable.
b. Configure all LAN physical interfaces so that RIP updates are not sent out to the LANs.
c. Be sure to use the version of RIP that supports classless routing.
d. Prevent RIP from automatically summarizing networks.
e. Configure RIP to automatically send the default route that is already configured on **[[Main]]** to **[[Lodovici]]**.

Step 10: Configure Network Monitoring

Configure NTP and Syslog server logging on **[[Main]]**.

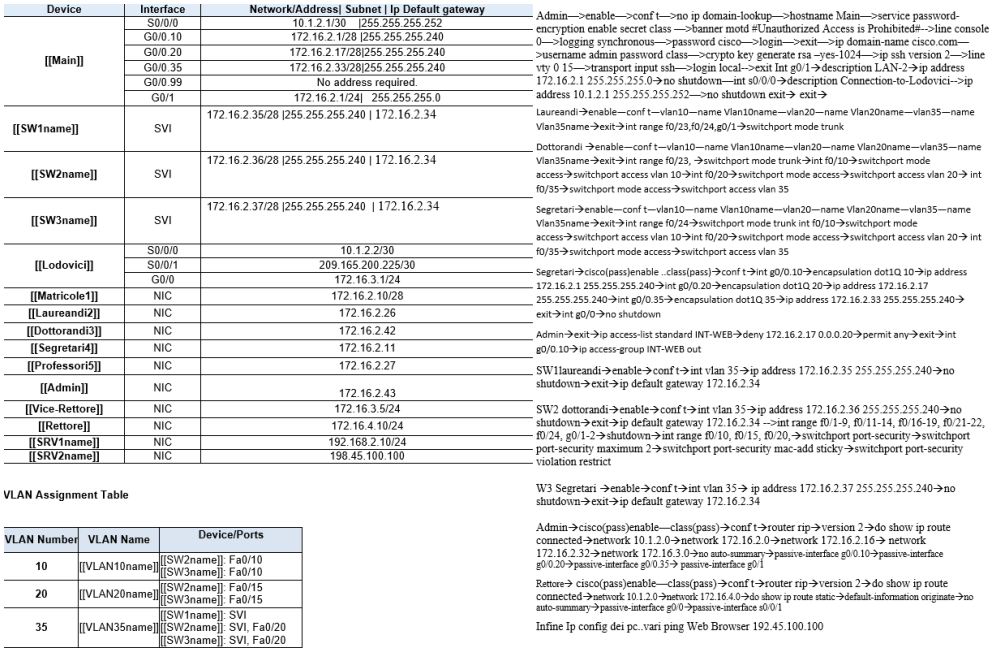
a. Activate the logging and debug timestamp services.
b. Configure **[[Main]]** as an NTP client. The NTP server is **[[SRV1name]]** with the address of **172.16.3.5**.
c. Configure Syslog to send **debug level** messages to the **[[SRV1name]]** logging server.

Step 11: Configure Host Addressing

Address the hosts that are connected to **[[SW2name]]** so that they have connectivity to the IP address of the **[[SRV2name]]** server on the Internet. Use the information provided in the Addressing Table

Figura 4.23: Istruzioni per CCNA2

Di seguito verranno mostrate le soluzioni per questo esame.



Device	Interface	Network/Address| Subnet | Ip Default gateway
[[Main]]	S0/0/0	10.1.2.1/30 |255.255.255.252
	G0/0.10	172.16.2.1/28 |255.255.255.240
	G0/0.20	172.16.2.17/28|255.255.255.240
	G0/0.35	172.16.2.33/28|255.255.255.240
	G0/0.99	No address required.
	G0/1	172.16.2.1/24| 255.255.255.0
[[SW1name]]	SVI	172.16.2.35/28 |255.255.255.240 | 172.16.2.34
[[SW2name]]	SVI	172.16.2.36/28 |255.255.255.240 | 172.16.2.34
[[SW3name]]	SVI	172.16.2.37/28 |255.255.255.240 | 172.16.2.34
[[Lodovici]]	S0/0/0	10.1.2.2/30
	S0/0/1	209.165.200.225/30
	G0/0	172.16.3.1/24
[[Matricole1]]	NIC	172.16.2.10/28
[[Laureandi2]]	NIC	172.16.2.26
[[Dottorandi3]]	NIC	172.16.2.42
[[Segretari4]]	NIC	172.16.2.11
[[Professori5]]	NIC	172.16.2.27
[[Admin]]	NIC	172.16.2.43
[[Vice-Rettore]]	NIC	172.16.3.5/24
[[Rettore]]	NIC	172.16.4.10/24
[[SRV1name]]	NIC	192.168.2.10/24
[[SRV2name]]	NIC	198.45.100.100

VLAN Assignment Table

VLAN Number	VLAN Name	Device/Ports
10	[[VLAN10name]]	[[SW2name]]: Fa0/10 [[SW3name]]: Fa0/10
20	[[VLAN20name]]	[[SW2name]]: Fa0/15 [[SW3name]]: Fa0/15
35	[[VLAN35name]]	[[SW1name]]: SVI [[SW2name]]: SVI, Fa0/20 [[SW3name]]: SVI, Fa0/20

Admin—>enable—>conf t—>no ip domain-lookup—>hostname Main—>service password-encryption enable secret class —>banner motd #Unauthorized Access is Prohibited#-->line console 0—>logging synchronous—>password cisco—>login—>exit—>ip domain-name cisco.com—>username admin password class—>crypto key generate rsa –yes-1024—>ip ssh version 2—>line vty 0 15—>transport input ssh—>login local-->exit Int g0/1→description LAN-2→ip address 172.16.2.1 255.255.255.0→no shutdown—int s0/0/0→description Connection-to-Lodovici-->ip address 10.1.2.1 255.255.255.252—>no shutdown exit→ exit→

Laureandi→enable—conf t—vlan10—name Vlan10name—vlan20—name Vlan20name—vlan35—name Vlan35name→exit→int range f0/23,f0/24,g0/1→switchport mode trunk

Dottorandi →enable—conf t—vlan10—name Vlan10name—vlan20—name Vlan20name—vlan35—name Vlan35name→exit→int range f0/23, →switchport mode trunk→int f0/10→switchport mode access→switchport access vlan 10→int f0/20→switchport mode access→switchport access vlan 20→ int f0/35→switchport mode access→switchport access vlan 35

Segretari→enable—conf t—vlan10—name Vlan10name—vlan20—name Vlan20name—vlan35—name Vlan35name→exit→int range f0/24→switchport mode trunk int f0/10→switchport mode access→switchport access vlan 10→int f0/20→switchport mode access→switchport access vlan 20→ int f0/35→switchport mode access→switchport access vlan 35

Segretari→cisco(pass)enable ..class(pass)→conf t→int g0/0.10→encapsulation dot1Q 10→ip address 172.16.2.1 255.255.255.240→int g0/0.20→encapsulation dot1Q 20→ip address 172.16.2.17 255.255.255.240→int g0/0.35→encapsulation dot1Q 35→ip address 172.16.2.33 255.255.255.240→ exit→int g0/0→no shutdown

Admin→exit→ip access-list standard INT-WEB→deny 172.16.2.17 0.0.0.20→permit any→exit→int g0/0.10→ip access-group INT-WEB out

SW1laureandi→enable→conf t→int vlan 35→ip address 172.16.2.35 255.255.255.240→no shutdown→exit→ip default gateway 172.16.2.34

SW2 dottorandi→enable→conf t→int vlan 35→ip address 172.16.2.36 255.255.255.240→no shutdown→exit→ip default gateway 172.16.2.34 -->int range f0/1-9, f0/11-14, f0/16-19, f0/21-22, f0/24, g0/1-2→shutdown→int range f0/10, f0/15, f0/20,→switchport port-security→switchport port-security maximum 2→switchport port-security mac-add sticky→switchport port-security violation restrict

W3 Segretari →enable→conf t→int vlan 35→ ip address 172.16.2.37 255.255.255.240→no shutdown→exit→ip default gateway 172.16.2.34

Admin→cisco(pass)enable—class(pass)→conf t→router rip→version 2→do show ip route connected→network 10.1.2.0→network 172.16.2.0→network 172.16.2.16→ network 172.16.2.32→network 172.16.3.0→no auto-summary→passive-interface g0/0.10→passive-interface g0/0.20→passive-interface g0/0.35→ passive-interface g0/1

Rettore→ cisco(pass)enable—class(pass)→conf t→router rip→version 2→do show ip route connected→network 10.1.2.0→network 172.16.4.0→do show ip route static→default-information originate→no auto-summary→passive-interface g0/0→passive-interface s0/0/1

Infine Ip config dei pc..vari ping Web Browser 192.45.100.100

Figura 4.24: SoluzioniCCNA2

4.3 Variable Manager

Alcune sezione dell'activity wizard vengono usate in contesti più complessi. Variable Manager consente agli autori di aggiungere dinamismo alle attività. Queste funzionalità consentono all'autore di creare attività che cambiano ogni volta che vengono caricate o ripristinate. Questa funzionalità è abilitata creando pool di valori e quindi creando variabili che utilizzano i valori del pool per abilitare le funzionalità dinamiche. Le variabili consentono di modificare molti aspetti di un'attività, inclusi, ma non limitati, i nomi dei dispositivi, l'indirizzamento IP, le istruzioni di instradamento, i record DHCP e DNS. Esistono quattro tipi di variabili che possono essere creati nel Variable Manager e sono: *Seed, Numero, Stringhe e Indirizzi IP*. Ad eccezione di Seeds, le variabili vengono create utilizzando una combinazione di un pool di risorse e una variabile associata. Ogni scheda di tipo ha una posizione per inserire sia il pool che le informazioni variabili. La scheda seed, grazie alla semplicità del tipo combina entrambe le parti in un'unica operazione. Numeri, stringhe e indirizzi IP possono essere assegnati a una variabile generata una volta o in modo casuale ogni volta che lo studente esegue un'attività. Ciò consente allo studente di acquisire più pratica con un'attività che varia nelle sue caratteristiche superficiali, ma è strutturalmente uguale. In seguito si convertirà un'attività di traceroute semplice e statica in una dinamica che avrà istruzioni diverse e risponderà ogni volta alle configurazioni di rete. Facendo clic sulla casella di controllo, una tabella delle variabili verrà mostrata durante l'Activity Wizard (fig.4.25). I nomi delle variabili possono sempre essere digitati manualmente. La tabella semplifica l'inserimento di questi in istruzioni(fig.4.25) o nell'Albero di valutazione.

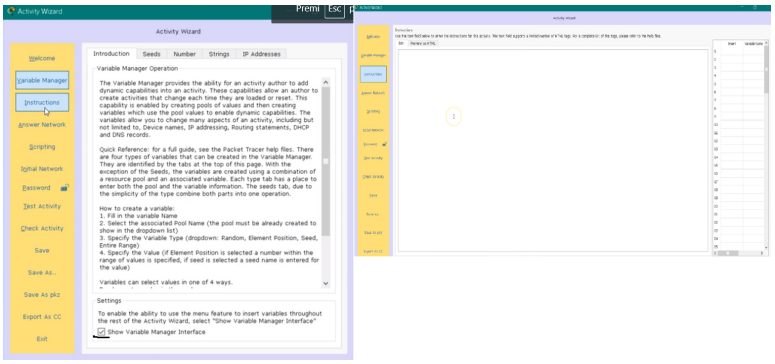


Figura 4.25: Variable Manager

Creating Pools. Un pool è un intervallo o un insieme di valori da cui può trarre una variabile. Vi sono pool di: numeri, di indirizzi IP e di stringhe. Per tutte le attività abilitate alle variabili, si inizia definendo i pool. I pool di numeri vengono creati immettendo il minimo e massimo numero per il pool. L'intervallo del pool include i valori finali. Per aggiungere un pool di stringhe, si inizia dando un nome al pool, è buona pratica assegnare nomi plurali. Per i pool di stringhe, ciascuna stringa nel pool è separata da un punto e virgola. Gli intervalli di pool Ip sono definiti dall'indirizzo di rete, dalla Mask e dai primi e ultimi indirizzi IP. Per iniziare, bisogna inserire il nome di un pool, un indirizzo di rete e una subnet mask, questo identifica l'intera rete utilizzata (fig.4.26).

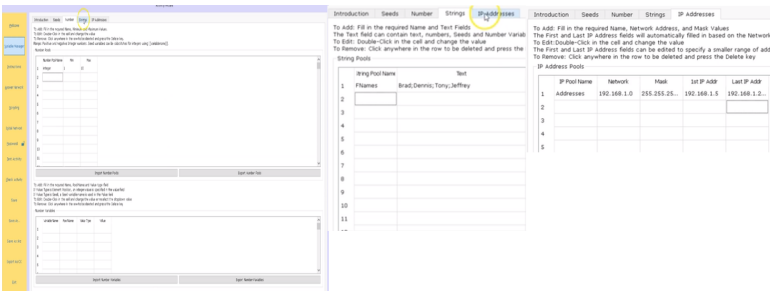


Figura 4.26: CreatePools

Creating Variables. È possibile impostare le variabili per selezionare i valori in uno dei 4 modi. Dal menu a discesa se si seleziona Random, il valore verrà selezionato in modo casuale da qualsiasi valore nel pool. Selezionando Element Position, il valore sarà un numero intero che seleziona ogni volta la stessa posizione dal pool. Seed fa riferimento a una posizione definita da una variabile Seed nella scheda Seed. Questo è un metodo che consente di utilizzare la stessa posizione in più selezioni di variabili. L'intero intervallo è una variabile utilizzata nella rete di risposta dell'Attività guidata per accettare qualsiasi input corretto purché sia contenuto nel pool associato. La sequenza tipica per la creazione di una variabile è:

1. Compilare la variabile Nome.

2. Selezionare il nome del pool associato (il pool deve essere già creato per essere visualizzato nell'elenco a discesa).

3. Specificare il tipo di variabile (menu a discesa: casuale, posizione dell'elemento, seme, intero intervallo).

4. Specificare il valore (se si seleziona Element Position viene specificato un numero compreso nell'intervallo di valori, se si seleziona seed, viene immesso un nome seed per il valore), random è l'impostazione predefinita.

The entire range selection assegna l'intera gamma del pool alla variabile.
Random selection disegna un singolo valore dal pool, una volta estratto quel valore non verrà più disegnato. Sostituendo la posizione dell'elemento con un numero si disegna un valore statico basato sull'indice di posizione dell'elemento dal pool. È possibile assegnare più variabili a un singolo pool. I valori numerici consentono di aggiungere numeri dinamici in uno scenario PT. Questi sono spesso usati come gli spettacoli grafici, creando una serie di numeri che possono essere concatenati e usati come indirizzi IP. (fig.4.27).
I seed sono un tipo speciale di variabile, possono essere creati in un unico passaggio anziché in due. Per utilizzare un valore di seed, fare riferimento al nome seed. I valori dei seed dovrebbero essere considerati come valori di indice per la selezione di altre variabili di dati, mentre non è necessario. Bisogna assicurarsi che l'intervallo del pool sia maggiore o uguale all'intervallo di valori dei seed. L'intervallo di seed valido va da 0 a 2.147.483.647. Un seed dovrebbe essere un valore positivo, anche se i valori negativi sono legali, altrimenti utilizzarli come indici in altri pool variabili e le variabili possono causare risultati imprevedibili. Vengono creati come un pool di numeri, specificare il nome di seed, i valori minimo e massimo. La colonna del valore di test consente l'annullamento della funzione variabile a scopo di test. Per vedere eventuali limitazioni usando i seed, bisogna assicurarsi di leggere le istruzioni sulla pagina Seed (fig.4.28).
I pool di stringhe possono essere utilizzati per creare nomi diversi per i dispositivi nell'attività Packet Tracer, o ancora come Seeds e Numbers ovunque sia possibile utilizzare una variabile. Le variabili di testo possono anche essere utilizzate nell'area delle istruzioni per modificare il testo dello scenario. Poiché Packet Tracer inizialmente converte tutte le stringhe, le stringhe di testo possono essere utilizzate anche per indirizzi IP come gli spettacoli del pool di ottetti IP.
I pool di indirizzi IP consentono schemi di indirizzamento dinamici in Packet Tracer, ma consentono anche configurazioni dinamiche nella rete iniziale, compresi i record DNS e DHCP. Consentono inoltre più risposte corrette, ad esempio negli schemi di indirizzamento

Using Variables In The Instructions. Con le variabili già definite e l'interfaccia di Gestione variabili attivata, l'aggiunta di variabili alle istruzioni è semplice. Invece di dire "Bill" nelle istruzioni, è possibile sostituirlo con la variabile "Fnam1" per estrarre casualmente un nome dal pool Fnames ogni volta che l'attività viene reimpostata. Lo stesso vale per il valore dell'età e l'indirizzo IP. Per inserire la variabile, fare clic sulla freccia sulla prima colonna accanto a "Fnam1". Si noti che la sintassi per le variabili è il nome della variabile racchiuso tra parentesi quadre. In seguito si completa aggiungendo variabili al resto delle istruzioni. Per visualizzare l'anteprima delle istruzioni visualizzate, si fa clic sul pulsante Attività di test, ogni volta che si preme reset, si noterà che cambiano le variabili. Un'impostazione importante da notare è l'interfaccia Show Variable Manager nella parte inferiore dello schermo. Selezionando questa casella di controllo è possibile impostare o assegnare variabili nel testo Istruzioni, Elementi di valutazione e Item iniziali. È possibile aggiungere tutte le variabili create facendo clic

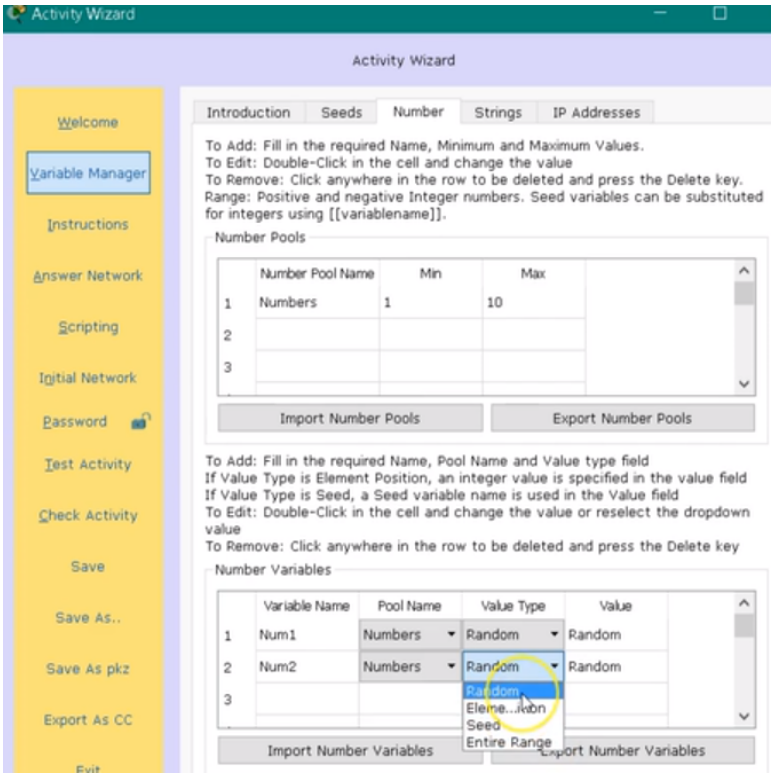


Figura 4.27: Creating Variables

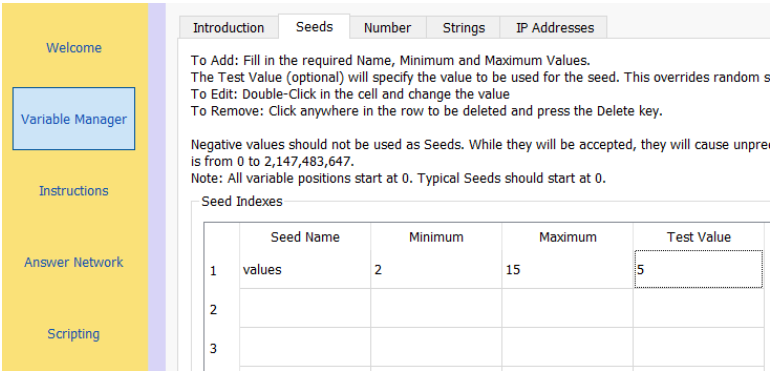


Figura 4.28: Seeds

sulla freccia accanto al nome della variabile. Nel pannello Istruzioni, posizionare il cursore nel punto in cui si desidera posizionare la variabile, quindi fare clic sul pulsante Inserisci nell'interfaccia di Gestione variabili (fig.4.30). Nelle voci di valutazione e nelle voci iniziali, solo le voci contrassegnate da un punto verde possono essere assegnate a una variabile. Per rimuovere un'assegnazione della variabile, selezionare la variabile appropriata e premere Elimina sulla tastiera.

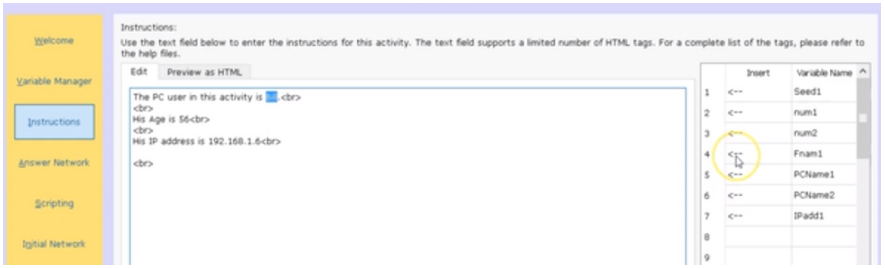


Figura 4.29: Variable Instructions

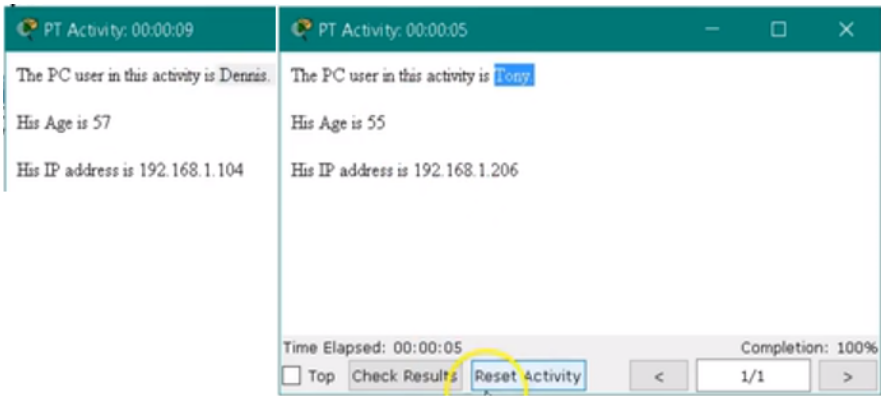


Figura 4.30: Variable Instructions

Using Variables In Network Topology. Le variabili possono anche essere applicate ai nomi di visualizzazione del dispositivo. Tuttavia, è necessario prestare attenzione durante l'assegnazione di variabili ai nomi di visualizzazione del dispositivo poiché il nome visualizzato della periferica risultante nella rete di risposta deve corrispondere al nome visualizzato nella rete dell'utente. Per cambiare il nome visualizzato in una variabile, digitare il nome della variabile tra parentesi quadre. Per il PC di origine utilizzare PCName1. Per il PC di destinazione, utilizzare PCName2. Per assicurarsi che le variabili siano le stesse per le reti Initial e answer, vai alla rete iniziale e fai clic su Copia. Per vedere il risultato usa il pulsante dell'attività di test. Fai clic su Ripristina attività per vedere cambiare i nomi. Il cambiamento dei nomi dei dispositivi nello spazio di lavoro si rifletterà anche nell'albero di valutazione.

Esempi:

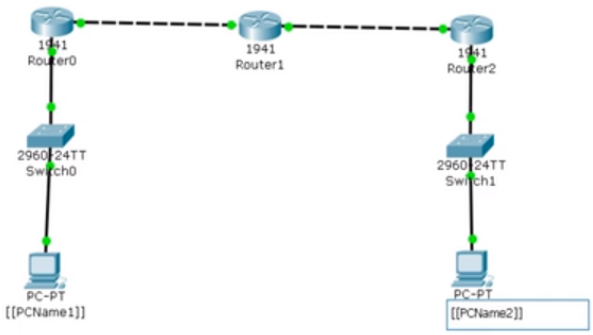


Figura 4.31: Variable Instructions

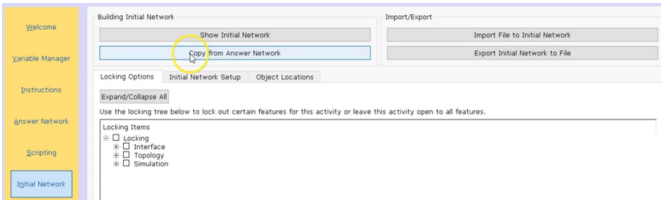


Figura 4.32: Variable Network

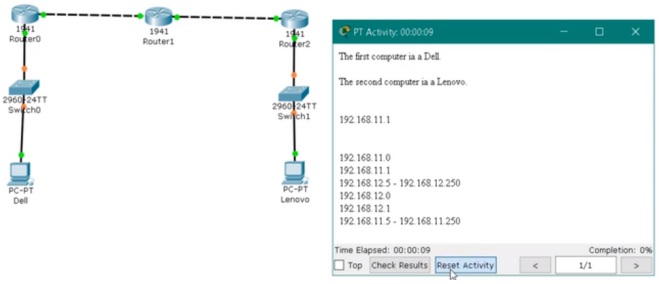


Figura 4.33: Variable Instructions

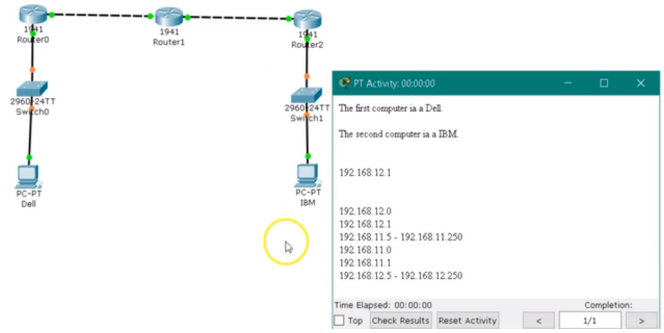


Figura 4.34: Variable Instructions

4.4 Scoring Model/Scripting e Activity Sequencer

Sezioni che potranno essere fonte di approfondimento in futuro sono: lo *Scoring Model/Scripting e l'Activity Sequencer*. *The Scoring Model(modello di punteggio)* è un processo di "Evidence Centered Design" con il quale valutare i prodotti di lavoro attraverso l'applicazione di regole di punteggio e feedback testuali. Il modello di punteggio viene utilizzato per creare regole complesse per la valutazione delle attività. Quando si utilizza il nuovo modello di calcolo del punteggio, è possibile visualizzare un feedback personalizzato per ogni prodotto di lavoro nell'albero di valutazione (feedback sia positivo che negativo) nonché un feedback complessivo e parziale. Non è nemmeno necessario collegare il testo di feedback a un prodotto di lavoro se lo scopo è quello di fornire un semplice messaggio all'utente. *Il motore di scripting* è un componente di Packet Tracer che è stato progettato per consentire una maggiore flessibilità nella creazione di regole di punteggio per le attività di Packet Tracer che utilizzano il nuovo modello di punteggio. Il motore di scripting è ciò che consente a questo modello di punteggio complesso di esistere. Ogni elemento creato nel modello di calcolo del punteggio esiste come oggetto nel motore di script in modo che sia accessibile da qualsiasi regola di espressione / calcolo del punteggio creata dall'utente. Un esempio di dove il motore di calcolo del punteggio e il motore di script sarebbero utili è quando un istruttore desidera visualizzare un messaggio all'utente indicando che l'indirizzamento IP è per lo più corretto, ma non completamente corretto e non del tutto scorretto. Questo può accadere quando ci sono diversi dispositivi sul palco e uno o due dei tre sono indirizzati correttamente, ma il terzo no. Utilizzando il nuovo modello di punteggio, è possibile fornire questo tipo di feedback basato sulla combinazione di più prodotti di lavoro. Il vantaggio principale qui è la facilità di personalizzazione in scenari di punteggio complessi, oltre a un modello più allineato con il processo Evidence Centered Design.
Un altro metodo per creare delle activity e che è stato aggiunto di recente nell'ultima versione di Packet Tracer è: *l'Activity Sequencer*, lo si trova su Exstension—Activity Sequence editor. Si inizia creando i file PKA, si crea una sequenza logica di attività per renderlo più facile allo studente. Le attività devono avere un punteggio della rete di risposta. Si seleziona il numero di attività che si sono create, il nome dell'activity, la minima percentuale per superare l'activity e appena si completano i parametri cliccare Generate (fig.4.35). Importante notare il percorso in cui il file viene salvato dopo aver creato la generazione del file pks, perchè poi bisogna andare nella directory e copiare/incollare il file nella cartella in cui si trovano le attività. È possibile modificare il file dell'attività in qualsiasi momento per renderlo migliore o aggiornato senza alcun effetto sul sequencer.

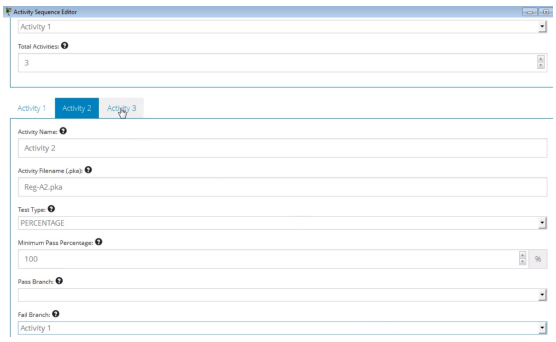


Figura 4.35: Activity Sequencer

5. Conclusioni

In questo elaborato è stato analizzato il simulatore di reti Packet Tracer con il quale sono state eseguite alcune simulazioni e configurate tipologie di rete. L'idea che ha dato vita al progetto si basa su una necessità di "aggiornare" i vecchi moduli di esami, visti e rivisti. Si può affermare che in generale le simulazioni sono un valido strumento di supporto allo studio e allo sviluppo di nuove tecnologie o per il miglioramento di quelle esistenti, in quanto riescono a diminuire i costi e i tempi dovuti alla ricerca permettendo nel contempo una analisi più approfondita del caso preso in esame. Non bisogna però dimenticare che i simulatori modellano sempre una realtà semplificata, nella quale alcuni fattori non vengono volutamente tenuti in considerazione. Quindi è bene verificare che la presenza di questi aspetti nel mondo reale sia ai fini pratici effettivamente ininfluente sul fenomeno osservato prima di considerare validi i risultati ottenuti con il calcolatore. Non c´è lavoro o esercizio che viene eseguito al meglio, se dietro non ha una progettazione di laboratorio con tanto di test. Allora quale miglior programma di Cisco Packet Tracer per simulare le reti da implementare con i dispositivi della casa californiana. Anche se il programma non è realizzato in italiano il suo utilizzo è immediato, ottimale iscriversi ad un corso Cisco per utilizzare il sistema in modo professionale. Su internet sono presenti vari esercizi completi (estensione pkt) per esercitarsi. Packet Tracer è presente anche nella versione mobile sia per Android che per iOS.

5.1 Competenze acquisite e Sviluppi Futuri

Gli studenti che esplorano e sperimentano con Packet Tracer sviluppano:

1. Curiosità intellettuale e capacità di pensiero critico.
2. Capacità di innovazione e creatività.
3. Sicurezza nelle proprie capacità e abilità decisionali.
4. L'uso di Packet Tracer per la collaborazione in team e le attività di competizione sviluppa competenze sociali, di comunicazione e di negoziazione.
5. Capacità di problem solving.
6. L'ambiente di simulazione di Packet Tracer facilita la comprensione di concetti tecnologici complessi.

Considerando questa tesi come base di partenza, ci sono alcuni possibili sviluppi futuri.

- Creazione di nuovi esami anche per CCNA3 e CCNA4

- Come utilizzare le funzionalità più complesse di PT come per esempio (IOT, Scoring Model/Scripting e l'Activity Sequencer).
- PT è un'applicazione di rete (peer to peer) che utilizza la rete reale (connessioni socket TCP) per trasportare i pacchetti virtuali Packet Tracer. L'applicazione PT in esecuzione su un computer può comunicare con l'applicazione PT in esecuzione su uno o più altri computer. Questa connessione tra più istanze di PT supporta il lavoro di gruppo, i giochi in classe, la collaborazione, le competizioni, l'interazione istruttore-studente a distanza e il social networking.

5.2 Ringraziamenti

Ringrazio il mio relatore Dott. Fausto Marcantoni per il tempo dedicato e nell'affidarmi questa tesi.

Ringrazio il mio correlatore Prof. Marco Macari, per la disponibilità dimostrata per lo sviluppo di questo lavoro.

Ringrazio l'Università degli studi di Camerino, il dipartimento di Informatica e tutti i professori dei corsi di studi che ho frequentato.

Ringrazio tutti i miei colleghi di corso e di studio.

Come non ricordare e ringraziare il mio conquilino Fabio e i suoi splendidi genitori per avermi accolto come un figlio nella loro casa, a causa del terremoto.

Un grandissimo grazie va a tutti i miei amici. A tutti gli amici che ho conosciuto a Camerino, che mi hanno accompagnato in questo periodo di studi e che hanno trascorso con me lunghe giornate in questo piccolo paese. A tutti gli amici che mi hanno sostenuto a distanza e che conosco da anni con i quali ho passato attimi indimenticabili.

Un ringraziamento speciale va alla mia ragazza Donatella, per avermi aiutato nei momenti più difficili, soprattutto negli ultimi mesi di Università.

I miei più grandi ringraziamenti vanno a tutta la mia famiglia, per avermi sempre sostenuto e data la fiducia necessaria per arrivare fino a questo traguardo.

Ringrazio me stesso, autore di questa Tesi, per essere riuscito con tenacia, sacrificio e costanza a raggiungere questo obiettivo.

Grazie a tutti per aver reso questi anni indimenticabili !!!

A. More Packet Tracer

A.1 Servizi PT

Packet Tracer offre una vasta gamma di dispositivi finali, a partire da PC e laptop, fino a tablet, PDA e persino una TV.Tra i servizi più importanti invece si citano i seguenti:

1. **Servizio HTTP**: offre un server Web che esegue i protocolli HTTP e HTTPS. Una casella di testo sotto la sezione HTTP fornisce opzioni per creare e modificare HTML statico pagine. Questi vengono visualizzati quando si accede a questo server tramite il browser web utilità di altri dispositivi finali. Questo servizio è attivo per impostazione predefinita.

2. **Servizio DHCP**: può essere utilizzato per assegnare indirizzi IP ai router. Questa sezione ha opzioni per creare e modificare pool DHCP di indirizzi IP. Ha un pool predefinito chiamato serverPool, che non può essere rimosso o modificato. Questo servizio è disattivato per impostazione predefinita.

3. **Servizio TFTP**: può essere immensamente utile quando si apprende il backup e ripristino di immagini Cisco IOS e file di configurazione. Questa sezione elenca diversi IOS immagini da router e switch disponibili in Packet Tracer. Se un file è stato copiato da un dispositivo di rete al server TFTP, anche questo verrà visualizzato.Questo servizio è attivo per impostazione predefinita.

4. **FTP**:ha più funzionalità rispetto a TFTP. Gli utenti possono essere creati e possono essere concessi i permessi a ciascuno di essi. Questa sezione elenca anche i file che sono stati caricati. Non esiste un client GUI per accedere al server FTP. Ma il comando linea sotto la scheda Desktop fornisce il client della riga di comando FTP.

5. **Servizio DNS**: serve per risolvere i nomi di dominio in indirizzi IP. Il servizio DNS offre i seguenti tipi di record: A, CNAME, SOA e NS. Sebbene questa interfaccia sembra semplice e completo, è possibile configurare configurazioni DNS multilivello. Un pulsante della cache DNS consente di visualizzare le richieste DNS memorizzate nella cache e ha una funzionalità che cancella questa cache. Questo servizio è disattivato per impostazione predefinita.

6. **SYSLOG**: questo protocollo fornisce un servizio di registrazione centralizzato. Impostazione dell'IP del server Syslog su puntare all'IP del server configurato da un dispositivo di rete riempie la tabella in Config scheda con tutti i messaggi di registrazione generati dal dispositivo. Questo servizio è acceso per impostazione predefinita.

7. **AAA**: sta per autenticazione, autorizzazione e contabilità. Questo servizio è utilizzato per la gestione centralizzata delle credenziali di tutti i dispositivi di rete. Supporta il "RADIUS" e protocolli di autenticazione "TACACS".Le opzioni in questa sezione consentono di creare utenti e configurare le credenziali di rete da utilizzare.

8. **NTP**: Network Time Protocol assicura che gli orologi di tutti i dispositivi siano sincronizzati propriamente. Questa sezione ha un calendario per impostare la data e l'ora. Opzionalmente, NTP l'autenticazione può anche essere configurata. Una volta impostato il tempo corretto per il server,tutti i dispositivi di rete possono essere configurati per sincronizzare i loro orologi da questo server. Questo servizio è attivo per impostazione predefinita.

9. **Firewall / Firewall IPv6:**: poiché il server ha ora due interfacce di rete, la funzione firewall è stata introdotta in PT Versione 6. Questa sezione consente di configurare le regole in entrata che corrisponde agli indirizzi IP di origine / destinazione e ai numeri di porta locale / remota. In base alla corrispondenza, la connessione può essere consentita o negata.

A.2 Alcune utility dei dispositivi finali

I dispositivi finali hanno una scheda Desktop, che fornisce molte utilità per il test e il debug della rete.Le seguenti utilità sono disponibili per PC, laptop, PDA e tablet PC.

- **Configurazione IP**: questa opzione è usata per scegliere tra un indirizzo IP dinamico e statico. Immissione di un indirizzo IP statico riempie il campo Subnet Mask; in base alla classe dell'indirizzo IP, questo campo può anche essere modificato se necessario. Se DHCP è configurato su Server-PT, scegliere DHCP qui ottiene un indirizzo IP in modo dinamico. A partire da Packet Tracer versione 6, questa utility ha anche una sezione per configurare gli indirizzi IPv6.

- **Prompt dei comandi**: questa utility simula la riga di comando offerta nei sistemi operativi Windows. Sono disponibili solo un numero limitato di comandi, ma sono sufficienti per testare la Rete. I seguenti comandi sono quelli disponibili:

  ? arp delete dir ftp help ipconfig ipv6config netstat nslookup ping snmpget snmpgetbulk snmpset ssh telnet tracert.

- **VPN**: l'utilità VPN viene utilizzata per creare una connessione VPN per comunicazioni sicure.Perché questo funzioni, un router deve essere configurato come server VPN.

- **E-mail**: questa è un'utilità client di posta elettronica che può essere utilizzata per inviare e ricevere e-mail. Il primo l'ora è aperta, deve essere configurata con il server di posta in arrivo (POP3),Server di posta in uscita (SMTP) e credenziali. Un dispositivo Server-PT deve esistere nella topologia con la sua sezione EMAIL configurata.

Bibliografia e Sitografia

[1] "Che cosa è una rete"
https://www.informaticapertutti.com

[2] "Importanza dei Simulatori"
http://www.diit.unict.it

[3] "Classificazione Modelli di Simulazione"
http://www.isci.it/isciTC/references/sistemi/cap_2.pdf

[4] "Virl vs GNS3"
https://www.speaknetworks.com/cisco-virl-better-gns3/

[5] "CiscoIOS"
https://www.cisco.com/c/en/us/support/docs/
ios-nx-os-software/ios-software-releases-110/13178-15.html

[6] "Open-Source Routing and Network Simulation"
http://www.brianlinkletter.com

[7] "NetSim Boson"
http://www.boson.com

[8] "NS2"
http://http://twiki.di.uniroma1.it

[9] "How SDN will Shape Networking" Open Networking Summit 2011.

[10] "Software-Defined Networking (SDN) Definition, Open Networking Foundation".
https://www.opennetworking.org/sdn-resources/sdn-definition.

[11] "OpenFlow"
http://archive.openflow.org/.

[12] "Key Benefits of OpenFlow-Based SDN, Open Networking Foundation".
https://www.opennetworking.org/?p=321&option=com_wordpress&
Itemid=164.

[13] "Mininet".
http://mininet.org/.

[14] "Vantaggi e Limitazioni Mininet".
https://github.com/mininet/mininet/wiki/
Introduction-to-Mininet

[15] "Sito Ufficiale Cisco".
`http://www.cisco.com`

[16] "Guida Ping e PDU" `http://www.ettorepanella.com`

[17] "Utilizzo di PacketTracer"
`http://www.swzone.com`

[18] "Packet Tracer nel CCNA"
`http://www.eforhum.it`

[19] "CCNA Labs/Activities"
`https://ccnav6.com`

[20] "Simulation Mode"
`http://packettracer.wikia.com`

[21] "Overview-of-activity-wizard"
`http://studylib.net`

[22] "Comandi base CCNA1-CCNA2"
`https://www.slideshare.net`

[23] Sito Ufficiale Fausto Marcantoni,Lucidi Lezioni del corso Reti Internet Sicurezza (indirizzamento)
`http://computerscience.unicam.it/marcantoni/`

M.Baldi,P.Nicoletti, "Internetworking", 1999
A.Jesin, "Packet Tracer Network Simulator", 2017
L.Bramo,L.Peterson, "Experiences with Network Simulators", 1996