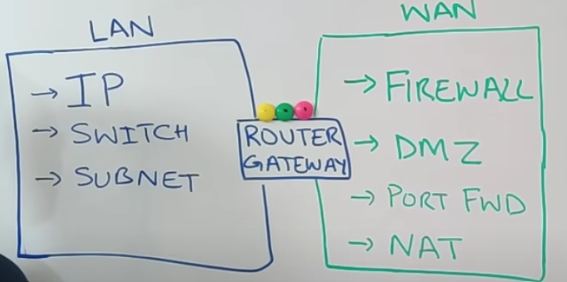
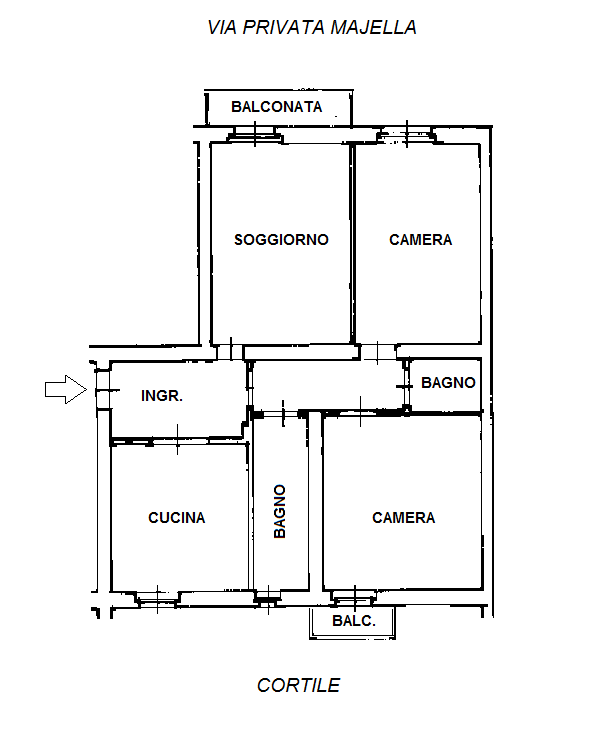
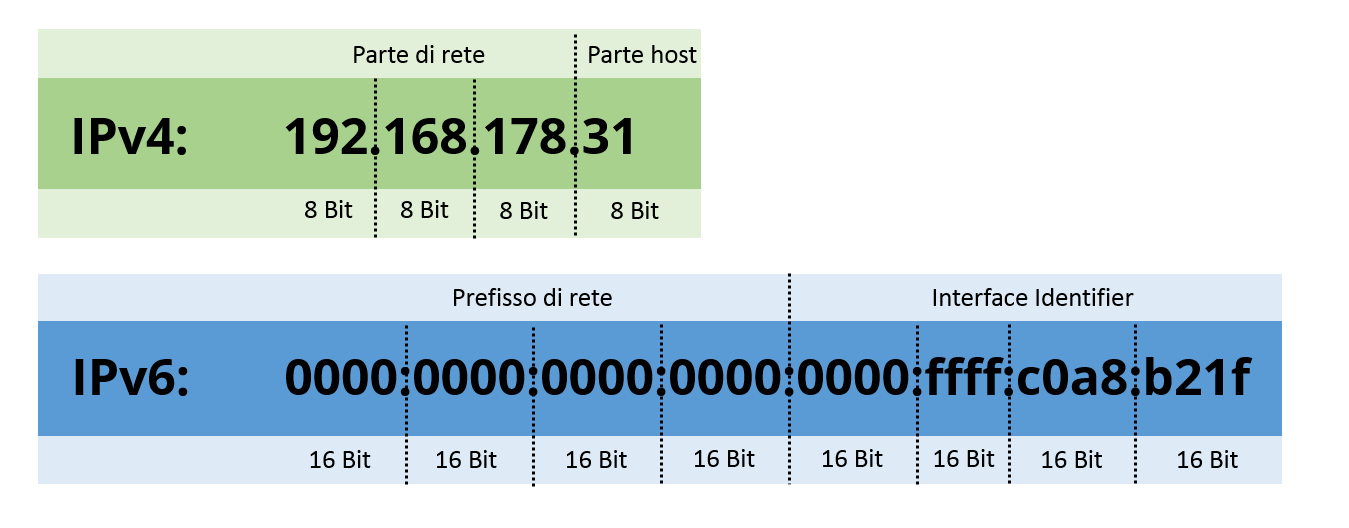
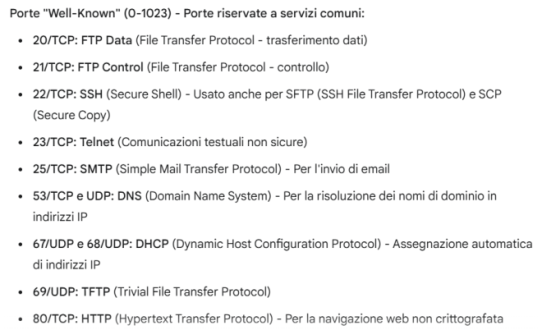
**Le reti TCP- IP**

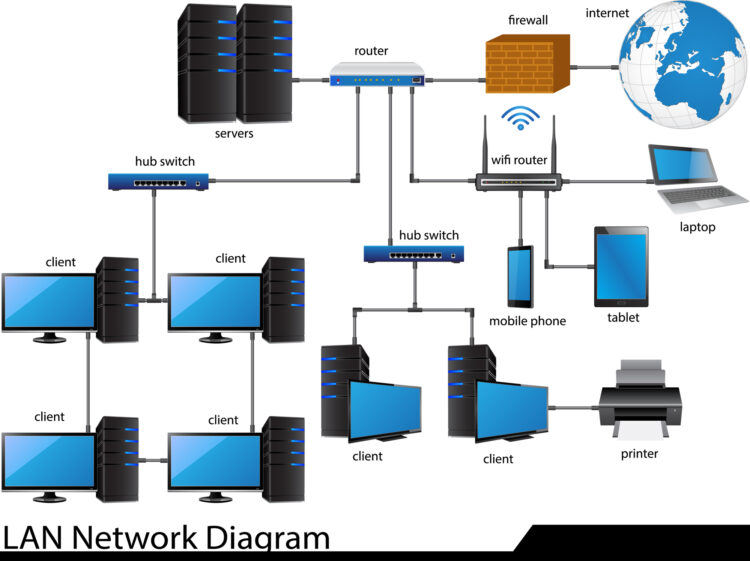
1. **Indirizzo IP**
2. **Switch**
3. **Net e Subnet**
4. **Router – Gateway**
5. **NAT (Network Address Translation)**
6. **Firewall**
7. **DMZ (Demilitarized Zone)**
8. **Port Forwarding (Inoltro Porte)**
9. **VLAN (Virtual LAN)**
10. **Inter VLAN**
11. **Proxy**
12. **Cisco packet tracer**
13. **Cavo ethernet**
14. **Switch livello 3 (routing)**
15. **Rip come protocollo di routing dinamico**



**Indirizzo IP (Internet Protocol)**

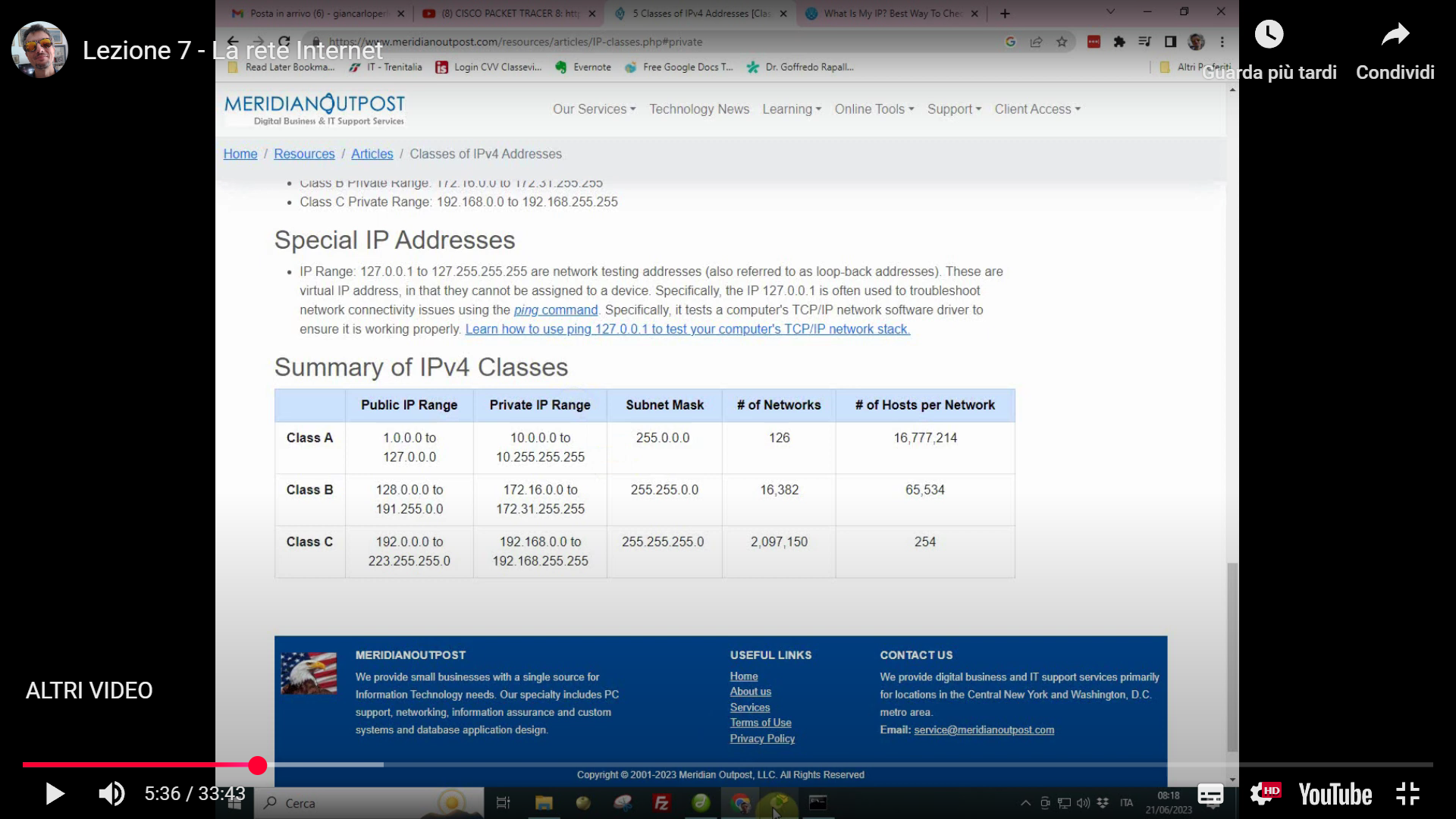
** **** **

****  ****

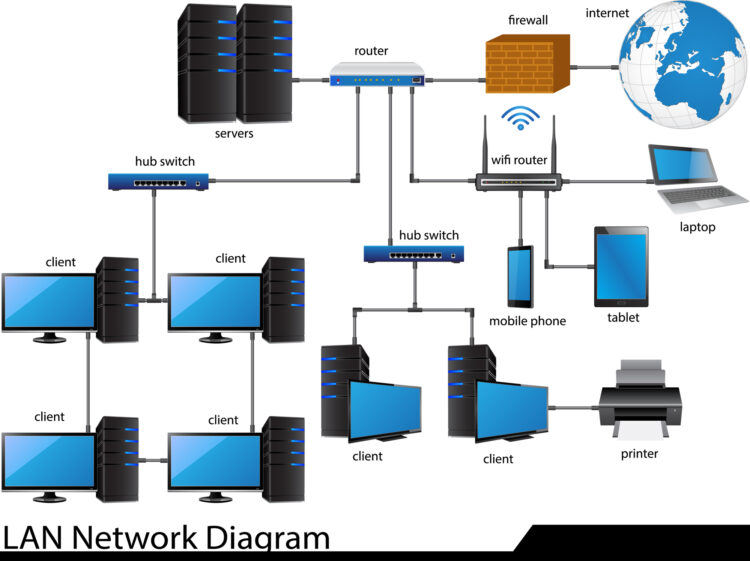
Immagina l'indirizzo IP come il "numero civico" unico di ogni dispositivo (computer, smartphone, stampante, ecc.) collegato a una rete, sia essa la tua rete domestica o Internet. È un'etichetta numerica che permette ai dispositivi di trovarsi e comunicare tra loro.

* **Formato:** Gli indirizzi IP che incontri più spesso sono gli IPv4, che si presentano come quattro numeri separati da punti (es. 192.168.1.10). Esistono anche gli IPv6, più lunghi e complessi, nati per far fronte all'esaurimento degli IPv4.
* **Funzione:** Quando invii un'email, navighi su un sito web o chatti con un amico, il tuo dispositivo usa l'indirizzo IP del destinatario per indirizzare i dati nella giusta direzione.

****

**Net e Subnet (Sottorete)**

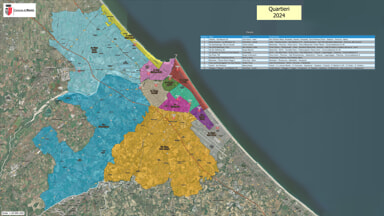
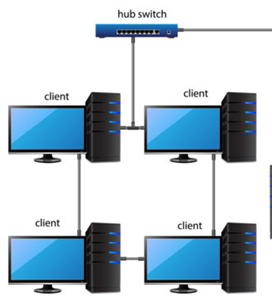
**Net**



Una rete di computer è un insieme di dispositivi di elaborazione (come computer, server, router, ecc.) interconnessi che possono comunicare tra loro e condividere risorse. Questi dispositivi utilizzano protocolli di comunicazione per trasmettere dati, consentendo la condivisione di informazioni, risorse (come stampanti o file), e la collaborazione tra utenti

**Subnet**

****

Una subnet è come un "quartiere" all'interno della tua rete più grande. Immagina una città (la tua rete) divisa in quartieri (subnet).

* **Perché esistono:** Le subnet servono a dividere una rete di grandi dimensioni in segmenti più piccoli e gestibili. Questo migliora l'efficienza, la sicurezza e le prestazioni della rete.
* **Come funziona:** I dispositivi all'interno della stessa subnet possono comunicare direttamente tra loro. Per comunicare con dispositivi in subnet diverse, è necessario passare attraverso un gateway.
* **Maschera di sottorete (Subnet Mask):** Per definire una subnet, si usa una "maschera di sottorete". È un numero che, in combinazione con l'indirizzo IP, determina quale parte dell'indirizzo identifica la rete (il "quartiere") e quale parte identifica il dispositivo specifico (il "numero civico" all'interno del quartiere).

**Switch**



Uno **switch** (commutatore) è un dispositivo di rete che collega insieme più dispositivi (computer, stampanti, server, ecc.) all'interno della stessa rete locale (LAN).

In breve, il suo compito è ricevere i dati da un dispositivo e inoltrarli in modo **intelligente** solo al dispositivo di destinazione corretto, invece di inviarli a tutti i dispositivi come farebbe un hub. Questo rende la rete più efficiente, veloce e sicura, riducendo il traffico superfluo.

**Router - Gateway**



Il router - gateway è come un "punto di confine" o un "ufficio postale" che permette ai dati di viaggiare da una rete all'altra.

* **Funzione:** Se un dispositivo nella tua rete domestica (ad esempio, il tuo PC) vuole accedere a Internet o comunicare con un dispositivo in una subnet diversa, invia i dati al gateway. Il gateway ha il compito di instradare questi dati verso la loro destinazione al di fuori della subnet locale.
* **Di solito:** Nelle reti domestiche, il gateway è quasi sempre il tuo router Wi-Fi. È lui che "connette" la tua rete domestica a Internet. Integra insieme 4 dispositivi diversi:

1. Switch
2. Modem
3. Hot spot
4. Router

**Esempio Pratico:**

Immagina di voler spedire una lettera:

* **Indirizzo IP:** È l'indirizzo completo sulla busta (nome, via, numero civico, CAP, città).
* **Subnet:** La città in cui si trova l'indirizzo. Tutte le case nella stessa città possono usare lo stesso ufficio postale locale per le lettere interne alla città.
* **Gateway:** L'ufficio postale locale. Se devi spedire una lettera fuori città, la porti all'ufficio postale, che poi la invierà all'ufficio postale della città di destinazione.

In sintesi:

* L'**indirizzo IP** identifica in modo univoco un dispositivo.
* La **subnet** raggruppa dispositivi logicamente per una gestione più efficiente.

Il **gateway** è il punto di uscita dalla tua rete locale per raggiungere altre reti o Internet.

**NAT (Network Address Translation)**

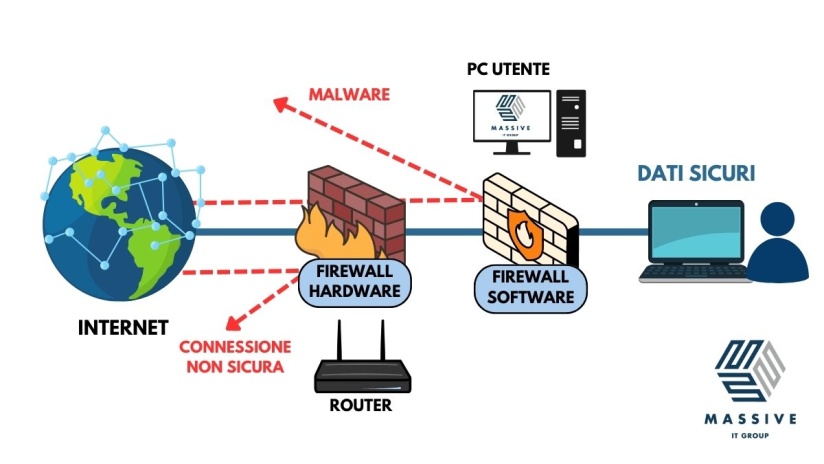
Il NAT, o traduzione degli indirizzi di rete, è una tecnica che consente a più dispositivi su una rete locale (LAN) di condividere un unico indirizzo IP pubblico per accedere a Internet. Funziona traducendo gli indirizzi IP privati dei dispositivi interni in un indirizzo IP pubblico quando i dati escono dalla rete, e viceversa quando i dati rientrano.

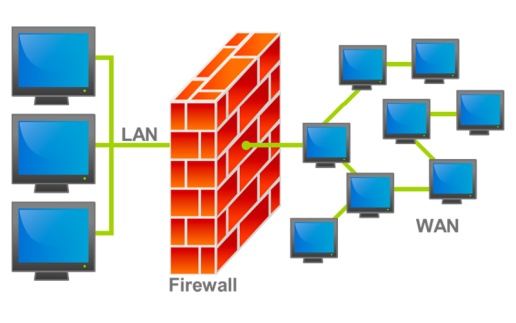
**Perché è usato?**

* **Risparmio di indirizzi IP pubblici:** Gli indirizzi IPv4 pubblici sono limitati. Il NAT permette a molte aziende e abitazioni di usare un solo indirizzo IP pubblico.
* **Sicurezza:** Maschera la topologia interna della rete, rendendo più difficile per gli aggressori esterni conoscere gli indirizzi IP dei singoli dispositivi.

**Come funziona?** Quando un dispositivo interno invia una richiesta a Internet, il router (che esegue il NAT) sostituisce l'indirizzo IP privato del dispositivo con il proprio indirizzo IP pubblico. Mantiene una tabella di traduzione per associare le risposte in arrivo al dispositivo interno corretto.

**Firewall**





Un firewall è un sistema di sicurezza di rete che monitora e controlla il traffico di rete in entrata e in uscita in base a regole di sicurezza predefinite. Agisce come una barriera tra una rete interna fidata e sicura e una rete esterna non fidata (come Internet).

**Tipi principali:**

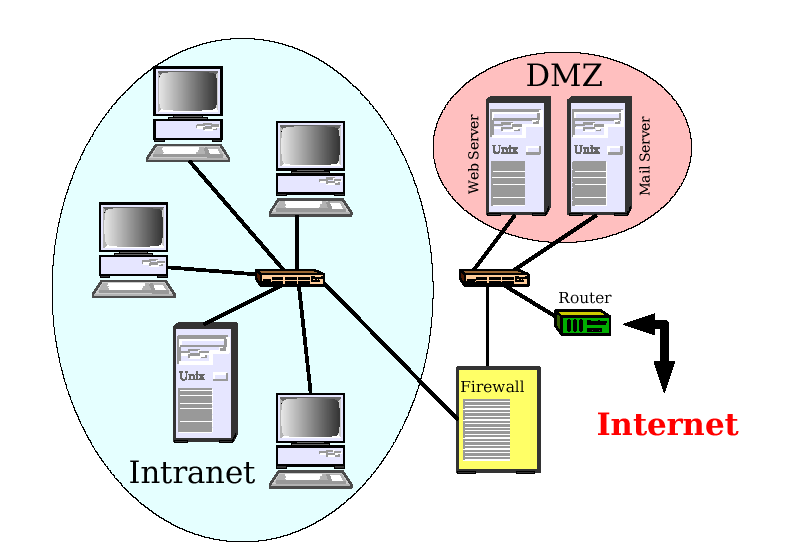
* **Firewall basati su pacchetti (Packet-filtering firewalls):** Esaminano ogni pacchetto di dati che attraversa la rete, confrontando l'intestazione del pacchetto con un insieme di regole predefinite (indirizzo IP di origine/destinazione, porta, protocollo).
* **Firewall basati sullo stato (Stateful inspection firewalls):** Non solo esaminano i pacchetti individuali, ma tengono traccia dello stato delle connessioni attive per determinare se un pacchetto è legittimo.
* **Firewall applicativi (Application-layer firewalls o Proxy firewalls):** Operano al livello dell'applicazione, ispezionando il contenuto effettivo dei pacchetti e capendo i protocolli specifici (es. HTTP, FTP). Offrono la massima sicurezza ma possono essere più lenti.

**Funzioni principali:**

* Bloccare accessi non autorizzati.
* Filtrare contenuti dannosi.
* Controllare l'accesso a risorse specifiche.
* Registrare tentativi di accesso e attacchi.

**DMZ (Demilitarized Zone)**





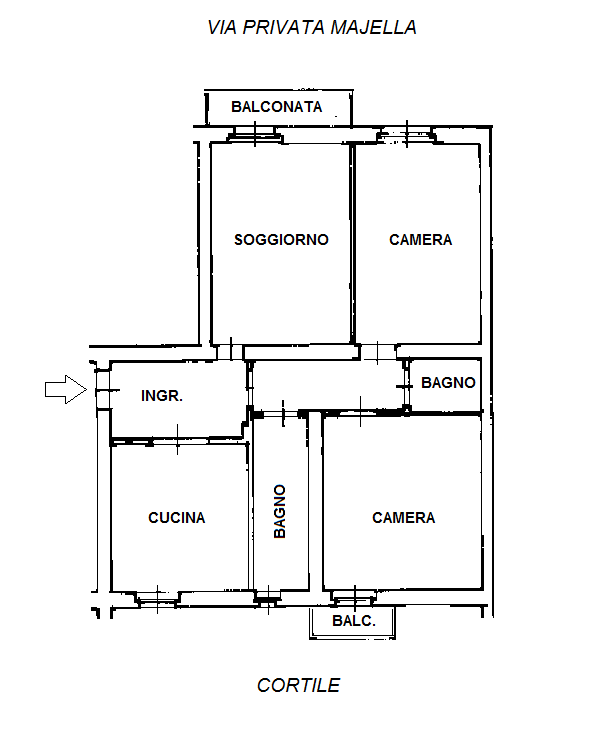
Una DMZ, o zona demilitarizzata, è una sottorete fisica o logica che contiene i servizi di una rete accessibili al pubblico (ad esempio, server web, server e-mail, server DNS) e che si trova tra la rete interna (privata e sicura) e la rete esterna non fidata (Internet).

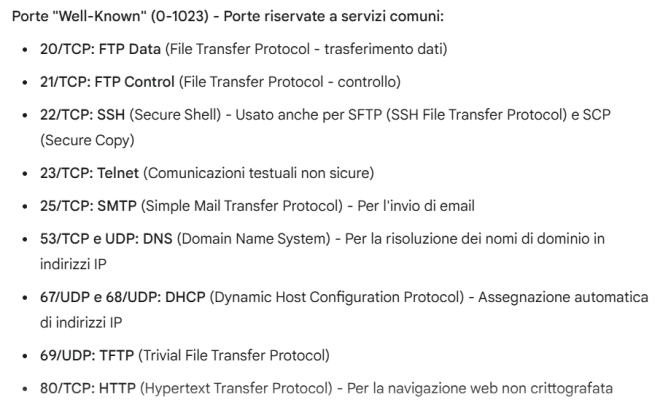
**Perché è usata?**

* **Sicurezza:** Isola i server pubblici dalla rete interna. Se un server nella DMZ viene compromesso, l'attaccante non ha accesso diretto alla rete interna. Agisce come un "cuscinetto" tra la rete interna e Internet.
* **Prestazioni:** I server nella DMZ possono essere configurati per gestire un alto volume di traffico senza sovraccaricare il firewall principale o rallentare la rete interna.

**Come è implementata?** Tipicamente, una DMZ è implementata con due firewall: uno tra la rete interna e la DMZ, e uno tra la DMZ e Internet. In questo modo, il traffico in entrata deve passare attraverso un firewall per accedere alla DMZ e poi attraverso un secondo firewall per accedere alla rete interna.

**Port Forwarding (Inoltro Porte)**

**** ****

**** ****

Il port forwarding è una tecnica che reindirizza le richieste di connessione da una porta specifica di un router a una porta specifica di un dispositivo all'interno della rete locale (LAN). È fondamentale per rendere accessibili dall'esterno servizi o applicazioni che risiedono su un dispositivo all'interno della LAN, che altrimenti sarebbe nascosto dal NAT.

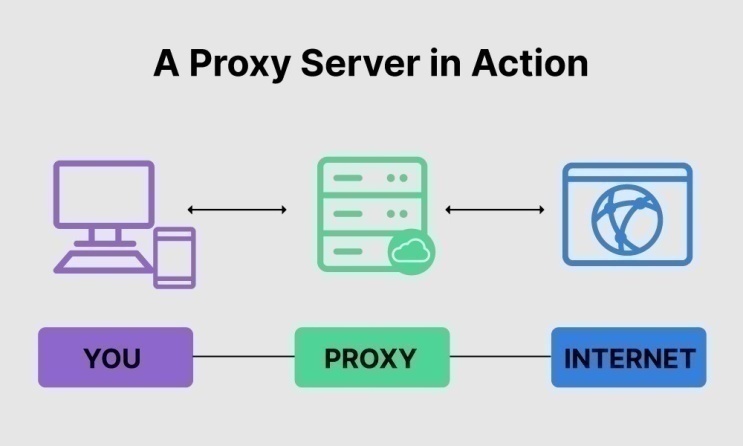
**Come funziona?** Immagina di avere un server web (o un sistema di videocamere di sicurezza, o un server di gioco) sulla tua rete interna con un indirizzo IP privato (es. 192.168.1.100). Normalmente, nessuno dall'esterno può raggiungere questo server usando l'indirizzo IP pubblico della tua rete.

Con il port forwarding, configuri il tuo router in modo che quando riceve traffico su una certa porta pubblica (es. porta 80 per il web), lo reindirizzi a un indirizzo IP privato specifico e una porta specifica sulla tua rete interna (es. 192.168.1.100, porta 80).

**Esempio:**

* **Scenario:** Vuoi accedere al tuo server web domestico da Internet.
* **Configurazione:** Sul tuo router, imposti il port forwarding in modo che il traffico che arriva sulla porta 80 (standard HTTP) del tuo indirizzo IP pubblico venga inoltrato all'indirizzo IP locale del tuo server web (es. 192.168.1.100) sulla porta 80.
* **Risultato:** Quando qualcuno digita l'indirizzo IP pubblico della tua rete nel browser, il router riceve la richiesta sulla porta 80 e la reindirizza al tuo server web interno, che risponde alla richiesta.

**Proxy server**



Un **server proxy** (o semplicemente "proxy") è un sistema informatico (un server o un software) che funge da **intermediario** tra il tuo dispositivo (client) e un altro server su Internet (ad esempio, il server di un sito web che vuoi visitare).

Immagina di voler chiedere un libro in biblioteca. Invece di andare direttamente tu a prenderlo, mandi un amico (il proxy) che lo prende al posto tuo e te lo porta. In questo scenario, la biblioteca non sa che sei tu a volere il libro, ma solo che il tuo amico lo sta chiedendo.

**Come funziona un server proxy?**

Quando utilizzi un proxy, la tua richiesta per accedere a un sito web o a una risorsa online non va direttamente al server di destinazione. Invece:

1. **Tu invii la richiesta al server proxy.**
2. **Il server proxy riceve la tua richiesta.**
3. **Il server proxy inoltra la richiesta al server di destinazione** (il sito web che vuoi visitare) a proprio nome, utilizzando il suo indirizzo IP.
4. **Il server di destinazione risponde al server proxy.**
5. **Il server proxy inoltra la risposta al tuo dispositivo.**

**A cosa serve un server proxy?**

I proxy vengono utilizzati per diverse ragioni:

* **Privacy e Anonimato:** Essendo l'intermediario, il server proxy maschera il tuo indirizzo IP reale, mostrando al server di destinazione solo l'indirizzo IP del proxy. Questo può aumentare la tua privacy online, rendendo più difficile tracciare le tue attività.
* **Aggirare Restrizioni Geografiche o Censura:** Se un sito web è bloccato nella tua regione o nel tuo paese, puoi usare un proxy situato in una località dove il sito è accessibile per aggirare il blocco.
* **Migliorare la Velocità (Caching):** Alcuni proxy memorizzano una copia delle pagine web e dei contenuti più richiesti (cache). Se un utente richiede una risorsa già presente nella cache del proxy, il proxy può fornirla direttamente, riducendo i tempi di caricamento e il traffico di rete. Questo è particolarmente utile in grandi reti aziendali.
* **Sicurezza e Filtraggio:** I proxy possono agire come un firewall, filtrando il traffico in entrata e in uscita. Possono essere configurati per bloccare l'accesso a siti web specifici, contenuti indesiderati o minacce conosciute. Le aziende spesso li usano per controllare l'uso di Internet da parte dei dipendenti.
* **Monitoraggio del Traffico:** Nelle reti aziendali o istituzionali, i proxy possono monitorare e registrare il traffico di rete, fornendo dati utili per l'analisi e la sicurezza.
* **Bilanciamento del Carico (Reverse Proxy):** Esistono anche i "reverse proxy" che si posizionano di fronte a uno o più server web. In questo caso, il reverse proxy riceve le richieste dai client e le distribuisce tra i vari server, bilanciando il carico e migliorando le prestazioni e l'affidabilità.

**Tipi di proxy:**

Esistono diversi tipi di proxy, a seconda della loro funzione e del livello di anonimato che offrono:

* **Proxy Web (HTTP/HTTPS):** Sono i più comuni e gestiscono il traffico relativo alla navigazione web.
* **Proxy SOCKS:** Sono più versatili, in quanto possono gestire qualsiasi tipo di traffico (non solo HTTP/HTTPS) e vengono spesso usati per lo streaming, i giochi o le applicazioni P2P.
* **Proxy Trasparenti:** Non nascondono il tuo indirizzo IP e spesso non sono visibili all'utente. Sono usati principalmente per il caching o il filtraggio da parte di ISP, scuole o aziende.
* **Proxy Anonimi:** Nascondono il tuo indirizzo IP, ma rivelano di essere un server proxy.
* **Proxy Elite (o ad alto anonimato):** Nascondono sia il tuo indirizzo IP che il fatto di essere un proxy, offrendo il massimo livello di anonimato.
* **Proxy di Distorsione:** Si identificano come server proxy ma forniscono un falso indirizzo IP del client.

**Cisco packet tracer**

**Cisco Packet Tracer** è un software di simulazione di rete sviluppato da Cisco Systems. È uno strumento didattico molto utilizzato per apprendere i concetti di networking e per esercitarsi nella configurazione e nel troubleshooting di reti informatiche.

Ecco alcuni punti chiave per capire cos'è e a cosa serve:

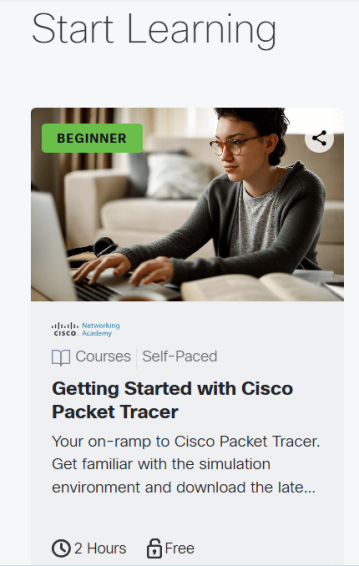
* **Simulazione di rete:** Packet Tracer permette di creare e simulare topologie di rete complesse in un ambiente virtuale. Non hai bisogno di acquistare hardware fisico costoso (router, switch, server, PC reali, ecc.) per sperimentare.
* **Ambiente virtuale sicuro:** Puoi testare diverse configurazioni, protocolli e scenari senza il rischio di compromettere una rete reale o danneggiare apparecchiature.
* **Dispositivi virtuali:** Il software include una vasta gamma di dispositivi virtuali, come router, switch (Layer 2 e Layer 3), server (HTTP, DHCP, DNS, ecc.), firewall, access point, PC, laptop, smartphone, tablet e telefoni IP.
* **Interfaccia intuitiva:** Offre un'interfaccia drag-and-drop facile da usare che semplifica la creazione delle topologie di rete.
* **Configurazione CLI (Command Line Interface):** Permette di configurare i dispositivi Cisco utilizzando una simulazione della riga di comando (CLI) reale, proprio come faresti con l'hardware fisico. Questo è fondamentale per chi studia per certificazioni Cisco come la CCNA.
* **Visualizzazione del flusso dei pacchetti:** Consente di visualizzare in dettaglio come i pacchetti di dati viaggiano attraverso la rete, permettendo di comprendere meglio il funzionamento dei protocolli. Ha sia una modalità in tempo reale che una modalità di simulazione, dove è possibile controllare il tempo e osservare il traffico pacchetto per pacchetto.
* **Scopi educativi:** È ampiamente utilizzato da studenti e insegnanti in corsi di networking (in particolare quelli della Cisco Networking Academy) per esercitarsi, creare progetti e prepararsi agli esami di certificazione.
* **Supporto a diversi protocolli:** Supporta una vasta gamma di protocolli di rete a diversi livelli (applicazione, trasporto, rete), inclusi TCP/IP, OSPF, EIGRP, BGP, RIP, VLAN, VPN, ecc.
* **Collaborazione:** Packet Tracer supporta un sistema multi-utente che consente a più utenti di connettere più topologie tra loro attraverso una rete di computer.

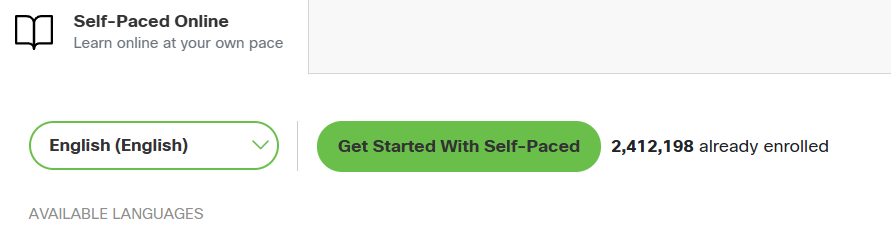
In sintesi, Cisco Packet Tracer è un potente "laboratorio virtuale" che consente a chiunque, dai principianti agli esperti, di imparare, progettare, configurare e risolvere problemi di rete in un ambiente simulato, senza la necessità di hardware fisico.

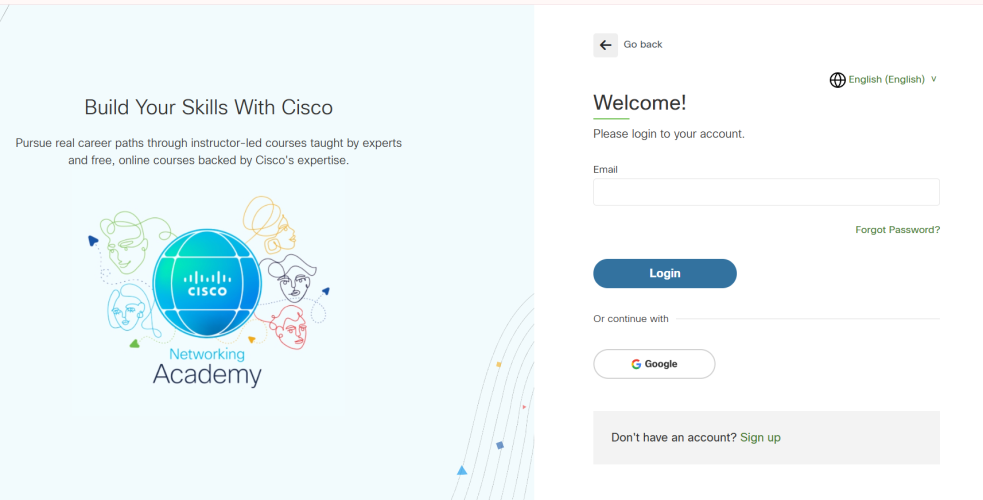
Per installare Cisco Packet Tracer gratuitamente, è necessario scaricare il software dal sito Web di Cisco Networking Academy e seguire le istruzioni di installazione. Per farlo, devi prima registrarti e creare un account sul sito.

Ecco una guida dettagliata:

1. **Visita il sito web di Cisco Networking Academy:** Sul sito, troverai un pulsante "Iscriviti per scaricare il pacchetto tracciante". <https://www.netacad.com/>

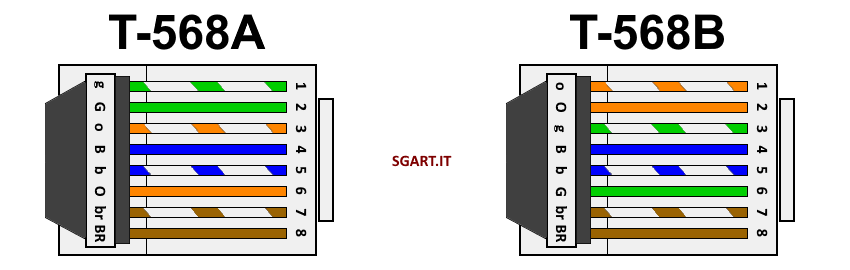
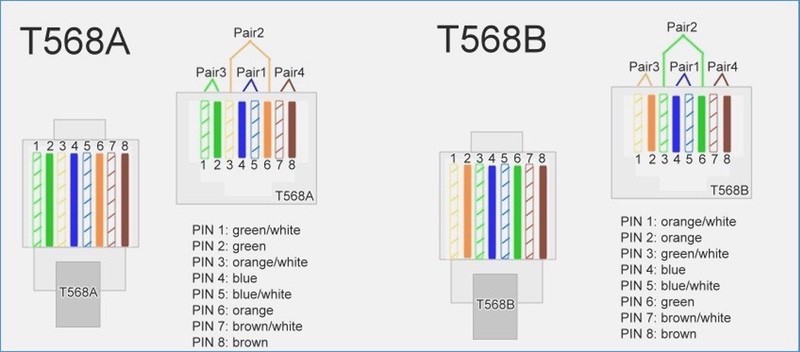






1. **Registrati:** Se non hai ancora un account, segui il processo di registrazione e crea un account.
2. **Iscriviti al corso Packet Tracer:** Una volta registrato, iscriviti al corso "Introduzione a Packet Tracer" o a un corso che include Packet Tracer come strumento di simulazione.
3. **Scarica Packet Tracer:** Una volta iscritto al corso, potrai accedere al download di Packet Tracer.
4. **Installa Packet Tracer:** Segui le istruzioni di installazione forniste durante il download.
5. Nota: È importante assicurarsi di avere un account Cisco Networking Academy per accedere al download e all'uso gratuito di Packet Tracer.

**Cavo ethernet**



Generalmente, un cavo Ethernet (che usa il connettore **RJ45**) contiene **8 pin**. L'utilizzo di questi pin dipende dalla velocità della rete e dallo standard di cablaggio.

**Quanti pin vengono usati?**

* **Per le reti 10 Mbps (10BASE-T) e 100 Mbps (100BASE-TX - Fast Ethernet):** Di solito vengono utilizzate **solo 4 dei 8 pin**, ovvero due coppie di fili: una per la trasmissione dei dati e una per la ricezione. I pin coinvolti sono tipicamente il **1, 2, 3 e 6**. Gli altri pin (4, 5, 7, 8) sono presenti ma non vengono utilizzati per la trasmissione dei dati a queste velocità.
* **Per le reti 1000 Mbps (1000BASE-T - Gigabit Ethernet) e superiori (10 Gigabit Ethernet, ecc.):** Vengono utilizzati **tutti gli 8 pin** (tutte e quattro le coppie di fili) per permettere velocità di trasferimento dati più elevate.

**Standard di cablaggio**

Esistono due standard principali per il cablaggio dei cavi Ethernet:

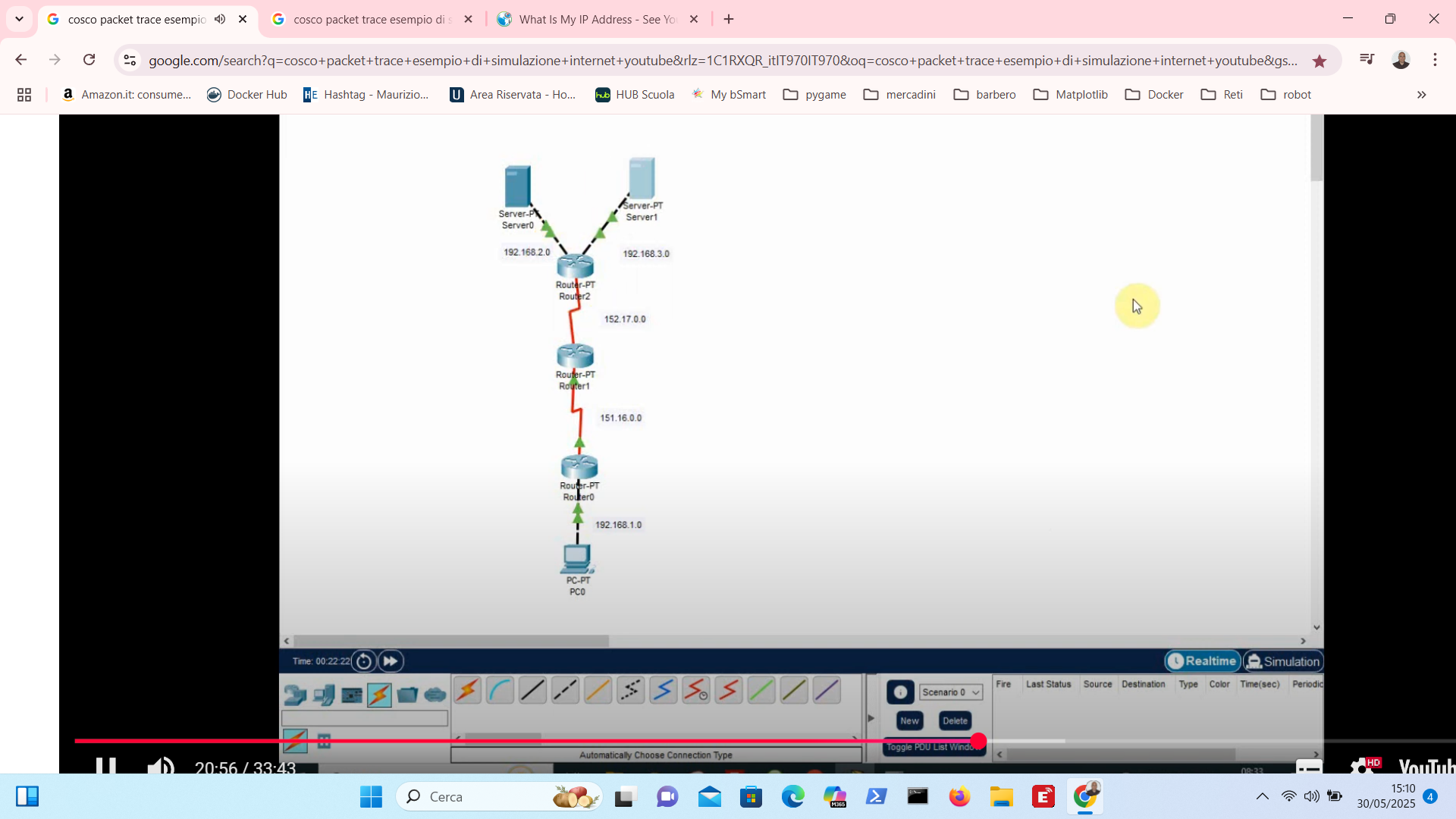
* **T568A**
* **T568B**

Entrambi gli standard specificano l'ordine in cui i fili colorati all'interno del cavo devono essere collegati ai pin del connettore RJ45. La differenza principale tra i due è l'interscambio delle coppie verde e arancione.

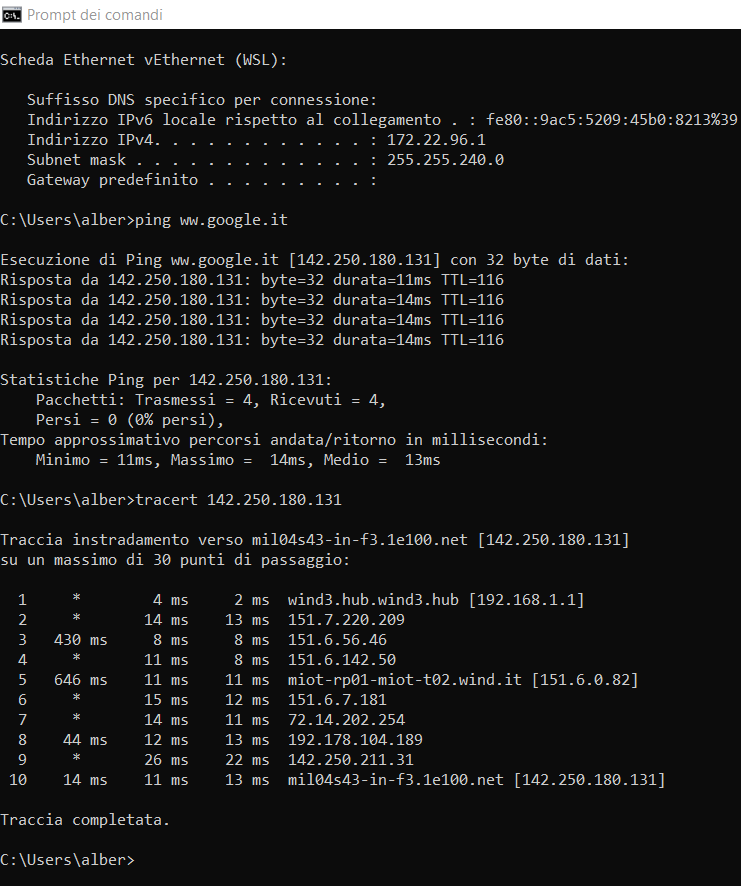
* **Cavo diretto (Straight-through cable):** Entrambe le estremità del cavo sono cablate con lo stesso standard (es. T568B su entrambi i lati). Questo è il tipo di cavo più comune e viene usato per collegare dispositivi diversi (es. computer a switch, router a switch).
* **Cavo incrociato (Crossover cable):** Un'estremità del cavo è cablata con lo standard T568A e l'altra con lo standard T568B. Questo "incrocia" i pin di trasmissione e ricezione, ed è stato storicamente utilizzato per collegare direttamente dispositivi simili (es. computer a computer, switch a switch) senza un hub o uno switch. Tuttavia, molti dispositivi di rete moderni hanno una funzione di **Auto MDI/MDI-X** che rileva automaticamente il tipo di cavo e si adatta di conseguenza, rendendo i cavi crossover meno necessari.

Quindi, sebbene un cavo Ethernet abbia sempre 8 pin, la quantità effettiva di pin usati per la trasmissione dei dati dipende dalla velocità della rete e, in alcuni casi, dal tipo di cablaggio (diretto o incrociato) e dalla presenza di funzionalità avanzate nei dispositivi.

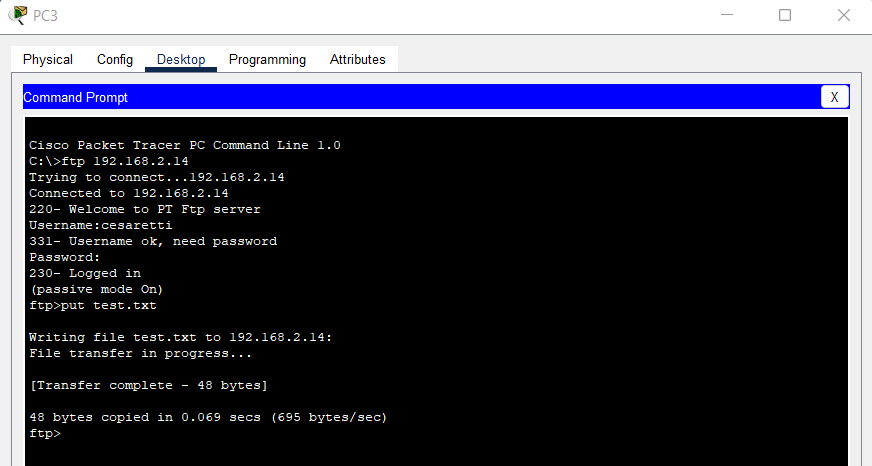
**Simuliamo la rete internet**



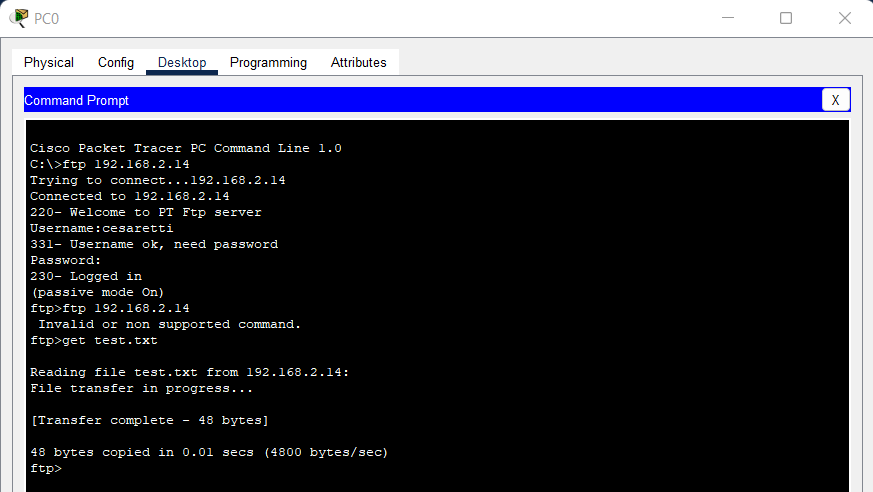
**Tracert <indirizzo ip>**



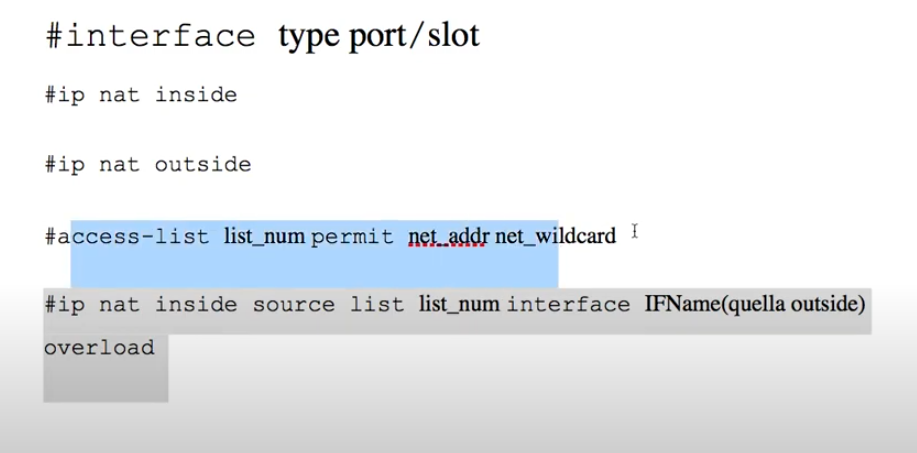
**FTP upload**



**FTP download**

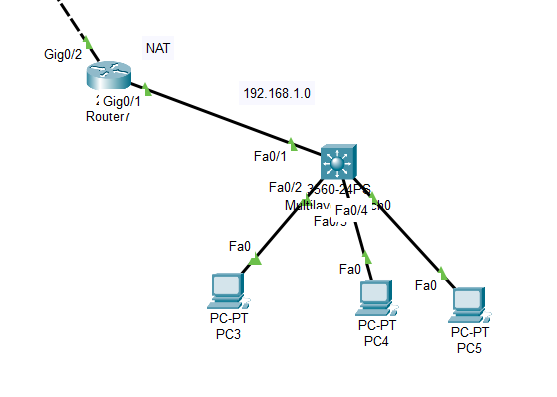


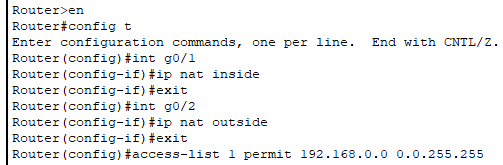
**NAT (network address translation)**



Esempio

**Configuriamo il router utilizzando il metodo delle access list**



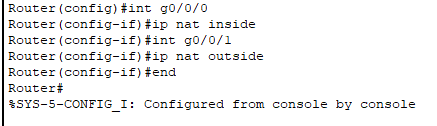




Router 3 della rete 192.168.2.0

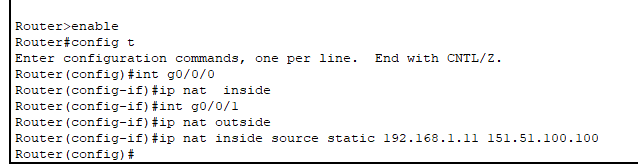


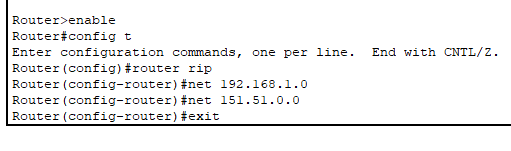


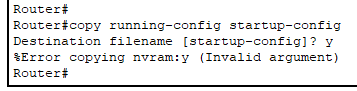




Router 1 della rete 192.168.1.0









**VLAN**

Le VLAN (Virtual Local Area Network) sono una tecnologia fondamentale nella gestione delle reti moderne, soprattutto in ambienti aziendali complessi. Il loro utilizzo si basa su diversi scopi e offre numerosi vantaggi:

**1. Segmentazione Logica della Rete:**

* **Separazione del traffico:** Le VLAN permettono di dividere una rete fisica in più reti logiche separate. Questo significa che dispositivi che si trovano sulla stessa infrastruttura hardware (stessi switch, stessi cavi) possono essere raggruppati in reti virtuali diverse, isolate tra loro. Ad esempio, si può creare una VLAN per il reparto marketing, una per l'amministrazione, una per il supporto tecnico, e una per gli ospiti.
* **Riduzione dei domini di broadcast:** Ogni VLAN crea un proprio dominio di broadcast. In una rete tradizionale senza VLAN, i messaggi di broadcast (pacchetti inviati a tutti i dispositivi) si propagano a tutti i dispositivi collegati. Questo può generare traffico inutile e rallentare la rete. Con le VLAN, il traffico di broadcast è confinato all'interno della singola VLAN, migliorando le prestazioni generali della rete.

**2. Sicurezza Migliorata:**

* **Isolamento dei dati sensibili:** Separando i dipartimenti o i tipi di traffico in VLAN diverse, si riduce la possibilità che utenti non autorizzati accedano a dati sensibili. Ad esempio, i dati finanziari possono essere isolati in una VLAN dedicata, inaccessibile al resto della rete.
* **Limitazione dei movimenti di minacce:** Se un dispositivo in una VLAN viene compromesso da malware o attacchi, il danno è contenuto all'interno di quella VLAN, rendendo più difficile la propagazione della minaccia al resto della rete.
* **Implementazione di politiche di sicurezza:** Le VLAN semplificano l'applicazione di politiche di sicurezza specifiche per ogni gruppo di utenti o tipo di traffico. Ad esempio, è possibile configurare regole di firewall più stringenti per una VLAN contenente server critici.

**3. Ottimizzazione delle Prestazioni:**

* **Riduzione della congestione:** Confinando il traffico di broadcast e segmentando la rete, si riduce il volume di traffico su ciascun segmento, diminuendo la congestione e migliorando la velocità e la reattività della rete.
* **Prioritizzazione del traffico:** È possibile assegnare priorità diverse al traffico di diverse VLAN. Ad esempio, il traffico vocale (VoIP) o video può essere inserito in una VLAN dedicata con priorità più alta per garantire una comunicazione fluida e senza interruzioni.

**4. Gestibilità e Flessibilità:**

* **Facilità di gestione:** Le VLAN semplificano l'organizzazione dei dispositivi di rete in gruppi logici, rendendo più facile la gestione della rete, la risoluzione dei problemi e l'implementazione di nuove configurazioni.
* **Scalabilità:** Le VLAN consentono di espandere facilmente la rete aggiungendo nuove sottoreti senza dover modificare drasticamente l'infrastruttura fisica esistente.
* **Flessibilità negli spostamenti:** Se un utente si sposta fisicamente all'interno dell'edificio, può rimanere nella stessa VLAN semplicemente ricollegando il suo dispositivo alla nuova porta. Questo elimina la necessità di riconfigurare gli switch o modificare la topologia fisica della rete.
* **Supporto multi-tenant:** In ambienti dove più aziende o dipartimenti condividono la stessa infrastruttura di rete (ad esempio, in un edificio per uffici condiviso o un data center), le VLAN permettono di mantenere i dati e il traffico di rete separati e privati per ogni entità.

**5. Costi Ridotti:**

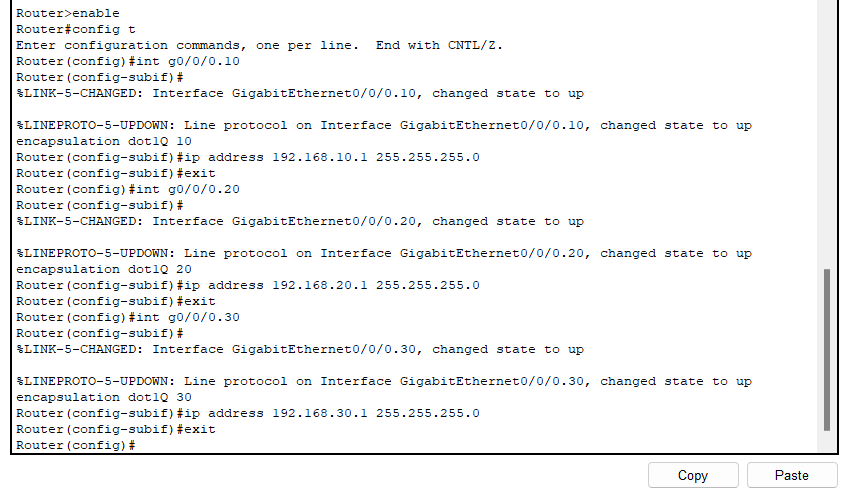
* **Meno hardware:** Le VLAN consentono di utilizzare una singola infrastruttura di switch e cablaggio per supportare più reti logiche, riducendo la necessità di acquistare e installare switch fisici aggiuntivi per ogni segmento di rete. Questo si traduce in un notevole risparmio di costi e tempo.

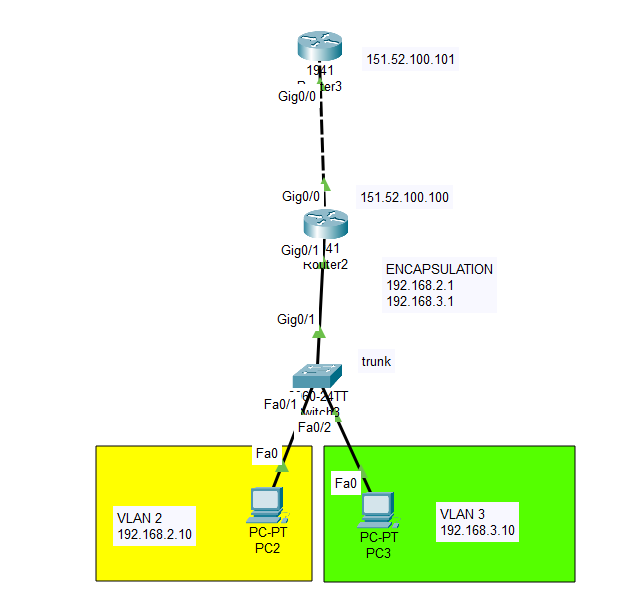
In sintesi, le VLAN sono uno strumento potente per gli amministratori di rete che desiderano migliorare la sicurezza, le prestazioni, la gestibilità e la flessibilità della propria infrastruttura di rete, il tutto con un'ottimizzazione dei costi.

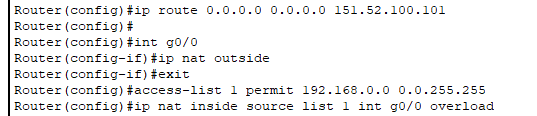
**Inter VLAN**

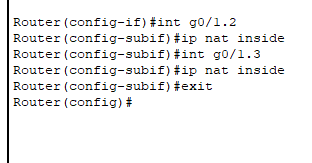
**Soluzione tramite un router**

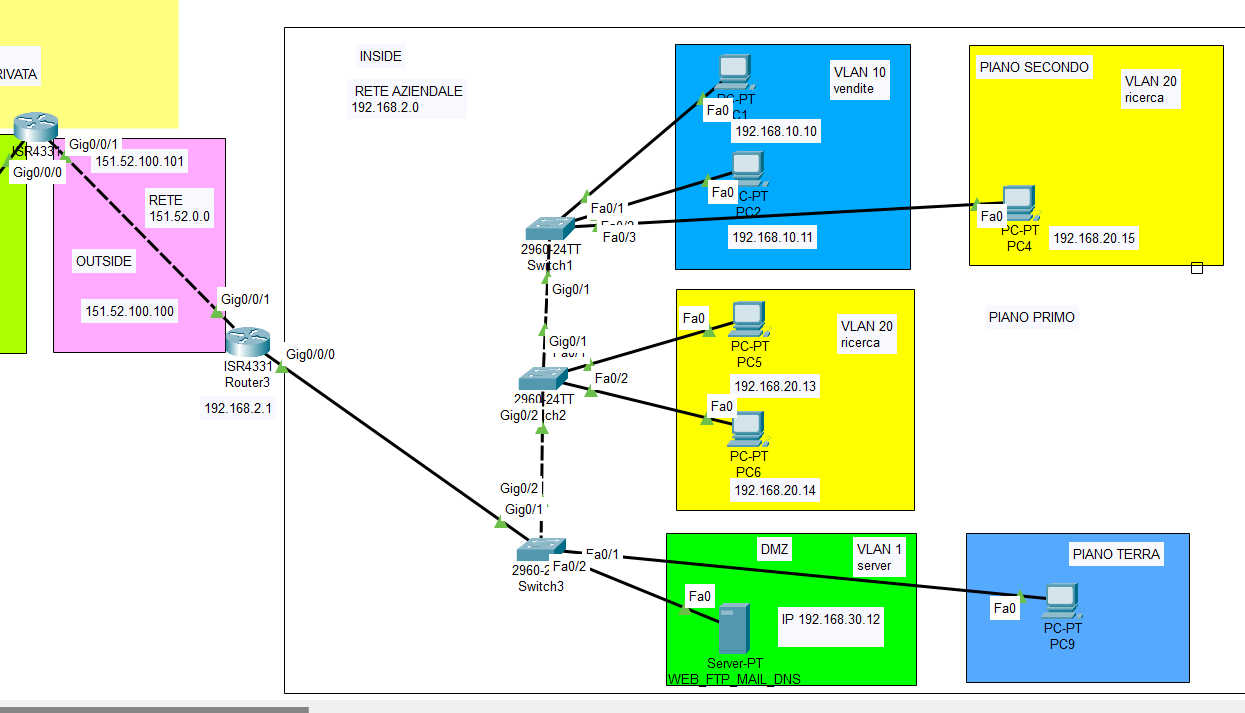
Questi sono i comandi per configurare il router per le tre reti VLAN





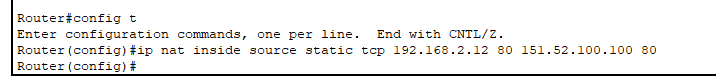


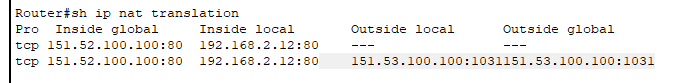




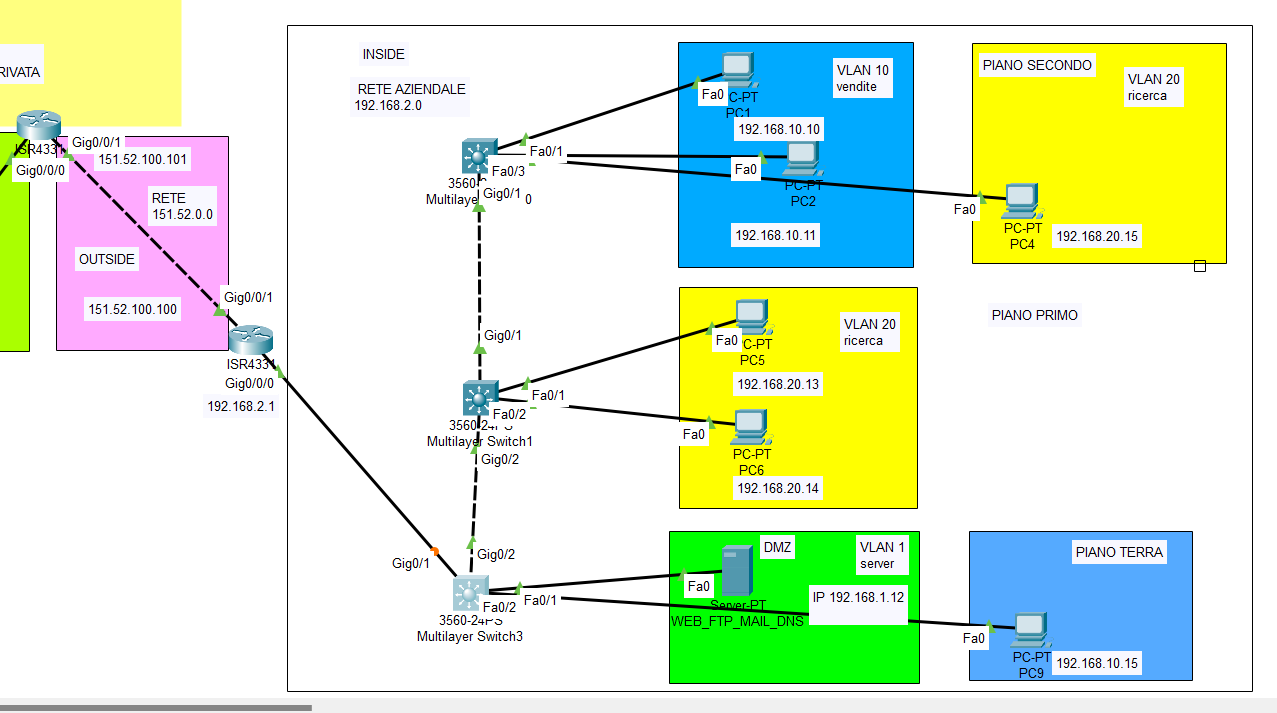


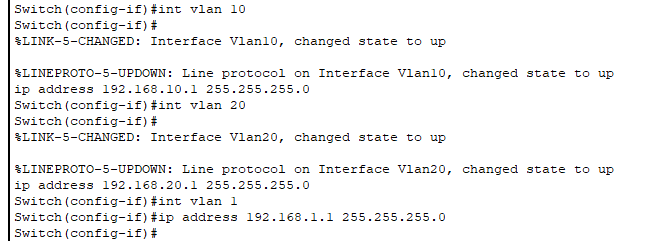
**Port forwording**

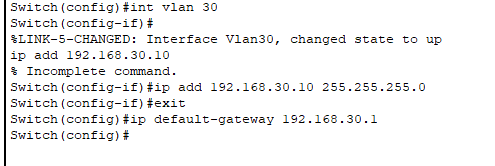




Switch livello 3 (routing)



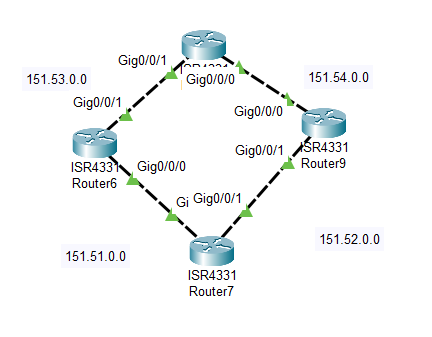


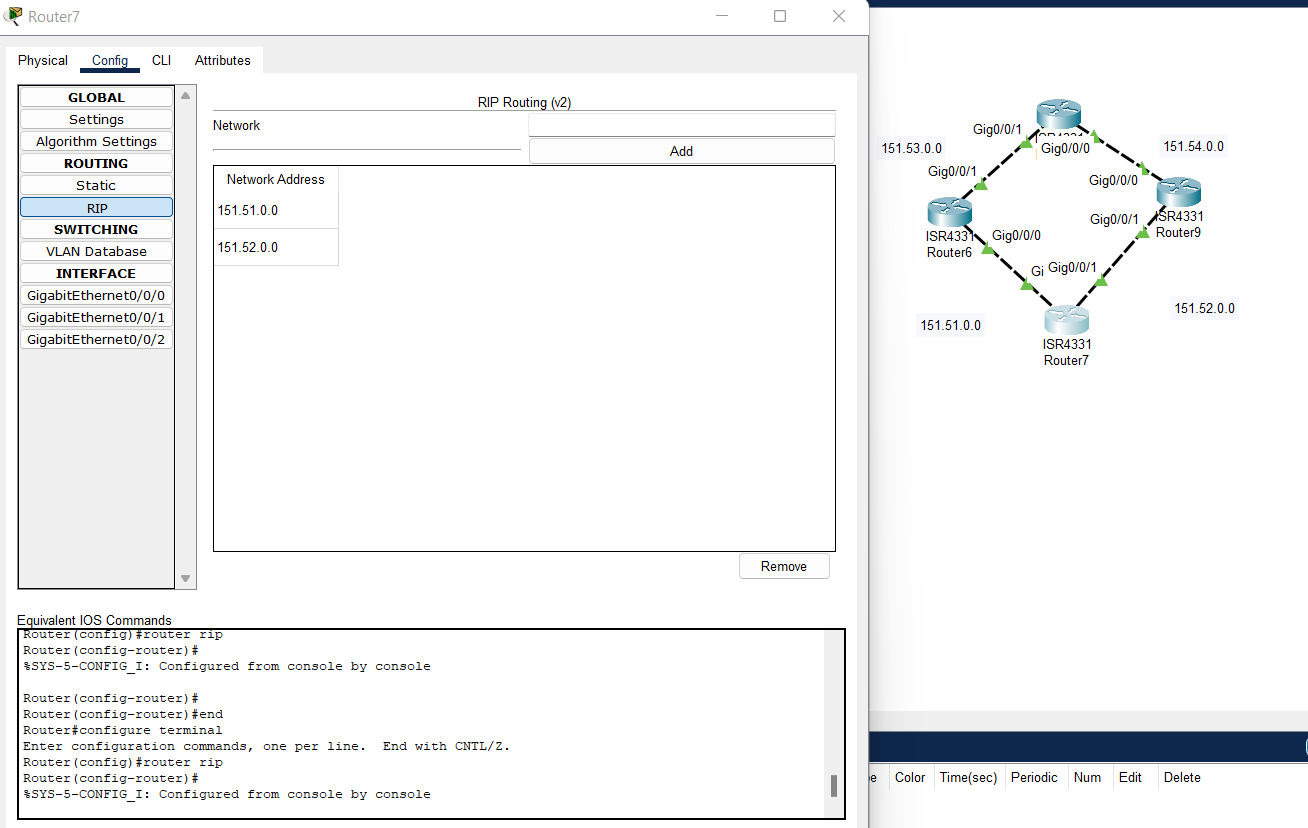




RIP

Si mettono le due reti che arrivano al router, e si impostano su ogni router





In Cisco Packet Tracer, il **Routing Information Protocol (RIP)** è un protocollo di routing dinamico di tipo **distance-vector**. Ecco una spiegazione di cos'è e come funziona:

**Cos'è il RIP?**

* **Protocollo di Routing Dinamico:** A differenza del routing statico (dove le rotte sono configurate manualmente), RIP consente ai router di scoprire automaticamente le rotte verso altre reti e di aggiornare le proprie tabelle di routing.
* **Distance-Vector:** Questo significa che i router RIP non hanno una mappa completa della rete. Invece, ogni router conosce le rotte verso le reti vicine (i "vettori") e la "distanza" (il costo) per raggiungerle. Ricevono informazioni di routing dai loro vicini e, in base a queste informazioni, aggiornano le proprie tabelle. Si parla spesso di "routing by rumor" (routing per sentito dire) perché ogni router si fida delle informazioni che riceve dai suoi vicini.
* **Metric (Metrica): Hop Count (Conteggio Salti):** RIP utilizza il numero di "hop" (salti) come metrica per determinare il percorso migliore. Un hop è un router che un pacchetto attraversa per raggiungere la sua destinazione. Il percorso con il minor numero di hop è considerato il migliore.
* **Limitazione degli Hop:** RIP ha un limite massimo di 15 hop. Un percorso con 16 hop o più è considerato irraggiungibile. Questo limita l'uso di RIP in reti molto grandi.
* **Interior Gateway Protocol (IGP):** RIP è un IGP, il che significa che è progettato per il routing all'interno di un singolo sistema autonomo (Autonomous System - AS), ovvero un gruppo di reti e router gestiti da una singola entità amministrativa.
* **Aggiornamenti Periodici:** I router RIP inviano aggiornamenti completi della loro tabella di routing ai loro vicini a intervalli regolari (solitamente ogni 30 secondi). Questi aggiornamenti consentono ai router di mantenere le loro tabelle aggiornate e di adattarsi ai cambiamenti della rete.

**Versioni di RIP:**

* **RIPv1:** È la versione più vecchia. Non supporta il routing classless (cioè non invia le informazioni della subnet mask negli aggiornamenti) e utilizza il broadcast per gli aggiornamenti.
* **RIPv2:** È la versione più comunemente usata in Packet Tracer. Supporta il routing classless (quindi invia le subnet mask) e utilizza il multicast (all'indirizzo 224.0.0.9) per gli aggiornamenti, riducendo il traffico di rete rispetto al broadcast. Esiste anche una versione per IPv6 chiamata RIPng.

**Caratteristiche e Meccanismi di RIP (per prevenire i loop di routing):**

* **Split Horizon:** Un router non pubblicizza una rotta attraverso l'interfaccia da cui l'ha appresa. Questo aiuta a prevenire i loop di routing.
* **Route Poisoning:** Quando una rotta diventa irraggiungibile, viene annunciata con una metrica di 16 (infinito) per indicare che non dovrebbe essere utilizzata.
* **Hold-down Timers:** Dopo aver ricevuto un aggiornamento che indica una rotta come non disponibile, un router mette quella rotta in uno stato di "hold-down" per un certo periodo, ignorando eventuali aggiornamenti che potrebbero riabilitarla prematuramente.

**Vantaggi del RIP:**

* **Semplicità:** È facile da configurare e comprendere, rendendolo un buon punto di partenza per imparare i protocolli di routing dinamico.
* **Adatto a piccole reti:** A causa delle sue limitazioni (come il limite di 15 hop), è più adatto per reti di piccole e medie dimensioni.

**Svantaggi del RIP:**

* **Lento nella convergenza:** Gli aggiornamenti periodici e i meccanismi di prevenzione dei loop possono rendere la rete lenta a convergere (cioè a raggiungere uno stato stabile in cui tutti i router hanno informazioni di routing coerenti) dopo un cambiamento.
* **Banda sprecata:** L'invio di aggiornamenti completi della tabella di routing ogni 30 secondi può sprecare banda di rete, specialmente in reti più grandi.
* **Limite di hop:** Il limite di 15 hop lo rende inadatto per reti estese.
* **Mancanza di informazioni complete:** Essendo un protocollo distance-vector, non ha una visione completa della topologia di rete, il che può portare a percorsi subottimali.

In Cisco Packet Tracer, puoi simulare e configurare facilmente RIP per capire come funziona il routing dinamico in un ambiente controllato.

