



IIS ETTORE MAJORANA

ANNO SCOLASTICO 2015/2016

INDIRIZZO DI STUDI "INFORMATICA E TELECOMUNICAZIONI"

ARTICOLAZIONE "TELECOMUNICAZIONI"

CLASSE: 5 TL

TOMMASO COLOMBO

PROGETTAZIONE E CREAZIONE DI UNA INFRASTRUTTURA DI RETE

Indice

1-Scopo del progetto (**pag.3**)

2-Strumenti utilizzati (**pag.3**)

3-Similazione reti tramite packet tracer (**pag.4>5**)

4-Procedimento (**pag. 6**)

5-Cenni teorici (**pag.7>18**)

6-Subnetting (**pag.19**)

(Parte CLIL)

7-Piano di indirizzamento (**pag.20>24**)

8-Configurazione interfacce (**pag.25>26**)

9-Configurazione tabelle di routing e protocolli DHCP e RIP (**pag.27>34**)

10-Configurazione VPN e funzione NAT(**pag.35>49**)

(Parte SISTEMI)

11-Internet of Things (**pag.50**)

12-Rilievo da sensori in rete locale con HTTP (**pag.51>58**)

(Parte TECNOLOGIA)

Scopo del progetto

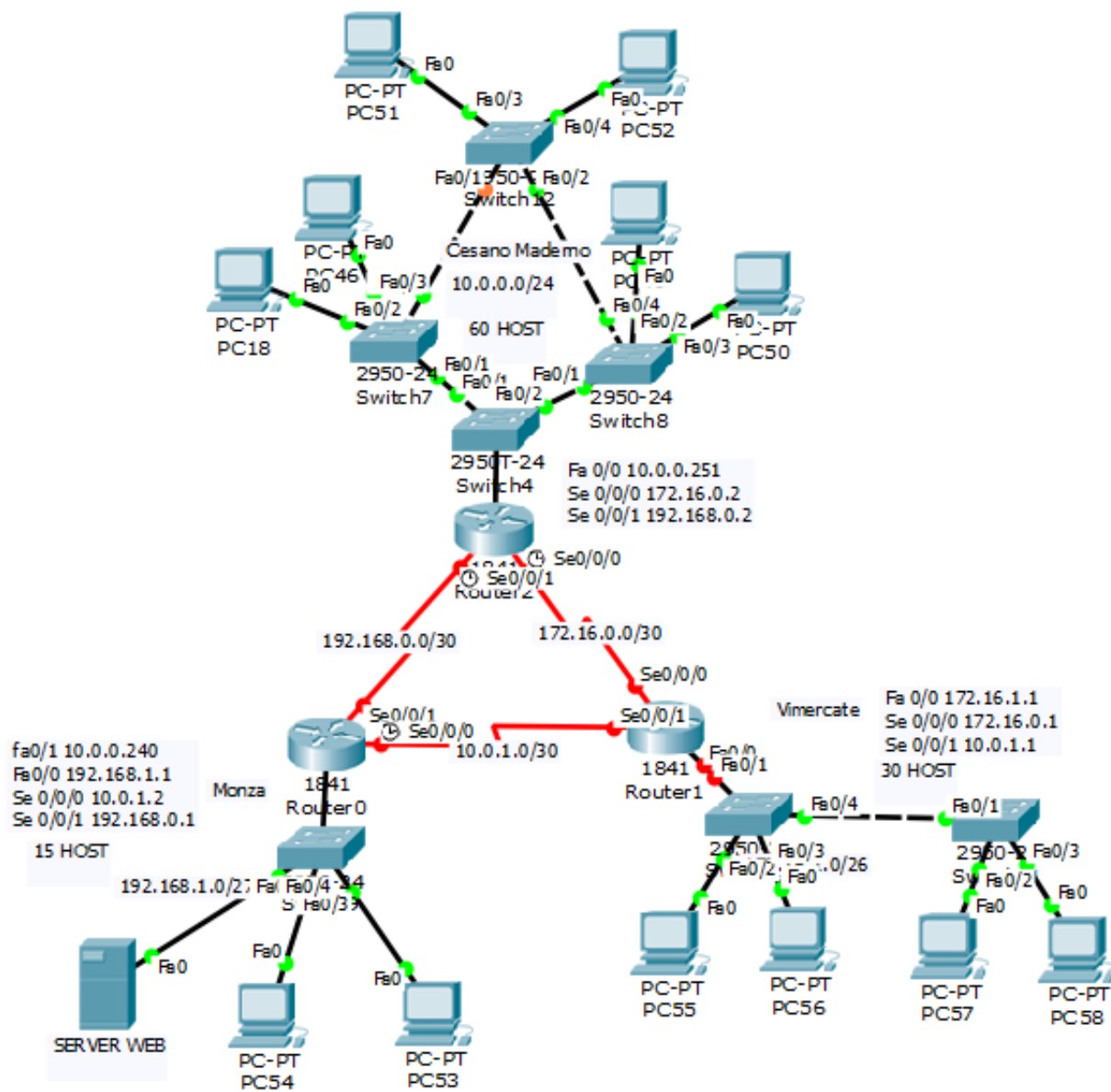
- Realizzare una rete Intranet aziendale, con 3 sedi collegate fra loro, Monza, Vimercate, Cesano .
- Assegnare a ciascuna rete il corretto blocco di indirizzi IP privati.
- Configurare le interfacce utilizzando le porte seriali Se 0/0/0 e Se 0/0/1 per le connessioni tra i router utilizzando cavi DTE-DCE.
- Configurazione delle tabelle di routing su ogni router in modo statico.
- Configurazione del protocollo RIP per la compilazione delle tabelle di routing in modo dinamico.
- Configurazione del protocollo DHCP disponibile sui router.
- Test di funzionamento della rete.
- Collegare un router con funzione di ISP(Internet Service Provider) al router di Monza.
- Instaurare un collegamento sicuro VPN tra una sede esterna e la rete Intranet.
- Configurare la funzione NAT.
- Verificare che dalla rete esterna sia possibile collegarsi al Server Web presente nella rete di Monza.

Strumenti utilizzati

- PC.
- Router Cisco 1841 (x3 intranet) (x2 rete esterna e ISP).
- Programma “ advanced subnet calculator” di Solarwinds.
- Programma CCP (Cisco Configure Professional).
- Emulatore di terminale GTKTerm.
- Client SSH Putty.
- Switch amministrabile 2950.
- Cavi DTE-DCE.
- Cavo console.
- Cavi ethernet.

Simulazione reti tramite Cisco Packet Tracer

-Rete intranet.



The diagram illustrates a network topology with three main sections:

- Rete edificio 2:** Contains a PC (PC-PT PC18) connected to a switch (2950-24 Switch3) via Fa0. The switch is connected to Router4 (1841) via Fa0/15. Router4 has a serial interface (Se0/0/0) connected to the ISP.
- rete ISP:** Contains Router ISP (1841) with serial interfaces (Se0/0/0 and Se0/0/1) connecting to the other two networks.
- COLLEGAMENTO INTERROTTO:** Contains Router Monza (1841) with a serial interface (Se0/0/1) connected to the ISP and a fast Ethernet interface (Fa0/0) connected to a switch (2950-24 Switch4). The switch is connected to a web server (SERVER WEB) via Fa0 and to two PCs (PC-PT PC6 and PC-PT PC2) via Fa0/12 and Fa0/4 respectively.

The red path indicates the connection from Router4 (Rete edificio 2) to Router Monza (COLLEGAMENTO INTERROTTO) via the ISP (rete ISP).

N.B: Per effettuare il collegamento con il router ISP è stato interrotto il collegamento seriale tra i router di Monza e Cesano, i quali potranno comunicare tramite il router di Vimercate.

Procedimento

-Il progetto consiste nella realizzazione di una di rete Intranet aziendale, con tre sedi, Monza, Vimercate e la sede principale di Cesano (rete del laboratorio), reti collegate tra loro da 3 router collegati a loro volta tramite cavi DTE-DCE, che simulano un collegamento punto a punto.

-Stabilire per ogni rete un piano di indirizzamenti, calcolando che nella sede di Cesano ci sono almeno 60 host, nella sede di Monza almeno 15 host e nella sede di Vimercate almeno 30 host.

-Una volta stabilito il piano di indirizzamento assegnare gli indirizzi a ciascuna interfaccia.

-Configurare i router assegnando gli indirizzi IP tramite la porta di servizio Fa0/1 e per quella di Cesano la Fa0/0, sono stati scelti i seguenti indirizzi:

- Router Monza: 10.0.0.240/24
- Router Vimercate: 10.0.0.241/24
- Router Cesano : 10.0.0.251/24

-Una volta configurati i router tramite cavo console è possibile accedervi tramite un altro computer in rete tramite il programma Putty (sempre a riga di comando), da dove sarà possibile configurare le interfacce di ciascuna rete. Utilizzeremo le porte Fa 0/1 come interfaccia di servizio, tranne per il router di Cesano che viene utilizzata la porta Fa 0/0.

Interfaccia di servizio Fa 0/1	Interfaccia di servizio Fa0/1	interfaccia di servizio Fa0/0
Ip 10.0.0.241/24	Ip 10.0.0.240/24	10.0.0.251
Vimercate	Monza	Cesano.

-In seguito configuriamo la tabella di routing di ciascun router in modo statico, e predisponiamo anche il protocollo RIP, per l'assegnazione in modo automatico delle route, in modo tale che come vedremo dopo quando la rete sarà modificata il protocollo RIP compili automaticamente le tabelle di routing, le Route sono configurabili o via riga di comando tramite porta console o putty, oppure tramite via grafica (GUI) tramite l'apposito programma CCP.

-Per il corretto funzionamento dei computer all'interno della rete si imposta su ogni router il protocollo DHCP, che assegna un indirizzo dinamico in automatico ai computer collegati all'interno di ogni rete, è anche possibile come nel nostro caso scegliere gli indirizzi da riservare ai computer.

-Una volta che la rete delle tre sedi è correttamente configurata e funzionante, si può procedere con la fase successiva del progetto, ovvero realizzare una simulazione di un collegamento tramite provider (ISP) simulandolo con un router, dove un altro edificio aziendale sarà connesso alla prima rete tramite un collegamento sicuro VPN. Configurabile tramite il programma Cisco CCP.

-Verificare in fine che si riesca a comunicare tramite le 2 reti, e che dalla rete esterna sia raggiungibile un server WEB presente nella rete di Monza.

Cenni Teorici

Programmi utilizzati

CCP: Cisco Configure Professional, è un programma free di Cisco il quale serve per la configurazione di router o altri apparecchiature Cisco tramite la GUI, via grafica, per noi l'utilizzo di questo programma servirà in seguito quando dovremo impostare il protocollo RIP o OSPF, sarebbe possibile anche impostare i comandi da noi eseguiti via riga di comando ma è stato scelto da noi di effettuare le configurazioni in questo modo.

Il programma è molto utile anche perché ogni volta che effettui un'operazione via grafica vengono sempre anche visualizzati i comandi che andrebbero inseriti via riga di comando (CLI).

Advanced subnet calculator: programma free di Solarwinds, scaricabile dal sito www.solarwinds.com/free-tools/advanced-subnet-calculator

molto utile per la creazione di piani di indirizzamento. Infatti tramite questo programma è possibile inserendo il blocco di indirizzi privati scelto e il numero di host voluti calcolare automaticamente gli indirizzi da assegnare agli host e la subnet mask.

E' molto utile anche la possibilità di esportare questi piani di indirizzamenti su fogli di calcolo, così da elaborare i dati forniti. Il programma assegna già in automatico il primo indirizzo alla subnet cioè alla rete stessa e l'ultimo indirizzo al broadcast.

Putty: Putty è un programma client SSH/Telnet per la configurazione remota a linea di comando di apparati molto semplice da utilizzare; inserendo da un qualsiasi pc in rete l'indirizzo del router da configurare e il metodo da utilizzare per la connessione, cioè SSH o telnet, sarà possibile entrare nel router; ovviamente per effettuare l'accesso sarà necessario inserire username e la password pre impostati sul router.

Le principali differenze tra SSH e telnet sono che il telnet non presenta nessun tipo di crittografia ed è più intercettabile, mentre il protocollo ssh è dotato di crittografia quindi rende la comunicazione molto più sicura.

GTKterm: questo programma è un emulatore di terminale che consente di entrare in configurazione di un router o uno switch cisco tramite il collegamento fisico via porta console e non via Ethernet.

Protocolli utilizzati

Protocollo IP: Un Internet Protocol (IP) è un protocollo di rete appartenente alla suite di protocolli TCP/IP su cui è basato il funzionamento della rete Internet.

È un protocollo di interconnessione di reti (Inter-Networking Protocol), classificato al livello di rete del modello ISO/OSI, nato per interconnettere reti eterogenee per tecnologia, prestazioni, gestione, pertanto implementato sopra altri protocolli di livello collegamento, come Ethernet.

È un protocollo a pacchetto senza connessione e di tipo best effort nel senso che fa il massimo di quello che può fare senza garantire alcuna forma di affidabilità della comunicazione in termini di controllo di errore, controllo di flusso e controllo di congestione, a cui quindi dovranno supplire i protocolli di trasporto di livello superiore (livello 4) quale ad esempio TCP. Quindi funziona in connection less.

La versione correntemente usata del protocollo IP, è detta anche IPv4 per distinguerla dalla più recente IPv6, nata dall'esigenza di gestire meglio il crescente numero di computer (host) connessi ad Internet. Il principale compito di IP è l'indirizzamento e l'instradamento (commutazione) tra sottoreti.

La definizione delle modalità o procedure (denominate routing) tese a individuare il percorso di rete per interconnettere due qualunque sottoreti, durante una comunicazione tra host sorgente di una certa sottorete e host destinatario di un'altra sottorete.

Attualmente vi sono due versioni del protocollo IP operative:

IPv4, che è il protocollo IP originario caratterizzato da indirizzi IPv4 a 32 bit, 2^{32} indirizzi;

IPv6, che è il protocollo IP caratterizzato da indirizzi IPv6 a 128 bit, 2^{128} indirizzi;

Il protocollo IP che risiede in tutti i dispositivi collegati in rete, decide l'instradamento dei pacchetti IP, cioè sceglie l'interfaccia di uscita su cui inoltrare i pacchetti IP in modo che siano instradati verso la rete IP di destinazione, consultando una tabella di routing.

Analizziamo un header IPv4 e un header IPv6:

IPv4 = di solito 20 Byte, versione (IPv4 o IPv6), ToS (da priorità a pacchetti di tipo VoIP o video), flags (per gestire eventuali frammentazioni), TTL (contatore che scende a ogni router, a 0 il pacchetto viene distrutto inviando un messaggio all'host mandante), chk (rilevazione d'errore), protocol number (identifica il protocollo dello strato superiore), ed infine gli indirizzi IP source address e destination address.

IPv6 = 40 Byte + header opzionali, più semplice in verità ma più pesante per la lunghezza dell'indirizzo stesso, contiene la versione (IPv4 o IPv6), traffic class (8 bit che danno la priorità ad un pacchetto), flow label (20 bit consente di instradare allo stesso modo pacchetti provenienti da sorgenti diverse sullo stesso percorso, velocizza l'instradamento), next header (8 bit indica protocollo dello strato superiore e eventuali header opzionali), hop limit (come il TTL IPv4).

Indirizzi IP privati si intendono alcune classi di indirizzi IPv4, riservate alle reti locali allo scopo di ridurre le richieste di indirizzi pubblici. Si dividono in varie classi a seconda delle esigenze.

Chiunque può utilizzare questi indirizzi per la propria rete locale, perché i pacchetti con tali indirizzi non vengono utilizzati per l'indirizzamento e instradamento tramite protocollo IP dai router Internet verso la rete di trasporto, ed il loro riutilizzo su altre reti locali, oltre a ridurre il numero di indirizzi IP utilizzati come da obiettivo originario, non genera conflitti con analoghi indirizzi posti su altre reti locali in quanto non visibili dall'esterno della sottorete locale risultando appunto privati e non indirizzi IP pubblici.

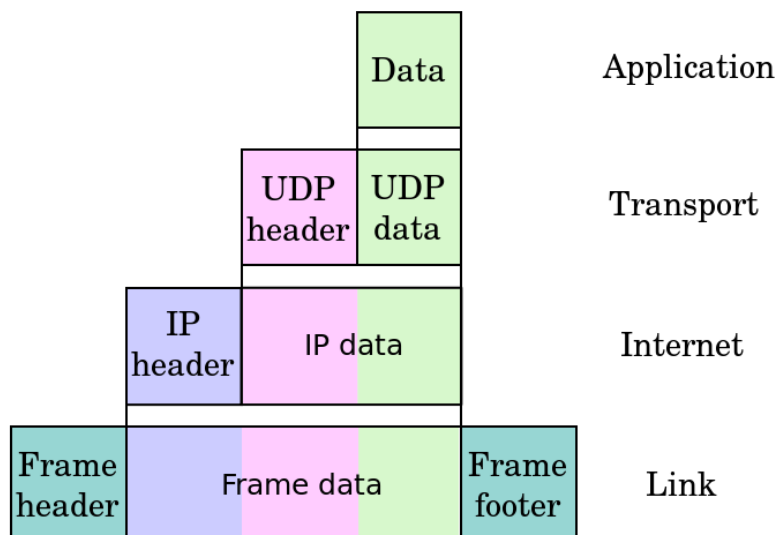
Nel caso occorra connettere ad Internet una rete locale che utilizza queste classi di indirizzi si deve perciò ricorrere al network address translation (PAT o NAT overload) il quale moltiplica (o mappa) più indirizzi IP privati su un solo indirizzo IP pubblico, visibile all'esterno della sottorete ed utilizzabile per l'instradamento.

L'idea di usare indirizzi IP privati nasce dall'esigenza di limitare l'uso di indirizzi IPv4 il cui numero è limitato a 2^{32} indirizzi (circa 4 miliardi) ed in via di esaurimento col crescere del numero degli host connessi in Rete ed allo spreco di indirizzi dovuto all'assegnazione di classi di indirizzi non pienamente utilizzate (saturazione di IPv4).

<u>Class</u>	<u>Address Range</u>	<u>Default Subnet Mask</u>
A	10.0.0.0 - 10.255.255.255	255.0.0.0
B	172.16.0.0 - 172.31.255.255	255.255.0.0
C	192.168.0.0 – 192.168.255.255	255.255.255.0

In seguito l'utilizzo di questo metodo a classi Classfull, è stato sostituito con il Classless, ovvero puoi utilizzare la maschera che preferisci.

Indirizzo IP pubblico è un indirizzo IP nello spazio di indirizzamento della rete internet che è allocato univocamente e potenzialmente accessibile da qualsiasi altro indirizzo IP pubblico cioè utilizzabile per l'indirizzamento e l'instradamento tramite protocollo IP. La distinzione tra indirizzi IP pubblici e privati è un concetto legato a IPv4, in quanto IPv6 non prevede un concetto di indirizzo IP privato analogo. Gli indirizzi IP pubblici sono rilasciati e regolamentati dall'ICANN tramite una serie di organizzazioni delegate. Tuttavia è da tener presente che a livello mondiale e nazionale i primi provider di connessione Internet si sono accaparrati un numero sproporzionato di indirizzi IP.



- schema di incapsulamento

Protocollo RIP: Routing Information Protocol (RIP) è un protocollo di routing di tipo Distance Vector, che impiega il numero di hop come metrica. RIP evita i routing loop adottando un limite massimo di hop dalla sorgente verso la destinazione. Il numero massimo di hop consentito è 15. Questo numero di hop limita in ogni caso il diametro della rete consentito da RIP. Un numero di hop equivalente a 16 viene considerato come metrica infinita per indicare le rotte inaccessibili che non verranno installate in tabella di routing.

In origine ogni router RIP inviava aggiornamenti completi ogni 30 secondi. A quel tempo le tabelle di routing erano ridotte e di conseguenza la banda impiegata per gli aggiornamenti. Con la crescita delle reti è risultato evidente che sarebbe potuto esserci un picco di traffico non indifferente ogni 30 secondi, anche nel caso in cui i router fossero avviati in maniera asincrona. Si credeva che, a fronte di un boot asincrono, gli updates di routing sarebbero stati differenziati nel tempo. Sally Floyd e Van Jacobson hanno dimostrato nel 1994 che, senza leggere variazioni dei timer di update, dopo un lasso di tempo i timer si sincronizzavano automaticamente.

Nella maggior parte degli scenari attuali, RIP non viene utilizzato come prima scelta poiché convergenza e scalabilità sono qualitativamente inferiori rispetto a EIGRP, OSPF o IS-IS (questi ultimi due sono protocolli link-state) e (senza RMTI) avere un limite di hop limita parecchio la dimensione di utilizzo della rete. Tuttavia RIP è facile da configurare a causa dei pochi parametri rispetto ad altri protocolli di routing. RIP utilizza UDP come protocollo di trasporto, sulla porta riservata 520.

Il protocollo RIP è un po' antiquato, la versione che utilizzeremo noi è la versione 2 (RIPv2).

Protocollo DHCP: Dynamic Host Configuration Protocol (DHCP) (protocollo di configurazione IP dinamica) è un protocollo di rete di livello applicativo che permette ai dispositivi o terminali di una certa rete locale di ricevere automaticamente a ogni richiesta di accesso a una rete IP (quale una LAN) la configurazione IP necessaria per stabilire una connessione e operare su una rete più ampia basata su Internet Protocol, cioè operare con tutte le altre sottoreti scambiandosi dati, purché anch'esse integrate allo stesso modo con il protocollo IP. Il protocollo è implementato come servizio di rete ovvero come tipologia di server: ad es. nei sistemi Unix e Unix-like è implementato nel demone dhcpd, in quelli basati su Active Directory di Microsoft e/o Windows Server dal servizio server dhcp.

Oppure come nel nostro caso il DHCP è fornito dal router, che assegna gli indirizzi in modo automatico agli host presenti nella sua rete, assegnando gli indirizzi tra quelli scelti dall'amministratore di rete come dedicati per gli host, in oltre il dhcp può assegnare degli indirizzi che rimangono poi salvati in modo statico assegnando ad un indirizzo IP l'indirizzo MAC di quello specifico host.

FUNZIONE NAT: il network address translation o NAT, ovvero traduzione degli indirizzi di rete, conosciuto anche come network masquerading, native address translation, è una tecnica che consiste nel modificare gli indirizzi IP dei pacchetti in transito su un sistema che agisce da router all'interno di una comunicazione tra due o più host.

Sono molto note anche alcune tipologie specifiche di NAT, come il NAT normale che associa un indirizzo pubblico a ciascun indirizzo privato, mentre il PAT o NAT overload associa un indirizzo pubblico a una rete IP, gli host si riconoscono tramite il numero di porta.

Tecnologie e strumenti utilizzati

VLAN: il termine VLAN (Virtual LAN) indica un insieme di tecnologie che permettono di segmentare il dominio di broadcast, che si crea in una rete locale (tipicamente IEEE 802.3) basata su switch, in più reti locali logicamente non comunicanti tra loro, ma che condividono globalmente la stessa infrastruttura fisica di rete locale.

Le applicazioni di questa tecnologia sono tipicamente legate ad esigenze di separare il traffico di gruppi di lavoro o dipartimenti di una azienda, per applicare diverse politiche di sicurezza informatica.

Sono quindi realizzabili come nel nostro caso tramite uno switch amministrabile.

VPN: In telecomunicazioni una VPN (virtual private network) è una rete di telecomunicazioni privata, instaurata tra soggetti che utilizzano, come infrastruttura di trasporto, un sistema di trasmissione pubblico e condiviso, come ad esempio la rete Internet.

Lo scopo delle reti VPN è quello di offrire alle aziende, a un costo inferiore, le stesse possibilità delle linee private in affitto, ma sfruttando reti condivise pubbliche: si può vedere dunque una VPN come l'estensione, a scala geografica, di una rete locale privata aziendale che colleghi tra loro siti interni all'azienda stessa variamente dislocati su un ampio territorio, sfruttando l'instradamento tramite IP per il trasporto su scala geografica e realizzando di fatto una rete LAN, detta appunto "virtuale" e "privata", logicamente del tutto equivalente a un'infrastruttura fisica di rete (ossia con collegamenti fisici) appositamente dedicata.

I collegamenti VPN operano la crittografia dei dati tramite il protocollo IPsec, abbreviazione di IP Security, è uno standard per reti a pacchetto che si prefigge di ottenere connessioni sicure su reti IP. La sicurezza viene raggiunta attraverso funzionalità di autenticazione, cifratura e controllo di integrità dei pacchetti IP (datagrammi). La capacità di fornire protezione o sicurezza viene fornita quindi a livello di rete il cui IP appartiene, e questo fatto rende questo protocollo trasparente al livello delle applicazioni che non devono quindi essere modificate.

Ci sono diversi tipi di VPN; noi utilizzeremo il Site to Site, che consiste nel creare un collegamento sicuro da una rete ad un'altra (nel nostro caso) anche via internet, quindi il collegamento viene instaurato via software.

Server WEB: In informatica un server web (o web server) è un'applicazione software che, in esecuzione su un server, è in grado di gestire le richieste di trasferimento di pagine web di un client, tipicamente un web browser. La comunicazione tra server e client avviene tramite il protocollo HTTP, che utilizza di default la porta TCP 80, o eventualmente la versione sicura HTTPS, che utilizza invece la 443. L'insieme di tutti i web server interconnessi a livello mondiale dà vita al World Wide Web.

Teoricamente un qualsiasi dispositivo per cui sia disponibile qualche software che agisca come server web può diventare un server web, ma solitamente i dispositivi che ospitano server web sono sistemi hardware dedicati e ottimizzati a tale scopo. Ad esempio si può installare un server web su un normale PC allo scopo di testare in locale un insieme di pagine web oppure per consentire l'accesso ai propri documenti da altri client host, sia in rete locale, sia via Internet, come nel nostro caso.

Router: apparati ottimizzati nell'hardware e nel software per l'interconnessione di reti private e pubbliche. Un instradatore (dall'inglese router) è un dispositivo elettronico che, in una rete informatica a commutazione di pacchetto, si occupa di instradare i dati, suddivisi in pacchetti, fra reti diverse. È quindi, a livello logico, un nodo interno di rete deputato alla commutazione di livello 3 del modello OSI o del livello internet nel modello TCP/IP. L'instradamento può avvenire verso reti direttamente connesse, su interfacce fisiche distinte, oppure verso altre sottoreti non limitrofe che, grazie alle informazioni contenute nelle tabelle di instradamento, siano raggiungibili attraverso altri nodi della rete

Ovviamente i processi di elaborazione per l'indirizzamento e l'instradamento introducono dei ritardi aggiuntivi sulla linea di uscita come del resto in tutti i tipi di commutatori e apparati di rete.

Attualmente vi sono due versioni del protocollo IP operative:

IPv4, che è il protocollo IP originario caratterizzato da indirizzi IPv4 a 32 bit;

IPv6, che è il protocollo IP caratterizzato da indirizzi IPv6 a 128 bit;

Il protocollo IP che risiede in tutti i dispositivi collegati in rete, decide l'instradamento dei pacchetti IP, cioè sceglie l'interfaccia di uscita su cui inoltrare i pacchetti IP in modo che siano instradati verso la rete IP di destinazione, consultando una tabella di routing.

Una tabella di routing è considerabile come una tabella di n righe ed m colonne, in cui in ogni riga viene denominata route in quanto fornisce le informazioni necessarie per inoltrare dei pacchetti IP verso una certa rete IP di destinazione.

Le informazioni contenute in una tabella di routing sono:

- **Indirizzo IP della rete di destinazione;**
- **Subnet mask**, che permette di determinare il prefisso di rete associato all'indirizzo IP di destinazione.
- **Next hop (Gateway)**, indirizzo IP a cui va inoltrato un pacchetto IP affinché possa raggiungere la rete IP di destinazione specificata in quella route.
- **Metrica (distanza amministrativa)**, è un numero che consente di stabilire delle priorità nel caso in cui vi siano rotte che portano verso una stessa destinazione (va però detto che la metrica e la distanza amministrativa sono in verità due cose diverse, infatti la metrica consente di scegliere la route migliore offerta da un protocollo di routing, mentre la distanza amministrativa consente di scegliere la route migliore tra quelle offerte dalle varie sorgenti di routing) .

La decisione di instradamento dei pacchetti IP viene fatta dal protocollo IP di un dispositivo leggendo l'indirizzo IP di destinazione contenuto nell'header dei pacchetti IP da instradare, determinando la rete IP di destinazione e ricercando nella tabella di routing le informazioni necessarie per poter inoltrare i pacchetti verso la rete di destinazione.

Quando un dispositivo collegato in rete deve instradare dei pacchetti IP e non trova nella propria tabella di routing una route specifica verso la loro rete di destinazione, allora invia quei pacchetti all'indirizzo IP indicato come next hop nella default route e che costituisce il gateway predefinito.

I Router costituiscono i nodi a commutazione di pacchetto che interconnettono fra loro reti e sottoreti IP. Il loro compito principale è quello di decidere l'instradamento dei pacchetti IP che ricevono in ingresso e il loro inoltramento sull'interfaccia di uscita collegata al link che porta verso la rete IP a cui appartiene l'host di destinazione.

Quindi un router effettua l'inoltro (forwarding) dei pacchetti scegliendo nella tabella di routing il percorso migliore, cioè quello con metrica inferiore, tramite cui raggiungere la rete di destinazione.

Hardware di un router: CPU, RAM, NVRAM (contiene i file di configurazione), Flash (fa le veci dell'hard disk e contiene il S.O), ROM (contiene il firmware per l'avvio del router), bus di interconnessione, interfacce e porte integrate, slot di espansione per ulteriori interfacce ecc.

Firmware: programma avvio (bootstrap), programmi di diagnostica all'avvio (POST, Power On Self Test) ecc.

Da un punto di vista funzionale le porte/interfacce possono essere distinte in:

Porte di ingresso, che ricevono e controllano i frame in ingresso, estraendo da essi i pacchetti IP,

Porte di uscita, che incapsulano i pacchetti IP negli opportuni frame del protocollo di linea impiegato su quel link, inserendo gli eventuali indirizzi di livello 2;

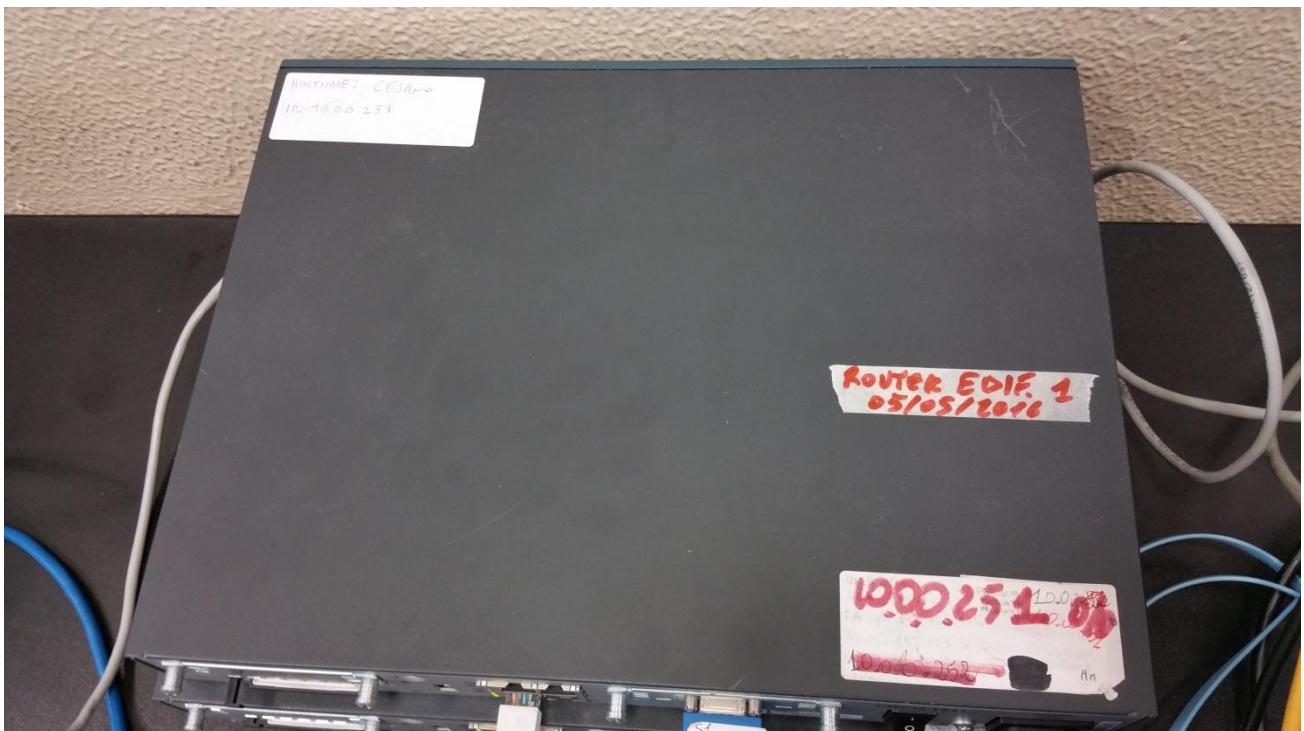
A seconda degli impieghi e dei requisiti i router possono essere così classificati:

Access router: impiegati nella rete di accesso, cioè nelle connessioni tra utenti residenziali, uffici, piccole aziende e ISP; nei router di accesso possono essere attivate le funzioni firewall, per proteggere una rete contro accessi indesiderati, e NAT.

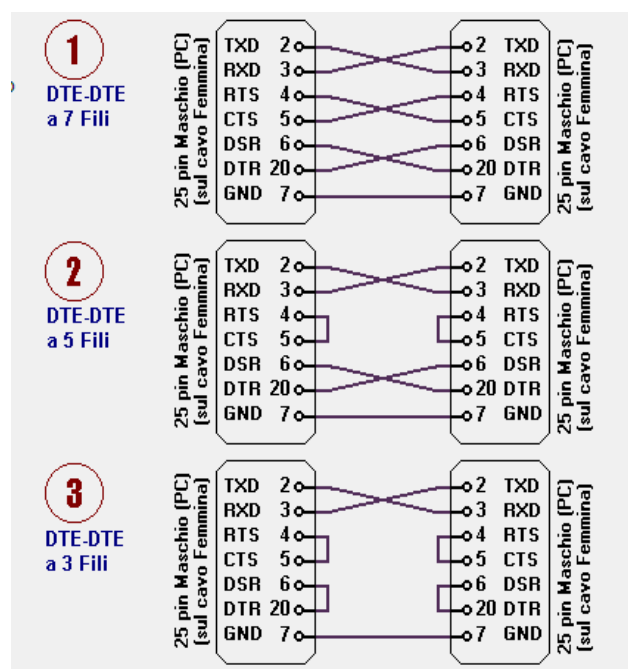
Enterprise router: sono impiegati per realizzare reti IP in aziende medio-grandi e nelle reti di campus; i router utilizzati esclusivamente all'interno di reti private sono spesso sostituiti da layer 3 switch in quanto questi ultimi sono ottimizzati per realizzare reti private anche di grandi dimensioni.

Backbone router: sono impiegati per interconnettere varie reti IP e per realizzare le grandi reti IP multiservizio che costituiscono i backbone IP degli operatori delle telecomunicazioni.

I router, e più in generale i dispositivi che implementano il protocollo IP, inseriscono automaticamente nella loro tabella di routing le route verso le reti IP direttamente connesse alle loro interfacce, in quanto i loro parametri sono ricavabili dalla configurazione delle interfacce stesse. Per le reti non direttamente connesse è invece necessario provvedere alla compilazione e all'aggiornamento delle tabelle di routing.



Cavi DTE-DCE:



-Parlando di piedinatura, il Cavo DTE è "dritto" ovvero manda Tx su Tx ed Rx su Rx, mentre il cavo DCE li inverte, quindi quando li vai a collegare insieme puoi comunicare. Noi li utilizziamo per simulare il collegamento a lunga distanza da sede a sede, va ricordato che con questi cavi dal lato DCE va impostata la velocità di clock sulle interfacce necessarie.

Switch amministrabile: Nella tecnologia delle reti informatiche, uno switch (inglese 'switch'; commutatore) è un dispositivo di rete che si occupa di commutazione a livello datalink (collegamento) del modello ISO/OSI. Lo switch agisce sull'indirizzamento e sull'instradamento all'interno delle reti LAN mediante l'indirizzo fisico (MAC), selezionando i frame ricevuti e dirigendoli verso il dispositivo corretto (leggendo l'indirizzo MAC di destinazione). L'instradamento avviene per mezzo di una corrispondenza univoca porta-indirizzo.

Lo switch ha un comportamento analogo a quello del bridge, mentre si differenzia dal router che opera a livello 3 (internetworking), mettendo in comunicazione più reti locali attraverso il protocollo IP, e dall'hub che invece è solamente un ripetitore multiporta di strato fisico ovvero diffusivo senza indirizzamento. L'instradamento attraverso switch è in grado di ridurre il dominio di collisione presente nelle reti locali broadcast in maniera più efficiente ed efficace rispetto al bridge.

Per decidere su quale porta inoltrare un frame ricevuto, uno switch deve possedere una funzione di instradamento. Questa è basata sull'apprendimento passivo progressivo degli indirizzi MAC sorgente contenuti nei frame inoltrati che lo switch associa univocamente alla rispettiva porta di provenienza: questa associazione porta-indirizzo viene poi memorizzata in una tabella di instradamento di livello 2 chiamata tabella di switching o forwarding database. Gli indirizzi appresi e memorizzati nella tabella vengono "dimenticati" dopo un certo tempo dalla loro ultima apparizione per motivi di scalabilità e flessibilità con eventuale variazione del numero e della posizione nella rete dei terminali utenti..

-Esistono 3 metodologie di instradamento che possono essere utilizzate da uno switch:

- cut-through
- store-and-forward
- fragment-free

Nella prima tipologia lo switch si limita a leggere l'indirizzo MAC del destinatario e quindi manda il contenuto del frame contemporaneamente alla sua lettura. In questo caso l'invio dei frame non attende la ricezione completa dello stesso. Questo tipo di switch è quello con latenza minore.

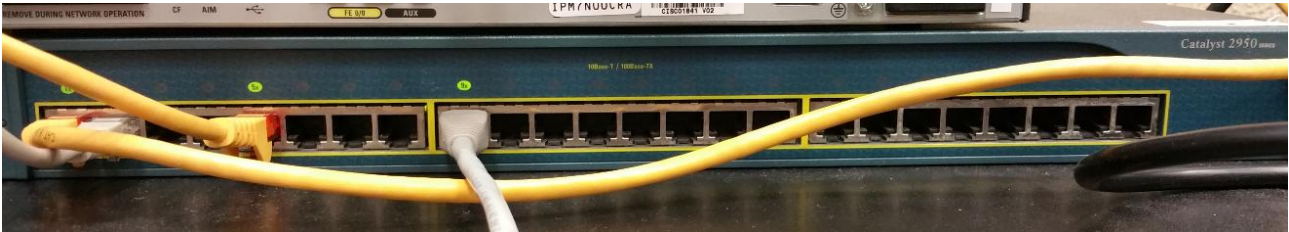
Negli switch store-and-forward invece viene letto l'intero frame e ne viene calcolato il cyclic redundancy check (CRC) confrontandolo con il campo FCS all'interno del frame. Solo se i due valori corrispondono il frame viene mandato al destinatario, altrimenti non viene trasmesso. Questi tipi di switch consentono di bloccare frame contenenti errori ma hanno una latenza maggiore.

L'ultima tipologia è un compromesso tra le due precedenti in quanto si leggono i primi 64 bytes del frame in modo da rilevare solo alcune anomalie nel frame.

Gli switch fragment-free e cut-through possono essere impiegati solamente nello switching simmetrico ovvero dove trasmettitore e ricevitore operano alla stessa velocità, gli switch store-and-forward invece consentono anche lo switching asimmetrico.

Tramite uno switch amministrabile i vari parametri possono essere modificati e configurati dall'utente, cosa che non è possibile sugli switch non amministrabili che sono pre configurati, è inoltre possibile realizzare delle **VLAN**(virtual local area network), dove all'interno di una stessa rete si creano più sotto reti a livello software, tramite appunto lo switch amministrabile.

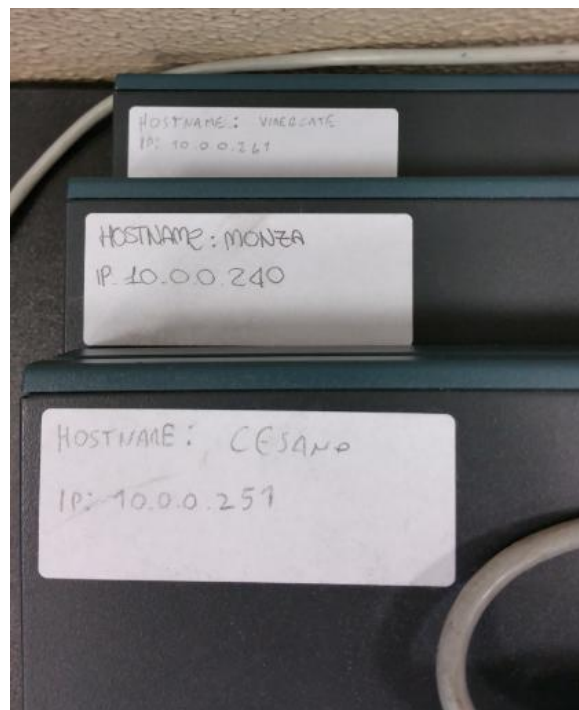
Switch



Router



I nostri router, Monza, Cesano, Vimercate



Subnetting

Subnetting reduces overall network traffic and improves network performance. It also enables an administrator to implement security policies such as which subnets are allowed or not allowed to communicate together.

There are various ways of using subnets to help manage network devices. Network administrators can group devices and services into subnets that are determined by:

Location, such as floors in a building

Organizational unit

Device type

Any other division that makes sense for the network.

Every interface on a router is connected to a network. The IP address and subnet mask configured on the router interface are used to identify the specific broadcast domain. Recall that the prefix length and the subnet mask are different ways of identifying the network portion of an address.

Subnet Mask	Binary	CIDR	Subnets	Hosts
255.255.255.255	11111111. 11111111. 11111111. 11111111	/32	n/a	n/a
255.255.255.254	11111111. 11111111. 11111111. 11111110	/31	n/a	n/a
255.255.255.252	11111111. 11111111. 11111111. 11111100	/30	64	2
255.255.255.248	11111111. 11111111. 11111111. 11111000	/29	32	6
255.255.255.240	11111111. 11111111. 11111111. 11110000	/28	16	14
255.255.255.224	11111111. 11111111. 11111111. 11100000	/27	8	30
255.255.255.192	11111111. 11111111. 11111111. 11000000	/26	4	62
255.255.255.128	11111111. 11111111. 11111111. 10000000	/25	2	126
255.255.255.0	11111111. 11111111. 11111111. 00000000	/24	1	254

To calculate the number of hosts that can be supported, use the formula 2^n (where the n is the number of 0 in the subnet mask address), There are two subnet addresses that cannot be assigned to a host, the network address and the broadcast address, so we must subtract 2.

For example If there are 7 zeroes at the end of the bits of the mask, so the calculation is $2^7 = 128 - 2 = 126$. This means that each of the subnets has 126 valid host addresses.

There are two type of subnetting, classless and classfull, classless is a more recent method and you can use all available masks, while in the clasfull you could only use predetermined blocks. It's passed to the classless to get more free addresses available.

Piano di indirizzamento

Calcoli piano di indirizzamento

E' stato contato che all'interno del laboratorio di **Cesano** sono presenti 8 computer, un router che funziona anche da firewall, due switch, 1 server stampa e 1 server dns, 1 server ftp, 1 server asterik ed un server web, mentre gli indirizzi IP degli switch router e server devono per forza essere statici affinché gli host possano sempre trovarli, gli indirizzi per i pc sono forniti in automatico da un server DHCP, che però alle 8 macchine fisse in laboratorio è stato assegnato un indirizzo statico, cioè una volta che l'ha assegnato lo tiene in memoria, associandoci un indirizzo MAC di ciascuna macchina.

Abbiamo quindi calcolato che almeno 60 indirizzi liberi servono all'interno della rete, lasciando eventualmente qualche indirizzo libero per eventuali connessioni occasionali da parte di altri dispositivi. Quindi :

$2^6 - 2 = 62$ host disponibili, quindi l'indirizzo di rete sarà 10.0.0.0 e una subnet Mask di 255.255.255.192

Con l'indirizzo 10.0.0.0 riservato alla subnet stessa e il 10.0.0.63 riservato al broadcast.

Tuttavia abbiamo deciso che trattandosi di un laboratorio dove possono essere eseguiti numerosi test o prove, la maschera 255.255.255.192 lascia liberi troppi pochi host, così è stato scelto di lasciare una maschera di 255.255.255.0 in modo che sia disponibili molti indirizzi liberi per eventuali prove. Quindi con il seguente piano di indirizzamento :

IP	Mask	Notes ...	
10.0.0.0	255.255.255.0	Subnet Address	
10.0.0.1	255.255.255.0		
10.0.0.2	255.255.255.0		
10.0.0.3	255.255.255.0		
10.0.0.4	255.255.255.0		
10.0.0.5	255.255.255.0		

.....

10.0.0.249	255.255.255.0		
10.0.0.250	255.255.255.0		
10.0.0.251	255.255.255.0	interfaccia Fa 0/0	
10.0.0.252	255.255.255.0		
10.0.0.253	255.255.255.0		
10.0.0.254	255.255.255.0		
10.0.0.255	255.255.255.0	Broadcast Address	

Avendo così ben 256 indirizzi, calcolando che il 10.0.0.251, 10.0.0.240, 10.0.0.241 sono riservati per le interfacce di configurazione dei router.

Tramite il **programma Advanced subnet** calculator inserendo l'indirizzo di rete e scegliendo la maschera tra quelle esistenti è possibile visualizzare ogni indirizzo IP, oppure tramite un'altra funzione siamo in grado di trovare la maschera inserendo il numero di host desiderati o viceversa.

Address Details

Classful Subnet Calculator

CIDR Calculator


Subnet Addresses

IP Address


10.0.0.0

Subnet Mask

255.255.255.192



Generate Addresses



Copy

IP	Mask	Notes ...
10.0.0.0	255.255.255.192	Subnet Address
10.0.0.1	255.255.255.192	
10.0.0.2	255.255.255.192	
10.0.0.3	255.255.255.192	
10.0.0.4	255.255.255.192	
10.0.0.5	255.255.255.192	
10.0.0.6	255.255.255.192	
10.0.0.7	255.255.255.192	
10.0.0.8	255.255.255.192	
10.0.0.9	255.255.255.192	
10.0.0.10	255.255.255.192	
10.0.0.11	255.255.255.192	
10.0.0.12	255.255.255.192	
10.0.0.13	255.255.255.192	
10.0.0.14	255.255.255.192	
10.0.0.15	255.255.255.192	
10.0.0.16	255.255.255.192	

.....

10.0.0.58	255.255.255.192	
10.0.0.59	255.255.255.192	
10.0.0.60	255.255.255.192	
10.0.0.61	255.255.255.192	
10.0.0.62	255.255.255.192	
10.0.0.63	255.255.255.192	Broadcast Address

- Questo programma assegna già in modo automatico l'indirizzo di broadcast e di rete, è possibile tramite l'apposito comando copiare gli indirizzi e incollarli all'interno di un foglio di calcolo (come vedremo più avanti) in modo da poter assegnare gli indirizzi a nostro piacimento o elaborare i dati.
- Ora stabiliamo il piano di indirizzamento per le reti di **Monza e Vimercate**, possiamo calcolarle facilmente tramite il programma Advanced subnet Calculator, che calcola in automatico il piano di indirizzamenti:

Vimercate		
IP	Mask	Notes ...
172.16.1.0	255.255.255.192	Subnet Address
172.16.1.1	255.255.255.192	Gateway Fa 0/0
172.16.1.2	255.255.255.192	
172.16.1.3	255.255.255.192	
172.16.1.4	255.255.255.192	
172.16.1.5	255.255.255.192	
172.16.1.6	255.255.255.192	
172.16.1.7	255.255.255.192	
172.16.1.8	255.255.255.192	
172.16.1.9	255.255.255.192	

.....

172.16.1.49	255.255.255.192	
172.16.1.50	255.255.255.192	
172.16.1.51	255.255.255.192	
172.16.1.52	255.255.255.192	
172.16.1.53	255.255.255.192	
172.16.1.54	255.255.255.192	
172.16.1.55	255.255.255.192	
172.16.1.56	255.255.255.192	
172.16.1.57	255.255.255.192	
172.16.1.58	255.255.255.192	
172.16.1.59	255.255.255.192	
172.16.1.60	255.255.255.192	
172.16.1.61	255.255.255.192	
172.16.1.62	255.255.255.192	
172.16.1.63	255.255.255.192	Broadcast Address

IP	Mask	Notes ...
192.168.1.0	255.255.255.224	Subnet Address
192.168.1.1	255.255.255.224	gateway Fa0/0
192.168.1.2	255.255.255.224	
192.168.1.3	255.255.255.224	
192.168.1.4	255.255.255.224	
192.168.1.5	255.255.255.224	
192.168.1.6	255.255.255.224	
192.168.1.7	255.255.255.224	
192.168.1.8	255.255.255.224	
192.168.1.9	255.255.255.224	
192.168.1.10	255.255.255.224	
192.168.1.11	255.255.255.224	
192.168.1.12	255.255.255.224	
192.168.1.13	255.255.255.224	
192.168.1.14	255.255.255.224	
192.168.1.15	255.255.255.224	
192.168.1.16	255.255.255.224	
192.168.1.17	255.255.255.224	
192.168.1.18	255.255.255.224	
192.168.1.19	255.255.255.224	
192.168.1.20	255.255.255.224	
192.168.1.21	255.255.255.224	
192.168.1.22	255.255.255.224	
192.168.1.23	255.255.255.224	
192.168.1.24	255.255.255.224	
192.168.1.25	255.255.255.224	
192.168.1.26	255.255.255.224	
192.168.1.27	255.255.255.224	
192.168.1.28	255.255.255.224	
192.168.1.29	255.255.255.224	
192.168.1.30	255.255.255.224	
192.168.1.31	255.255.255.224	Broadcast Address

- Alla pagina successiva possiamo notare le 3 reti delle sedi, cesano in alto, rispettivamente Monza e Vimercate in basso, possiamo poi notare i vari blocchi di indirizzi e le interfacce utilizzate, da notare anche tutte le reti presenti, non solo quelle delle sedi ma anche quelle tra i collegamenti da router a router, in totale abbiamo quindi 6 sotto reti.

-Vediamo ora gli indirizzi assegnati alle interfacce tra i collegamenti router – router.

Vimercate-Monza		
IP	Mask	Notes ...
10.0.1.0	255.255.255.252	Subnet Address
10.0.1.1	255.255.255.252	Serial 0/0/1 vimercate
10.0.1.2	255.255.255.252	Serial 0/0/0 Monza Dce
10.0.1.3	255.255.255.252	Broadcast Address

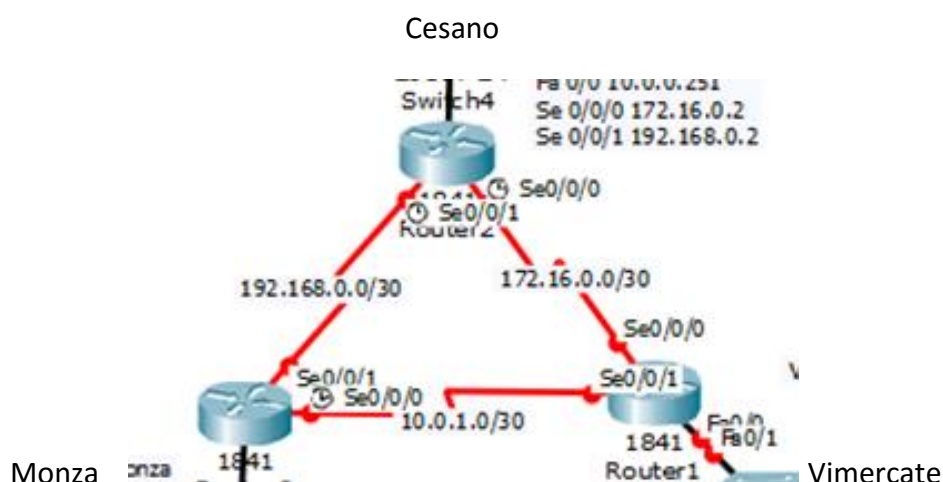
Vimercate – Cesano		
IP	Mask	Notes ...
172.16.0.0	255.255.255.252	Subnet Address
172.16.0.1	255.255.255.252	Serial 0/0/0 Vimercate
172.16.0.2	255.255.255.252	Serial 0/0/0 Cesano DCE
172.16.0.3	255.255.255.252	Broadcast Address

Monza-Cesano		
IP	Mask	Notes ...
192.168.0.0	255.255.255.252	Subnet Address
192.168.0.1	255.255.255.252	Monza Se 0/0/1
192.168.0.2	255.255.255.252	Cesano Se 0/0/1 Dce
192.168.0.3	255.255.255.252	Broadcast Address

-Dove a fianco all'interfaccia è segnato il "Dce" sarà l'interfaccia su cui andrà impostata la velocità di clock tramite il comando: **clock rate 115200**

-Nelle tabelle sopra riportate possiamo vedere anche gli indirizzi assegnati a ciascuna interfaccia, gli indirizzi di rete e gli indirizzi di broadcast, oppure possiamo vedere gli indirizzi liberi da assegnare agli host.

-Sempre prestando attenzione alle interfacce su cui andrà impostata la velocità di **clock DCE**.



Configurazione interfacce

-Una volta stabilito il piano di indirizzamento completo bisognerà configurare ciascun router e le sue interfacce nel seguente modo:

```
monza#conf t
Enter configuration commands, one per line. End with CNTL/Z.
monza(config)#interface Fa0/0
monza(config-if)#ip address 192.168.1.1
% Incomplete command.

monza(config-if)#ip address 192.168.1.1 255.255.255.224
monza(config-if)#no shu
monza(config-if)#description interfaccia rete di Monza
monza(config-if)#exit
monza(config)#interface Se0/0/0
monza(config-if)#ip address 10.0.1.2 255.255.255.252
monza(config-if)#clock rate 115200
monza(config-if)#no shu
monza(config-if)#exit
monza(config)#interface Se0/0/1
monza(config-if)#ip address 192.168.0.1 255.255.255.252
monza(config-if)#no shu
monza(config-if)#exit
```

-Per verificare che il router non sia configurato collegandolo tramite porta console , bisogna come prima cosa entrare in configurazione e creare un account(per la sicurezza del router) una volta creato (facendo attenzione alla password e allo username) sarà possibile impostare l'indirizzo IP di riferimento e configurare le interfacce, vediamo i comandi utilizzati:

- >ena \ per entrare in modalità privilegiata, ovvero dove si effettua la configurazione.
- # show run \ serve per visualizzare la configurazione di fabbrica.
- #conf t \ si entrerà in modalità di configurazione.
- #hostname cesano \ impostiamo l'hostname
- #username docente privilege 15 secret docente \ impostiamo username e password (docente)
- #interface Fa0/1 \ entriamo nell'interfaccia Fa0/1
- #IP address 10.0.0.251 255.255.255.0 \impostiamo l'indirizzo IP assegnato all'interfaccia
- #no shutdown \ effettua l'attivazione dell'interfaccia di rete

- **#exit** \ uscita dall'interfaccia

-Questo procedimento va effettuato per ogni interfaccia di ogni router che verrà collegata alla rete, cioè per le **Fa 0/0 Fa0/1** e le seriali **Se0/0/0 Se0/0/1**

-Vanno aggiunti in seguito dei comandi da effettuare sul router per abilitare l'accesso tramite via grafica (GUI)

- **#IP http authentication local**

- Per consentire l'accesso anche da console solo tramite username e password:

- **#line con 0**

- **#login local**

- **#exit**

- Per consentire l'accesso tramite ssh e telnet

- **#line vty 0 15**

- **#login local**

- **#transport input telnet ssh**

- **#end**

-Una volta finita la configurazione bisogna assolutamente ricordarsi di salvare i cambiamenti nella startup config (NVRAM), altrimenti i dati inseriti andranno persi al riavvio, visto che la running configuration, cioè la configurazione corrente viene cancellata ad ogni riavvio .

- **#Copy run start** \ ed in seguito premere invio per la conferma.

-Per la connessione da remoto ai router possiamo utilizzare il programma **putty** sapendo l'indirizzo IP l'username e la password, sempre utilizzando telnet o ssh via riga di comando(CLI). Mentre se si vuole utilizzare l'interfaccia grafica (GUI) si può utilizzare il programma Cisco Configuration Professional. Se invece un router è privo di un indirizzo IP, cioè non è ancora stata configurata una porta di servizio sulla quale collegarsi per la configurazione sarà necessario collegarsi tramite la porta console, utilizzando il programma **GTKterm**, che permette la configurazione diretta del router tramite la porta console. Da lì, poi, si creerà un account come abbiamo precedentemente visto impostando un indirizzo IP che darà l'accesso tramite putty.

Configurazione tabelle di routing

Configuriamo ora le tabelle di routing di ciascun router in modo statico, ovvero dobbiamo indicare i percorsi tramite il “**next hop**”, quindi sono i percorsi che i router dovranno tenere in considerazione per raggiungere le reti che non sono direttamente collegate a ciascuno di essi.

-Vediamo ora la configurazione di una route tramite riga di comando, è possibile farlo o tramite il programma GTKterm (LINUX), TeraTerm (Windows) ecc.. via console, o tramite Putty ,oppure via grafica tramite il programma CCP.

Noi abbiamo scelto di configurare le route via riga di comando:

-Prima di tutto collegarsi al router interessato, se necessario entrare in modalità privilegiata tramite il comando “ **> enable** ”.

-Ora entriamo in modalità di configurazione con il comando “ **#configure terminal** ”.

-ora che siamo in modalità di configurazione possiamo inserire le nostre route, proponiamo una route di esempio **#ip route 172.16.0.0 255.255.255.252 10.0.1.1 1**

- dove il primo è l’indirizzo della rete di destinazione seguito dalla sua maschera, 10.0.1.1è il Next hop, cioè l’indirizzo dell’interfaccia su cui il router dovrà instradare per raggiungere la rete con l’indirizzo precedente. L’ultimo valore 1, rappresenta la metrica, ovvero la precedenza che ha una route, infatti viene scelta sempre la route con la metrica minore, le route statiche di solito se non viene specificata la metrica come nel nostro caso è sempre 1, quindi ha la precedenza rispetto al protocollo rip che ha una metrica più elevata.

-una volta inserite le route si esegue il comando **#end** per uscire dalla modalità di configurazione ed è molto importante ricordarsi di salvare le modifiche nella startup configuration, tramite il comando **#copy run start** così in caso di riavvio del router le modifiche non vanno perse.

-Vediamo ora le route che sono state impostate da noi in modo statico:

Router di Monza:

```
User Access Verification
Username: docente
Password:
monza#ena
monza#conf t
Enter configuration commands, one per line. End with CNTL/Z.
monza(config)#ip route 172.16.0.0 255.255.255.252 10.0.1.1
monza(config)#ip route 172.16.1.0 255.255.255.192 10.0.1.2
monza(config)#ip route 10.0.0.0 255.255.255.0 192.168.0.1
monza(config)#end
monza#
*Jan  1 01:39:39.403: %SYS-5-CONFIG_I: Configured from console by docente on console
monza#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
monza#
monza#
```

Negli altri 2 router sono stati inserite le seguenti route:

Cesano

```
ip route 10.0.1.0 255.255.255.252 192.168.0.1
ip route 172.16.1.0 255.255.255.192 172.16.0.1
ip route 192.168.1.0 255.255.255.224 192.168.0.1
```

Vimercate

```
ip route 10.0.0.0 255.255.255.0 172.16.0.2 222
ip route 192.168.0.0 255.255.255.252 172.16.0.2 222
ip route 192.168.1.0 255.255.255.224 10.0.1.2 222
```

-Le tabelle di routing possono essere visualizzate tramite il comando “**show IP route**”.

-Inserendo le route bisogna prestare attenzione, nel caso si sbagli a inserire una route il programma lo segnala,

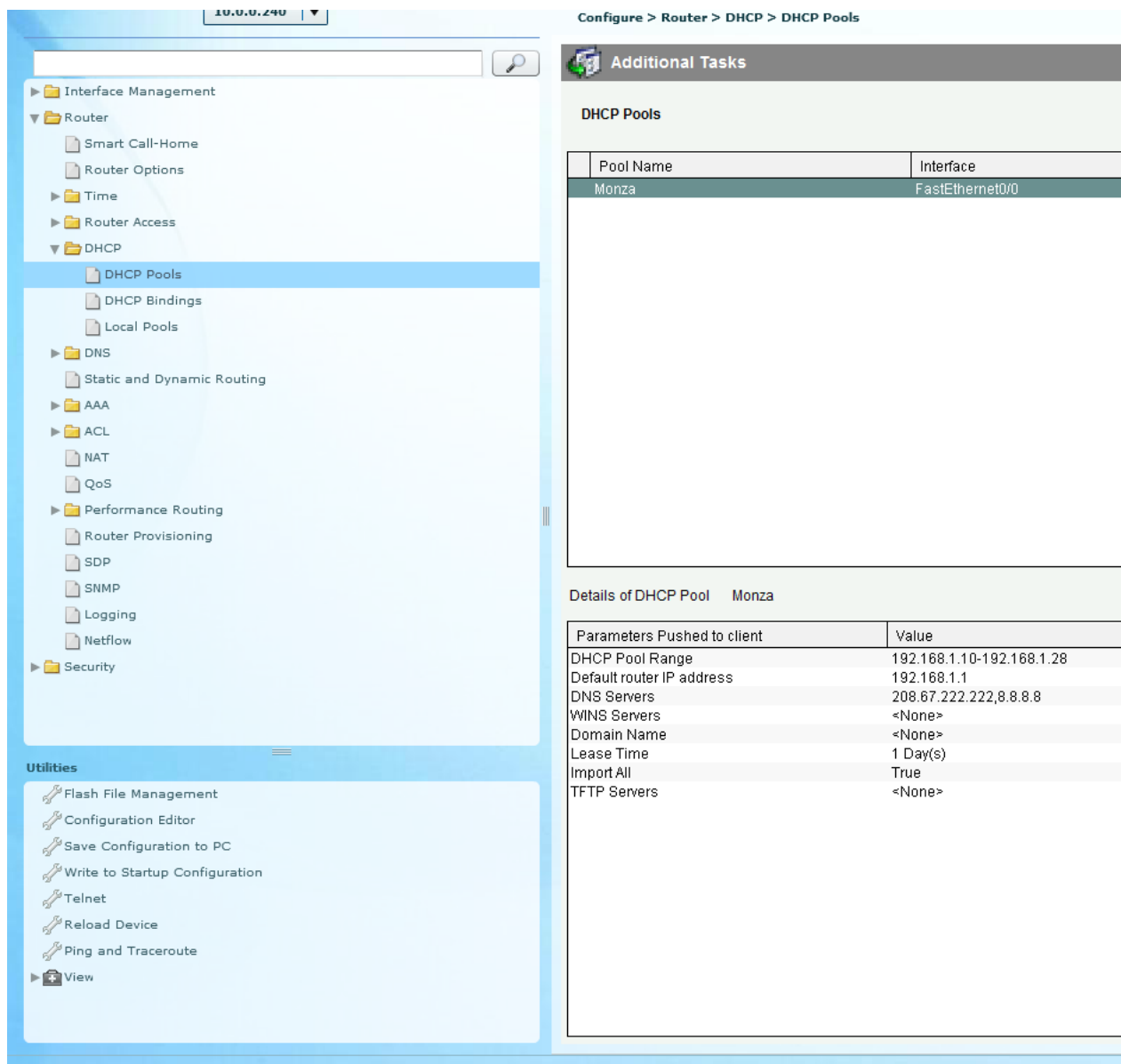
```
router-251-cesano(config)#ip route 172.16.1.0 255.255.255.192 172.16.0.2
%Invalid next hop address (it's this router)
```

Tuttavia la route viene inserita ugualmente, dovrà essere dunque cancellata per il corretto funzionamento della rete.

-Una volta compilate tutte le tabelle di routing, verifichiamo tramite un ping se i router sono stati configurati correttamente e sono in grado di scambiarsi pacchetti IP. Per fare questo abbiamo collegato dei computer su ciascuna rete, e abbiamo provato a effettuare il ping da un computer di una rete a un computer di un'altra, per fare questo era necessario che i computer avessero un determinato indirizzo IP, così è stato configurato su ciascun router il **protocollo DHCP**.

Configurazione protocollo DHCP

Il protocollo DHCP è facilmente configurabile tramite il programma Cisco Configure Professional, bisogna andare nella sezione DHCP, selezionare DHCP pools e premere il tasto add.



The screenshot displays the Cisco Configure Professional interface for configuring DHCP. The left sidebar shows a navigation tree with 'DHCP Pools' selected. The main area on the right is titled 'Configure > Router > DHCP > DHCP Pools'. It features an 'Additional Tasks' section and a table of DHCP Pools. The table has two columns: 'Pool Name' and 'Interface'. One pool named 'Monza' is listed, associated with 'FastEthernet0/0'. Below the table, the 'Details of DHCP Pool Monza' are shown in a table format.

Pool Name	Interface
Monza	FastEthernet0/0

Parameters Pushed to client	Value
DHCP Pool Range	192.168.1.10-192.168.1.28
Default router IP address	192.168.1.1
DNS Servers	208.67.222.222,8.8.8.8
WINS Servers	<None>
Domain Name	<None>
Lease Time	1 Day(s)
Import All	True
TFTP Servers	<None>

-Premendo su add è possibile configurare il protocollo DHCP e comparirà la seguente schermata dove dovremo impostare l'indirizzo di rete, la maschera, gli indirizzi riservati agli host, i DNS server e la default route, e se necessario è possibile salvare le configurazioni in un server TFTP.

DHCP Pool Name:

DHCP Pool Network: Subnet mask:

DHCP Pool

Starting IP:

Ending IP:

Lease Length

☐ Never Expires ☒ User Defined

Days:

HH:MM :

DHCP Options

DNS Server1(*): WINS Server1(*):

DNS Server2(*): WINS Server2(*):

Domain Name(*): Default Router(*):

TFTP Server1(*): TFTP Server2(*):

☒ Import all DHCP Options into the DHCP server database(*)

(*) optional fields.

-Questa è ad esempio la configurazione del DHCP di Monza, possiamo vedere come sia stato scelto di riservare per gli indirizzi dinamici forniti dal DHCP gli indirizzi dal 192.168.1.10 al 192.168.1.28.

-Ora ciascun computer è munito di un apposito indirizzo IP, sempre verificabile dal prompt dei comandi con il comando `ipconfig`, per riassegnare un indirizzo IP bisogna utilizzare il comando `ipconfig /release` per rilasciarlo, e il comando `ipconfig /renew` per far in modo che il dhcp gli assegni un nuovo indirizzo.

-Possiamo procedere con la verifica della rete tramite il comando **"ping indirizzo"** dal prompt dei comandi di un computer in rete, per verificare il corretto funzionamento della rete, abbiamo ottenuto i seguenti risultati:

Da Cesano a Monza:

```
C:\Users\Tele>ping 192.168.1.12

Esecuzione di Ping 192.168.1.12 con 32 byte di dati:
Risposta da 192.168.1.12: byte=32 durata=3ms TTL=254
Risposta da 192.168.1.12: byte=32 durata=1ms TTL=254
Risposta da 192.168.1.12: byte=32 durata=1ms TTL=254
Risposta da 192.168.1.12: byte=32 durata=1ms TTL=254

Statistiche Ping per 192.168.1.12:
    Pacchetti: Trasmessi = 4, Ricevuti = 4,
    Persi = 0 (0% persi),
Tempo approssimativo percorsi andata/ritorno in millisecondi:
    Minimo = 1ms, Massimo = 3ms, Medio = 1ms

C:\Users\Tele>
```

Da Cesano a Vimercate:

```
C:\Users\Tele>ping 172.16.1.20

Esecuzione di Ping 172.16.1.20 con 32 byte di dati:
Risposta da 172.16.1.20: byte=32 durata=14ms TTL=126
Risposta da 172.16.1.20: byte=32 durata=14ms TTL=126
Risposta da 172.16.1.20: byte=32 durata=14ms TTL=126
Risposta da 172.16.1.20: byte=32 durata=14ms TTL=126

Statistiche Ping per 172.16.1.20:
    Pacchetti: Trasmessi = 4, Ricevuti = 4,
    Persi = 0 (0% persi),
Tempo approssimativo percorsi andata/ritorno in millisecondi:
    Minimo = 14ms, Massimo = 14ms, Medio = 14ms

C:\Users\Tele>
```

Da Vimercate a Monza:

```
C:\Users\Tele>ping 10.0.0.20

Esecuzione di Ping 10.0.0.20 con 32 byte di dati:
Risposta da 10.0.0.20: byte=32 durata=14ms TTL=125
Risposta da 10.0.0.20: byte=32 durata=14ms TTL=125
Risposta da 10.0.0.20: byte=32 durata=14ms TTL=125
Risposta da 10.0.0.20: byte=32 durata=14ms TTL=125

Statistiche Ping per 10.0.0.20:
    Pacchetti: Trasmessi = 4, Ricevuti = 4,
    Persi = 0 (0% persi),
Tempo approssimativo percorsi andata/ritorno in millisecondi:
    Minimo = 14ms, Massimo = 14ms, Medio = 14ms
```

Possiamo quindi confermare il corretto funzionamento della rete.

Configurazione protocollo RIP

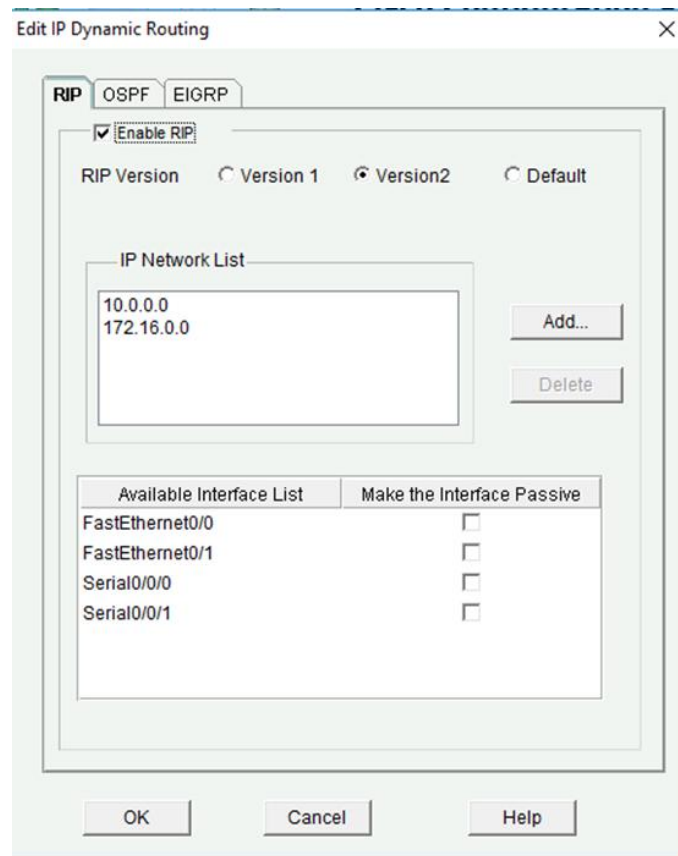
- Passiamo ora alla configurazione del protocollo RIP, il quale avrà una metrica più elevata e entrerà in funzione solo nel caso si verifichino interruzioni di un collegamento e le route statiche non possano servire per raggiungere la rete di destinazione. Il RIP sarà anche molto importante in seguito, dove la rete verrà modificata per consentire il collegamento al router ISP, lì sarà lui a compilare automaticamente le tabelle di routing perché la rete subirà una modifica per cui le route statiche non sarebbero in grado di collegare l'intera rete.
- Il protocollo RIP è facilmente configurabile tramite il programma CCP, dove è sufficiente inserire i dati di accesso di un router per poter entrarci:

Selected community: **New Community** . Select a device from the table below. Use the buttons at the bottom to continue.

Filter | 6 rows retrieved |

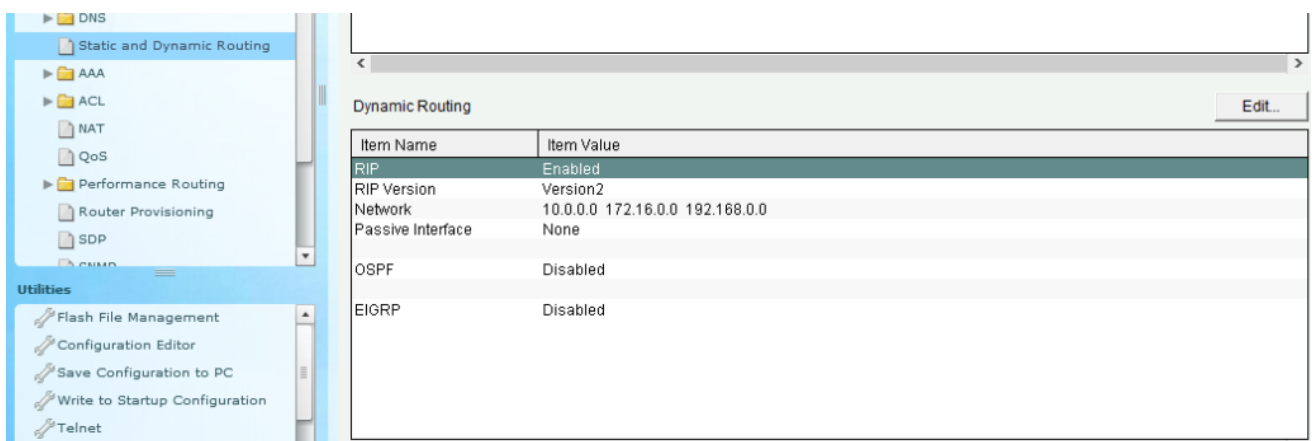
IP address / Hostname	Router Hostname	Connection Type	Discovery Status
10.0.0.251		Non secure	Not discovered
10.0.0.240	monza	Non secure	Discovered
10.0.0.241		Non secure	Not discovered
172.26.0.1		Non secure	Not discovered
172.26.3.254		Non secure	Not discovered
10.0.0.252		Non secure	Not discovered

- Una volta essere entrati nel router basterà selezionare la parte dedicata alle route static and dynamic routing, selezionare il protocollo RIP e configurarlo nel seguente modo:



-Selezionando la **versione 2**, e poi il RIP vuole che inserisci le **reti direttamente connesse al router**, configurandolo in questo modo su tutti i router provvederà lui stesso a compilare le tabelle di routing.

Cesano



Monza

Application Help

Home Configure Monitor

Select Community Member: 10.0.0.240

Configure > Router > Static and Dynamic Routing

Routing

Static Routing

Destination Network	Prefix	Prefix Mask	Forwarding	Interface or IP address	Optional	Distance
10.0.0.0	255.255.255.0	192.168.0.2			1	
172.16.0.0	255.255.255.252	10.0.1.1			1	
172.16.1.0	255.255.255.192	10.0.1.1			1	

Dynamic Routing

Item Name	Item Value
RIP	Enabled
RIP Version	Version2
Network	10.0.0.0 172.16.0.0
Passive Interface	None
OSPF	Disabled
EIGRP	Disabled

Vimercate

Static and Dynamic Routing

Dynamic Routing

Item Name	Item Value
RIP	Enabled
RIP Version	Version2
Network	10.0.0.0 172.16.0.0
Passive Interface	None
OSPF	Disabled
EIGRP	Disabled

-Una volta configurato il RIP procediamo con l'interruzione di un collegamento, mettendo in shutdown un'interfaccia, e verificando tramite il comando **tracert** dal prompt dei comandi che il rip sia funzionante, e ci mostra pure il percorso effettuato.

```
Traccia instradamento verso PC-TELE-N1 [10.0.0.21]
su un massimo di 30 punti di passaggio:

 1      <1 ms      <1 ms      <1 ms  192.168.1.1
 2      11 ms      11 ms      11 ms  10.0.1.1
 3      14 ms      13 ms      13 ms  PC-TELE-N1 [10.0.0.21]

Traccia completata.

C:\Users\Tele>tracert 10.0.0.21

Traccia instradamento verso PC-TELE-N1 [10.0.0.21]
su un massimo di 30 punti di passaggio:

 1      <1 ms      <1 ms      <1 ms  192.168.1.1
 2      11 ms      11 ms      11 ms  192.168.0.2
 3      13 ms      13 ms      13 ms  PC-TELE-N1 [10.0.0.21]

Traccia completata.
```

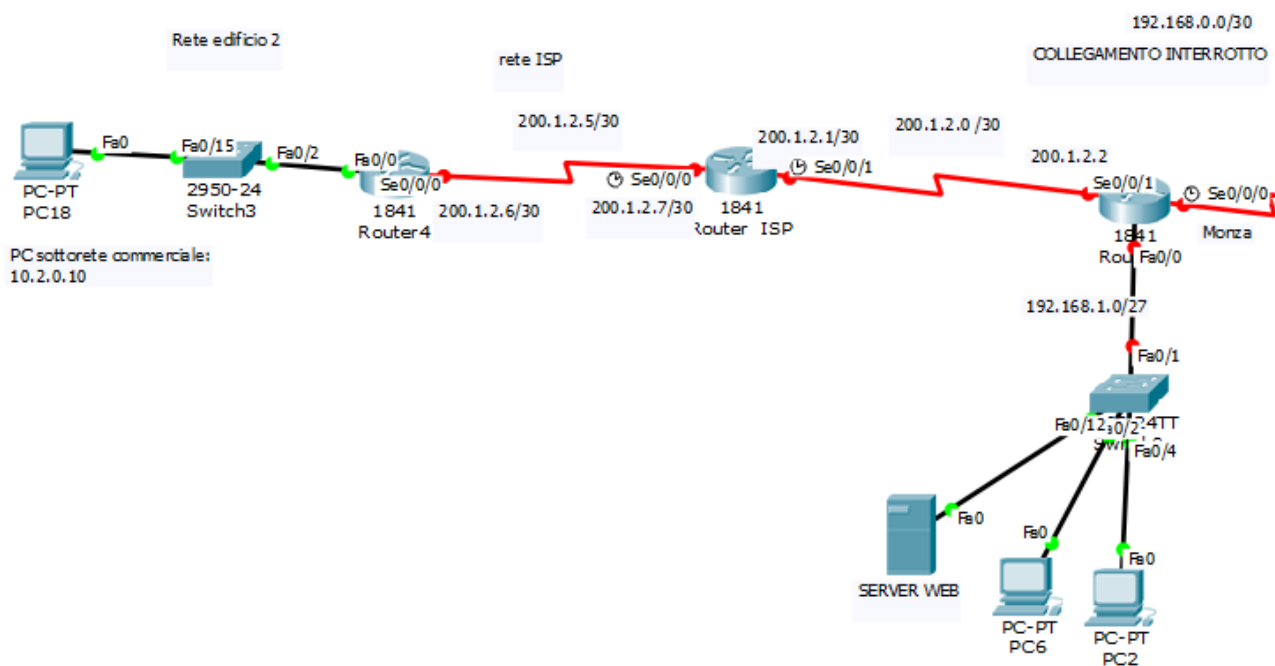
Possiamo vedere il tracer prima e dopo l'interruzione del collegamento da Monza a Cesano. E' stato testato anche il comando ping con un collegamento interrotto ed il RIP è stato dimostrato funzionare correttamente, anche se nel caso in cui la rete sia completa, il RIP non sceglie sempre il percorso più veloce per raggiungere la rete di destinazione.

Configurazione VPN

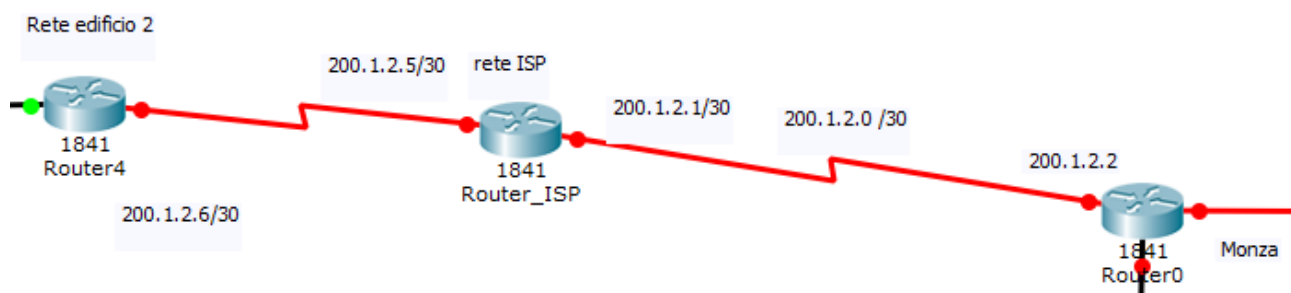
-Per creare la VPN abbiamo preso altri 2 router e uno switch amministrabile, creando un altro edificio con 1 solo router, connesso alle nostre reti tramite un router che simula un collegamento internet via provider, con tanto di indirizzi IP pubblici.

- La nuova rete è composta da 1 router ed uno switch amministrabile che divide la rete in 3 VLAN, la parte commerciale è quella in cui verrà messo il computer su cui andremo a fare i test.

-Per il collegamento con la nostra rete si è reso necessario modificarla poiché le porte seriali erano tutte occupate, la rete risultante è fatta in questo modo:



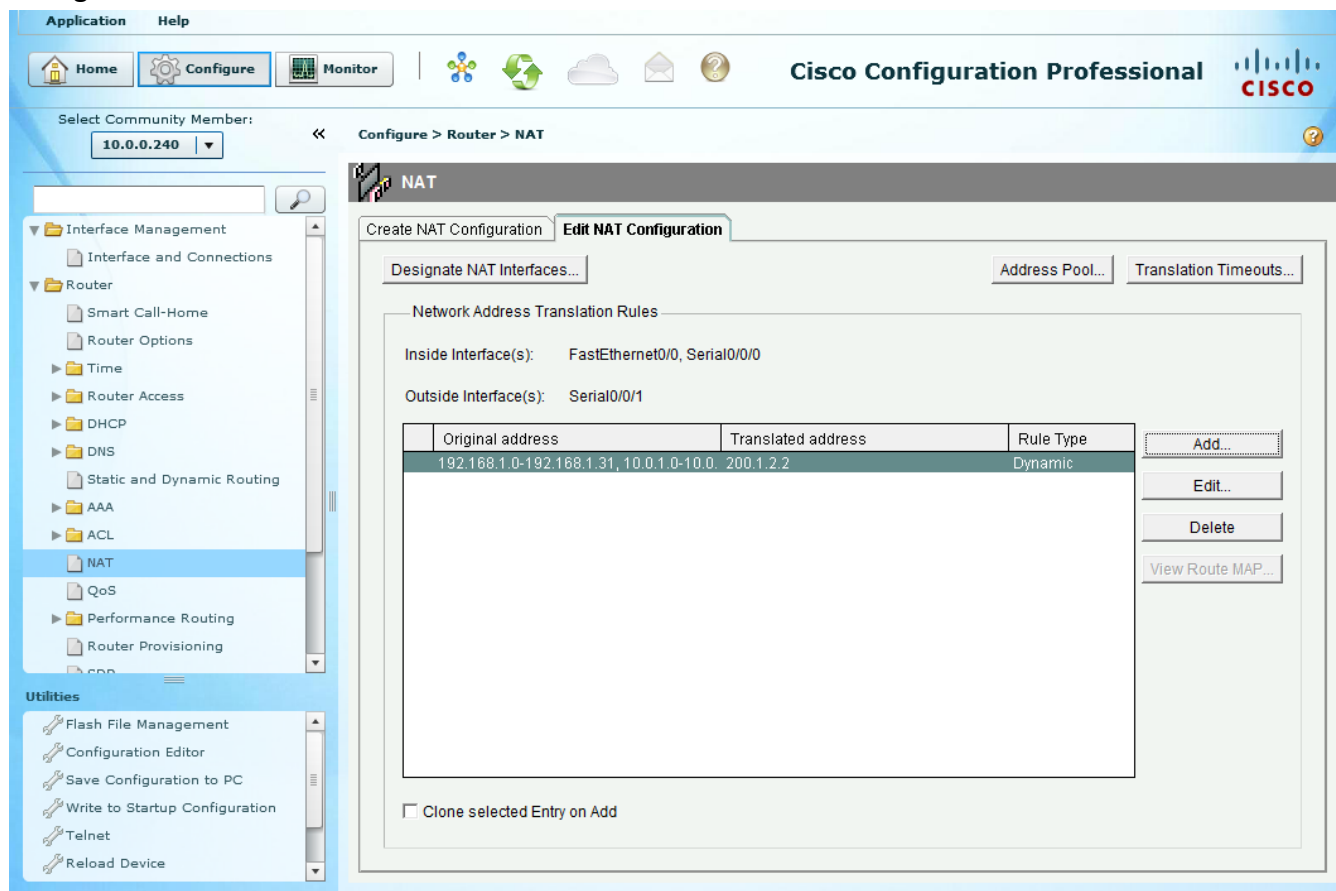
-Sono stati assegnati i seguenti indirizzi IP



-E' stato curato da noi principalmente il lato che va dalla nostra rete al router ISP, possiamo notare l'indirizzo di rete pubblico 200.1.2.0/30 dove sono stati assegnati l'indirizzo 200.1.2.2 all'interfaccia su Monza, mentre è stato dato l'indirizzo 200.1.2.1 all'interfaccia sul router ISP.

Configurazione NAT

-Per simulare un vero collegamento via internet, è stato necessario configurare la funzione NAT, configurabile facilmente tramite CCP:



-E' sufficiente creare un nuovo NAT, inserendo le porte interessate (come sopra riportato) e le reti da cui gli indirizzi dovranno essere tradotti.

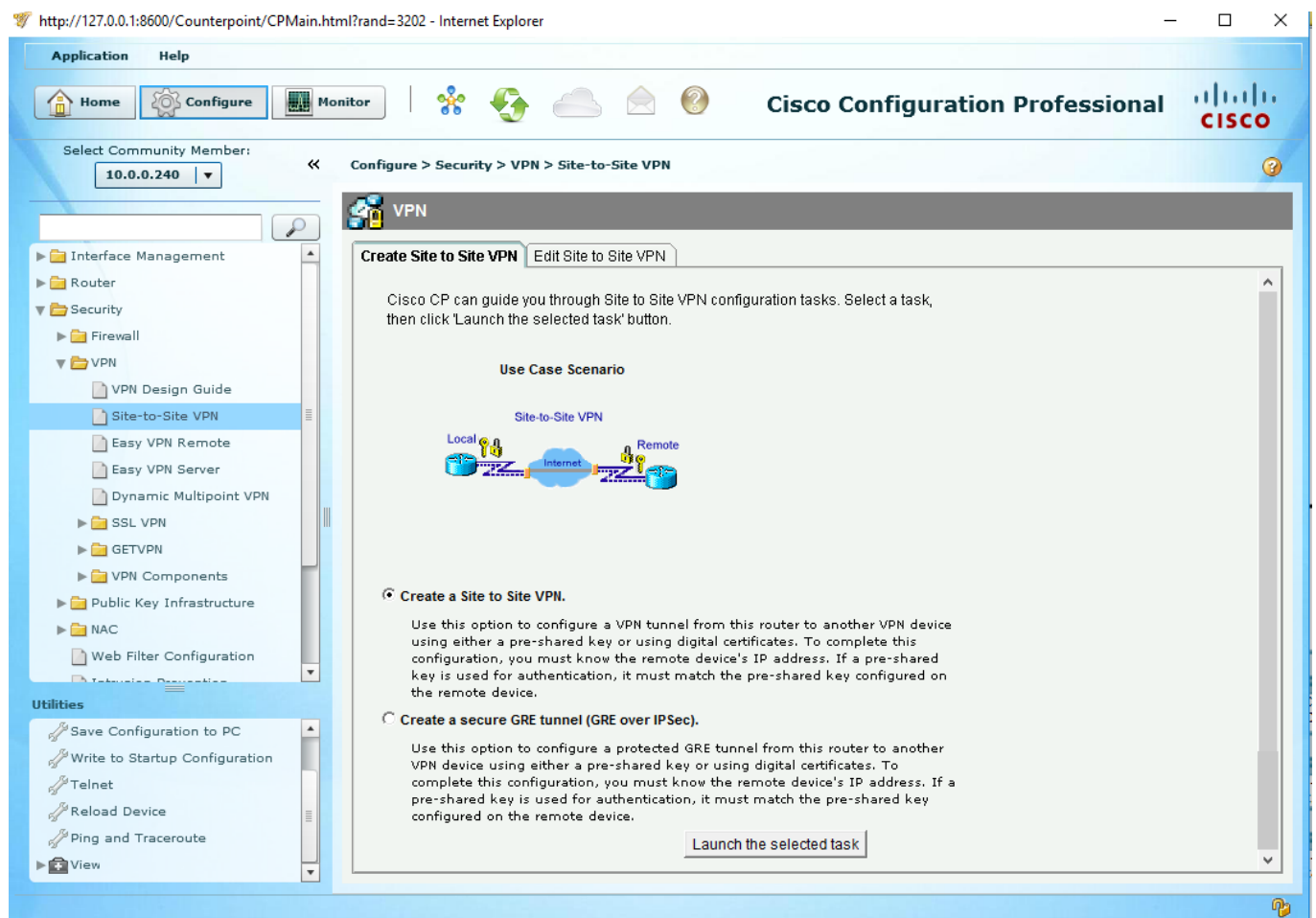
-Una volta impostato il NAT se si vuole effettuare ad esempio un ping dall'edificio 2 a un computer sulla nostra rete di Monza bisogna impostare una rete VPN. Ovviamente il NAT e anche la VPN andranno configurati su entrambe le reti.

Con il comando **IP nat trans** possiamo verificare gli indirizzi che effettivamente sono tradotti dal NAT.

```
Username: docente
Password:
monza#show ip nat trans
Pro Inside global      Inside local      Outside local      Outside global
icmp 200.1.2.2:1        192.168.1.10:1    200.1.2.1:1        200.1.2.1:1
udp 200.1.2.2:52279     192.168.1.10:52279 8.8.8.8:53          8.8.8.8:53
udp 200.1.2.2:52279     192.168.1.10:52279 208.67.222.222:53   208.67.222.222:53
udp 200.1.2.2:52388     192.168.1.10:52388 8.8.8.8:53          8.8.8.8:53
udp 200.1.2.2:52388     192.168.1.10:52388 208.67.222.222:53   208.67.222.222:53
udp 200.1.2.2:53438     192.168.1.10:53438 8.8.8.8:53          8.8.8.8:53
udp 200.1.2.2:53438     192.168.1.10:53438 208.67.222.222:53   208.67.222.222:53
udp 200.1.2.2:56111     192.168.1.10:56111 8.8.8.8:53          8.8.8.8:53
udp 200.1.2.2:56111     192.168.1.10:56111 208.67.222.222:53   208.67.222.222:53
udp 200.1.2.2:56854     192.168.1.10:56854 8.8.8.8:53          8.8.8.8:53
udp 200.1.2.2:56854     192.168.1.10:56854 208.67.222.222:53   208.67.222.222:53
udp 200.1.2.2:58334     192.168.1.10:58334 8.8.8.8:53          8.8.8.8:53
udp 200.1.2.2:58334     192.168.1.10:58334 208.67.222.222:53   208.67.222.222:53
udp 200.1.2.2:62322     192.168.1.10:62322 8.8.8.8:53          8.8.8.8:53
udp 200.1.2.2:62322     192.168.1.10:62322 208.67.222.222:53   208.67.222.222:53
udp 200.1.2.2:62447     192.168.1.10:62447 8.8.8.8:53          8.8.8.8:53
udp 200.1.2.2:62447     192.168.1.10:62447 208.67.222.222:53   208.67.222.222:53
monza#
```

-Ora possiamo procedere con la configurazione della VPN, il procedimento viene effettuato tramite via grafica con CCP perché ha a riga di comando sarebbero da inserire più di 60 comandi.

-Fase 1



-Sotto la sezione VPN troviamo diversi tipi, il tipo che andremo ad utilizzare noi è il Site to Site (punto a punto). CCP offre anche un sistema di “aiuto” che ci può guidare durante la configurazione.

Select Transform Set

Select the transform set that you want to use from this list.

Details of the Selected Transform Set

This area supplies details about the selected transform set. Not all types of encryption, authentication, and compression have to be configured; therefore, some columns may not contain values.

To learn the possible values each column may contain, click [Add or Edit Transform Set](#).

Name

The name given to this transform set.

ESP Encryption

The type of Encapsulating Security Protocol (ESP) encryption used. If ESP encryption is not configured for this transform set, this column will be empty.

ESP Authentication

The type of ESP authentication used. If ESP authentication is not configured for this transform set, this column will be empty.

AH Authentication

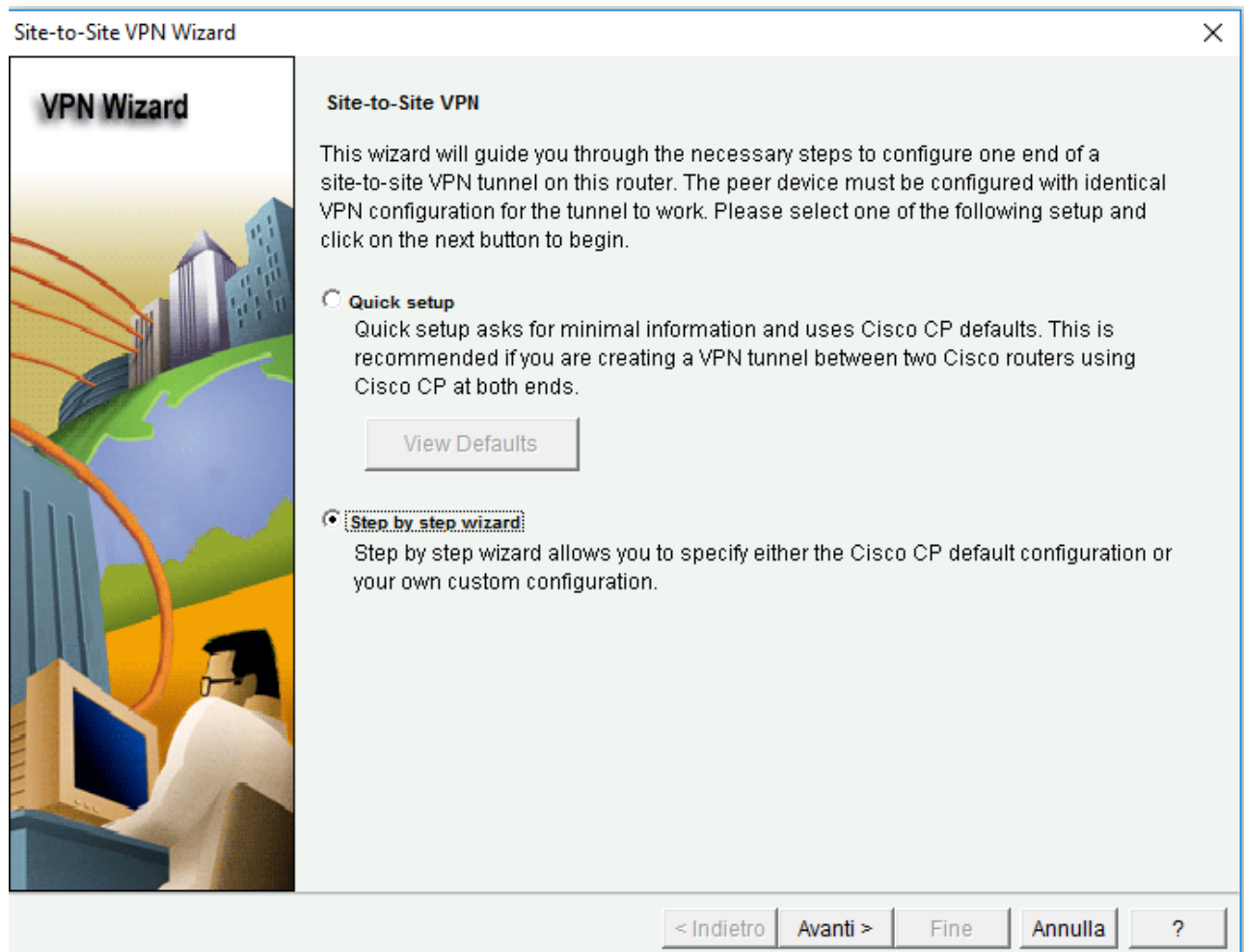
The type of Authentication Header (AH) authentication used. If AH authentication is not configured for this transform set, this column will be empty.

IP Compression

If IP compression is configured for this transform set, this field contains the value COMP-LZS.

Note IP compression is not supported on all routers.

-Lanciamo quindi l'inizio della configurazione:



Selezioniamo la configurazione step by step wizard che ci permette di configurare la VPN a nostro piacimento passo per passo .

-Fase 2

Site-to-Site VPN Wizard

VPN Wizard

VPN Connection Information

Select the interface for this VPN connection: Serial0/0/1 Details...

Peer Identity

Select the type of peer(s) used for this VPN connection: Peer with static IP address

Enter the IP address of the remote peer: 200.1.2.6

Authentication

Authentication ensures that each end of the VPN connection uses the same secret key.

☒ Pre-shared Keys ☐ Digital Certificates

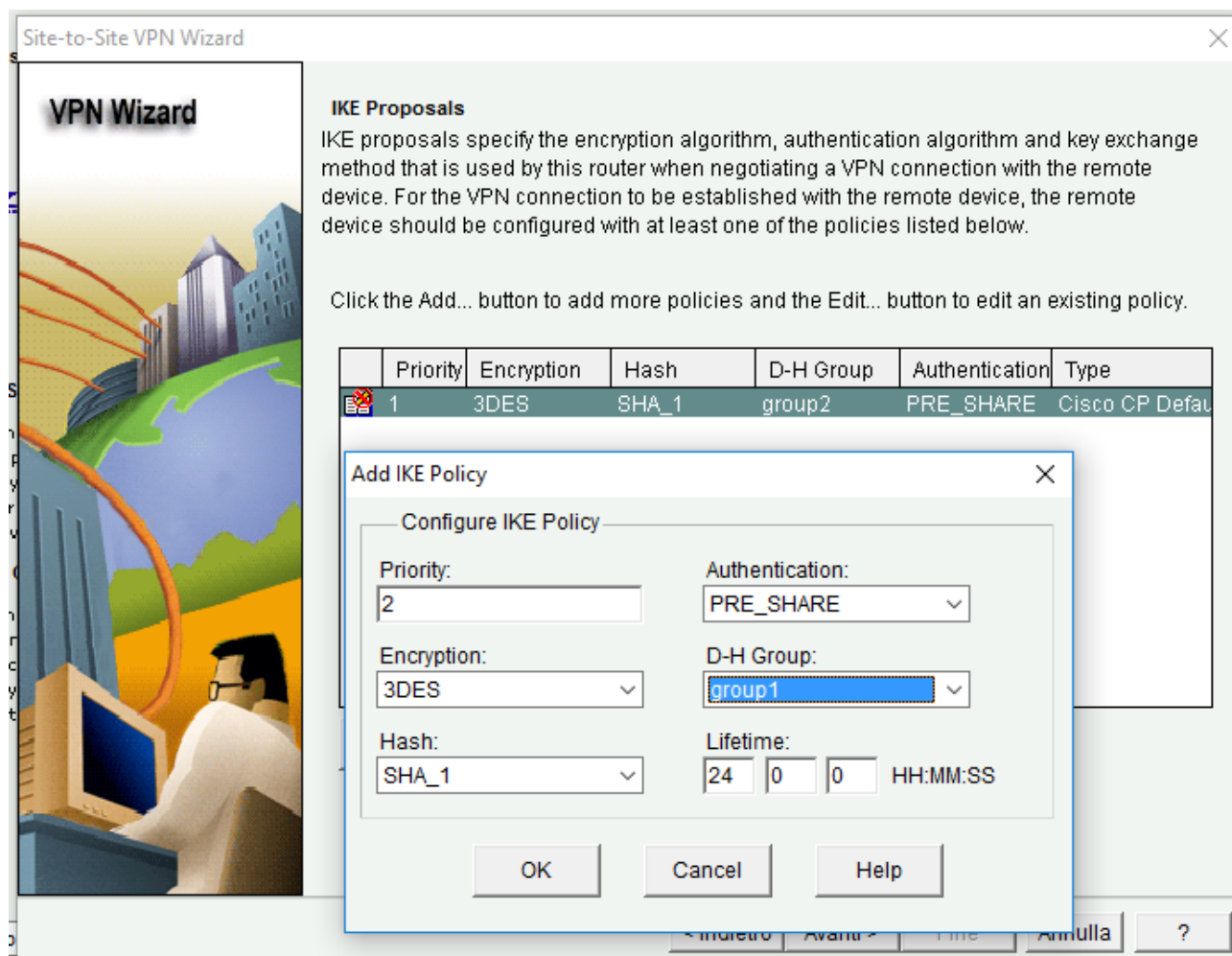
pre-shared key: *****

Re-enter Key: *****

< Indietro Avanti > Fine Annulla ?

Qui dobbiamo selezionare l'interfaccia su cui vogliamo instaurare la VPN, dobbiamo inserire l'indirizzo dell'interfaccia sul router dove la VPN terminerà e inserire una chiave per la crittografia di pre-share, che nel nostro caso è "labtelecom".

-Fase 3



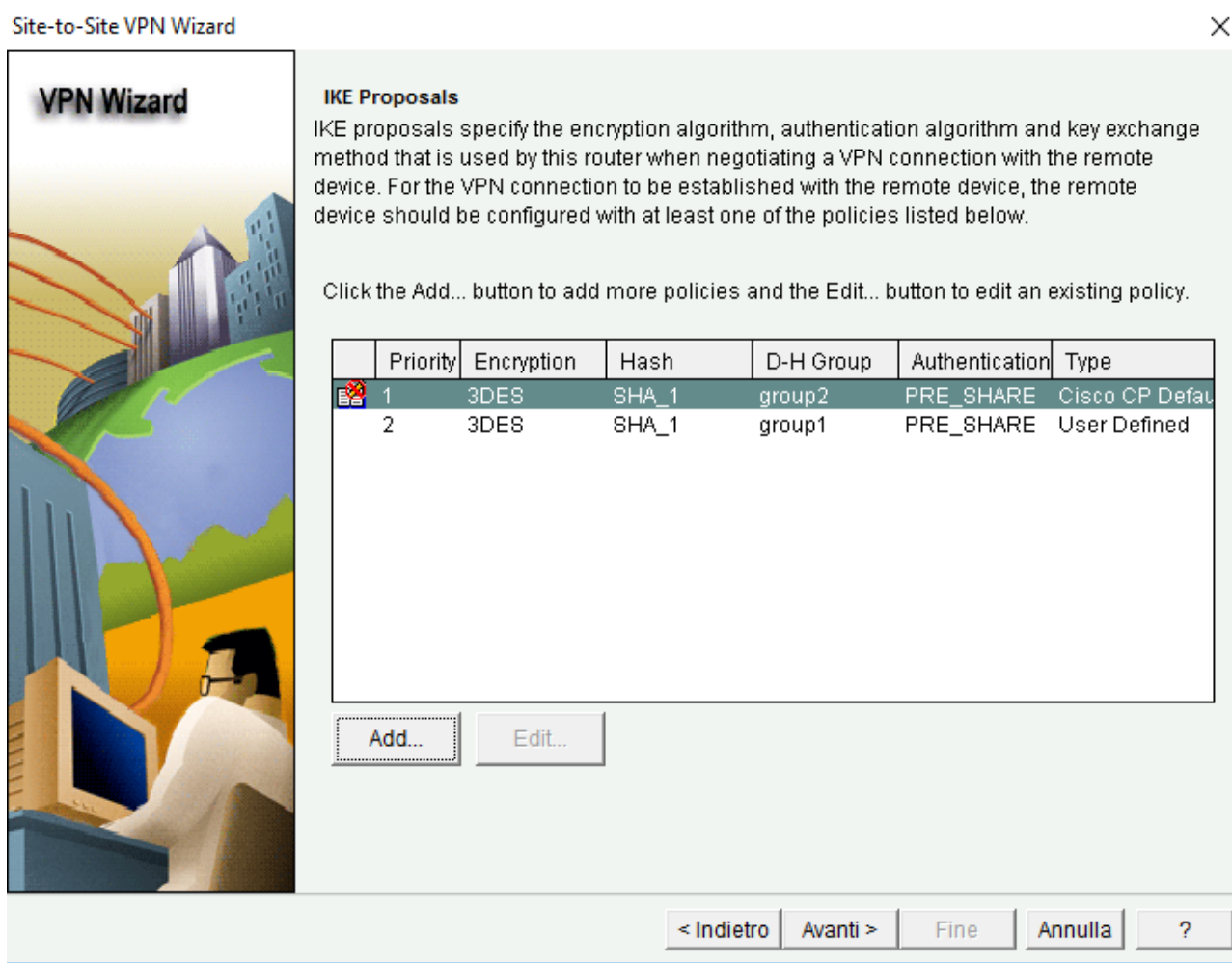
- Dobbiamo ora settare l'IKE, ovvero le specifiche dell'algoritmo con cui verrà criptata la comunicazione, abbiamo scelto un tipo di crittografia 3DES, che è una via di mezzo per non rallentare troppo la comunicazione, il Triple DES (DES triplo) è un cifrario a blocchi basato sulla ripetizione del Data Encryption Standard (DES) per tre volte, quindi è un metodo di cifratura. Viene poi selezionato SHA_1 nel campo hash, L'algoritmo di hash elabora qualunque mole di bit (in informatica si dice che elabora dati "grezzi"). Si tratta di una famiglia di algoritmi che soddisfa questi requisiti:

L'algoritmo restituisce una stringa di numeri e lettere a partire da un qualsiasi flusso di bit di qualsiasi dimensione (può essere un file ma anche una stringa). L'output è detto digest.

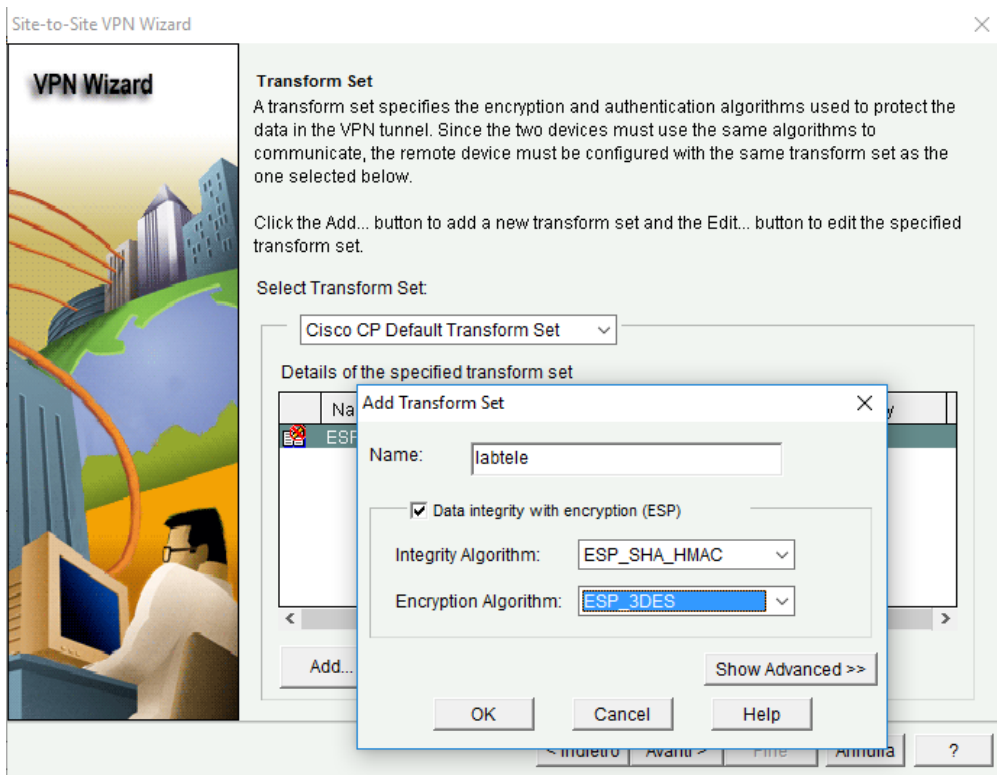
L'algoritmo non è invertibile, ossia non è possibile ricostruire il documento originale a partire dalla stringa che viene restituita in output ovvero è una funzione unidirezionale, quest'ultima caratteristica non è indispensabile se si usano gli hash per controllare gli errori nei trasferimenti dei dati, dove le eventuali funzioni di crittaggio possono venir svolte in altre aree del protocollo. Con il termine SHA si indica una famiglia di cinque diverse funzioni crittografiche di hash sviluppate a partire dal 1993 dalla National Security Agency (NSA) e pubblicate dal NIST come standard federale dal governo degli USA (FIPS PUB 180-4). La sigla SHA sta per Secure Hash Algorithm.

- Come ogni algoritmo di hash, l'SHA produce un message digest, o "impronta del messaggio", di lunghezza fissa partendo da un messaggio di lunghezza variabile. La sicurezza di un algoritmo di hash risiede nel fatto che la funzione non sia reversibile (non sia cioè possibile risalire al messaggio originale conoscendo solo questo dato) e che non deve essere mai possibile creare intenzionalmente due messaggi diversi con lo stesso digest. Gli algoritmi della famiglia sono denominati SHA-1, SHA-224, SHA-256, SHA-384 e SHA-512: le ultime 4 varianti sono spesso indicate genericamente come SHA-2, per distinguerle dal primo. Il primo produce un digest del messaggio di soli 160 bit, mentre gli altri producono digest di lunghezza in bit pari al numero indicato nella loro sigla (SHA-256 produce un digest di 256 bit). L'SHA-1 è il più diffuso algoritmo della famiglia SHA ed è utilizzato in numerose applicazioni e protocolli.

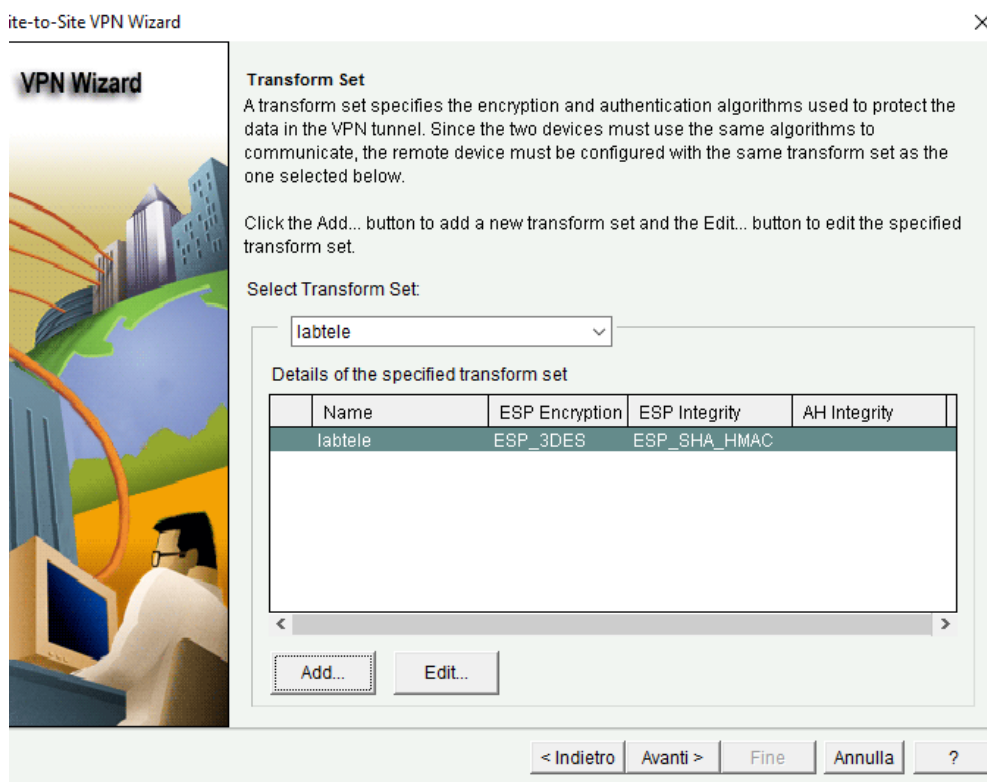
-Infine si seleziona un metodo di autenticazione PRE_SHARE(che sarebbe la fase ancora prima dove verrà poi decisa la chiave di cifratura.



-Fase 4



Con questa fase si stabiliscono gli algoritmi per la crittografia dei dati all'interno del tunnel VPN.



-Fase 5

Site-to-Site VPN Wizard

VPN Wizard

Traffic to protect
IPSec rules define the traffic, such as file transfers (FTP) and e-mail (SMTP) that will be protected by this VPN connection. Other data traffic will be sent unprotected to the remote device. You can protect all traffic between a particular source and destination subnet, or specify an IPSec rule that defines the traffic types to be protected.

☒ Protect all traffic between the following subnets

Local Network	Remote Network
Enter the IP address and subnet mask of the network where IPSec traffic originates.	Enter the IP Address and Subnet Mask of the destination Network.
IP Address: <input type="text" value="192.168.1.0"/>	IP Address: <input type="text" value="10.2.0.0"/>
Subnet Mask: <input type="text" value="255.255.255.224"/> or <input type="text" value="27"/>	Subnet Mask: <input type="text" value="255.255.255.224"/> or <input type="text" value="27"/>

☐ Create/Select an access-list for IPSec traffic ...


< Indietro Avanti > Fine Annulla ?

Ora stabiliamo le reti tra le quali dovrà essere stabilito il collegamento con il TUNNEL VPN, ovvero la 192.168.1.0 e la 10.2.0.0 con le proprie maschere, ovviamente dal lato opposto le reti saranno inserite in modo inverso.

-Fase 6

Site-to-Site VPN Wizard



VPN Wizard

Summary of the Configuration

Click Finish to deliver the configuration to the router.

Interface: Serial0/0/1
Peer Device: 200.1.2.6
Authentication Type : Pre-shared key
pre-shared key: *****

IKE Policies:

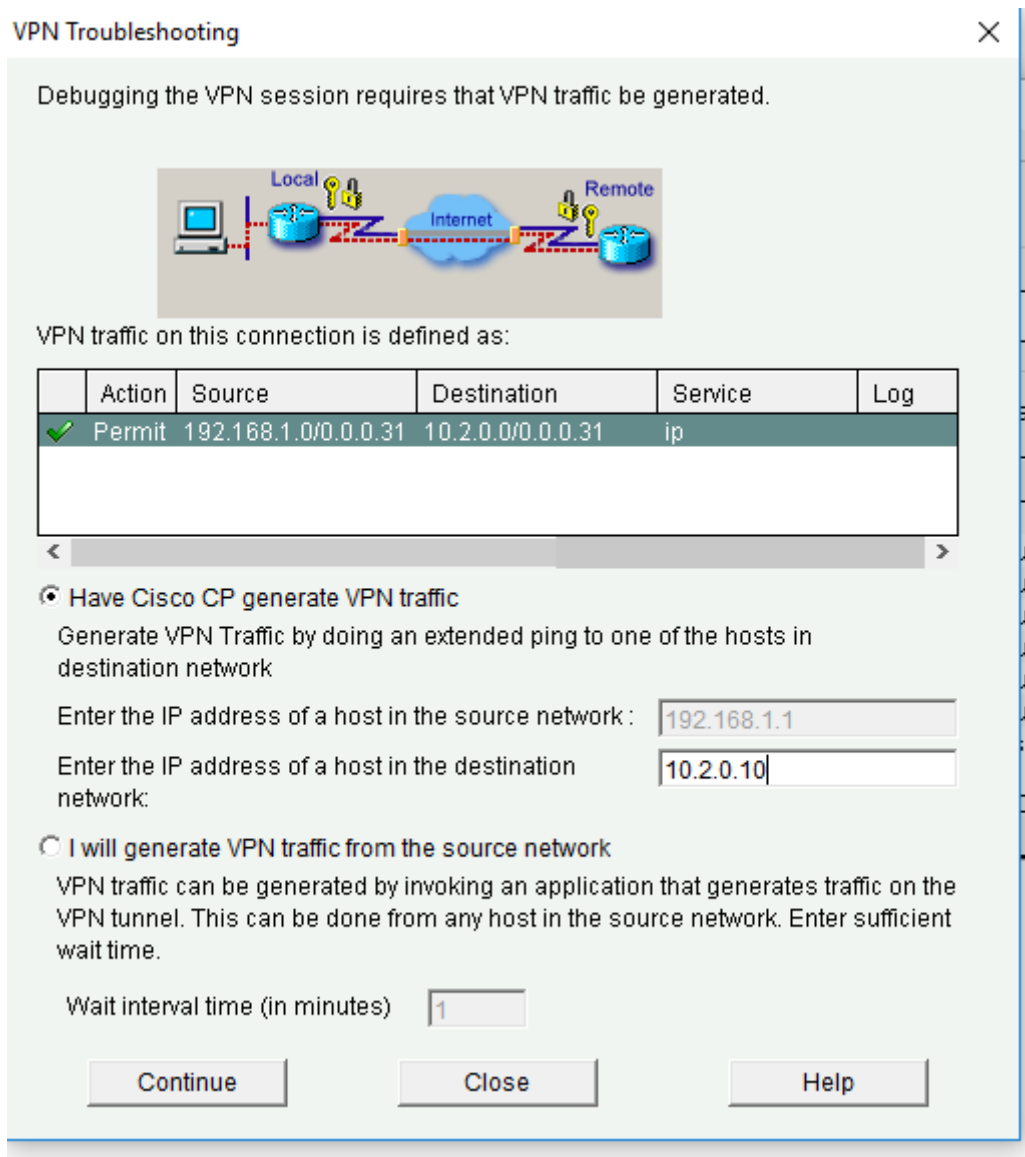
Hash	DH Group	Authentication	Encryption
SHA_1	group1	PRE_SHARE	3DES
SHA_1	group2	PRE_SHARE	3DES

Transform Sets:
Name: labtele
ESP Encryption: ESP_3DES
ESP Integrity: ESP_SHA_HMAC
Mode: TUNNEL

☐ Test VPN connectivity after configuring.

< Indietro Avanti > Fine Annulla ?

Qui vengono riassunte le impostazioni da noi scelte, e viene proposto un test per il funzionamento della VPN. Sarà possibile testare anche la VPN tramite questa funzione, la quale tenterà di mettersi in contatto con un host presente nella rete opposta.



-Una volta terminata la configurazione della VPN su entrambi i router e verificato che essa sia attiva (Up):

VPN									
Create Site to Site VPN Edit Site to Site VPN									
Status	Interface	Description	IPSec Policy	Seq No	Peers	Transform Set	IPSec Rule	Type	
Up	Serial0/0/1	Tunnel to 200.1.2.6	SDM_CMAP_1	1	200.1.2.6	labtele	100	Static	

non resta che provare a effettuare un ping da un computer nella rete dell'edificio 2 fino alla rete di Monza, il quale dovrà essere possibile nonostante il NAT grazie al collegamento VPN.

Test funzionamento VPN

Ping da un computer dell'edificio 2 sull'interfaccia esterna del router di monza.

```
C:\Users\Tele>ping 200.1.2.1

Esecuzione di Ping 200.1.2.1 con 32 byte di dati:
Risposta da 200.1.2.1: byte=32 durata=10ms TTL=254
Risposta da 200.1.2.1: byte=32 durata=10ms TTL=254
Risposta da 200.1.2.1: byte=32 durata=10ms TTL=254
Risposta da 200.1.2.1: byte=32 durata=10ms TTL=254

Statistiche Ping per 200.1.2.1:
    Pacchetti: Trasmessi = 4, Ricevuti = 4,
    Persi = 0 (0% persi),
Tempo approssimativo percorsi andata/ritorno in millisecondi:
    Minimo = 10ms, Massimo = 10ms, Medio = 10ms
```

Ping effettuato sempre da un computer dell'edificio 2 su un computer nella rete di monza, quindi questo verifica il funzionamento della VPN e del NAT.

```
C:\Users\Tele>ping 192.168.1.10

Esecuzione di Ping 192.168.1.10 con 32 byte di dati:
Risposta da 192.168.1.10: byte=32 durata=33ms TTL=126
Risposta da 192.168.1.10: byte=32 durata=34ms TTL=126
Risposta da 192.168.1.10: byte=32 durata=34ms TTL=126
Risposta da 192.168.1.10: byte=32 durata=34ms TTL=126

Statistiche Ping per 192.168.1.10:
    Pacchetti: Trasmessi = 4, Ricevuti = 4,
    Persi = 0 (0% persi),
Tempo approssimativo percorsi andata/ritorno in millisecondi:
    Minimo = 33ms, Massimo = 34ms, Medio = 33ms
```


- Abbiamo infine inserito nella rete di Monza un Server Web (con indirizzo IP 192.168.1.10) che può essere raggiunto anche dall'edificio 2 tramite il TUNNEL VPN, si è quindi in grado anche di aprire le pagine web contenute in esso.

```
C:\Users\Tele>ping 192.168.1.10

Esecuzione di Ping 192.168.1.10 con 32 byte di dati:
Richiesta scaduta.
Risposta da 192.168.1.10: byte=32 durata=33ms TTL=62
Risposta da 192.168.1.10: byte=32 durata=33ms TTL=62
Risposta da 192.168.1.10: byte=32 durata=34ms TTL=62

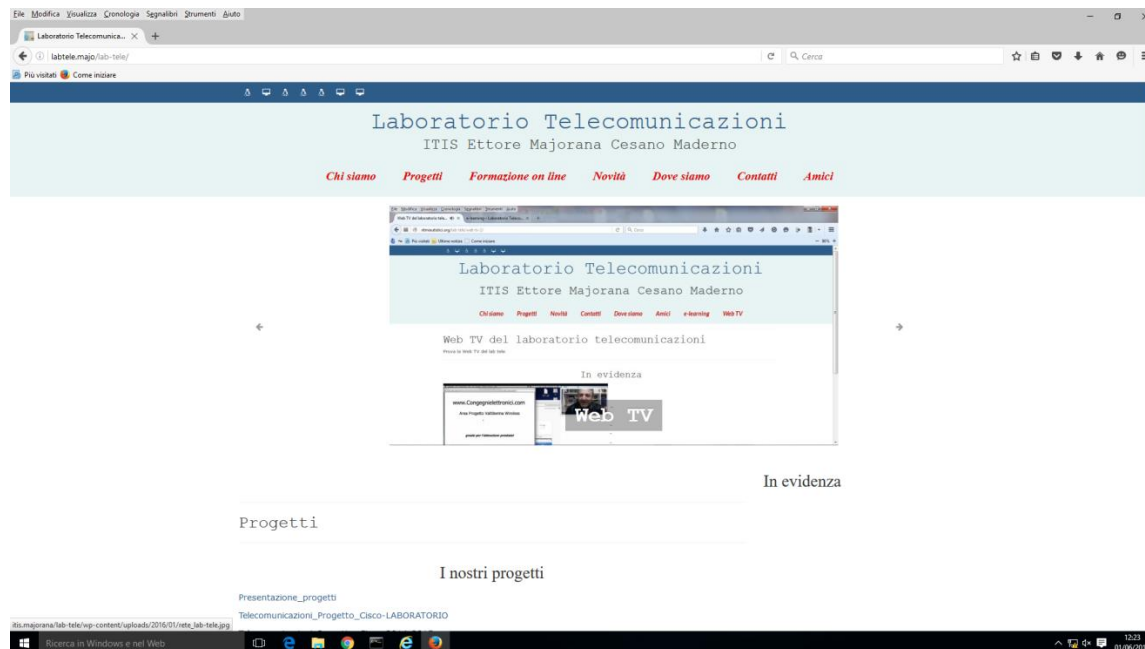
Statistiche Ping per 192.168.1.10:
    Pacchetti: Trasmessi = 4, Ricevuti = 3,
    Persi = 1 (25% persi),
    Tempo approssimativo percorsi andata/ritorno in millisecondi:
        Minimo = 33ms, Massimo = 34ms, Medio = 33ms

C:\Users\Tele>ping labtele.majo

Esecuzione di Ping labtele.majo [192.168.1.10] con 32 byte di dati:
Risposta da 192.168.1.10: byte=32 durata=33ms TTL=62
Risposta da 192.168.1.10: byte=32 durata=33ms TTL=62
Risposta da 192.168.1.10: byte=32 durata=33ms TTL=62
Risposta da 192.168.1.10: byte=32 durata=33ms TTL=62

Statistiche Ping per 192.168.1.10:
    Pacchetti: Trasmessi = 4, Ricevuti = 4,
    Persi = 0 (0% persi),
    Tempo approssimativo percorsi andata/ritorno in millisecondi:
        Minimo = 33ms, Massimo = 33ms, Medio = 33ms
```

Ping effettuato dall'edificio 2 al server presente nella rete di Monza, come si vede dall'immagine il ping funziona anche inserendo il nome del sito stesso grazie alla configurazione del **file hosts**. E' pure possibile dal computer nell'edificio 2 quindi aprire la pagina web stessa.



Risultati

Abbiamo anche testato i vari indirizzi dei router tramite il comando ping dal prompt dei comandi di un qualsiasi pc in rete, per verificare se i router sono raggiungibili. I nostri router sono risultanti raggiungibili.

La rete finale e tutti i test svolti sono stati eseguiti con successo, va ricordato che per impostare una VPN o un firewall(non nel nostro caso), il router deve poter supportare queste funzioni, infatti ci sono router che non posso effettuare queste operazioni.

E' poi consigliabile di salvare le configurazioni di ogni router in un server TFTP presente in rete, così che sia possibile nel caso ricaricare le configurazioni sui router in qualsiasi momento . Utilizzando i seguenti comandi:

```
R-contabile-ed1#erase nvram
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
R-contabile-ed1#
*Jan  1 02:45:12.111: %SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
R-contabile-ed1#copy tftp://10.0.0.52 start
Source filename []? monza-config
Destination filename [startup-config]?
Accessing tftp://10.0.0.52 /monza-config...
Loading monza-config from 10.0.0.52 (via FastEthernet0/1): !
[OK - 1504 bytes]
[OK]
1504 bytes copied in 12.128 secs (124 bytes/sec)
R-contabile-ed1#
R-contabile-ed1#
*Jan  1 02:46:21.379: %SYS-5-CONFIG_NV_I: Nonvolatile storage configured from tftp://10.0.0.52/monza-config by studente on console
R-contabile-ed1#
```

Internet of Things

- Internet delle cose (o, più propriamente, Internet degli oggetti o IoT, acronimo dell'inglese Internet of Things) è un neologismo riferito all'estensione di Internet al mondo degli oggetti e dei luoghi concreti.

-L'Internet delle cose è una possibile evoluzione dell'uso della Rete: gli oggetti (le "cose") si rendono riconoscibili e acquisiscono intelligenza grazie al fatto di poter comunicare dati su se stessi e accedere ad informazioni aggregate da parte di altri. Le sveglie suonano prima in caso di traffico, le scarpe da ginnastica trasmettono tempi, velocità e distanza per gareggiare in tempo reale con persone dall'altra parte del globo, i vasetti delle medicine avvisano i familiari se si dimentica di prendere il farmaco. Tutti gli oggetti possono acquisire un ruolo attivo grazie al collegamento alla Rete.

L'obiettivo dell'internet delle cose è far sì che il mondo elettronico tracci una mappa di quello reale, dando un'identità elettronica alle cose e ai luoghi dell'ambiente fisico. Gli oggetti e i luoghi muniti di etichette Identificazione a radio frequenza o Codici QR comunicano informazioni in rete o a dispositivi mobili come i telefoni cellulari.

I campi di applicabilità sono molteplici: dalle applicazioni industriali (processi produttivi), alla logistica, fino all'efficienza energetica, all'assistenza remota e alla tutela ambientale.

Lo scopo è quindi fornire un indirizzo IP ad ogni "cosa" (lavatrici, forni...) in modo ad esempio di essere sempre aggiornati sul loro funzionamento tramite uno smartphone, gli indirizzi IPv6 rendono possibile l'assegnazione di un indirizzo a tutto, visto che hanno 2^{128} indirizzi disponibili.

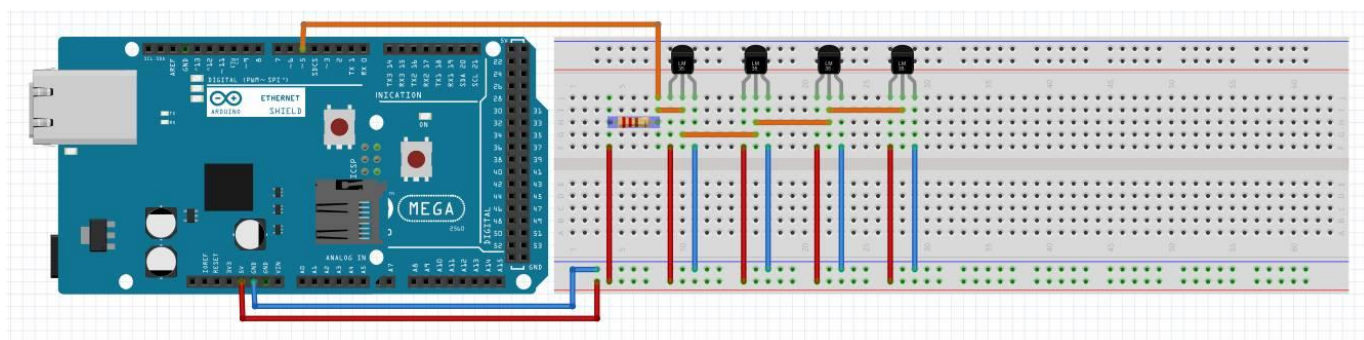
-Per esempio possiamo mettere in rete dei sensori di temperatura, utilizzando un arduino e uno Shield Ethernet per fornirgli un indirizzo IP, quindi potremo poi tramite un qualsiasi PC in rete collegarci e visualizzare la temperatura appositamente stampata all'interno di una pagina HTML.

Rilevo da sensori in rete locale con http

SCOPO: Tramite lo shield arduino connettere in rete arduino, rilevare la temperatura da sensori dallas su one wire e visualizzare i risultati su pagina HTML.

STRUMENTI E COMPONENTI UTILIZZATI: PC, Arduino Mega, Shield Arduino, One wire Bus, Basetta, sensori Dallas x4.

SCHEMA ELETTRICO:



In verità nel circuito pratico i sensori dallas sono su un one wire, cioè su un unico bus che si collega al pin 5 di arduino.

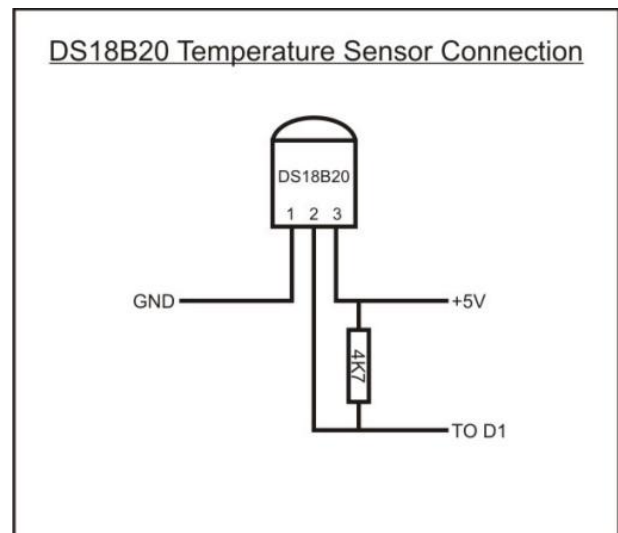
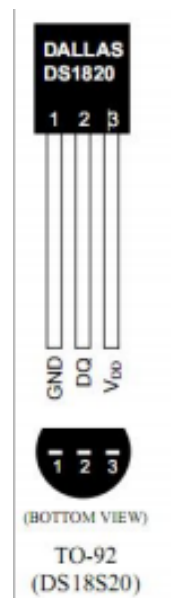
OneWire Bus:



Il bus 1-Wire è un protocollo di comunicazione, introdotto dalla americana Dallas (ora Maxim/Dallas) semiconductor, che permette di interfacciare dispositivi logici i quali memorie, sonde, e molti altri ad un microcontrollore mediante un solo filo (più la massa). Proprio questa semplicità di architettura/cablaggio ha reso questo bus molto diffuso in campo "hobbystico" e non laddove la velocità nella acquisizione dati non rappresenta un requisito fondamentale. E' possibile collegare al bus molti dispositivi contemporaneamente in quanto ognuno di essi dispone di un proprio indirizzo univoco che permette di distinguerlo dagli altri. Il bus 1-Wire è pensato per essere un bus del tipo single-master, multi-slave. Il Master può ripristinare il livello logico alto tramite una opportuna resistenza di pull-up collegato ai normali 5V dati da arduino.

Quindi abbiamo collegato **sul bus ben 4 sensori dallas**, ognuno con un indirizzo diverso e unico, in seguito tramite il programma siamo andati a leggere su ciascuno di essi la temperatura registrata nonostante fossero tutti sullo stesso bus.

Sensore Dallas:



Tensione di alimentazione da 3.0V a 5.5V.

Il

Il sensore DS18B20 è una sonda in grado di rilevare una temperatura compresa nel campo -55°C÷125°C con un'accuratezza di $\pm 0.5^{\circ}\text{C}$ nel campo -10°C÷85°C. Il campionamento della temperatura è effettuato su 12 bit in virgola fissa con 4 cifre decimali.

Per poter funzionare questo programma necessita di due librerie:

OneWire + DallasTemperature

le

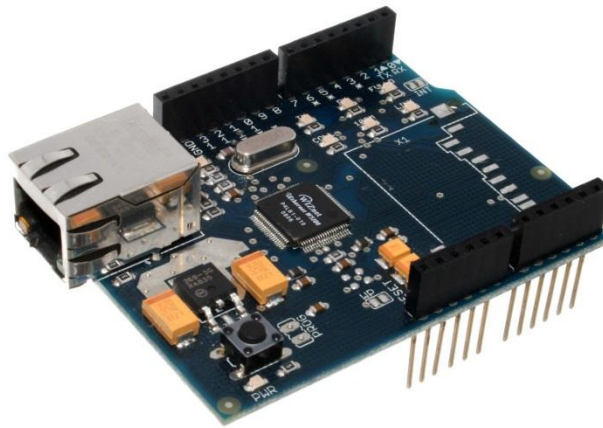
quali devono essere scaricate sul desktop del proprio computer, scomprese in due cartelle e poi caricate da Sketch -> **Importa libreria -> Add library**. Le nuove librerie verranno installate nella cartella Arduino presente nella directory Home. Fare attenzione che la cartella DallasTemperatureControl che si ottiene dal file Zip non deve avere spazi o segni.

Utilizzando il OneWire bus possiamo collegare più sensori dallas sullo stesso cavo, ogni sensore ha un proprio indirizzo unico così che arduino possa sempre riconoscerli, anche se il loro ordine cambia.

Shield ethernet : sopra l'Arduino Mega da noi utilizzato:



Viene posta questa scheda, appunto lo shield ethernet per arduino,



Questa scheda combaciante con i pin arduino, riporta sopra i pin di arduino non utilizzati da essa in modo che non vadano persi, la scheda è dotata di porta ethernet appunto, e con la giusta programmazione è in grado di dare un indirizzo ip ad arduino, noi quindi avendogli assegnato un indirizzo ip, inserendolo in un browser possiamo visualizzare la pagina sul IP dell'arduino, nel nostro caso visualizzeremo le temperature che saranno appositamente stampate in linguaggio html dal programma svolto in arduino.

Come vedremo più avanti nel programma lo shield è dunque dotato di un indirizzo MAC fornito dal costruttore nella versione 2.0, mentre nella prima versione l'indirizzo può essere scelto direttamente dal programmatore.

Procedimento

- 1- Mettere in rete Arduino applicandogli lo Shield Ethernet e collegarlo in rete.
- 2- Una volta collegato assegnarli n indirizzo IP tramite il programma eseguito.
- 3- Fare un test di connessione (ping) per verificare il corretto funzionamento dello shield ethernet, quindi fare il ping dell'indirizzo assegnato, se va a buon fine significa che l'arduino è ora visibile in rete tramite lo shield ethernet.
- 4- Montare ora sul circuito il one wire bus con i 4 sensori Dallas per il rilevamento di temperatura.
- 5- Realizzare il programma che sia in grado di misurare la temperatura e tramite protocollo http inserendo l'ip in un browser sia possibile visualizzare la pagina HTML che visualizzi la temperatura letta dai sensori Dallas.
- 6- Verificare in fine che la temperatura letta sulla pagina html risulti uguale a quella stampata su monitor seriale.

Programma per l'impostazione di un IP su arduino con Shield Ethernet

```
#include <SPI.h>
#include <Ethernet2.h> // librerie della scheda shield ethernet
byte mac[]={0x90,0xA2,0xDA,0x10,0x1F,0xBC}; // indirizzo MAC della shield ethernet
byte ip[]={10,0,0,101}; // indirizzo ip impostato
char Data_PX;
EthernetServer ArduinoServer(80);
void setup()
{
    Serial.begin(9600);
    Ethernet.begin(mac,ip);
    ArduinoServer.begin();
}
void loop()
{
    delay(10);
}
```

- Occorre inserire le librerie necessarie per il funzionamento dello shield ethernet, l'indirizzo mac scheda ethernet2 è impostato dal costruttore e indicato nel sotto della scheda, mentre l'indirizzo ip va inserito dal programmatore, il quale deve assicurarsi un indirizzo esistente e libero all'interno della rete.

Test Ping

Dal prompt dei comandi di un qualsiasi pc in rete immettere il comando “ ping 10.0.0.101 “ o l’indirizzo ip assegnato all’arduino, nel nostro caso 10.0.0.101. dopo di che ci arriverà una risposta con il tempo impiegato per contattare l’host oppure il messaggio nullo in caso che l’host non sia raggiungibile.

```
C:\Users\4 TL>ping 10.0.0.101
Esecuzione di Ping 10.0.0.101 con 32 byte di dati:
Risposta da 10.0.0.101: byte=32 durata=1ms TTL=128
Risposta da 10.0.0.101: byte=32 durata<1ms TTL=128
Risposta da 10.0.0.101: byte=32 durata<1ms TTL=128
Risposta da 10.0.0.101: byte=32 durata<1ms TTL=128
```

Conferma di corretta connessione con l’host .

Programma completo:

```
#include <SPI.h>
#include <Ethernet2.h>           // librerie shield ethernet
#include <OneWire.h>             //librerie one bus wire
#include <DallasTemperature.h>   // librerie per sensori dallas

byte mac[]={0x90, 0xA2,0xDA, 0x10, 0x1F, 0xBA}; // indirizzi MAC e IP dello shield ethernet
byte ip[]={10,0,0,101};          // quindi di arduino
char Data_RX;
int temperatura;
EthernetServer ArduinoServer(80);

float t1;
float t2;
float t3;
float t4;

OneWire bus(5);
DallasTemperature sensor(&bus);
DeviceAddress ind1 = {0x28, 0x80, 0x22, 0x09, 0x07, 0x00, 0x00, 0x66}; // dichiarazione degli indirizzi
DeviceAddress ind2 = {0x28, 0xCA, 0x2B, 0x74, 0x05, 0x00, 0x00, 0x55}; // MAC di ogni sensore dallas
DeviceAddress ind3 = {0x28, 0xFB, 0x37, 0x74, 0x05, 0x00, 0x00, 0xD2};
DeviceAddress ind4 = {0x28, 0x9F, 0x55, 0x09, 0x07, 0x00, 0x00, 0x25};
void setup()
{
  Serial.begin(9600);
  Ethernet.begin(mac,ip);
  ArduinoServer.begin();      // inizializzazione di monitor seriale,arduino,sensori,shield
  Serial.begin(9600);
  sensor.begin();
}
```

-inserisco le librerie, imposto le variabili da utilizzare e imposto l’indirizzo ip dell’arduino, dichiaro in oltre gli indirizzi dei sensori dallas collegati al one wire bus, e in fine inizializzare i nostri strumenti nel void setup.


```

void loop()
{
  sensor.requestTemperatures(); // a tutti i sensori avvio conversione
                                // leggo le temperature di ogni sensore e stampo
  Serial.print("\n lettura temperatura.....\n");

  t1 = sensor.getTempC(ind1);
  t2 = sensor.getTempC(ind2);
  t3 = sensor.getTempC(ind3);          // acquisizione della temperatura
  t4 = sensor.getTempC(ind4);

  Serial.print(t1);
  Serial.println(" gradi C ");          // comandi per la scrittura a monitor
  Serial.print(t2);
  Serial.println(" gradi C ");          // seriale della temperatura
  Serial.print(t3);
  Serial.println(" gradi C ");
  Serial.print(t4);
  Serial.println(" gradi C ");

  /*
  ascolto le richieste dei client, controllo se ci sono dati da leggere
  e creo un oggetto relativo al client che sta interrogando l'ethernet shield
  */
  EthernetClient pc_client = ArduinoServer.available();

```

- Impostiamo la rilevazione della temperatura e la stampa di essa all'interno del monitor seriale di arduino.

```

EthernetClient pc_client = ArduinoServer.available();
                                //controllo se pc_client è "true"
                                //if(pc_client != false)

if(pc_client)
{
                                //se pc_client è true continua ad utilizzarlo
                                //controllo se il client è connesso

  while(pc_client.connected())
  {
                                //eseguo questo codice finché il client è connesso.
                                //controllo se ci sono byte disponibili per la lett

    if(pc_client.available())
    {
                                //leggo i byte disponibili
                                //provenienti dal client

      Data_RX = pc_client.read();          //invio i dati letti al serial monitor

      /*attendo che tutti i byte siano letti
      quando Data_RX contiene il carattere
      di nuova line capisco tutti i byte sono stati letti
      */
      if(Data_RX == '\n')
      {
        /*invio la risposta al client
        invio lo status code
        */
        pc_client.println("HTTP/1.1 200 OK");
        //imposto il data type
        pc_client.println("Content-Type: text/html");
        pc_client.println();

                                //invio codice html

```

- Preparazione per la scrittura HTML .

```

pc_client.print("<html><body><h1>");

pc_client.print("PAGINA RILEVAZIONE TEMPERATURE COLOMBO CATTANEO 5^TL ");
pc_client.print("<BR><BR> ");
pc_client.print("Temperatura sensore 1      ");
pc_client.print(t1);
pc_client.print("<BR><BR> ");
pc_client.print("Temperatura sensore 2      ");
pc_client.print(t2);
pc_client.print("    <BR><BR> ");
pc_client.print("Temperatura sensore 3      ");
pc_client.print(t3);
pc_client.print("<BR><BR> ");

pc_client.print("Temperatura sensore 4      ");
pc_client.print(t4);
pc_client.print("<BR><BR></h1></body></html> ");

//aspetto 1 ms affinché la risposta giunga al browser del client
delay(1);
//esco dal ciclo while una volta completato l'invio della risposta
break;
}

Serial.write(65);
Serial.write(Data_RX);
}
}

//chiudo la connessione
pc_client.stop();
}

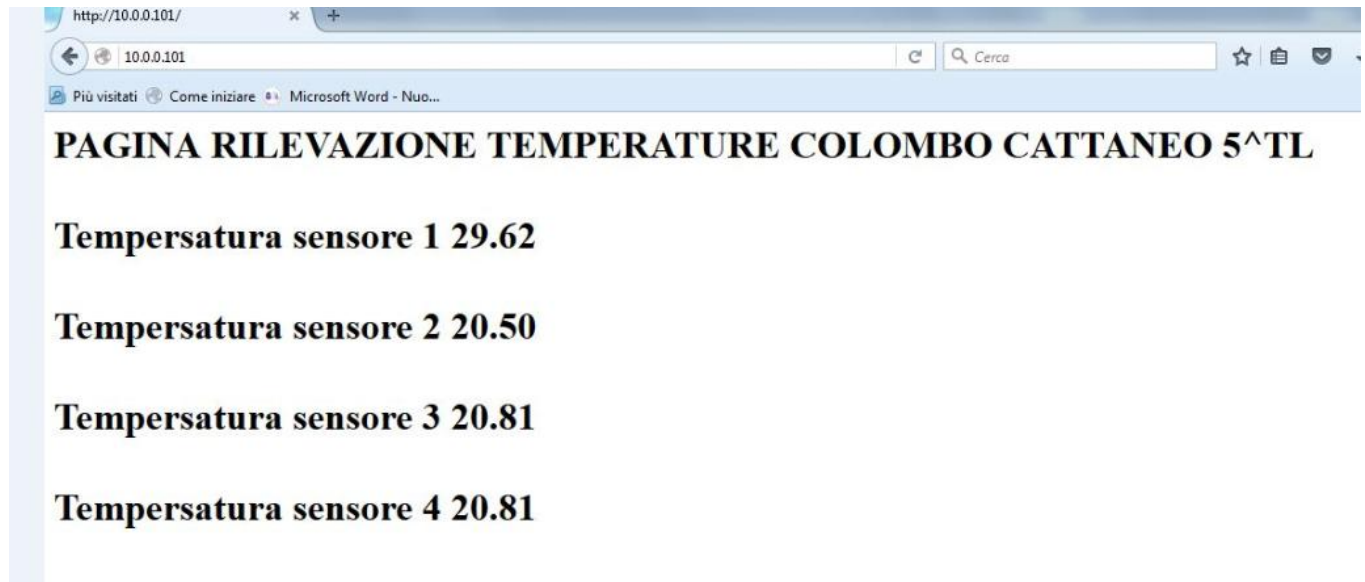
delay(10);
}

```

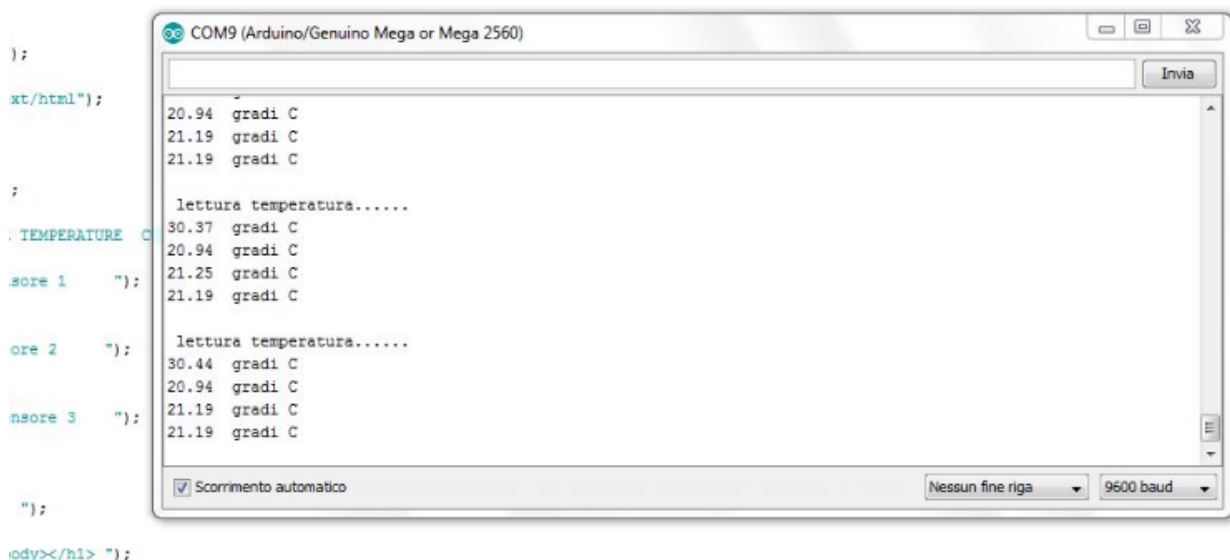
- Ora è sufficiente stampare all'interno della pagina HTML le temperature rilevate, ovviamente per fare questo occorre rispettare i parametri del linguaggio HTML.

Risultati

-Una volta caricato il programma e montato il circuito da un normale browser di qualsiasi computer in rete inserendo nella ricerca l'indirizzo IP del nostro arduino sarà visualizzata la temperatura registrata dai 4 sensori Dallas, (è sufficiente mettere l'indirizzo ip perché gli altri parametri http//: ecc.. vengono riempiti in automatico).



Mentre a monitor seriale vengono visualizzate ugualmente le temperature.



Possiamo quindi confermare che sia su monitor seriale che su browser vengono visualizzate le stesse temperature, ovviamente mentre su monitor seriale le temperature si aggiornano ogni tot impostato da programma sulla pagina html per aggiornare le temperature occorrerà ricaricare la pagina stessa.