Terza edizione
5° anno

DDI+ Didattica Digitale Integrata Plus

Elena Baldino, Renato Rondano,
Antonio Spano, Cesare Iacobelli

Internetworking

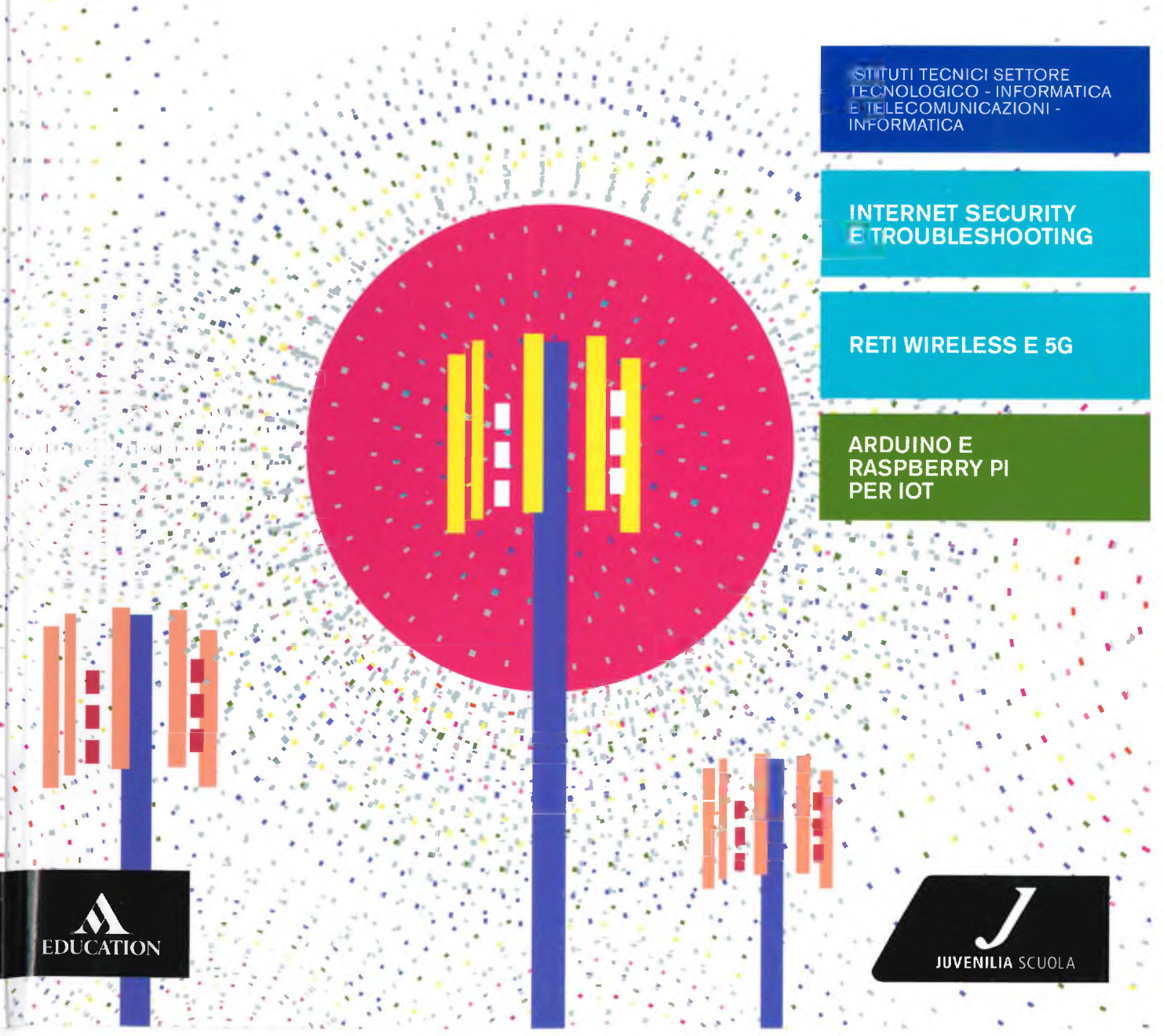
SISTEMI E RETI

ISTITUTI TECNICI SETTORE TECNOLOGICO - INFORMATICA E TELECOMUNICAZIONI - INFORMATICA

INTERNET SECURITY E TROUBLESHOOTING

RETI WIRELESS E 5G

ARDUINO E RASPBERRY PI PER IOT



EDUCATION

JUVENILIA SCUOLA

Elena Baldino, Renato Rondano,
Antonio Spano, Cesare Iacobelli

Internetworking

SISTEMI E RETI

Terza edizione - 5° anno

Configurazioni di vendita **Tipologia B** Libro cartaceo + HUB Young + HUB Kit	Volume 3	978-88-7485-748-7
	Volume 4	978-88-7485-752-4
	Volume 5 + Fascicolo *Esame di Stato*	978-88-7485-756-2
	Fascicolo *Esame di Stato*	978-88-7485-762-3
Guida e materiali per il docente	Guida per l'insegnante	978-88-7485-766-1

Inquadra il QR Code
e scopri tutte le configurazioni
e i prezzi dell'opera
mondadorieducation.it

zaino digitale
studio con un clic

LIBRO IN CHIARO

Il libro di testo in formato digitale e ogni contenuto digitale integrativo saranno fruibili esclusivamente dall'utente che ne chiederà la prima attivazione, per un periodo di tempo pari alla durata del corso della specifica materia a cui il libro si riferisce più un anno, a partire dal giorno della prima attivazione. Per i dettagli consulta il sito www.mondadorieducation.it

CONFEZIONE INDIVISIBILE
Internetworking. Sistemi e Reti - 5° anno
Terza edizione + Fascicolo Esame di Stato
+ Libro Digitale + Contenuti Digitali Integrativi

Prezzo al pubblico **Euro 23,80**

hub SCUOLA
LA PIATTAFORMA PER LA DIDATTICA DIGITALE INTEGRATA

hub YOUNG
L'APP PER USARE LA VERSIONE DIGITALE DEL LIBRO DI TESTO E I CONTENUTI DIGITALI INTEGRATIVI

hub KIT
I CONTENUTI DIGITALI INTEGRATIVI

hub SMART
L'APP PER GUARDARE I VIDEO, ASCOLTARE GLI AUDIO E ALLENARSI CON I TEST DALLO SMARTPHONE

hub CAMPUS
IL PORTALE DISCIPLINARE RICCO DI RISORSE PER IL DOCENTE

ISBN 978-88-7485-756-2
9 788874 857562

5° anno

Baldino Rondano Spano Iacobelli

INTERNETWORKING

JUVENILIA SCUOLA

E. Baldino, R. Rondano, A. Spano, C. Iacobelli

INTERNET WORKING

SISTEMI E RETI

JUVENILIA SCUOLA

www.mondadorieducation.it

FONT biancoenero®

Questo libro usa la font ad Alta Leggibilità *biancoenero®* di biancoenero edizioni, disegnata da Umberto Mischi. La font è gratuita per studenti e insegnanti.

Nuova edizione: marzo 2021

Edizioni

10 9 8 7 6 5 4 3 2 1
2025 2024 2023 2022 2021

Questo volume è stampato da:
Vincenzo Bona S.p.A. – Torino (TO)
Stampato in Italia – Printed in Italy

Il Sistema Qualità di Mondadori Education S.p.A. è certificato da Bureau Veritas Italia S.p.A. secondo la Norma UNI EN ISO 9001:2008 per le attività di: progettazione, realizzazione di testi scolastici e universitari, strumenti didattici multimediali e dizionari.

Redazione	GEM Milano
Progetto grafico	Angela Garignani
Impaginazione	GEM Milano
Proofreading	GEM Milano
Art direction del progetto grafico della copertina	46xy studio
Realizzazione della copertina	MOST - Themost.it Milano
Disegni	duDAT S.r.l. - Bologna, Edistudio Milano
Ricerca iconografica	duDAT S.r.l. - Bologna

Si ringrazia la Prof.ssa Sara Riccardo per la rilettura critica del testo.

Contenuti digitali

Progettazione	Fabio Ferri, Vincenzo Belluomo
Redazione	duDAT S.r.l. - Bologna (lezioni, esercizi)
Realizzazione	duDAT S.r.l. - Bologna (lezioni, mappe ed esercizi), Studio Frigo (audio)

PRESENTAZIONE

PREFAZIONE ALLA TERZA EDIZIONE

La terza edizione di *Internetworking – Sistemi e Reti* si presenta rinnovata nella sua articolazione su **tre volumi** per la classe terza, quarta e quinta. Nel primo e secondo volume i contenuti sono stati riorganizzati con l'obiettivo di proporre gli argomenti cardine previsti per quell'anno, inserendo nelle Unità finali i contenuti che possono essere affrontati anche nell'anno successivo.
L'opera offre numerose risorse testuali, laboratoriali e multimediali, che si integrano per realizzare un percorso ben articolato nel mondo complesso delle reti e dei sistemi. Alcuni argomenti fondamentali sono **introdotti e poi ripresi più volte nel corso dei tre anni**, per fornire agli studenti, al termine del percorso triennale, una solida preparazione teorica e pratica per affrontare l'Esame di Stato e il mondo del lavoro.
Sono stati rivisti e potenziati molti degli apparati didattici che costellano il progetto: mappe concettuali e sintesi di fine unità per una **didattica inclusiva**, attività esercitative a fine unità, attività progettuali per lo **sviluppo delle competenze**, laboratori ed esempi svolti nella teoria, schede per la didattica CLIL. La presentazione in PowerPoint dell'Unità, la **flipped classroom**, la **mappa concettuale** modificabile e le **risorse audio e multimediali** accessibili anche da smartphone tramite QR Code sono un importante corredo a disposizione del docente per un percorso strutturato di **Didattica Digitale Integrata**.
Internetworking affronta le problematiche del mondo delle reti e dei sistemi basando la trattazione sulle indispensabili **basi teoriche** e sullo **stato dell'arte** delle tecnologie presenti sul mercato e future.
L'obiettivo che ci poniamo è dunque non solo di fornire le conoscenze e le competenze utili attualmente, ma di permettere al futuro perito informatico di **integrarle con quelle emergenti**, offrendo strumenti che torneranno utili nella sua professione. Tra questi si evidenziano: la capacità di lavorare con gli standard internazionali, la comprensione di testi in lingua inglese, l'abilità nell'uso degli strumenti di analisi e di simulazione.
Per orientarsi in questo mondo complesso e offrire una chiave di lettura del contenuto dei volumi dell'opera, all'inizio di ogni volume è stata inserita una **mappa generale del volume** stesso, che presenta in modo organico le tematiche trattate e il modo in cui si correlano le une alle altre. Questo strumento permette al docente di personalizzare i diversi momenti didattici sulle specificità della propria classe, avendo sempre presente la **visione d'insieme**, e allo studente di capire come gli argomenti trattati nel corso dell'anno non siano isolati gli uni dagli altri ma **strettamente correlati tra loro**.

Nel volume per il quinto anno lo studio delle reti e dei sistemi è ampliato con la configurazione dei servizi di rete a garanzia della sicurezza in termini di accesso e privacy. Gli argomenti trattati spaziano dall'**Internet Security** per le reti wired, wireless e mobile ai data center aziendali con l'analisi delle **tecniche di virtualizzazione** e delle attuali **soluzioni in cloud**, per arrivare all'analisi degli **strumenti per la gestione e il monitoraggio delle reti**.
Il volume è corredato da un **fascicolo** con materiali utili per la preparazione ad affrontare l'**Esame di Stato** che include **temi d'esame svolti o proposti, percorsi per prepararsi alla colloquio orale**, una sezione dedicata alla **relazione di PCTO** e diverse schede con **percorsi di Educazione Civica**.

ELEMENTI DI NOVITÀ NEL VOLUME PER IL 5° ANNO

- Nell'Unità dedicata alla sicurezza delle reti locali, è stata aggiunta una parte **sulle VLAN e sul protocollo STP**, con esercitazioni da svolgere con Packet Tracer.
- Lo studio delle reti wireless e mobile (4G/5G) è stato arricchito con **nuove esercitazioni con Packet Tracer**, utilizzando anche le nuove funzionalità per l'**IoT**.
- Le tecniche e gli strumenti per il network management e il troubleshooting sono trattate in un'unica Unità.
- È presente una nuova Unità dedicata ad attività con **Arduino** e **Raspberry Pi orientate all'IoT** con l'utilizzo di reti wireless Bluetooth e Wi-Fi.
- Le esercitazioni proposte sono state aggiornate lato client alle release Windows 10 e Linux Ubuntu 20.04 LTS e lato server alle release Windows Server 2019 e Ubuntu Server 20.04 LTS.
- Le **esercitazioni con Packet Tracer** sono state completamente riviste con la nuova versione, che prevede una nuova interfaccia grafica, e aumentate di numero.

Gli Autori

INDICE

CONTENUTI DIGITALI INTEGRATIVI

PRESENTAZIONE
Guarda la presentazione dell'Unità

MAPPA MODIFICABILE

CASE STUDY
La sicurezza dei dati in rete
La sicurezza delle informazioni

TEST
Svolgi il test interattivo

AUDIO
Ascolta le risposte

AUDIO
Ascolta la pronuncia del testo

LETTURA
Verifica la traduzione

PRESENTAZIONE
Guarda la presentazione dell'Unità

MAPPA MODIFICABILE

CASE STUDY
Progettazione di una rete con 3 VLAN

FILE SORGENTI
Scarica i file

TEST
Svolgi il test interattivo

AUDIO
Ascolta le risposte

AUDIO
Ascolta la pronuncia del testo

LETTURA
Verifica la traduzione

PRESENTAZIONE
Guarda la presentazione dell'Unità

MAPPA MODIFICABILE

ESERCIZIO COMMENTATO
Architettura VPN

CONTENUTI DIGITALI INTEGRATIVI

FILE SORGENTI
Scarica i file
TEST
Svolgi il test interattivo
AUDIO
Ascolta le risposte
AUDIO
Ascolta la pronuncia del testo
LETTURA
Verifica la traduzione

PRESENTAZIONE
Guarda la presentazione dell'Unità
MAPPA MODIFICABILE
CASE STUDY
Sicurezza delle reti wireless
FILE SORGENTI
Scarica i file
TEST
Svolgi il test interattivo
AUDIO
Ascolta le risposte
AUDIO
Ascolta la pronuncia del testo
LETTURA
Verifica la traduzione

PRESENTAZIONE
Guarda la presentazione dell'Unità
MAPPA MODIFICABILE
CASE STUDY
Reti mobili per la domotica
FILE SORGENTI
Scarica i file
TEST
Svolgi il test interattivo
AUDIO
Ascolta le risposte
AUDIO
Ascolta la pronuncia del testo
LETTURA
Verifica la traduzione

INDICE

CONTENUTI DIGITALI INTEGRATIVI

PRESENTAZIONE
Guarda la presentazione dell'Unità

MAPPA MODIFICABILE

CASE STUDY
Virtualizzazione e cloud

TEST
Svolgi il test interattivo

AUDIO
Ascolta le risposte

AUDIO
Ascolta la pronuncia del testo

LETTURA
Verifica la traduzione

PRESENTAZIONE
Guarda la presentazione dell'Unità

MAPPA MODIFICABILE

CASE STUDY
Creazione di una rete e gestione degli accessi

TEST
Svolgi il test interattivo

AUDIO
Ascolta le risposte

AUDIO
Ascolta la pronuncia del testo

LETTURA
Verifica la traduzione

CONTENUTI DIGITALI INTEGRATIVI

PRESENTAZIONE
Guarda la presentazione dell'Unità

MAPPA MODIFICABILE

ESERCIZI COMMENTATI
Monitoraggio della rete
Troubleshooting

TEST
Svolgi il test interattivo

AUDIO
Ascolta le risposte

AUDIO
Ascolta la pronuncia del testo

LETTURA
Verifica la traduzione

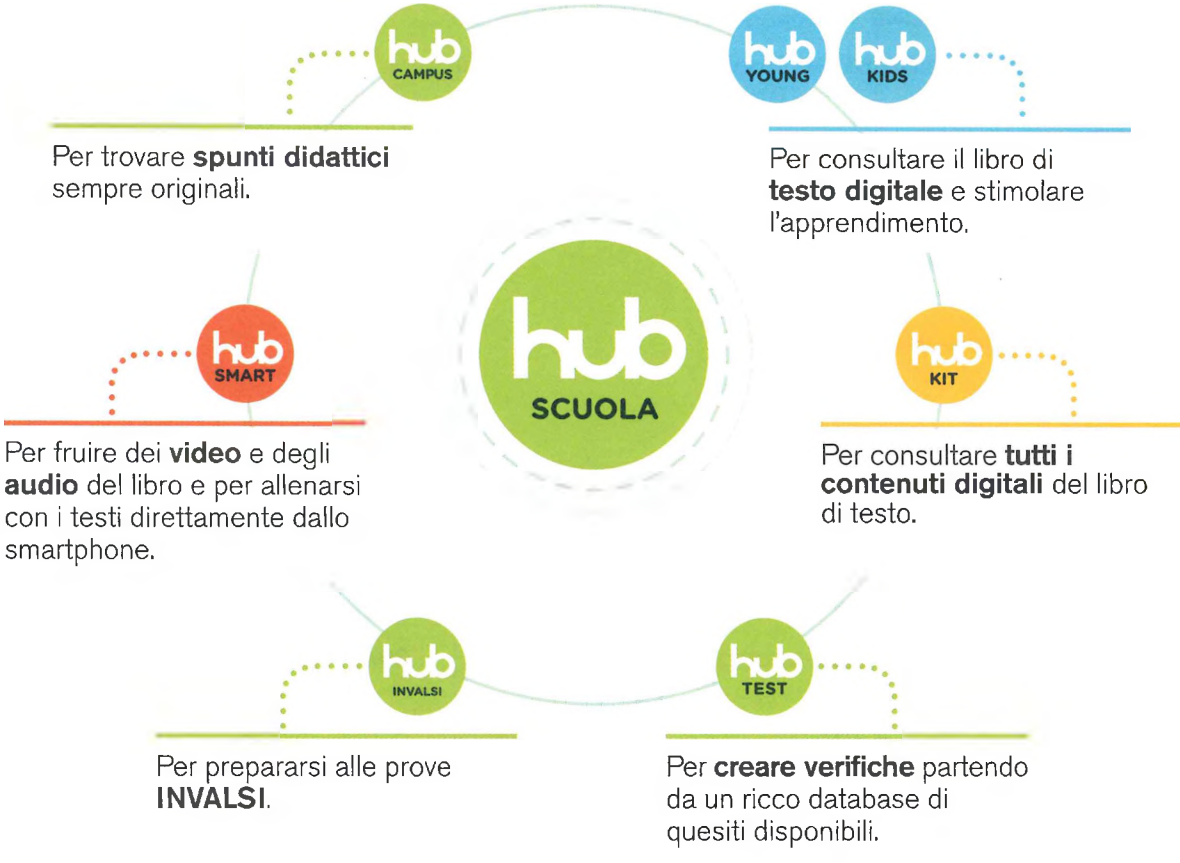
PRESENTAZIONE
Guarda la presentazione dell'Unità

MAPPA MODIFICABILE

FILE SORGENTI
Scarica i file

HUB Scuola: per una didattica digitalmente aumentata

HUB Scuola è la piattaforma che permette a studenti e docenti di **consultare il libro digitale, esplorare le risorse multimediali** integrate nel libro e **condividere i contenuti disponibili.**



Per accedere a hubscuola.it
Sei registrato? Usa le tue credenziali Mondadori Education e inizia a consultare i contenuti.
Non sei registrato? Clicca su **registrati** e compila il form.

Per Scaricare HUB Young o HUB Kids
L'App è scaricabile direttamente da **hubscuola.it** oppure dai principali store on line.
Lancia l'App, effettua il login e nella libreria troverai tutti i libri che hai attivato.

Link utili
- La piattaforma per la didattica digitale: **hubscuola.it**
- Il sito web con le nostre novità: **mondadorieducation.it**
- L'assistenza per tutti: **assistenza.hubscuola.it**

DDI+

Didattica Digitale Integrata Plus

Scopri i vantaggi della DDI Plus di Mondadori Education

È Integrata perché

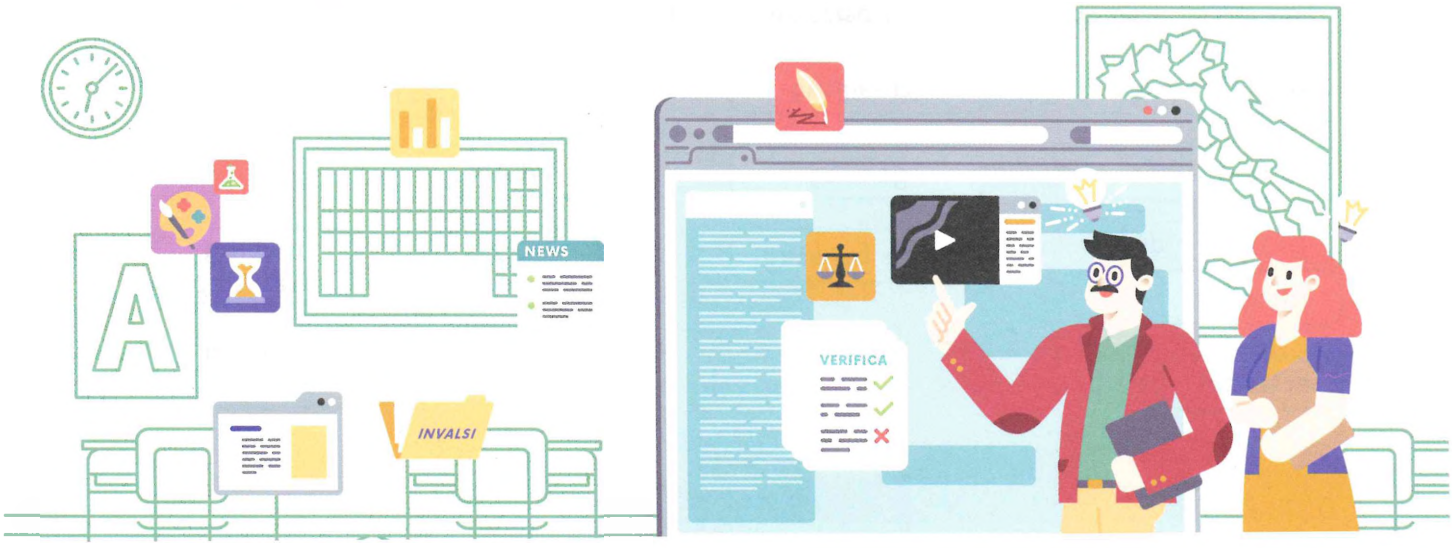
grazie ad **HUB Scuola** in un unico ambiente potrai trovare

- i vantaggi del **libro di testo**
- **contenuti digitali** complementari
- **servizi specifici** per la progettazione didattica
- **lezioni digitali** per tutte le aree disciplinari

Scopri di più su
mondadorieducation.it

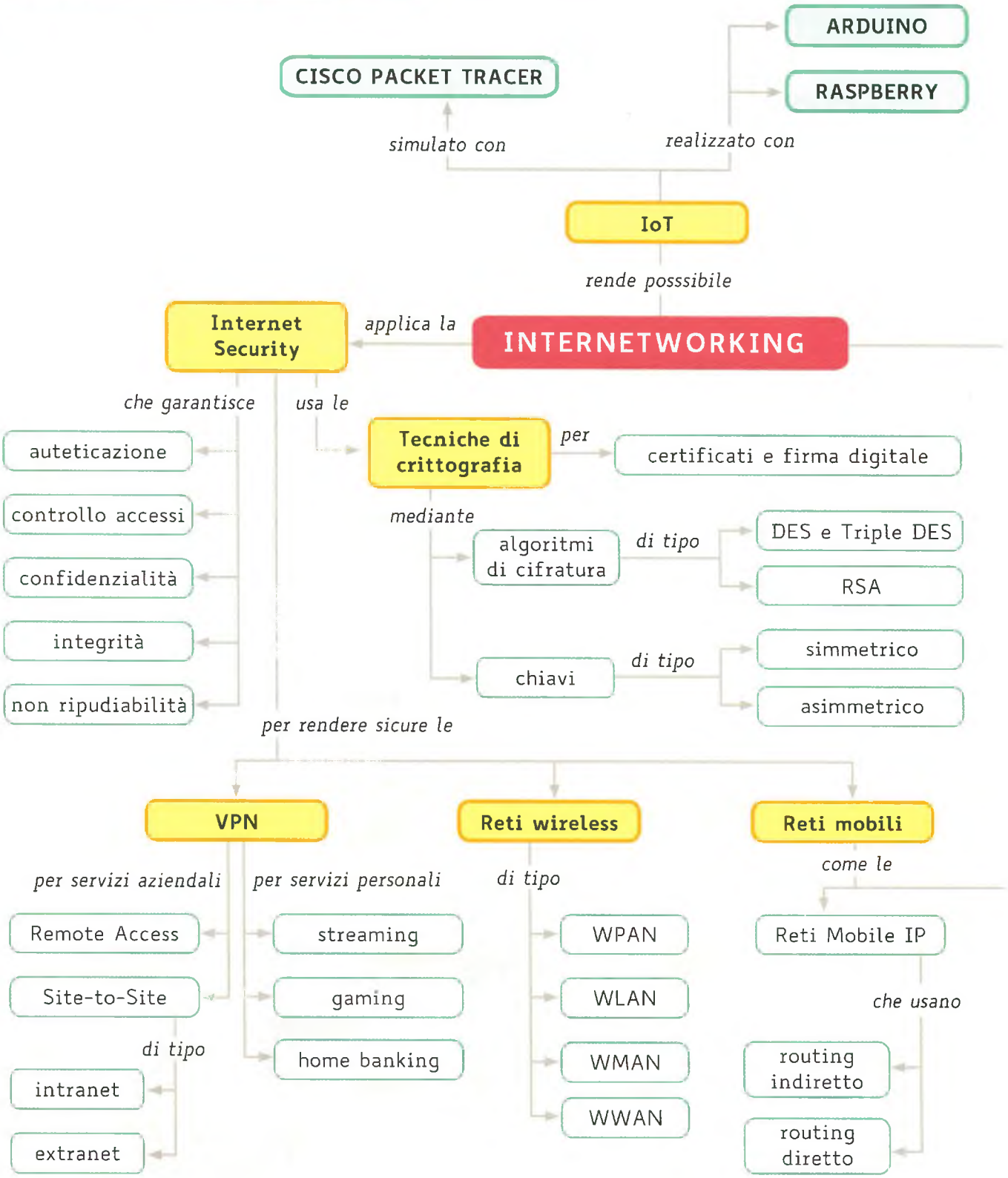
È Plus perché garantisce

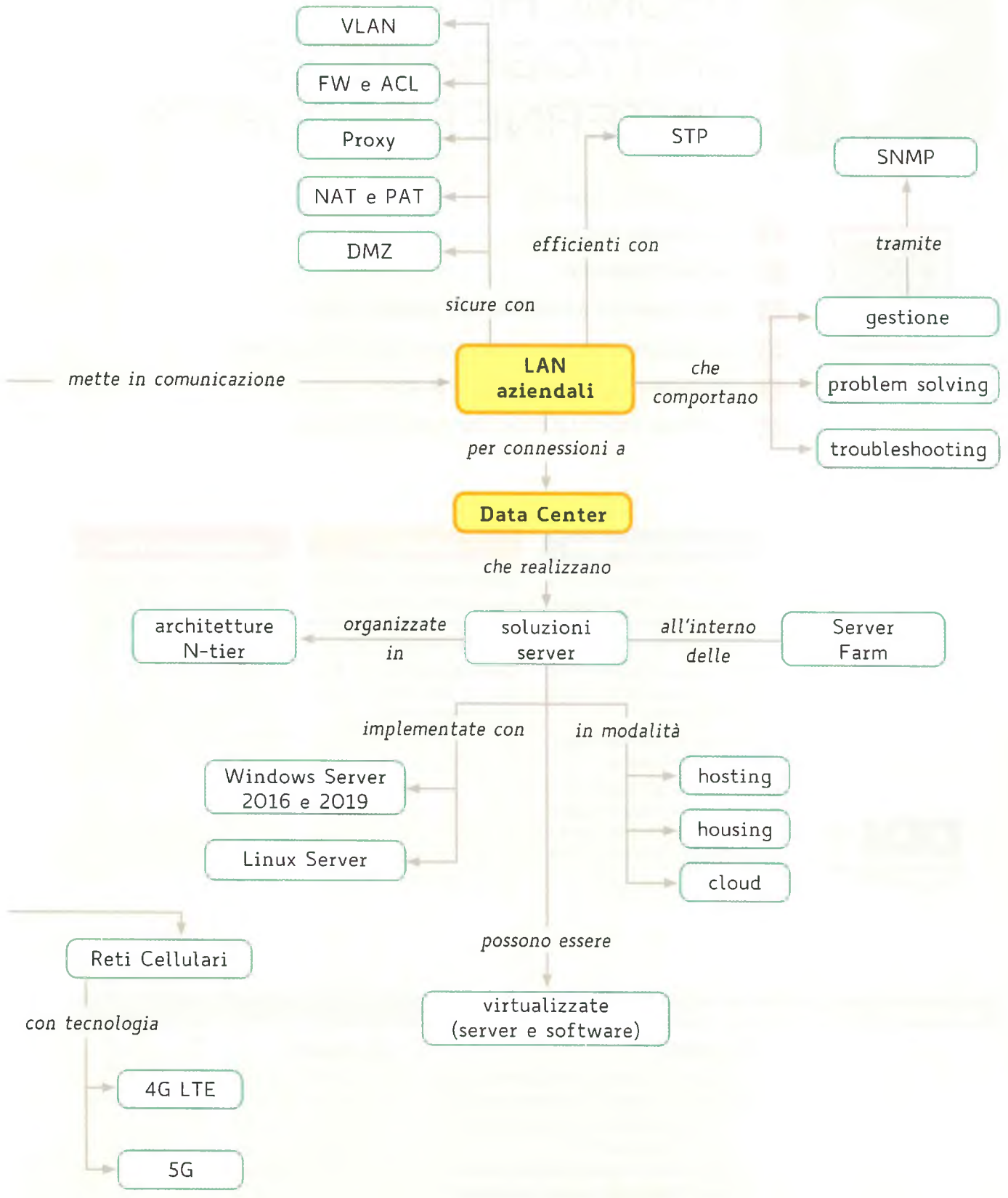
- più **innovazione** grazie a **nuove metodologie** didattiche e allo sviluppo di nuove competenze: *blended learning*, classe capovolta, *debate*, apprendimento cooperativo, contesti di realtà, sviluppo delle competenze interdisciplinari
- più **inclusione** promuovendo le abilità e le competenze di ciascun alunno
- più **personalizzazione** grazie a contesti di apprendimento, adatti a diversi stili cognitivi per la promozione dell'autonomia e della creatività
- più **ingaggio motivazionale** grazie a un apprendimento attivo
- più **feedback e valutazione** grazie a HUB Test e a griglie e strumenti anche per l'autovalutazione
- più **formazione qualificata** per i docenti per accompagnarli nella progettazione e nella pratica didattica



MAPPA DEGLI ARGOMENTI DEL VOLUME

L'Internetworking




VLAN
FW e ACL
Proxy
NAT e PAT
DMZ
STP
SNMP
efficienti con
tramite
sicure con
gestione
mette in comunicazione
LAN aziendali
che comportano
problem solving
troubleshooting
per connessioni a
Data Center
che realizzano
architetture N-tier
organizzate in
soluzioni server
all'interno delle
Server Farm
implementate con
in modalità
Windows Server 2016 e 2019
Linux Server
hosting
housing
cloud
possono essere
Reti Cellulari
virtualizzate (server e software)
con tecnologia
4G LTE
5G

UNITÀ 1

TECNICHE DI CRITTOGRAFIA PER L'INTERNET SECURITY

Guarda la **presentazione** dell'unità

IN QUESTA UNITÀ

conoscenze

Conoscere le problematiche relative alle trasmissioni di dati sensibili attraverso la rete pubblica Internet.

Conoscere le tecniche di crittografia applicate ai dati da trasmettere.

Conoscere i principali algoritmi di crittografia.

Conoscere i principali servizi che si basano sulla crittografia delle trasmissioni come i certificati digitali e la firma digitale.

abilità

Saper scegliere e configurare gli opportuni servizi di sicurezza in base alle richieste dell'azienda o dell'utente.

Saper utilizzare i servizi digitali che hanno sostituito l'uso del formato cartaceo.

competenze

Progettare reti per il trasferimento dei dati in base ai requisiti di sicurezza richiesti.

Gestire progetti secondo le procedure e gli standard previsti dai sistemi aziendali di gestione della qualità e della sicurezza.

DDI+ Didattica Digitale Integrata Plus

FLIPPED CLASSROOM

A casa

- Leggi la Lezione 1 di questa Unità;
- ricerca in Internet la documentazione sulla privacy di almeno due ASL su territorio italiano;
- confronta i risultati trovati e riassumi in un elenco gli aspetti principali.

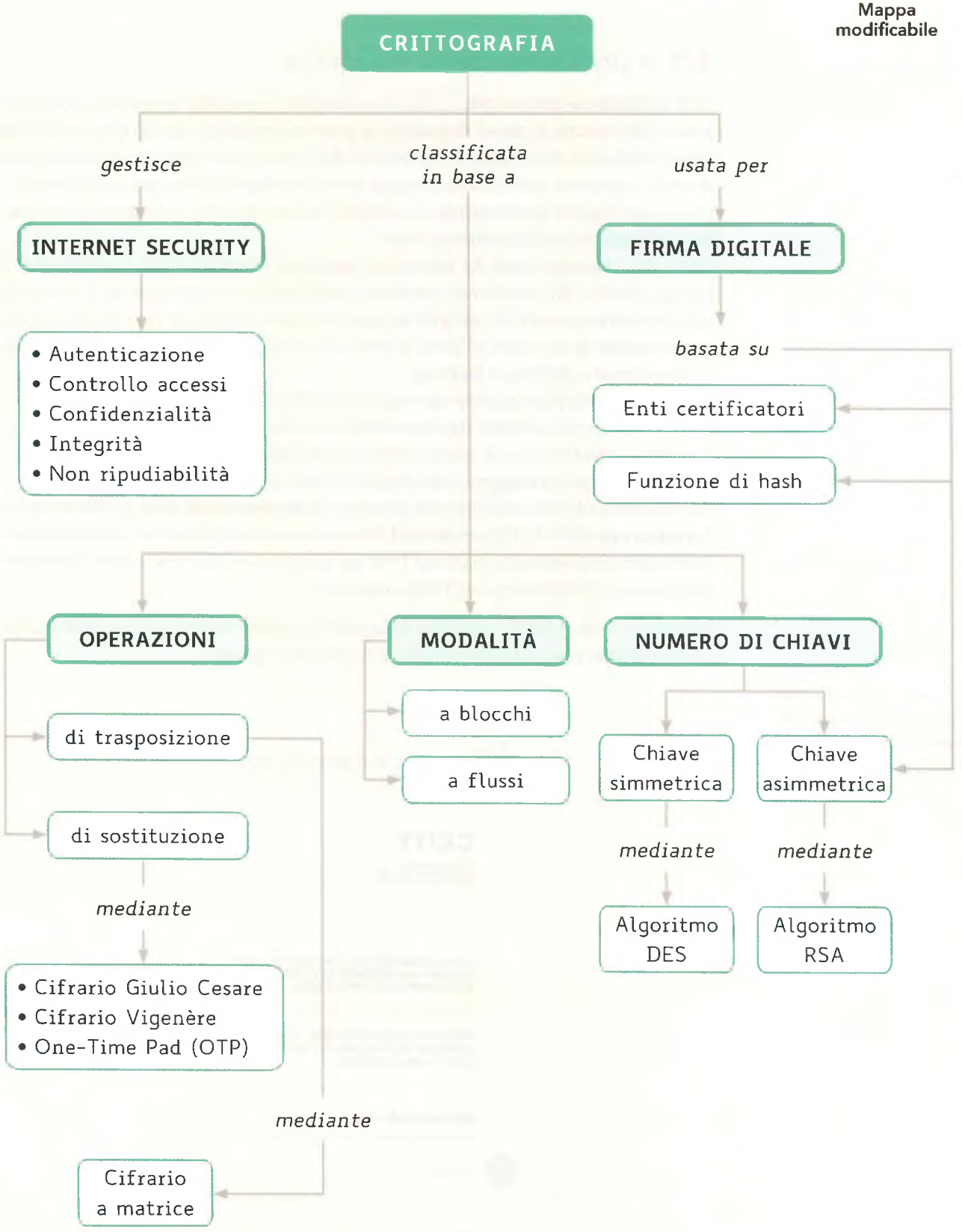
In classe

- Confrontate i risultati trovati;
- valutate se tra questi vi sono differenze sostanziali;
- discutete i motivi che spiegano le eventuali differenze.

MAPPA CONCETTUALE

DIDATTICA INCLUSIVA

Mappa modificabile



1 L'INTERNET SECURITY

1.1 Il problema della sicurezza

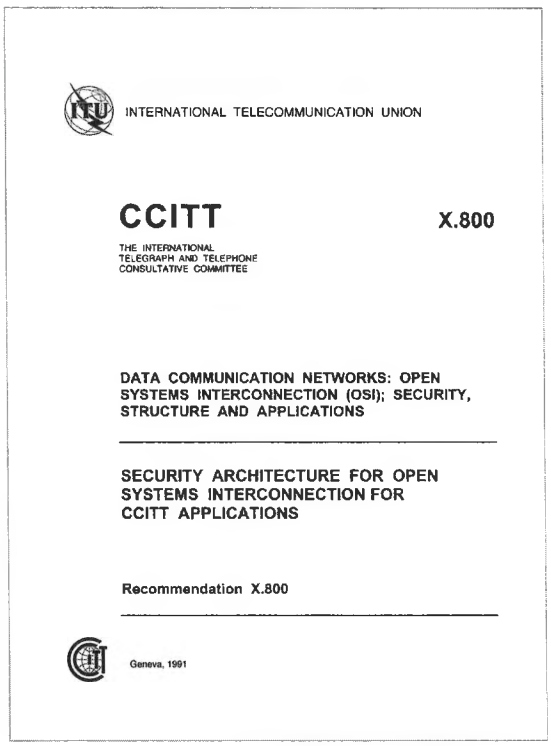
Con la diffusione sempre più capillare della rete Internet e dei suoi servizi, accompagnata dalla nascita di nuovi dispositivi, soprattutto mobili, in grado di accedere alla rete ed elaborare informazioni, il problema della sicurezza è diventato fondamentale. Se tutti i computer stand-alone possono avere problemi di sicurezza, questi aumentano notevolmente nel momento in cui due computer trasferiscono dati tra loro, cioè sono in qualche modo connessi in rete.

Oltre alla sicurezza fisica dei dati (locali adeguati, controllo degli accessi, unità di backup, file di LOG, programmi antivirus, tecniche di fault-tolerance, ecc.), l'uso delle reti richiede strumenti che permettano di proteggere le informazioni durante il loro trasferimento da un nodo all'altro. Si pensi allo sviluppo del commercio elettronico (e-commerce) o dell'home banking.

Attraverso la rete pubblica Internet vengono trasferiti PIN, codici di accesso, password: dati estremamente sensibili che non debbono essere assolutamente letti da altri che non siano il destinatario. A questo scopo nasce l'**Internet Security**: insieme di misure utilizzate per proteggere i dati durante la loro trasmissione sulla rete Internet.

Il documento alla base dell'Internet Security è la **Recommendation X.800 Security Architecture** dell'ITU-T (International Telecommunication Union-Telecommunication Standardization Sector), che fino al 1992 era nota come CCITT (Comité Consultatif International Téléphonique et Télégraphique).

In FIGURA 1 è mostrata la copertina della pubblicazione, mentre nel box della pagina a fianco è riportata l'Introduzione del documento originale.


INTERNATIONAL TELECOMMUNICATION UNION

CCITT X.800

THE INTERNATIONAL TELEGRAPH AND TELEPHONE CONSULTATIVE COMMITTEE

DATA COMMUNICATION NETWORKS: OPEN SYSTEMS INTERCONNECTION (OSI); SECURITY, STRUCTURE AND APPLICATIONS

SECURITY ARCHITECTURE FOR OPEN SYSTEMS INTERCONNECTION FOR CCITT APPLICATIONS

Recommendation X.800

Geneva, 1991

FIGURA 1 Copertina della "Recommendation X.800 Security Architecture"

IN ENGLISH PLEASE

Recommendation X.800

Security architecture for open systems interconnection for CCITT applications

Introduction

Recommendation X.200 describes the Reference Model for open systems interconnection (OSI). It establishes a framework for coordinating the development of existing and future Recommendations for the interconnection of systems.

The objective of OSI is to permit the interconnection of heterogeneous computer systems so that useful communication between application processes may be achieved. At various times, security controls must be established in order to protect the information exchanged between the application processes. Such controls should make the cost of improperly obtaining or modifying data greater than the potential value of so doing, or make the time required to obtain the data improperly so great that the value of the data is lost.

This Recommendation defines the general security-related architectural elements which can be applied appropriately in the circumstances for which protection of communication between open systems is required. It establishes, within the framework of the Reference Model, guidelines and constraints to improve existing Recommendations or to develop new Recommendations in the context of OSI in order to allow secure communications and thus provide a consistent approach to security in OSI.

A background in security will be helpful in understanding this Recommendation. The reader who is not well versed in security is advised to read Annex A first.

This Recommendation extends the Reference Model (Recommendation X.200) to cover security aspects which are general architectural elements of communications protocols, but which are not discussed in the Reference Model.

#prendinota

Le attività di standardizzazione nel campo delle telecomunicazioni cominciarono nel 1865 quando per volontà di Napoleone III venne svolta in Francia una conferenza internazionale che portò alla creazione della International Telegraph Union (ITU). Nel 1947 ITU fu trasformata in una Agenzia delle Nazioni Unite. Il CCITT (Comité Consultatif International Téléphonique et Télégraphique) venne creato nel 1956 a Ginevra per riunire vari comitati e agenzie del settore e fu rinominato ITU-T nel 1993.

X.800 impone dei requisiti di sicurezza che il sistema deve soddisfare:

1. **autenticazione**: assicurazione dell'identità dei soggetti coinvolti nella trasmissione;
2. **controllo degli accessi**: inibizione dell'uso di una risorsa da parte di soggetti non autorizzati;
3. **confidenzialità**: protezione della riservatezza dei dati (nessun soggetto terzo deve accedere ai dati dei soggetti coinvolti nella trasmissione);
4. **integrità**: assicurazione che i dati non siano stati alterati da soggetti non autorizzati;
5. **non ripudiabilità**: protezione contro la negazione di un soggetto coinvolto nella comunicazione (**paternità**).

1.2 Le tecniche di crittografia

Le tecniche di crittografia si occupano di garantire la sicurezza delle comunicazioni. L'applicazione di tali tecniche serve a conseguire l'Internet Security, ovvero a impedire o almeno rivelare e porre rimedio a eventuali violazioni della sicurezza durante la trasmissione delle informazioni.

#prendinota

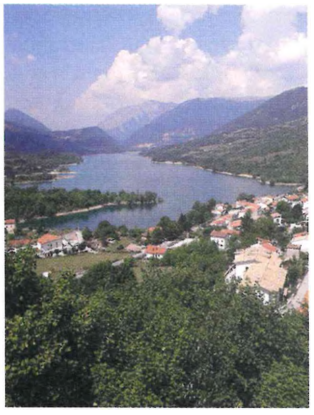
L'idea alla base della crittografia è quella di trasformare il messaggio da trasmettere in modo tale che solo utenti autorizzati riescano a leggerlo.

Di seguito alcuni esempi di violazioni della sicurezza nelle trasmissioni:

- attacco passivo (sniffing): la comunicazione viene ascoltata in modo non autorizzato;
- falsificazione dell'identità (spoofing): *A* comunica con *B* spacciandosi per *C*;
- negazione della paternità: *A* nega di aver inviato un precedente messaggio;
- attacco attivo: nella comunicazione tra *A* e *B*, *C* intercetta i messaggi e li sostituisce con altri da esso creati;
- rifiuto di servizio (Denial of Service, DoS): compromissione o disabilitazione in modo non autorizzato di alcuni servizi di rete.

La **steganografia** è invece l'insieme delle tecniche che permettono di nascondere l'esistenza del messaggio o della stessa comunicazione. In pratica, rispetto alla crittografia, il contenuto da trasmettere non viene modificato ma viene celato in un messaggio o in una immagine (FIGURA 2).

a.



b.

c.

FIGURA 2 a. Immagine con messaggio non segnalato. b. Particolare dell'immagine con messaggio segnalato. c. Messaggio

1.3 La sicurezza nella trasmissione

Le principali strategie di sicurezza nella trasmissione dei dati puntano sulla sicurezza mediante oscurazione (il sistema va configurato in modo da non essere visibile dall'esterno) o sulla sicurezza mediante confinamento (si protegge la rete nella sua globalità da attacchi esterni, isolandola).
Sono possibili anche strategie a livello di singolo host (ciascun host viene protetto separatamente, attraverso il sistema operativo o altro software locale) o di applicazione (si garantisce la protezione dei dati tramite meccanismi integrati nelle applicazioni).

Qualunque strategia si adotti, nella progettazione del servizio di sicurezza, si deve:

1. utilizzare un algoritmo per la trasformazione dei dati in chiaro in dati crittografati mediante una o più **chiavi** (la chiave è un parametro dell'algoritmo);
2. generare le chiavi da utilizzare per crittografare e decrittografare;
3. sviluppare metodi per la condivisione sicura delle chiavi;
4. specificare un protocollo che permetta di utilizzare l'algoritmo di crittografia e le chiavi segrete per comunicare in modo sicuro.

Le reti aziendali sicure, che utilizzano la rete pubblica Internet, si sono diffuse con l'introduzione delle VPN (Virtual Private Network) e dei protocolli di sicurezza dello stack IPsec che verranno trattati nella successiva Unità 3.

FISSA LE CONOSCENZE

- Che cos'è l'Internet Security?
- Qual è il documento alla base dell'Internet Security?
- Quali sono i requisiti di sicurezza che un sistema deve soddisfare?
- Qual è il primo passo nella progettazione di un servizio di sicurezza?

2 LA CRITTOGRAFIA

2.1 Cifrari e codici

La **#crittografia** è un insieme di procedure ideate allo scopo di nascondere il significato di un messaggio a tutti tranne al legittimo destinatario. Nella società dell'informazione l'utilizzo della crittografia è legato al problema della sicurezza delle transazioni attraverso la rete, in particolare quelle economiche.
Alla base delle principali tecniche di crittografia c'è un **cifrario**: in un cifrario ogni carattere del testo da cifrare viene trasformato in un altro carattere (appartenente allo stesso o a un altro alfabeto) attraverso un procedimento matematico detto algoritmo di crittografia.
Esistono anche tecniche di crittografia alla cui base c'è un **codice** anziché un cifrario: in un codice ogni carattere (o gruppo di caratteri) rappresenta un concetto, un'informazione legata a quella specifica trasmissione. Per esempio la X potrebbe voler dire «risiedo in Italia» e la Y «risiedo all'estero».

Si può notare come il codice sia strettamente legato al contesto in cui è utilizzato. Se cambio contesto devo cambiare codice.
Il cifrario invece è indipendente dal contesto e i caratteri che utilizza non hanno un significato particolare: sono solo un modo diverso di rappresentare i caratteri del messaggio da trasmettere.

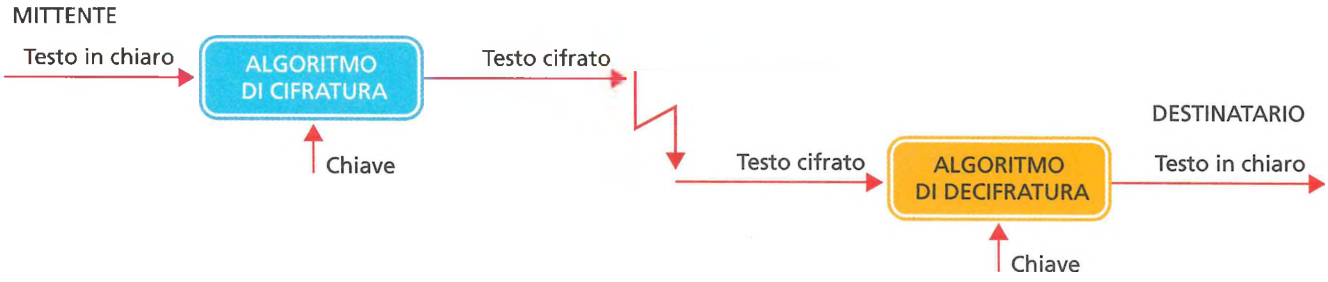
Per cifrare un testo occorrono essenzialmente due cose (FIGURA 3):
- un **algoritmo di cifratura** (pubblico);
- una **chiave** (segreta).

Per decifrare un testo servono le stesse due cose.

#techwords

La parola **crittografia** deriva dal greco: *kryptòs* = nascosto e *graphè* = scrittura.
La crittografia è l'arte del cifrare. La parola attualmente indica un procedimento che si applica principalmente nelle comunicazioni a mezzo tecnologico.
La crittoanalisi è l'insieme dei metodi per decifrare.

FIGURA 3 Schema di cifratura



Il **testo in chiaro** è il messaggio originale, non modificato e quindi comprensibile da chiunque lo intercetti se trasmesso integro.
Il **testo cifrato** è il messaggio che viene trasmesso sulla rete, modificato (ma reversibile) allo scopo di renderlo incomprensibile.
La **chiave** è una sequenza di bit di lunghezza finita, generata in modo casuale e impiegata come ingresso di un algoritmo crittografico, avente un'uscita dipendente da essa.

Notare che è solo la chiave a dover essere segreta o almeno molto difficile da individuare in tempi brevi.

#prendinota

I codici a volte sono utilizzati insieme ai cifrari per rendere ancora più difficile la comprensione del messaggio cifrato.

#prendinota

Rompere un cifrario significa semplicemente trovare una debolezza che permetta di arrivare al messaggio in chiaro senza conoscere la chiave.

L'algoritmo, data una certa chiave, deve essere in grado di generare un messaggio cifrato univoco, non generabile con altre chiavi e deve utilizzare una chiave diversa per ogni trasmissione sensibile. Non è necessario che l'algoritmo sia segreto, anzi deve essere pubblicamente testato per verificarne l'adeguatezza.
Uno dei cardini della teoria della crittografia è infatti il **Principio di Kerckhoffs** secondo il quale la sicurezza di un sistema crittografico è basata esclusivamente sulla conoscenza della chiave; in pratica si presuppone noto a priori l'algoritmo di cifratura e decifratura. Se si riesce a decifrare un messaggio senza la chiave si dice che il cifrario è stato rotto.
Possiamo quindi affermare che la sicurezza consiste fondamentalmente nel garantire o soddisfare due requisiti essenziali:

- bontà dell'algoritmo crittografico;
- difficoltà a scoprire la chiave.

2.2 Classificazione dei sistemi crittografici

I sistemi crittografici possono essere classificati in vario modo, in base al:

1. tipo di operazioni usate per trasformare il testo in chiaro in testo cifrato:
   - **crittografia a sostituzione**: ogni elemento del testo in chiaro è trasformato in un altro elemento;
   - **crittografia a trasposizione** (o permutazione): gli elementi del testo in chiaro sono riorganizzati;
2. modo in cui il testo in chiaro è elaborato:
   - **crittografia a blocchi**: il testo viene suddiviso in blocchi di N bit (dimensione fissa) e ogni blocco viene elaborato in modo indipendente dagli altri;
   - **crittografia a flusso**: elabora un quantitativo di bit variabile, senza una lunghezza predefinita;
3. numero di chiavi (distinte) utilizzate:
   - **crittografia a chiave simmetrica**: le chiavi del mittente e del destinatario sono identiche, quindi si ha una sola chiave;
   - **crittografia a chiave asimmetrica**: le chiavi sono diverse, una pubblica e una privata per ogni soggetto.

Vediamo di seguito le due tipologie di operazione usate per la trasformazione del testo: sostituzione e trasposizione.

2.3 Crittografia a sostituzione

Il **Cifrario di Giulio Cesare** è un facile esempio di crittografia a sostituzione basata su cifrario. Si narra che Giulio Cesare usasse per le sue corrispondenze riservate, come per esempio inviare ordini scritti ai suoi generali, un algoritmo semplice ma efficace per l'epoca. Scelta una chiave numerica, supponiamo il 5, ogni lettera in chiaro va sostituita dalla lettera che la segue di cinque posizioni nell'alfabeto come mostrato nella TABELLA 1 (che fa riferimento all'odierno alfabeto internazionale a 26 lettere).

TABELLA 1 Cifrario di Giulio Cesare con chiave = 5

Alfabeto non cifrato	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Alfabeto cifrato (chiave = 5)	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E

La tabella va intesa in modo circolare: dopo la Z c'è la A.

Il mittente (Cesare) e i destinatari (i generali) si dovevano accordare su una chiave numerica nota solo a loro.

In questo caso applicare l'algoritmo è molto semplice. Se per esempio il mittente vuole inviare la parola PASSWORD con chiave 5, essa diventa UFXXBTWI e questa sarà inviata. Il destinatario, conoscendo la chiave, potrà ricostruire il messaggio originale applicando l'algoritmo all'inverso.
Ovviamente si tratta di una tecnica che può facilmente essere violata (basta andare per tentativi). Inoltre le chiavi sono solo 26, poi i risultati si ripetono.

La **generalizzazione del Cifrario di Giulio Cesare** permette di rendere il cifrario più sicuro associando a ciascuna lettera del testo in chiaro una lettera scelta a caso. In questo modo la chiave, anziché un solo numero, è una sequenza di 26 numeri: ciascuno indica le posizioni da scorrere nell'alfabeto per trovare la lettera da sostituire. Per esempio: 3 (da A a D) - 9 (da B a K) - 10 (da C a M) - ...; Chiave = 3-9-10-...
Il cifrario in TABELLA 2 è il risultato finale di 26 sostituzioni a caso.

Alfabeto non cifrato	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Alfabeto cifrato random	D	K	M	U	L	A	J	S	R	G	Q	V	H	P	I	O	E	N	X	W	Z	C	F	Y	T	B

TABELLA 2 Cifrario di Giulio Cesare generalizzato

Vi sono ora 26! possibili chiavi, cioè più di 4 miliardi di diverse sequenze da 26 cifre. La situazione è migliorata ma rimane un punto debole: ogni lettera viene sempre ancora sostituita con la stessa lettera (al posto di tutte le A del testo in chiaro ci sarà sempre una D nel testo cifrato). Questo, unito alle caratteristiche dei linguaggi naturali (Italiano, Inglese, ecc.) come la maggiore o minore frequenza di certe lettere o le ripetizioni di certi gruppi di lettere, rende questi cifrari ancora deboli.

#prendinota

L'algoritmo funziona con n numero della lettera da criptare, a numero della lettera in chiaro, b numero della lettera della chiave. Per criptare: $n = a + b \pmod{26}$
Per decriptare: $n = -b + 26$

Il **Cifrario di Vigenère** supera l'ostacolo utilizzando una chiave che opera su un gruppo di lettere della stessa lunghezza della chiave (messaggio lungo come la chiave). Esso sostituisce ogni lettera in chiaro con una lettera cifrata scorrendo di tante posizioni quante sono indicate dal corrispondente numero della chiave.
Se per esempio abbiamo una chiave lunga 6 cifre: 3-15-2-6-21-8, otterremo la cifratura mostrata in TABELLA 3.

Testo in chiaro	O	T	T	O	B	I	T	F	A	N	N	O	U	N	B	Y	T	E
Chiave ripetuta	3	15	2	6	21	8	3	15	2	6	21	8	3	15	2	6	21	8
Testo cifrato	R	I	V	U	W	Q	W	U	C	T	I	W	X	C	D	E	0	M

TABELLA 3 Cifrario di Vigenère

In questo modo una lettera non viene sostituita sempre dalla medesima lettera, superando così il punto debole legato alle caratteristiche dei linguaggi. Il fatto che la chiave si ripeta a blocchi fissi però rende possibile violare questa cifratura.
Il **Cifrario One-Time Pad** (OTP) è un'evoluzione del cifrario di Vegenère. Si tratta di un cifrario con chiave di lunghezza pari alla lunghezza del testo in chiaro. Questa tecnica prevede inoltre che la chiave venga utilizzata una volta sola. One-Time Pad significa taccuino monouso.
La teoria della crittografia insegna che un cifrario è perfetto quando:

lunghezza della chiave ≥ lunghezza del messaggio

Usando una chiave aleatoria, lunga quanto il messaggio, casuale e che cambia ogni volta, si ottiene un cifrario perfetto (TABELLA 4).

TABELLA 4 Cifrario One-Time Pad (OTP)

Testo in chiaro	O	T	T	O	B	I	T	F	A	N	N	O	U	N	B	Y	T	E
Chiave NON ripetuta	2	16	3	6	21	2	4	14	1	6	20	8	1	15	7	6	19	5
Testo cifrato	Q	J	W	U	W	K	X	T	B	T	H	W	V	C	I	E	P	J

In questo caso la chiave va cambiata a ogni messaggio altrimenti comincerebbero ad apparire ripetizioni e somiglianze tra messaggi inviati, rompendo di fatto la sicurezza di OTP. OTP è l'unico algoritmo per cui si sia dimostrata *matematicamente* la sicurezza assoluta a condizione che la chiave sia veramente casuale e utilizzata una sola volta. La difficoltà diventa dunque da un lato generare chiavi sempre diverse, dall'altro distribuire chiavi così lunghe in modo sicuro. Di solito mittente e destinatario si scambiano in anticipo un congruo numero di chiavi attraverso un canale sicuro.

2.4 Crittografia a trasposizione

Una tecnica crittografica a trasposizione è il **Cifrario a matrice**.
Mittente e destinatario si accordano su una chiave segreta (per esempio la parola CIFRA). Il mittente scrive il testo in una matrice avente tante colonne quante sono le lettere della chiave e tante righe fino a contenere tutto il testo (riempiendo eventualmente la matrice con asterischi).

Se per esempio dobbiamo inviare il messsaggio "Ottobitfannounbyteeduebytefannounaword" nella TABELLA 5 vediamo come il mittente prepara il messaggio da inviare.

TABELLA 5 Cifrario a matrice con chiave = CIFRA

Chiave	C	I	F	R	A
Testo	O	T	T	O	B
	I	T	F	A	N
	N	O	U	N	B
	Y	T	E	E	D
	U	E	B	Y	T
	E	F	A	N	N
	O	U	N	A	W
	O	R	D	*	*

Il messaggio cifrato finale si ottiene prendendo le colonne della tabella secondo l'ordine alfabetico della chiave (nell'esempio di prima la colonna A, poi la colonna C, poi la F, quindi la I e infine la R). Il messaggio cifrato da inviare sarà quindi:

BNBDTNW*OINYUEOOTFUEBANDTTOTEFUROANEYNA*

Con questa tecnica gli elementi del testo in chiaro non sono stati sostituiti, sono stati riorganizzati.
Il destinatario, usando la stessa chiave, è in grado di ricostruire il messaggio individuando le colonne e posizionandole correttamente.
Anche questa tecnica crittografica può facilmente essere violata: i cifrari a trasposizione non sono sicuri. L'algoritmo può essere reso più robusto effettuando due o più trasposizioni (o permutazioni) successive anziché una sola.
Tuttavia una sostituzione seguita da una trasposizione rendono il cifrario molto più resistente. I moderni sistemi crittografici sfruttano questa tecnica.

FISSA LE CONOSCENZE

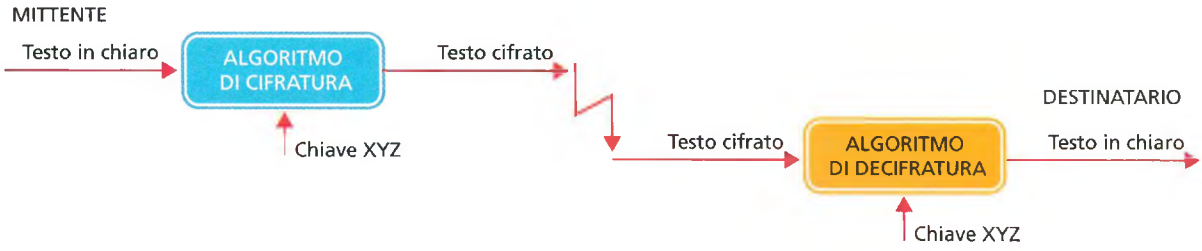
- Di che cosa tratta la crittografia?
- Che cos'è un cifrario?
- Che differenza c'è tra crittografia a sostituzione e crittografia a trasposizione?
- Elenca i principali esempi di crittografia a sostituzione.

3 CRITTOGRAFIA SIMMETRICA E ASIMMETRICA

3.1 Crittografia a chiave simmetrica

La crittografia a chiave simmetrica (o a chiave segreta) si basa sull'utilizzo di una sola chiave, usata dal mittente per cifrare e dal destinatario per decifrare (FIGURA 4). I cifrari a sostituzione e a trasposizione descritti nella Lezione precedente sono tutti a chiave simmetrica.

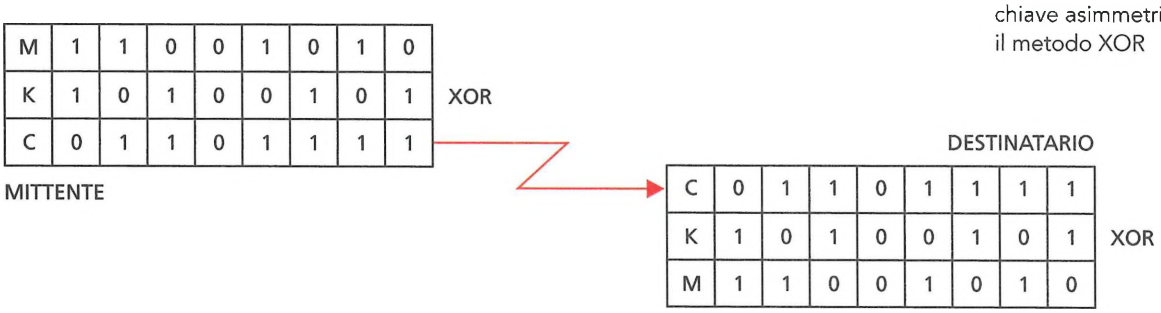
FIGURA 4 Crittografia a chiave simmetrica



Un altro esempio di crittografia a chiave simmetrica, che ha anche un algoritmo perfettamente simmetrico, è il **metodo XOR**.

Se il mittente deve trasmettere il messaggio in chiaro M = 11001010 con chiave K = 10100101, facendo l'XOR otterrà il messaggio cifrato C = 01101111 da trasmettere. Ricevuto il messaggio cifrato C = 01101111, il destinatario farà l'XOR con la stessa chiave K = 10100101 ottenendo così il messaggio originario M = 11001010.
Il procedimento è riassunto in FIGURA 5.

FIGURA 5 Crittografia a chiave asimmetrica con il metodo XOR



In questo caso l'algoritmo di decifratura è **identico** a quello di cifratura.
Negli esempi visti in precedenza, invece, l'algoritmo era sempre **inverso**. Per esempio con Giulio Cesare l'algoritmo di cifratura prevede uno spostamento in avanti nell'ordine alfabetico mentre l'algoritmo di decifratura prevede uno spostamento all'indietro.
Ovviamente gli attuali algoritmi di cifratura/decifratura in commercio prevedono operazioni ben più complesse che una semplice XOR, al fine di garantire la robustezza della tecnica di crittografia.
Nella prossima Lezione vedremo l'algoritmo **DES** (Data Encryption Standard) da cui si sono sviluppati i principali algoritmi simmetrici oggi in commercio.
Risulta ovvio che, anche nei sistemi a chiave simmetrica, la segretezza della chiave è determinante per garantire la sicurezza della comunicazione. La questione della sicurezza, ancora una volta, si riconduce al problema della distribuzione delle chiavi attraverso una trasmissione riservata, generando un circolo vizioso.

3.2 Crittografia a chiave asimmetrica

La crittografia a chiave asimmetrica (o a chiave pubblica) nasce per risolvere il problema della **distribuzione sicura delle chiavi**. Essa utilizza due chiavi per ciascun soggetto, una **privata**, nota solo al soggetto, l'altra **pubblica**, distribuita a tutti i possibili soggetti con cui il primo vuole comunicare in sicurezza.

Se per esempio abbiamo 3 soggetti *A*, *B* e *C*, avremo che:
A possiede: chiave privata di *A*, chiave pubblica di *B* e chiave pubblica di *C*;
B possiede: chiave privata di *B*, chiave pubblica di *A* e chiave pubblica di *C*;
C possiede: chiave privata di *C*, chiave pubblica di *A* e chiave pubblica di *B*.

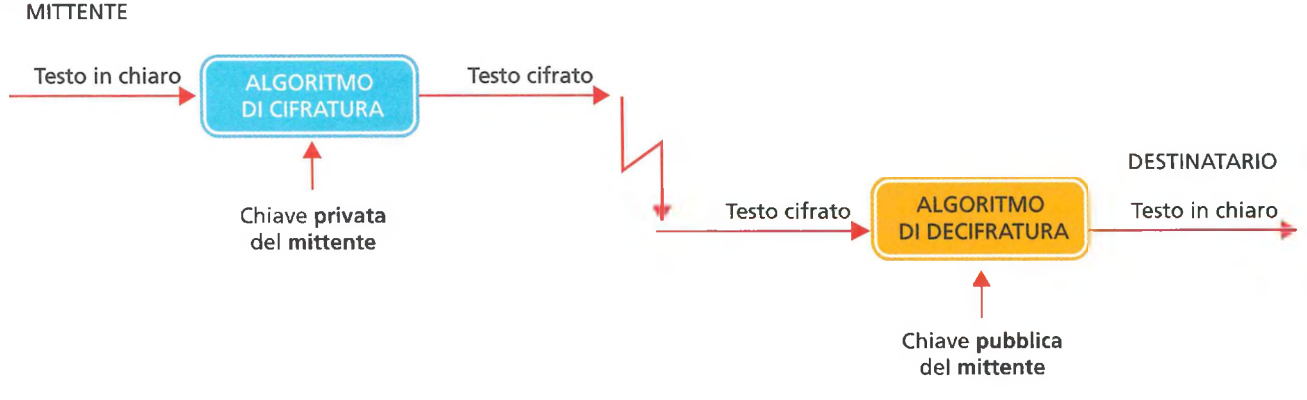
In generale il numero di chiavi totali da generare sarà sempre 2 × N dove N è il numero di soggetti che vogliono comunicare tra loro in sicurezza. A seconda di come vengono impiegate queste coppie di chiavi abbiamo 3 diversi possibili utilizzi.

1. Assicurare la riservatezza del dialogo: **confidenzialità** (FIGURA 6).
   Poiché solo il destinatario conosce la propria chiave privata, un ascoltatore non autorizzato non può decifrare la trasmissione. Notare come, in questo caso, viene utilizzata solo la coppia di chiavi del destinatario.
   Questi, infatti, dovrà aver precedentemente distribuito la sua chiave pubblica a tutti i possibili mittenti. Questo utilizzo, di per sé, non garantisce l'identità del mittente: chiunque tra i mittenti in possesso della chiave pubblica del destinatario potrebbe aver inviato il testo.

FIGURA 6 Confidenzialità

2. Garantire l'identità del mittente: **autenticazione** (FIGURA 7).
   Il destinatario sarà certo dell'identità del mittente da cui ha ricevuto il testo cifrato perché solo con la chiave pubblica avuta dal mittente stesso si riesce a decifrare quel testo.

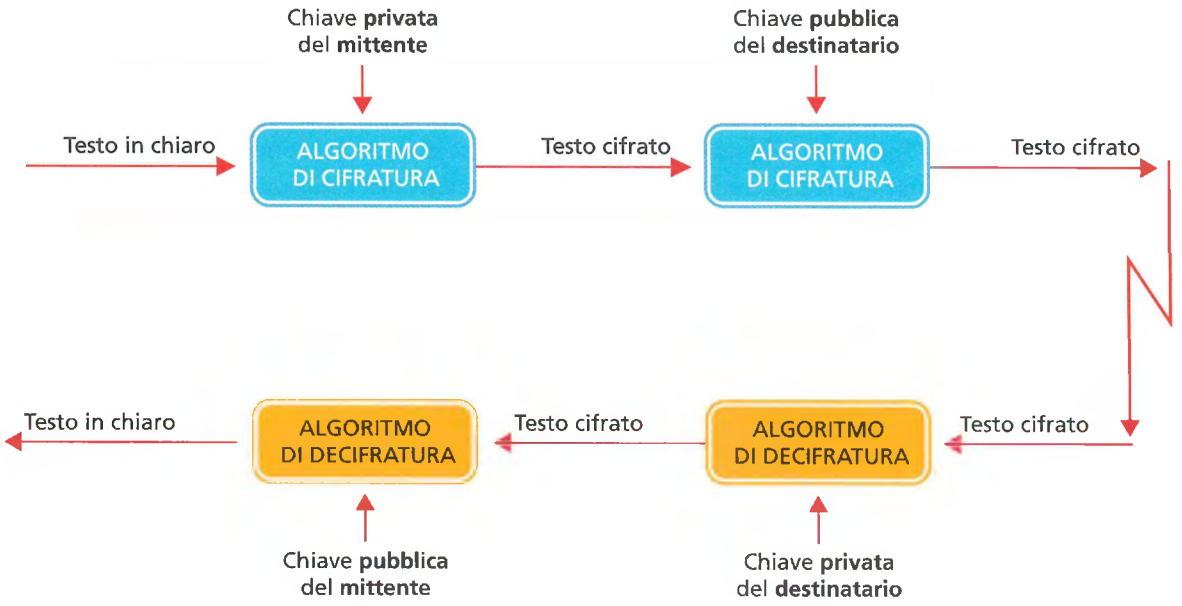
FIGURA 7 Autenticazione



Notare come, questa volta, venga utilizzata solo la coppia di chiavi del mittente. Questi dovrà avere precedentemente distribuito la sua chiave pubblica a tutti i destinatari a cui ha intenzione di trasmettere informazioni riservate.
In questo caso si perde la confidenzialità: chiunque in possesso della chiave pubblica del mittente potrà decifrare il testo. Ma in questo caso non è richiesto che il contenuto sia segreto, solo l'identità deve essere certa.
Se, per esempio, il Ministro dell'Istruzione invia una circolare ai Dirigenti Scolastici comunicando loro ufficialmente che le vacanze di Natale vanno dal 24/12 al 7/01, quel che conta è che i Dirigenti siano certi della provenienza del testo ricevuto e non importa se il contenuto viene letto da altri essendo una notizia di dominio pubblico.

3. Garantire la riservatezza della comunicazione, l'identità del mittente e l'integrità del messaggio: **confidenzialità**, **autenticazione** e **integrità** (FIGURA 8).
Questo utilizzo mette insieme i due casi precedenti e inoltre, poiché entrambi i soggetti usano le proprie chiavi private, è garantito anche che il messaggio non sia stato alterato (integrità).

FIGURA 8 Confidenzialità, autentificazione e integrità



La caratteristica vincente della crittografia a chiave asimmetrica è il fatto di non dover condividere la stessa chiave (quella privata) con nessuno. Quindi di non doverla distribuire, con i rischi che questo comporterebbe. Quella che si distribuisce è solo la chiave pubblica.

Per leggere un testo cifrato inviato da qualcuno occorre soltanto la chiave privata del destinatario (caso 1: la confidenzialità).
Per scrivere e inviare a qualcuno un testo cifrato occorre soltanto la chiave privata del mittente (caso 2: l'autenticazione).

In ogni caso, serve solo la chiave privata. E la chiave privata è quella che non viene distribuita.

Per poter cifrare un testo con una chiave e poi decifrarlo con una chiave completamente diversa al fine di riottenere il testo di partenza, occorre che le due chiavi siano **matematicamente correlate**.
Ma, pur conoscendo la chiave pubblica senza averne diritto (per esempio avendola intercettata mentre veniva distribuita), non deve essere possibile ricavare la chiave privata, o almeno deve essere molto difficile e richiedere lunghi calcoli.

Come sia possibile creare coppie di chiavi con queste caratteristiche lo vedremo nella successiva Lezione 5 analizzando l'algoritmo di tipo asimmetrico RSA (Rivest, Shamir, Adleman).

3.3 Autenticità delle chiavi pubbliche

L'elenco delle chiavi pubbliche è un potenziale punto debole per la sicurezza del sistema. Esiste, infatti, un rischio per l'autenticità: un soggetto può in malafede pubblicare una chiave a nome di un altro e utilizzarla per sostituirsi a lui.
Per risolvere il problema si ricorre a terze parti, dette **Certification Authority**, che garantiscono l'integrità e l'autenticità dell'elenco delle chiavi pubbliche (**Recommendation X.509 dell'ITU-T**).
La Certification Authority deve essere al di sopra di ogni sospetto, compatibilmente con il livello di sicurezza desiderato. Si tratta quindi di un ente pubblico o privato (es. Aruba, Poste Italiane, ecc.), che viene abilitato a emettere un certificato digitale. Questo ente dovrà seguire una procedura di certificazione basata su standard internazionali e in conformità alla normativa europea e nazionale in materia.
Questi enti vengono accreditati da un organismo istituito a livello nazionale in base alla Direttiva europea 1999/93/CE, recepita dal Decreto Legislativo 23 gennaio 2002, n. 10 che prescrive che «Ciascuno Stato membro provvede affinché venga istituito un sistema appropriato che consenta la supervisione dei prestatori di servizi di certificazione stabiliti nel loro territorio e rilascia al pubblico certificati qualificati».
Attualmente in Italia l'organismo che accredita i soggetti certificatori è l'AgId (Agenzia per l'Italia Digitale), istituito nel 2012, ereditando le funzioni di precedenti enti governativi come il Centro Nazionale per l'Informatica nella Pubblica Amministrazione (CNIPA). Oltre ad accreditare i certificatori, AgID ne controlla l'operato ed emana i regolamenti in conformità alla legislazione applicabile corrente.

Approfondiremo le Certification Authority nella successiva Lezione 6 di questa Unità, dove illustreremo strumenti come la firma digitale, per la quale gli enti certificatori giocano un ruolo determinante.

Case study
La sicurezza dei dati in rete

FISSA LE CONOSCENZE

- Quante chiavi servono nella crittografia simmetrica?
- Come funziona il meccanismo delle chiavi asincrone?
- Come si garantisce la confidenzialità, autentificazione e integrità
- Come si può garantire l'autenticità delle chiavi pubbliche?

4 GLI ALGORITMI DI CRITTOGRAFIA DES E TRIPLE DES

4.1 L'algoritmo a chiave simmetrica DES

Il capostipite dei moderni algoritmi di crittografia a chiave simmetrica è il **DES** (Data Encryption Standard), creato nel 1976 per il governo degli Stati Uniti.

Come abbiamo visto nella precedente Lezione, la crittografia a chiave simmetrica ha il grosso problema della segretezza della chiave legato alla sua distribuzione. Occorre dunque che anche l'algoritmo (e non solo la chiave) si faccia carico dell'onere di garantire la sicurezza. E per fare questo dovrà per forza essere piuttosto complesso. Partendo da un testo in chiaro e da una chiave segreta, deve generare testi casuali utilizzando un algoritmo deterministico.

Claude Shannon, ingegnere e matematico statunitense, considerato uno dei padri della teoria dell'Informazione, già negli anni Quaranta del secolo scorso mostrò che per ottenere il risultato sperato serve che l'algoritmo di cifratura abbia almeno due caratteristiche:

- **Confusion** (confusione): renda confusa la relazione tra il testo in chiaro e quello cifrato, tipicamente tramite la sostituzione dei caratteri in chiaro con caratteri diversi.
- **Diffusion** (diffusione): alteri la struttura del testo in chiaro spargendo i caratteri su tutto il testo cifrato, tipicamente permutando (trasponendo) i caratteri del testo in chiaro.

Ognuna di queste tecniche, se usata da sola, non basta e anche se vengono usate congiuntamente una sola volta non garantiscono la sicurezza. Quindi l'idea di base è quella di ripetere molte volte una serie di operazioni di confusione e diffusione (tramite sostituzioni e permutazioni).

Nel DES confusione e diffusione sono soddisfatte attraverso una serie (round) di permutazioni del messaggio e combinazioni del messaggio con la chiave.

Le sue caratteristiche principali sono:

- input:
  - testo in chiaro suddiviso in blocchi di dimensione fissa pari a 64 bit;
  - chiave a 56 bit, quindi 2^{56} possibili chiavi diverse (più di 7,2 miliardi);
- sequenza di passi:
  a. permutazione iniziale;
  b. suddivisione di ogni blocco in 2 sottoblocchi (sinistro e destro) da 32 bit;
  c. schedulazione della chiave in 16 sottochiavi da 48 bit ciascuna;
  d. sequenza di 16 round tra i due sottoblocchi e la chiave mediante XOR, sostituzioni e permutazioni;
  e. permutazione finale;
  f. scambio di posizione tra i due sottoblocchi per predisporre la decifratura;
- output:
  - testo cifrato suddiviso in blocchi di dimensione fissa pari a 64 bit.

Durante ogni round l'output della metà sinistra diventa l'input della destra e viceversa. Dopo il completamento di tutti i 16 round i due sottoblocchi vengono riuniti e sul risultato viene effettuata una permutazione inversa di quella iniziale. Infine si scambiano i sottoblocchi sinistro e destro per predisporre il blocco cifrato alla successiva decifrazione usando lo stesso algoritmo.

#prendinota

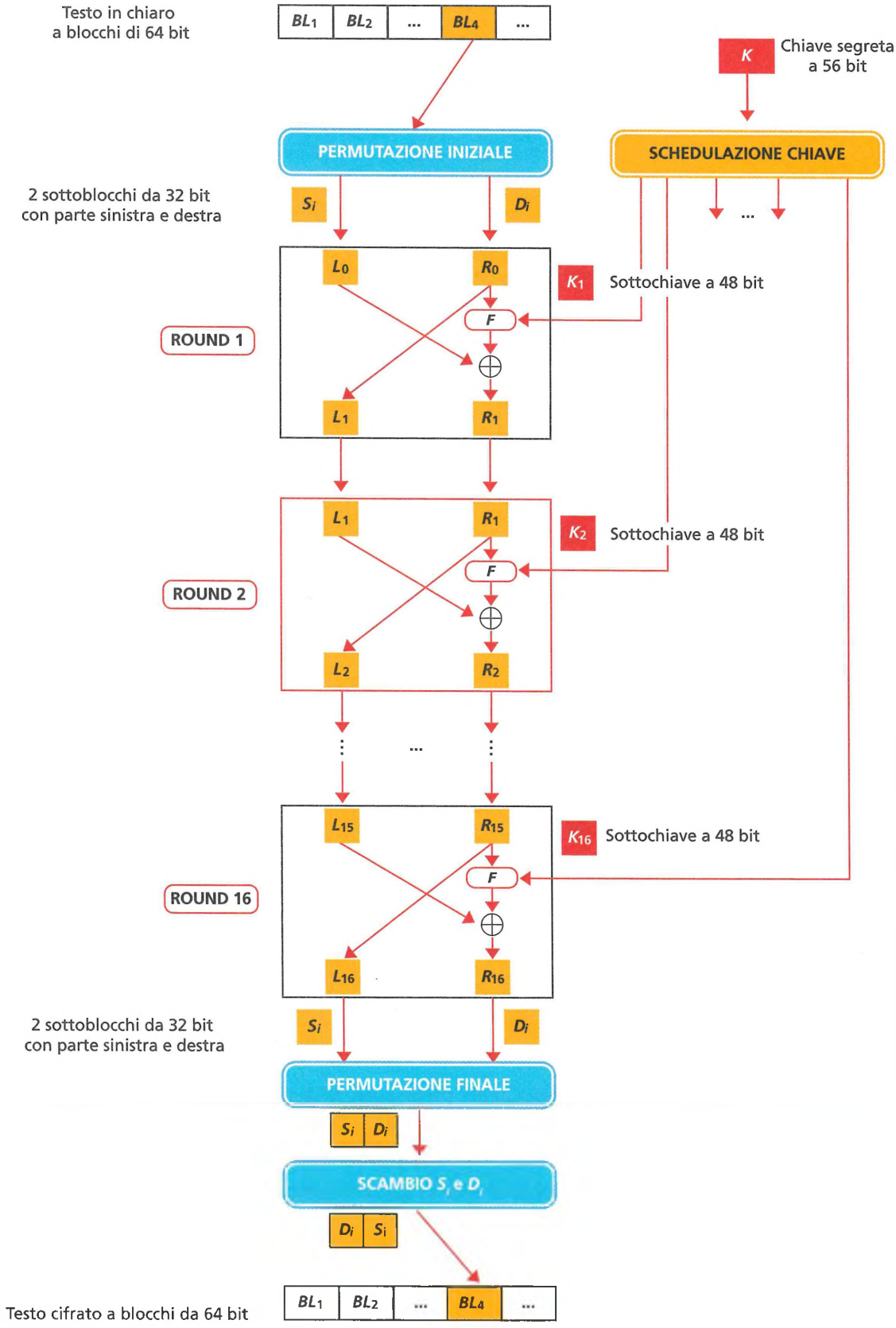
DES nel 1998 fu rotto in 3 giorni dalla EFF (Electronic Frontier Foundation) con una macchina dedicata del costo di $ 250.000. Nel 1999 tale tempo fu ridotto a 22 ore.

#prendinota

DES ha un ottimo effetto valanga: basta cambiare pochi bit nel testo in chiaro per ottenere molti bit cambiati nel testo cifrato.

FIGURA 9 Algoritmo DES

La FIGURA 9 illustra i passi eseguiti dall'algoritmo.



Analizziamo la sequenza di passi dell'algoritmo eseguita a ogni round.

Primo passo

Fa una permutazione iniziale del blocco considerato, basata su una matrice (8 × 8 dovendo lavorare su 64 bit) di permutazione casuale. Se per esempio il primo numero della matrice è 60, allora il 60° bit diventa il 1° bit del testo permutato; il 9° diventa il 2° e così via (FIGURA 10).

Secondo passo

Suddivide il testo permutato in 2 semiblocchi da 32 bit ciascuno detti S_i e D_i, intendendo la parte sinistra (alta) e la parte destra (bassa) dell'i-esimo blocco del testo. Questi 2 semiblocchi saranno l'input del primo round col nome di L_0 e R_0. Ma il primo round necessita anche di avere in input una chiave K_1.

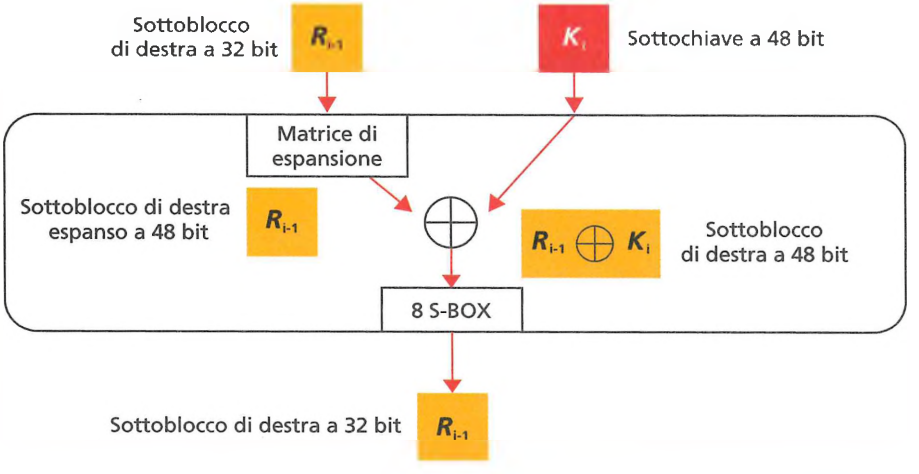
Terzo passo

Genera le 16 chiavi K_1, ..., K_{16} da 48 bit ciascuna, partendo da un'unica chiave da 56 bit. Anche per questa operazione viene usata una matrice di permutazione casuale di dimensione 8 × 7 poiché lavora su 56 bit. Tramite essa si rimescola e comprime la chiave in input (vengono eliminati i bit in posizione 9, 18, 22, 25, 35, 38, 43 e 54) per ottenere in output una chiave da 48 bit. Ogni chiave è associata a un round.

Quarto passo

Esegue i round e, all'i-esimo round, L_{i-1} e R_{i-1} saranno trasformati in L_i e R_i dall'XOR tra il semiblocco di sinistra (L_{i-1}) e l'output della funzione F ottenuto con chiave K_i. I round da eseguire sono 16 e funzionano tutti allo stesso modo.

Il cuore di tutto l'algoritmo è la funzione F (dall'iniziale del crittologo di IBM, Horst Feistel) eseguita a ogni round (FIGURA 11). A questa funzione è assegnato il compito di combinare insieme i 32 bit del semiblocco di destra con i 48 bit della chiave. Il cuore della funzione F sono le otto S-BOX. Non c'è nessuna possibilità che queste funzioni siano invertibili.



Esaminiamo nel dettaglio l'algoritmo. Inizialmente i 32 bit del blocco di destra R_{i-1} vengono espansi a 48 bit mediante una **matrice di espansione**: semplicemente alcuni bit vengono **ripetuti** (FIGURA 12).

Il funzionamento è identico alla matrice di permutazione. I 48 bit così ottenuti dall'espansione vengono messi in XOR con la K_i, chiave anch'essa di 48 bit. La nuova sequenza di 48 bit ottenuta viene suddivisa in 8 sottoblocchi da 6 bit ciascuno.

FIGURA 10 Permutazione iniziale

Testo in chiaro a blocchi da 64 bit

0	1	1	0	1	0	0	1
0	1	1	0	0	1	0	1
0	1	0	1	1	0	1	0
0	1	0	1	0	1	1	0
0	1	1	0	1	0	1	0
0	1	1	0	0	1	1	0
0	1	0	1	1	0	0	1
0	1	0	1	0	1	0	1

Matrice di permutazione

60	9	38	32	11	49	57	20
25	47	24	18	37	12	19	13
10	46	8	59	48	36	6	61
53	17	39	23	54	50	56	15
26	64	33	58	22	43	21	42
14	45	34	2	44	35	1	29
7	16	27	63	30	51	55	62
52	3	40	31	5	41	4	28

Testo permutato

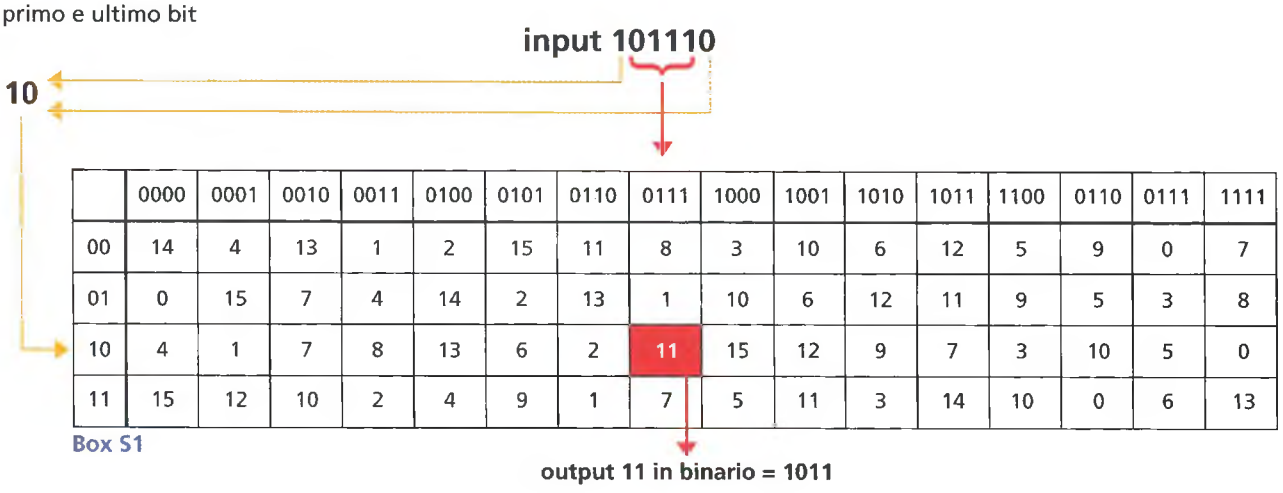
1	0	0	0				

FIGURA 11 La funzione F

FIGURA 12 Matrice di espansione

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

La 8 stringhe di 6 bit (totale 48 bit) vengono date in ingresso a 8 S-BOX diverse, ottenendo in uscita 8 stringhe di 4 bit ciascuna (totale 32 bit).
Compito della S-BOX è dunque un'operazione inversa a quella di espansione: si tratta di una **compressione** che riporta il sottoblocco a 32 bit.
Il punto cruciale per la sicurezza dell'intero algoritmo DES è la compressione tramite le S-BOX. Questa è infatti l'unica operazione non lineare dell'algoritmo, che quindi introduce caratteristiche di casualità.
La FIGURA 13 mostra come avviene una delle 8 **compressioni** da 6 bit di input a 4 bit di output.



	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	0110	0111	1111
00	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
01	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
10	4	1	7	8	13	6	2	11	15	12	9	7	3	10	5	0
11	15	12	10	2	4	9	1	7	5	11	3	14	10	0	6	13

FIGURA 13 Funzionamento di una S-BOX (compressione)

Quinto passo
Effettua una permutazione finale, inversa di quella iniziale, utilizzando un'altra matrice di permutazione e procedendo in modo analogo alla permutazione iniziale.

Sesto passo
Inverte semplicemente le posizioni di S_i e D_i al fine di predisporre il blocco cifrato alla successiva decifrazione usando lo stesso algoritmo.

L'algoritmo di decrittografia (**DES^{-1}**) applica gli stessi passi sfruttando le proprietà dell'XOR.
Quindi, invertendo il ruolo di S_i e D_i (e di conseguenza di L e R) e utilizzando le chiavi in ordine inverso, da K_{16} a K_1, si può ritornare al messaggio in chiaro passando attraverso le seguenti coppie:

$$(R_{16}, L_{16}) \xrightarrow{K_{16}} (R_{15}, L_{15}) \xrightarrow{K_{15}} (R_{14}, L_{14}) \xrightarrow{K_{14}} \dots \xrightarrow{K_1} (R_0, L_0)$$

4.2 Oltre il DES

L'algoritmo di crittografia DES (blocchi a 64 bit, chiavi a 56 bit) è il più semplice tra gli algoritmi di crittografia simmetrici.
Poiché nel tempo l'algoritmo DES è risultato non più adatto alle esigenze di sicurezza, si è cercato di ovviare al problema applicandolo ripetutamente o facendo derivare da esso nuovi algoritmi.

Il Triple DES è un algoritmo che richiede 3 chiavi di cifratura che vengono utilizzate per applicare 3 volte il DES.
Il processo di cifratura è diviso in 3 fasi:

- applicazione della chiave 1 al testo in chiaro per ottenere il testo cifrato (Crypt)
- applicazione della chiave 2 al testo cifrato per decifrarlo, ma avendo usato una chiave diversa da quella corretta si ottiene un testo nuovamente cifrato (Decrypt)
- applicazione della chiave 3 al nuovo testo (Crypt)

mentre il processo di decifratura è l'esatto opposto:

- utilizzo della chiave 3 per decifrare il testo cifrato (Decrypt)
- cifratura tramite la chiave 2 del testo appena decifrato con la chiave 3 (Crypt)
- decifratura del testo ottenuto con la chiave 2 utilizzando la chiave 1 (Decrypt)

Il Triple DES (chiamato anche 3DES) utilizza chiavi da 192 bit (di cui 168 effettivi e 24 di parità) poiché è formata dalle 3 chiavi DES. Ciascuna implementazione utilizza infatti chiavi da 64 bit (56 effettivi e 8 bit di parità).

Altri importanti algoritmi simmetrici che derivano dal DES sono:

- IDEA (International Data Encryption Algorithm)
  Algoritmo con blocchi a 64 bit e chiavi a 128 bit, è stato sviluppato presso il Politecnico di Zurigo e pubblicato nel 1991. Anche se inizialmente fu brevettato, ora è liberamente utilizzabile. È stato raccomandato da diversi organismi di standardizzazione come ITU e ISO per la sua robustezza e a oggi risulta ancora non violato.
- AES (Advanced Encryption Standard)
  Algoritmo con blocchi a 128 bit e chiavi a 128, 192 e 256 bit. È stato sviluppato da due crittografi belgi e utilizzato come standard dal governo degli USA. Si tratta di un algoritmo molto veloce, relativamente semplice da implementare, richiede poca memoria e offre un buon livello di protezione/sicurezza. Si basa su una rete a sostituzione e permutazione e non è una rete di Feistel.
- CAST (Carlisle Adams and Stafford Tavares)
  Algoritmo con blocchi a 64 o 128 bit e chiavi da 128 a 256 bit. Esitono infatti due versioni: CAST-128 e CAST-256. Questa è una rete di Feistel. I passaggi sono costituiti da 3 gruppi di operazioni dove la differenza fra di essi è minima e consiste in un'unica operazione (addizione, sottrazione o XOR).

#prendinota

Il DES e la maggior parte degli algoritmi derivati si basano sulla rete di Feistel. Questa è una struttura (inventata dal crittologo dell'IBM Horst Feistel) in cui la cifratura e decifratura sono operazioni molto simili, spesso identiche. Questo fa sì che invertendo il funzionamento del gestore della chiave si ottiene l'operazione inversa, permettendo così di poter usare gli stessi circuiti per la cifratura e la decifratura.

FISSA LE CONOSCENZE

- Che cosa si intende per Confusion e Diffusion?
- Quanti sono i round usati nella tecnica DES?
- Su che cosa si basa il Triple DES?

5 L'ALGORITMO DI CRITTOGRAFIA RSA

5.1 Algoritmi a chiave asimmetrica: RSA

L'RSA è un algoritmo a chiave asimmetrica che deve il suo nome alle iniziali dei matematici che lo crearono nel 1977: Ronald Rivest, Adi Shamir e Leonard Adleman. Come abbiamo detto nella precedente Lezione 3, gli algoritmi asimmetrici hanno il loro punto di forza nella **difficoltà a scoprire la chiave privata**, anche conoscendo quella pubblica. Una delle operazioni più difficili e lunghe da eseguire anche per i più potenti elaboratori è la **fattorizzazione di numeri a molte cifre**. Per fattorizzare un intero con 300 cifre provando a dividerlo per tutti i numeri primi a partire da 3, in media serviranno 10^{147} divisioni. Utilizzando hardware dedicati o intere reti di elaborazione parallela, servirebbero comunque anni per fattorizzarlo. Se poi il numero da fattorizzare è il prodotto di due numeri primi (quindi vi sono due e solo due fattori) molto grandi, allora diventa veramente difficile rompere il cifrario.

#prendinota

In matematica un numero **primo di Mersenne** è un numero primo esprimibile come: $N = 2^a - 1$.
Il numero primo più grande espresso come numero di Mersenne è stato scoperto nel 2016:

$$2^{74\,207\,281} - 1$$

Questo numero (con oltre due milioni di cifre) è stato calcolato e verificato da un computer della *University of Central Missouri*.

#techwords

L'**operatore mod** è l'operatore modulo di informatica e restituisce il resto intero della divisione tra i due operandi.

L'RSA si basa proprio sulla difficoltà nel fattorizzare un numero intero N molto grande ottenuto dal prodotto di due numeri primi (p e q, anch'essi molto grandi) che restano segreti. Vediamo i passi dell'algoritmo con un esempio:

1. Alice vuole trasmettere un messaggio m a Roberto: affinché il dialogo resti confidenziale sarà Roberto a dover creare la coppia di chiavi K_{PUB} e K_{PRI}, rispettivamente pubblica e privata.
2. Roberto crea la chiave pubblica costituita da una coppia di numeri $K_{PUB} = (N, N_{PUB})$ e la chiave privata costituita da una coppia di numeri $K_{PRI} = (N, N_{PRI})$.
   Come fa Roberto a creare le due chiavi matematicamente correlate in modo che si possa cifrare con una chiave e decifrare con l'altra?
   Per prima cosa sceglie due numeri primi p e q e li moltiplica tra loro ottenendo $N = p \cdot q$ (primo numero delle due chiavi).
   Poi calcola il prodotto $V = (p - 1) \cdot (q - 1)$ e sceglie N_{PRI} in modo tale che non abbia fattori in comune con V.
   Infine ricava N_{PUB} dall'equazione:
   $$(N_{PUB} \cdot N_{PRI}) \ \#\text{mod}\ V = 1$$
   Se per esempio:
   - scelgo $p = 3$ e $q = 11$ come numeri primi, da cui $N = 33$;
   - calcolo $V = (3 - 1) \cdot (11 - 1) = 20$;
   - scelgo $N_{PRI} = 7$ che non ha fattori in comune con $V = 20$;
   - tra le possibili soluzioni dell'equazione $(N_{PUB} \cdot 7) \bmod 20 = 1$ scelgo $N_{PUB} = 3$ visto che $(7 \times 3) \bmod 20 = 21 \bmod 20 = 1$;
   - avrò le chiavi $K_{PRI} = (33, 7)$ e $K_{PUB} = (33, 3)$.
3. Roberto distribuisce la chiave pubblica ad Alice e sta molto attento a **non divulgare** N_{PRI}.
4. Alice può cifrare e poi trasmettere m usando la chiave pubblica ricevuta. L'algoritmo RSA per cifrare utilizza la funzione:
   $$c = m^{N_{PUB}} \bmod N$$
   Se per esempio si vuole trasmettere semplicemente un numero (supponiamo $m = 16$) avremo che $c = 163 \bmod 33 = 4$.

5. Roberto ricevuto c può decifrare il testo usando la chiave privata tenuta segreta.
L'algoritmo RSA per decifrare utilizza la funzione $c = m^{N_{PUB}} \bmod N$.
Nell'esempio, avendo ricevuto $c = 4$ avremo che $m = 47 \bmod 33 = 16$.

Associando a ogni lettera un numero è possibile cifrare testi qualsiasi.

esempio

Supponiamo di dover cifrare con l'RSA la parola BYTE convertita in numeri in base alla posizione di ogni lettera nell'ordine alfabetico, quindi m = **225205**.

1) Scegliamo come numeri primi
$p = 17$ e $q = 5$, da cui $N = p \cdot q = 85$ e $V = (p - 1) \cdot (q - 1) = 64$.
2) Scegliamo $N_{PRI} = 5$ perché non ha fattori in comune con V.
3) Scegliamo $N_{PUB} = 13$ tra le possibili soluzioni dell'equazione $(N_{PUB} \cdot 5) \bmod 64 = 1$.
4) Quindi pronte le due chiavi $K_{PUB} = (85, 13)$ e $K_{PRI} = (85, 5)$, procediamo alla cifratura e alla decifratura come mostrato rispettivamente nella TABELLA 6 e nella TABELLA 7.

TABELLA 6 Passaggi della cifrazione

TESTO IN CHIARO	m	$m^{N_{PUB}}$	TESTO CIFRATO $c = m^{N_{PUB}} \bmod N$
B	2	8.192	32
Y	25	1.490.116.119.384.765.625	60
T	20	81.920.000.000.000.000	80
E	5	1.220.703.125	20

TABELLA 7 Passaggi della decifrazione

TESTO CIFRATO	$C^{N_{PRI}}$	$m = c^{N_{PRI}} \bmod N$	TESTO CIFRATO $c = m^{N_{PUB}} \bmod N$
32	52.521.875	2	B
60	777.600.000	25	Y
80	3.276.800.000	20	T
20	3.200.000	5	E

5.2 Vantaggi e svantaggi dell'RSA

La forza di quest'algoritmo sta nel fatto che è difficile calcolare N_{PRI} anche per chi conosce la chiave pubblica $K_{PUB} = (N, N_{PUB})$, perché bisognerebbe prima trovare i due numeri primi p e q che fattorizzano N. E come abbiamo detto all'inizio, fattorizzare i grandi numeri richiede anni e grande potenza di calcolo. Ecco perché i numeri primi sono alla base degli algoritmi di crittografia asimmetrica e vi sono grandi aziende pubbliche e private o enti di ricerca universitaria che non smettono di cercarli.
L'algoritmo RSA, nella realtà, opera a blocchi di bit e non carattere per carattere. Le chiavi che utilizza sono da 1024, 2048, 4096 o anche più bit.
Il grosso problema dell'RSA e in generale degli algoritmi asimmetrici è la loro lentezza e il largo uso delle risorse di elaborazione. RSA è 1000 volte più lento di DES dal punto di vista hardware e 100 volte dal punto di vista software.
La soluzione ottimale è quella di usare la crittografia simmetrica per cifrare i testi e sfruttare la crittografia asimmetrica solo per la breve fase di scambio della chiave segreta simmetrica. In questo modo si protegge la fase delicata della distribuzione delle chiavi simmetriche (grazie alla maggior sicurezza della crittografia asimmetrica) e poi si cifra velocemente (grazie alla maggior velocità della crittografia simmetrica).

FISSA LE CONOSCENZE

- Che cosa serve per generare testi casuali utilizzando un algoritmo deterministico?
- Perché è difficile scoprire una chiave privata?
- Quale è il grosso problema dell'RSA?

6 LA FIRMA DIGITALE E GLI ENTI CERTIFICATORI

6.1 La firma digitale

#prendinota

L'elenco degli enti certificatori accreditati attivi in Italia è reperibile all'indirizzo dell'AgID (Agenzia per l'Italia Digitale - Presidenza del Consiglio dei Ministri): *https://www.agid.gov.it/it/piattaforme/firma-elettronica-qualificata*.

A partire dal 1997, una serie di provvedimenti legislativi ha conferito valore giuridico alla **firma digitale**. La pubblicazione della Direttiva europea 1999/93/CE, nel gennaio del 2000, ha dato ulteriori impulsi al processo legislativo, imponendo un quadro comune agli Stati dell'Unione europea.

> La firma digitale, equivalente elettronico della tradizionale firma autografa su carta, è associata stabilmente al documento elettronico sulla quale è apposta e ne attesta con certezza l'**integrità**, l'**autenticità** e la **non ripudiabilità**.

Dal punto di vista tecnico e realizzativo la firma digitale è basata su un sistema a chiavi crittografiche asimmetriche, utilizza un certificato digitale rilasciato da un **ente certificatore** (Certification Authority) con specifiche capacità professionali garantite dallo Stato e viene creata mediante un dispositivo con elevate caratteristiche di sicurezza che in genere è una smart card.
La firma digitale di per sé non è in grado di garantire la reale identità del firmatario: questi potrebbe usare il nome di un terzo o anche un nome inventato.

È previsto quindi l'intervento di terze parti fidate, i **certificatori**, che verificano:

- l'identità di un soggetto e la corrispondenza con la titolarità della chiave pubblica di cifratura;
- attestano tali informazioni mediante l'emissione del certificato digitale;
- pubblicano tempestivamente la sospensione del certificato in apposite liste.

> Il file firmato digitalmente deve essere certificato dall'ente certificatore **prima** dell'invio. Attraverso il certificato il destinatario otterrà la chiave pubblica sicura che gli permetterà di verificare l'identità del mittente e l'integrità del documento.

Attualmente il nostro ordinamento prevede l'utilizzo di 3 formati per produrre file firmati digitalmente:

- **pkcs#7** (meglio noto come p7m): è il primo formato in uso fin dall'anno 1999 ed è quello che le Pubbliche Amministrazioni sono obbligate ad accettare;
- **PDF**: il 16 Febbraio 2006 è stato sottoscritto un protocollo d'intesa tra Adobe Systems Inc. e il CNIPA (Centro Nazionale per l'Informatica nella Pubblica Amministrazione) al fine di introdurre nel nostro ordinamento la possibilità di utilizzare il formato di firma definito nelle specifiche PDF, attraverso la RFC 3778;
- **XML**: è il formato più diffuso in settori come quello bancario e sanitario, in cui il linguaggio in questione ha assunto notevole rilevanza nella gestione elettronica dei flussi di dati.

Per leggere e verificare un file firmato digitalmente in formato PDF è sufficiente un comune lettore di questo formato, come Acrobat Reader, che consente, nelle ultime versioni, una perfetta lettura del contenuto e verifica dei parametri della firma. Per questo motivo la tendenza è che i documenti siano firmati in formato PDF.

6.2 Generare la firma digitale

Generare una firma digitale richiede la disponibilità del **kit di firma digitale**, composto dal dispositivo sicuro (smart card o token USB, FIGURA 14) e dal software di firma in grado di utilizzare lo specifico dispositivo di cui si è dotati.

FIGURA 14 Token USB

La procedura di firma è piuttosto banale: dopo aver reso disponibile il dispositivo, inserendo quindi la smart card nell'apposito lettore o inserendo il token USB nella porta specifica, l'applicazione di firma provvederà a richiedere l'inserimento del PIN di protezione, visualizzerà e richiederà di scegliere quale certificato si intende usare e procederà infine alla generazione della firma.
Sono disponibili anche alcuni servizi online di verifica della firma digitale come per esempio quello fornito da InfoCert (*www.firma.infocert.it/utenti/verifica.php*).

L'algoritmo di *apposizione* della firma digitale (FIGURA 15) prevede la creazione di un'**impronta** (message digest) attraverso la **funzione di hash**.

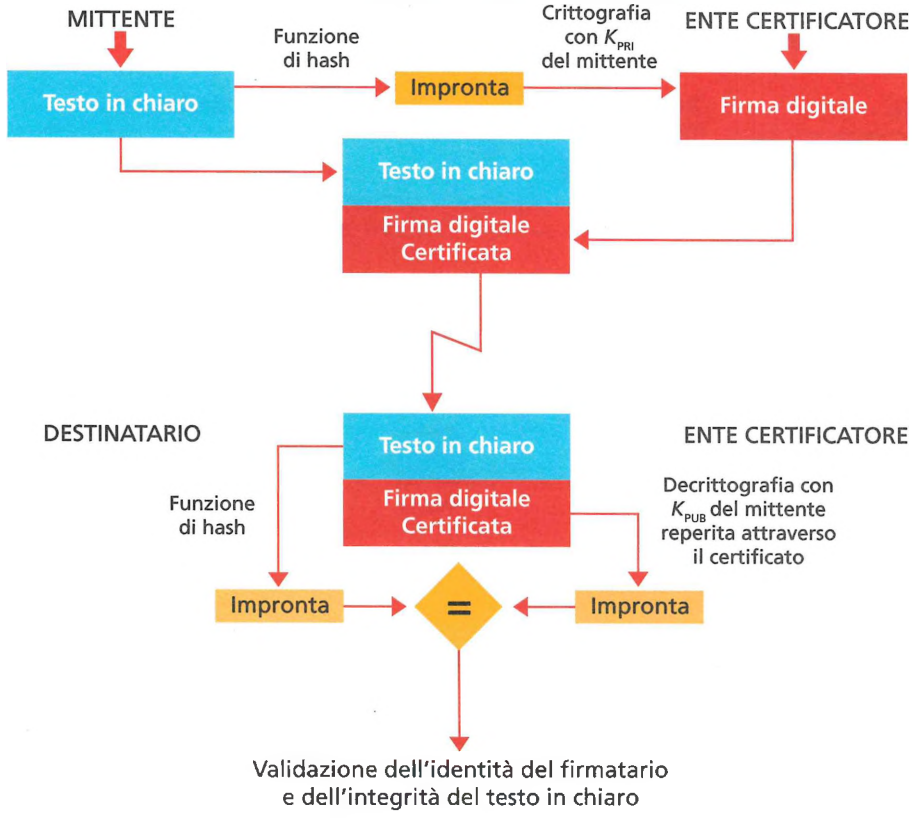


FIGURA 15 Meccanismo della firma digitale

In informatica una funzione crittografica di hash è un algoritmo matematico che trasforma dei dati di lunghezza arbitraria (messaggio) in una stringa binaria di dimensione fissa (128 o 160 bit). Gli algoritmi usati a questo proposito sono unidirezionali (one-way), quindi non invertibili (nota l'impronta, non si può ricostruire il testo che l'ha generata). Inoltre una funzione di hash deve avere un ottimo "effetto valanga", cioè cambiando anche solo un bit nel testo in chiaro, deve generare un'impronta completamente diversa.
A questo punto si può notare come, tecnicamente, **la firma digitale non sia altro che l'impronta crittografata** con la chiave privata del mittente validata dall'ente di certificazione.
Il destinatario, ricevuto il documento firmato e certificato digitalmente, calcolerà a sua volta l'impronta partendo dal testo in chiaro e usando la stessa funzione di hash, e poi la ricalcolerà utilizzando, questa volta, la chiave pubblica reperita attraverso il certificato. Se le due impronte risultano uguali allora vuol dire che il documento è stato firmato dalla persona giusta (identità) e non è stato modificato (integrità).

Oltre alla firma digitale, ci sono diversi altri servizi che si basano sugli enti certificatori:

- la **PEC** (Posta Elettronica Certificata);
- lo **SPID** (Sistema Pubblico di Identità Digitale);
- la **CNS** (Carta Nazionale dei Servizi),

per citare i più diffusi.

#prendinota

Nel corso del 2019 sono state generate complessivamente oltre 3,1 miliardi di firme digitali.

A titolo di esempio mostriamo brevemente cosa succede quando un possessore di PEC invia un messaggio a un altro utente PEC (FIGURA 16). Il gestore del dominio prende il messaggio, lo inserisce in una busta e vi appone una firma digitale (2). Il gestore PEC del destinatario verifica la firma (3) e invia un messaggio di conferma ricezione al mittente (4, 5). Durante tutti i passaggi, che vengono registrati, vengono emesse delle ricevute.

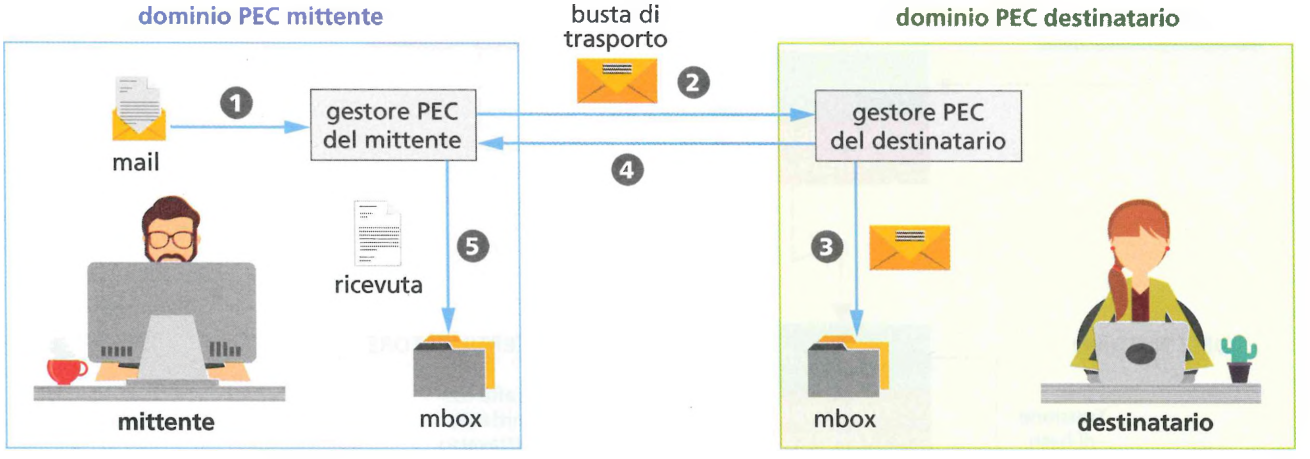


FIGURA 16 Meccanismo di invio e certificazione di una PEC

Case study
La sicurezza delle informazioni

FISSA LE CONOSCENZE

- Che cosa garantisce la firma digitale?
- Per che cosa viene utilizzata la funzione di hash?
- Quali sono i tre possibili formati utilizzabili per produrre file firmati digitalmente?

DIDATTICA INCLUSIVA

1 L'Internet Security

L'uso delle reti richiede strumenti che permettano di proteggere le informazioni durante il loro trasferimento da un nodo all'altro. Per il commercio elettronico (e-commerce) o l'home banking vengono trasferiti codici di accesso e password: l'Internet Security è l'insieme di misure utilizzate per proteggere i dati durante la loro trasmissione sulla rete Internet.

2 La crittografia

La crittografia è un insieme di procedure ideate allo scopo di nascondere il contenuto di un messaggio durante la trasmissione.
Per cifrare un testo occorrono due cose: un algoritmo di cifratura (pubblico) e una chiave (segreta). La sicurezza dipende dalla bontà dell'algoritmo crittografico e dalla difficoltà a scoprire la chiave. Tra le tecniche più semplici vi sono quelle a sostituzione e a trasposizione.

3 Crittografia simmetrica e asimmetrica

Le tecniche di crittografia più utilizzate sono quelle a chiave simmetrica, basata sulla segretezza dell'unica chiave, e a chiave asimmetrica, basata sulla difficoltà a scoprire la chiave privata anche conoscendo quella pubblica.

4 Gli algoritmi di crittografia DES e Triple DES

L'algoritmo di crittografia DES (Data Encryption Standard) con blocchi a 64 bit e chiavi a 56 bit, è il più semplice tra gli algoritmi di crittografia simmetrici. L'idea di base è quella di ripetere molte volte operazioni di confusione e diffusione del testo attraverso una serie di permutazioni del messaggio e combinazioni del messaggio con la chiave.

5 L'algoritmo di crittografia RSA

L'RSA (Rivest, Shamir, Adleman) è un algoritmo a chiave asimmetrica che si basa sulla difficoltà nel fattorizzare un numero intero N molto grande ottenuto dal prodotto di due numeri primi (p e q, anch'essi molto grandi) che restano segreti. L'algoritmo RSA opera a blocchi di bit e le chiavi che utilizza sono da 1024, 2048, 4096 o anche più bit.

6 La firma digitale e gli enti certificatori

La firma digitale, equivalente elettronico della firma autografa su carta, è associata stabilmente al documento elettronico sulla quale è apposta e ne attesta con certezza l'integrità, l'autenticità e la non ripudiabilità. La firma digitale utilizza un certificato digitale rilasciato da un ente certificatore (Certification Authority) e viene creata mediante un dispositivo apposito (in genere una smart card).

VERIFICA DI FINE UNITÀ

Test
Svolgi il **test interattivo**

Quali delle seguenti affermazioni sono vere (V) e quali false (F)?

1. La Recommendiaton X.800 impone una serie di requisiti di sicurezza che il sistema deve soddisfare. V F
2. Il cifrario di Giulio Cesare è una tecnica crittografica a trasposizione. V F
3. Il cifrario One-Time Pad utilizza la chiave una volta sola. V F
4. Il cifrario a matrice è una tecnica crittografica a trasposizione. V F
5. La crittografia a chiave asimmetrica si basa sull'utilizzo di una sola chiave. V F
6. La confusion si crea con la sostituzione mentre la diffusion con la permutazione. V F
7. L'algoritmo DES^{-1} applica gli stessi passi del DES sfruttando le proprietà dell'XOR. V F
8. La tecnica RSA è a chiave asimmetrica e a blocchi. V F
9. La firma digitale utilizza la crittografia a chiave simmetrica. V F

Domande a scelta multipla (una sola è la risposta esatta)

1. **Il Cifrario di Vigenère è:**
   - A a trasposizione e a chiave asimmetrica
   - B a trasposizione e a chiave simmetrica
   - C a sostituzione e a chiave simmetrica
   - D a sostituzione e a chiave asimmetrica

2. **La tecnica DES è:**
   - A a chiave simmetrica e a blocchi
   - B a chiave simmetrica e a flussi
   - C a chiave asimmetrica e a blocchi
   - D a chiave asimmetrica e a flussi

3. **L'algoritmo di applicazione della firma digitale su un documento utilizza la funzione di hash per:**
   - A creare l'impronta (digest)
   - B creare la chiave pubblica
   - C creare la chiave privata
   - D creare la certificazione digitale

4. **Quale formato non è previsto dal nostro ordinamento per produrre file firmati digitalmente?**
   - A PDF
   - B XML
   - C DOCX
   - D p7m

5. **Nell'algoritmo a chiave asimmetrica:**
   - A tengo nascosta la chiave privata e distribuisco quella pubblica
   - B tengo nascosta la chiave pubblica e distribuisco quella privata
   - C tengo nascosta sia la chiave privata che quella pubblica
   - D distribuisco sia la chiave privata che quella pubblica

6. **RSA vuol dire:**
   - A Really Secure Algorithm
   - B Reverse Secure Algorithm
   - C Rivest Shamir Adleman
   - D Rivest Secure Algorithm

Ascolta le **risposte**

PREPARATI PER IL COLLOQUIO ORALE

1. LEZIONE 1 **Quali requisiti la Recommendation X.800 Security Architecture dell'ITU-T impone al fine di garantire la sicurezza del sistema?**
2. LEZIONE 2 **Come vengono classificati i sistemi di crittografia?**
3. LEZIONE 3 **Come si fa a garantire l'identità del mittente (autenticazione) con la crittografia a chiave asimmetrica?**
4. LEZIONE 4 **Che cosa si deve fare nella progettazione di un servizio crittografico di sicurezza?**
5. LEZIONE 5 **Qual è il punto di forza dell'algoritmo a chiave asimmetrica RSA?**
6. LEZIONE 6 **Che cosa attesta la firma digitale?**

IN ENGLISH, PLEASE

CLIL

Ascolta la **pronuncia** del **testo** e verifica la **traduzione**

ABSTRACT

Network and system security

Security concerns involve hardware, software and, especially, the fundamental corporate assets of data and information. A cryptographic system consists of two elements: the algorithm and the key. The algorithm is a set of steps to change the message according to specific rules and with a specific key. The key is a sequence of digits (or characters).
The longer the key, the more complex and solid it is. The message is encrypted using the key and again can be decrypted with the key. In public key cryptography each user is assigned two different but complementary keys: a public key and a private key. Each key can only be used to decipher the messages cyphered with the other. This way one of the complementary keys (the public key) can be distributed widely, while the other (private) key is kept by its owner.
Asymmetric cryptography is used in digital signature. This not only provides authentication, but also data integrity (the message was not altered in transit) and non-repudiation (the signer cannot successfully claim they did not sign a message). The public key is distributed using digital certificates, usually issued by a certification authority (CA).

EXERCISES

Use the appropriate number to match words and meanings.

...	Key	1	A code for the secret transmission of messages.
...	Certification Authority	2	A message in its original readable form.
...	RSA	3	The translation of a message into coded form.
...	Cipher text	4	Set of characters that allow a user to be identified.
...	Encryption	5	A trusted entity that issues and revokes public key certificates.
...	Plain text	6	The encrypted form of the message.
...	Cipher	7	A numerical value used to control cryptographic operations, such as encryption or decryption.
...	Password	8	A public key cryptographic algorithm.

GLOSSARY

Access Control: ensures that resources are only granted to those users who are entitled to them.
Authentication: the process of confirming the claimed identity.
Confidentiality: the need to ensure that information is disclosed only to those who are authorized to view it.
Cryptanalysis: the mathematical science that deals with analysis of a cryptographic system. It studies how to convert the cipher text to plain text without knowing the key.
Cryptography: it concerns the principles, means, and methods for rendering plain information unintelligible and for restoring encrypted information to intelligible form.
Data Integrity: the property that data has not been altered in an unauthorized manner.
Digest: a cryptographic hash function containing a string of digits created by a one-way hashing formula. It is designed to protect the integrity of data.
Digital Signature: a type of electronic signature based on an asymmetric key pair system, which authenticates the origin and integrity of an electronic document.
Sniffing: monitoring or recording of data while it is being transmitted over a communications link, without altering or affecting the data.
Spoofing: attempt by an unauthorized entity to gain access to a system by posing as an authorized user.

LAVORARE PER COMPETENZE

COMPETENZE IN GIOCO

Competenze disciplinari

- Descrivere e documentare le soluzioni adottate.
- Gestire progetti secondo le procedure e gli standard previsti dai sistemi aziendali di gestione della qualità e della sicurezza.
- Utilizzare le reti e gli strumenti informatici nelle attività di studio, ricerca e approfondimento disciplinare.

Competenze chiave di cittadinanza

- Interpretare il testo.
- Risolvere problemi.
- Comunicare.
- Competenza digitale.

obiettivi formativi

- Stimolare l'approfondimento e la ricerca disciplinare.
- Consultare fonti Internet.
- Contestualizzare in un caso reale le nozioni teoriche acquisite studiando.
- Esporre i risultati della ricerca alla classe.

tempi

- Ricerca: 1 ora.
- Preparazione relazione: 2 ore.
- Presentazione relazione e dibattito in classe: 1 ora.
- Autovalutazione: 10 minuti.

strumenti

- Libro di testo.
- Dispositivo connesso a Internet
- Software PowerPoint.
- Proiettore collegato al computer in classe o in laboratorio.

TEMA PROPOSTO

*Proponiamo di seguito una parte del Tema d'Esame di **SISTEMI E RETI** suggerito nel 2015/16 per l'indirizzo INFORMATICA E TELECOMUNICAZIONI articolazione INFORMATICA.*
In base a quanto appreso in questa Unità, abbiamo gli strumenti per risolvere il terzo quesito della seconda parte del tema.

«Un giornale locale negli anni novanta realizzò una propria banca dati telematica per la distribuzione elettronica di un notiziario settimanale.
Gli utenti, previo abbonamento, si collegavano via modem e linea telefonica per la lettura degli articoli e l'invio di posta elettronica. [...]

Il nuovo direttore del giornale desidera effettuare l'ammodernamento del sistema, realizzando una nuova rete locale per il collegamento dei computer e di altri dispositivi [...].

Il candidato, formulate le opportune ipotesi aggiuntive, sviluppi i seguenti punti: [...]

3. i documenti, anche importanti, viaggiano sempre più spesso in rete ponendo in evidenza la necessità di garantire sia l'integrità degli stessi che l'identità del mittente. Descrivere la tecnica che garantisce quanto sopra, anche avvalendosi di schemi.»

SVOLGIMENTO

Ipotesi aggiuntive

Supponiamo che il giornale locale si avvalga di servizi digitali come la firma digitale e la posta elettronica certificata (PEC).

Descrizione

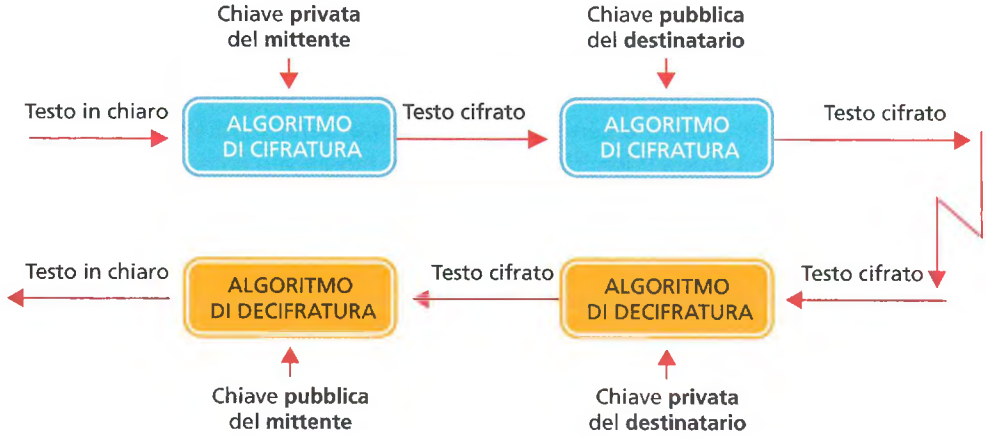
Il nuovo direttore del giornale avrà necessità di scambiare documenti riservati con il proprio editore e allo stesso modo i giornalisti avranno bisogno di trasmettere documenti confidenziali ai redattori.

La tecnica che garantisce l'integrità dei dati trasmessi e l'identità del mittente in un ambito di riservatezza è la crittografia a chiave asimmetrica.
La crittografia a chiave asimmetrica (o a chiave pubblica) utilizza due chiavi per ciascun soggetto: una privata, nota solo per esempio al direttore del giornale, l'altra pubblica, distribuita a tutti i redattori con cui il direttore vuole comunicare in sicurezza.

La massima sicurezza si ottiene quando mittente e destinatario si scambiano, prima della trasmissione dei documenti digitali, le reciproche chiavi pubbliche (la chiave privata non viene mai trasmessa). In questo modo, prima della trasmissione, il testo in chiaro subisce due cifrature da parte del mittente: la prima con la propria chiave privata e la seconda con la chiave pubblica ricevuta dal destinatario.

Naturalmente anche in fase di ricezione servirà una doppia decifratura da parte del destinatario: la prima con la propria chiave privata e la seconda con la chiave pubblica ricevuta dal mittente.

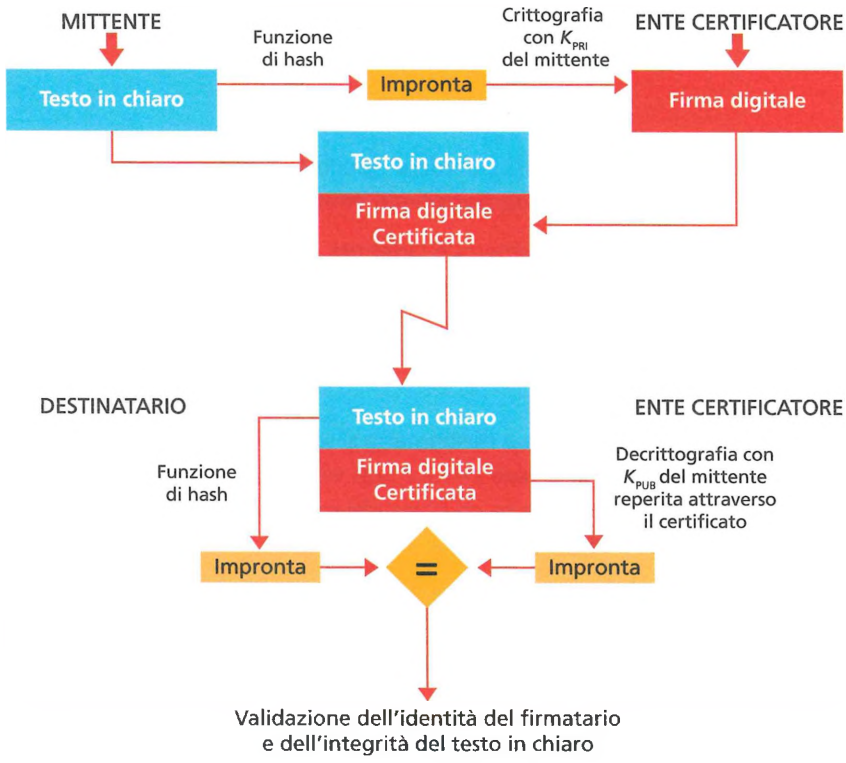
Lo schema seguente riassume i vari passaggi.



Qualora i documenti digitali da trasmettere debbano avere valore giuridico, è necessario che siano firmati.
La firma digitale è l'equivalente elettronico della tradizionale firma fatta a mano su carta. Essa viene associata al file sul quale è apposta e ne attesta con certezza l'integrità, l'autenticità e la non ripudiabilità.
Il servizio di firma digitale utilizza un certificato, digitale anch'esso, rilasciato da un ente certificatore (Certification Authority) con specifiche capacità professionali garantite dallo Stato. La firma viene apposta mediante un dispositivo con elevate caratteristiche di sicurezza, che in genere è una smart card.

L'algoritmo di apposizione della firma digitale prevede la creazione di un'impronta del testo attraverso la funzione di hash. L'impronta viene poi crittografata con tecnica asimmetrica mentre il testo viaggia in chiaro non essendo richiesta la riservatezza.
Allo stesso modo il destinatario decifrerà la firma ricevuta riottenendo l'impronta iniziale. Solo se l'impronta ricevuta e quella decifrata coincidono, avviene la validazione del documento.

Lo schema seguente riassume i vari passaggi.



Il mittente dunque firma il documento digitalmente, lo certifica attraverso l'Authority e poi lo invia.
Il destinatario, ricevuto il documento firmato e certificato digitalmente, verifica attraverso l'Authority che il documento sia stato firmato dalla persona giusta (identità) e non sia stato modificato (integrità).

A CASA

- Effettua una ricerca in Internet sulle principali tecniche di crittografia utilizzate comunemente, esaminando in particolare:
  – algoritmi di crittografia a chiave asimmetrica;
  – servizi digitali.
- Individua quali, tra i casi trovati, risulta affine al contesto illustrato nel tema proposto.
- Leggi l'esempio di svolgimento proposto per verificare se le tue ipotesi si adattano al caso preso in esame e se la trattazione proposta risulta completa nell'ottica dei risultati della tua ricerca.
- Raccogli i tuoi risultati in una presentazione in PowerPoint (massimo 5 slide).

IN CLASSE

- Condividi la presentazione dei tuoi risultati con i compagni.
- Confrontate e discutete insieme i casi che sono stati presentati.
- Stabilite quale caso rappresenta l'esempio migliore per completezza e che meglio si adatta alla realizzazione delle garanzie richieste nel tema d'esame.
- Procedi con l'autovalutazione.

AUTOVALUTAZIONE

ATTIVITÀ	LIVELLO			
	INIZIALE	BASE	INTERMEDIO	AVANZATO
Ho compreso senza difficoltà le richieste dell'attività proposta?	Ho compreso solo alcune delle richieste, aiutato dal docente. ☐	Con la guida del docente e la collaborazione dei compagni ho compreso quasi tutte le richieste. ☐	Ho compreso le richieste e in parte le ho svolte autonomamente. ☐	Ho identificato le richieste e le ho svolte senza difficoltà. ☐
Ho reperito le informazioni in rete senza difficoltà?	Ho reperito solo alcune delle informazioni utili, aiutato dal docente. ☐	Con la guida di insegnante e compagni ho reperito quasi tutte le informazioni. ☐	Ho reperito le informazioni utili autonomamente e le ho elaborate. ☐	Ho identificato le richieste e le ho svolte senza difficoltà. ☐
L'analisi dello scenario mi ha permesso di confrontarmi e capire meglio lo svolgimento proposto?	A partire dalla mia analisi, non sono stato in grado individuare nessun punto critico nello svolgimento proposto, rendendomi conto di aver sottovalutato e tralasciato molti aspetti. ☐	A partire dalla mia analisi ho individuato, con l'aiuto del docente, lacune e aspetti che non avevo trattato e che invece sono presenti nello svolgimento proposto. ☐	A partire dalla mia analisi, con l'aiuto del docente, sono stato in grado di confrontare le varie soluzioni, trovando i punti di contatto e le analogie nello svolgimento proposto. ☐	A partire dalla mia analisi, sono stato in grado di confrontare le varie soluzioni, trovando i punti di contatto e le analogie in modo dettagliato e completo. ☐
Sono riuscito a preparare una presentazione efficace?	La mia presentazione è stata minimale, con pochi concetti e molte lacune. ☐	La mia presentazione è risultata quasi completa, anche se i concetti sono stati sviluppati in modo approssimativo. ☐	La mia presentazione è risultata completa, anche se alcuni concetti potevano essere meglio approfonditi o descritti in modo più chiaro. ☐	La mia presentazione è risultata completa, con i concetti sviluppati in modo approfondito e comprensibile. ☐

UNITÀ 2

EFFICIENZA E SICUREZZA NELLE RETI LOCALI

Guarda la **presentazione** dell'unità

IN QUESTA UNITÀ

DDI+ Didattica Digitale Integrata Plus

conoscenze	abilità	competenze
Conoscere il funzionamento del protocollo Spanning Tree.	Saper predisporre gli apparati per segmentare la rete.	Saper ottimizzare la collocazione dei dispositivi e dei canali di comunicazione.
Conoscere le tecniche di filtraggio del traffico in rete.	Saper simulare una rete locale, anche virtuale.	Progettare reti locali sicure connesse a Internet.
Conoscere le modalità per garantire la privacy agli utenti di una rete.	Saper configurare e gestire una rete in riferimento a riservatezza e sicurezza.	

FLIPPED CLASSROOM

A casa

- Leggi le Lezioni di laboratorio 8 e 9 di questa Unità;
- indica in un report (massimo 1 pagina) quali delle soluzioni proposte sono le più efficaci per proteggere l'azienda.

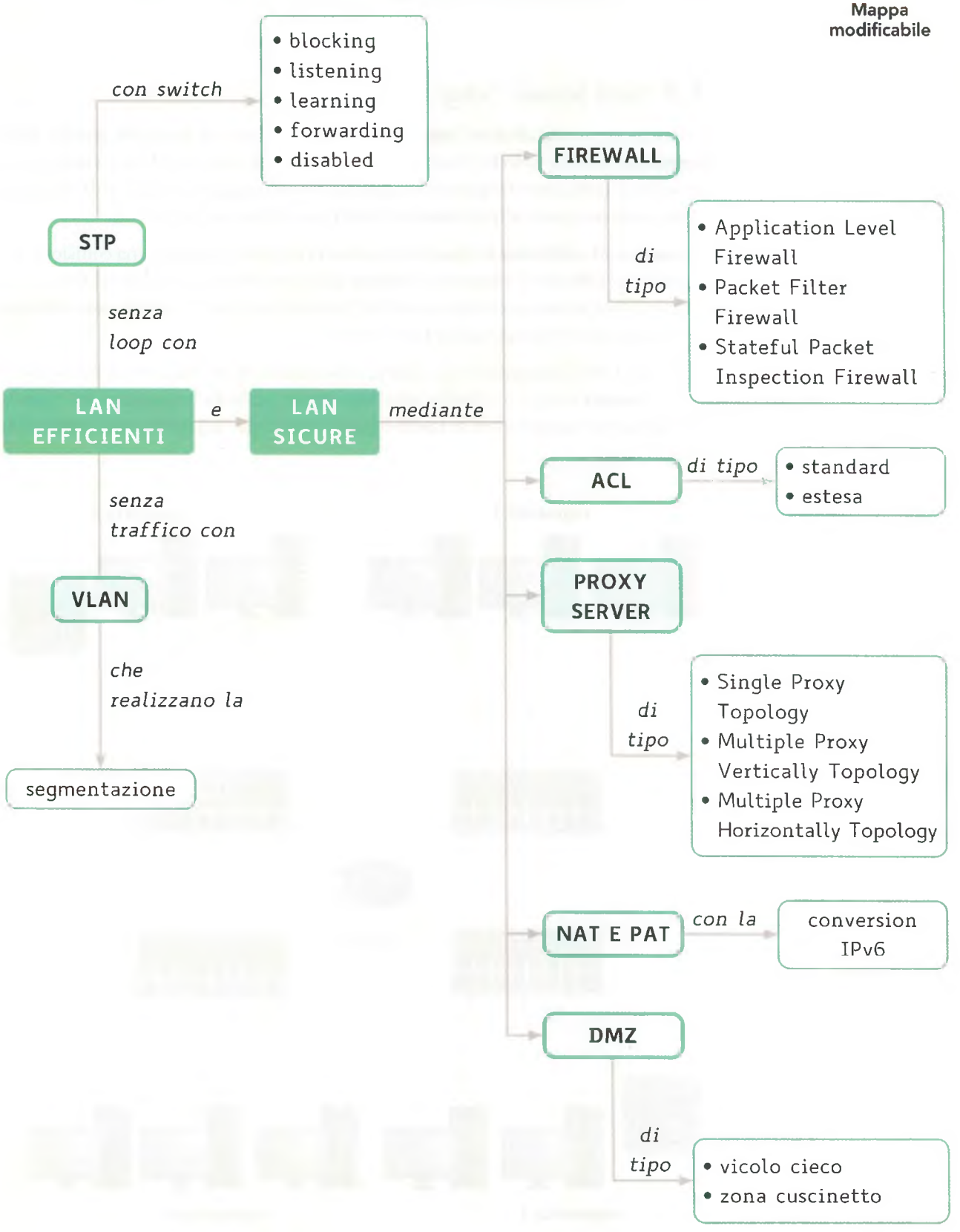
In classe

- Confrontate i report e discutete l'efficacia delle soluzioni proposte;
- individuate e descrivete le soluzioni aggiuntive approntabili per la protezione dell'azienda;
- raccogliete i risultati della discussione in uno schema riassuntivo.

MAPPA CONCETTUALE

DIDATTICA INCLUSIVA

Mappa modificabile



1 STP: IL PROTOCOLLO DI COMUNICAZIONE TRA GLI SWITCH

1.1 Reti locali "segmentate"

Le moderne reti locali sono "segmentate", cioè suddivise in parti più piccole, dette **segmenti**, tramite **switch** (o bridge, ma nel seguito parleremo solo di switch) al fine di isolare il traffico tra i segmenti e raggiungere una maggiore ampiezza di banda per ogni computer grazie alla creazione di domini di collisione più piccoli.

Il **dominio di collisione** di una rete è un'area in cui può verificarsi una collisione. Per esempio, se abbiamo 5 computer connessi allo stesso mezzo condiviso, i dati inviati da uno di essi possono collidere con i dati inviati da un altro. In questo caso abbiamo un dominio di collisione che contiene 5 host.

Oltre alle LAN segmentate con switch, è possibile creare segmenti di LAN utilizzando i **router** (FIGURA 1). Questa soluzione rende più lenta la trasmissione rispetto alla soluzione con gli switch (a meno di usare router che implementino funzionalità di switching).

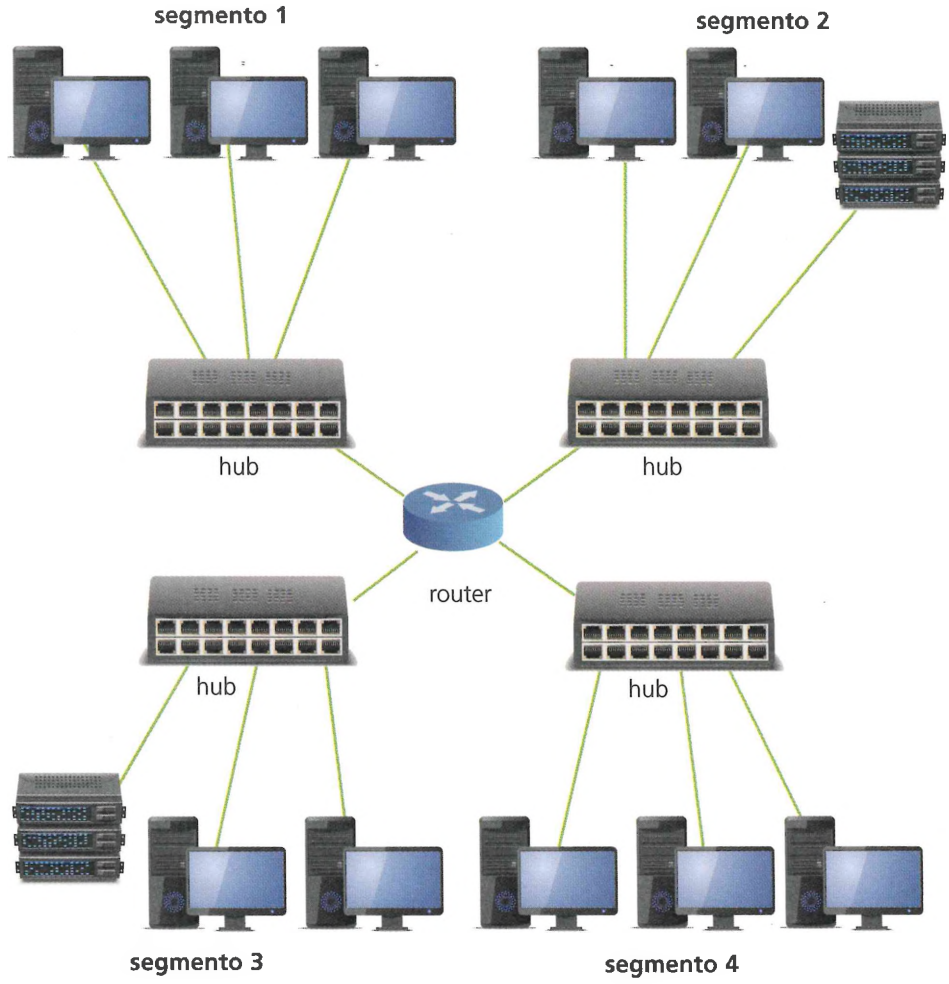


FIGURA 1 LAN segmentata con un router in 4 segmenti

Infatti il router è un apparato che opera a livello Network, basa le sue decisioni sugli indirizzi di rete (IP address) e non su quelli fisici (MAC address) e implementa algoritmi per trovare il percorso migliore che richiedono più tempo di elaborazione.
Spesso le reti con switch sono progettate con **percorsi fisici ridondanti** al fine di evitare che il guasto di un cavo o di una porta di un apparato possa portare al blocco delle trasmissioni sulla rete.
Se da un lato la duplicazione dei percorsi offre maggiori garanzie in termini di affidabilità e fault tolerance, dall'altro può dar luogo a effetti indesiderati (side effects), come la creazione di loop che portano al fenomeno detto "broadcast storm" che può in breve tempo bloccare la rete.
Un **broadcast storm** (letteralmente "tempesta di broadcast") avviene quando ci sono così tanti frame broadcast in un loop da impegnare tutta la banda disponibile. Un broadcast storm è inevitabile su una rete con percorsi ridondanti (FIGURA 2).

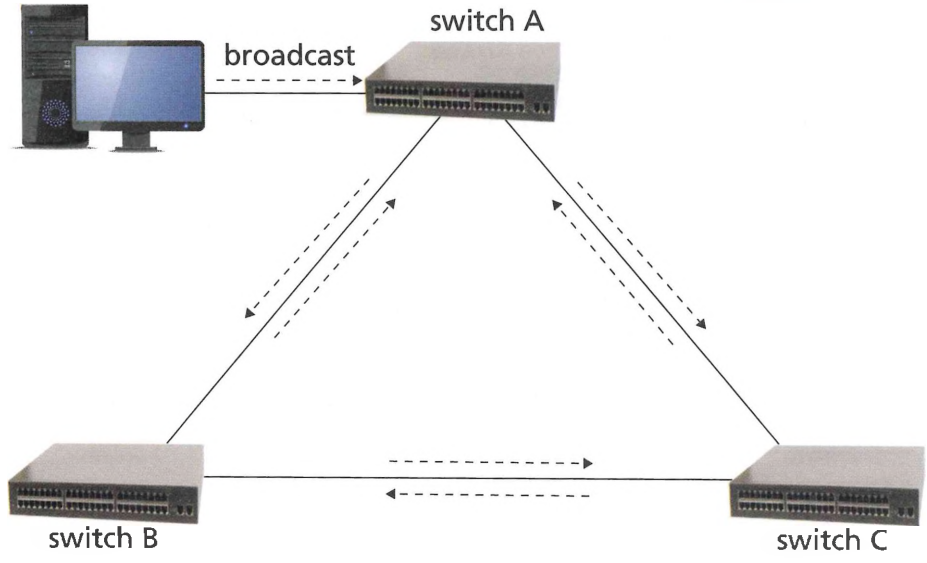


FIGURA 2 Loop con broadcast storm

Per evitare questi loop gli switch usano un protocollo per la gestione dei collegamenti, denominato **#STP** (Spanning Tree Protocol).

#techwords

STP (Spanning Tree Protocol) è così denominato in quanto il risultato dell'eliminazione dei loop è quello di creare un albero logico gerarchico.

1.2 Spanning Tree Protocol

STP è un protocollo definito nello standard IEEE 802.1 per realizzare reti LAN complesse senza loop. Con STP si crea un albero gerarchico che mantiene ancora disponibili i percorsi alternativi da usare in caso di necessità, quindi si lasciano loop fisici ma si eliminano a livello di topologia logica.
Infatti, una volta rilevato che esistono più percorsi tra i nodi della rete (loop), il protocollo STP crea una struttura ad albero relegando i percorsi ridondanti a uno stato di standby (*blocked*) della relativa porta dello switch.

STP permette che venga stabilito un solo percorso attivo alla volta tra due dispositivi della rete per evitare i loop, tuttavia stabilisce collegamenti ridondanti come alternative nel caso in cui il collegamento primario dovesse non essere più disponibile. Se in un certo istante un segmento della rete dovesse diventare irraggiungibile, l'algoritmo di Spanning Tree riconfigurerà la topologia logica, ristabilendo il

collegamento attraverso l'attivazione del percorso in standby (cioè attivando la porta prima inattiva).
Se non ci fosse la struttura di Spanning Tree, entrambi i collegamenti ridondanti potrebbero essere considerati il percorso primario, producendo così un loop infinito di traffico sulla LAN.
Nella FIGURA 3 si mostra un esempio di rete locale con 3 switch interconnessi A, B e C.

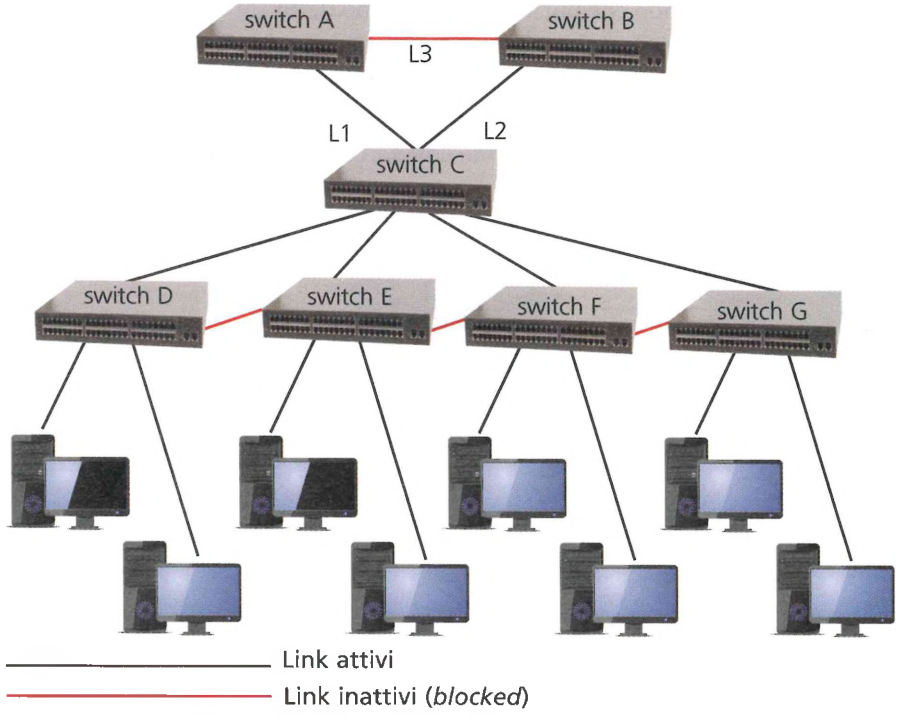


FIGURA 3 Esempio di LAN con STP

In assenza di STP, tra questi switch si avrebbe un loop, ma se STP è attivo, il link L3 (rosso) è messo in stato *blocked*, così non può essere usato per la trasmissione dati. Se si verificasse un guasto sui link L1 oppure su L2, il link L3 verrebbe attivato automaticamente. Questa soluzione fornisce quindi una condizione di ridondanza per la rete, senza incorrere nel problema dei loop.
Anche gli switch D, E, F e G forniscono una ridondanza sui link (per via dei collegamenti segnati in rosso) e se STP è attivo, vale quanto indicato prima per gli switch A, B e C.

Annotiamo che, per tradizione, il termine "bridge" continua a essere usato anche quando STP si applica a una rete con switch, poiché STP fu sviluppato per essere utilizzato con i bridge. Quindi quando si legge "bridge" (per esempio, root bridge) si deve pensare "switch" (root switch).

Ogni switch della LAN invia dei messaggi detti **BPDU** (Bridge Protocol Data Unit), trasmessi da tutte le porte per conoscere l'esistenza di altri switch e per eleggere un **root bridge** nella rete (cioè la radice dell'albero logico che si verrà a creare).

I BPDU contengono informazioni per:
- selezionare un solo switch come root dello Spanning Tree;
- calcolare il percorso più breve da ogni switch alla root;

- eleggere il **designated switch**, che per ogni LAN è lo switch più vicino alla root, attraverso cui passano tutte le comunicazioni della LAN;
- scegliere per ogni switch la **root port**, cioè l'interfaccia che dà il miglior percorso verso la root.

Le porte che fanno parte dello Spanning Tree sono le **designated port**, le altre sono bloccate.
Quando si attiva l'algoritmo per la creazione dello Spanning Tree, trascorre un certo tempo, da 30 a 50 secondi, prima che la topologia logica della rete *converga*, ossia che tutte le porte degli switch siano nello stato *blocked* o *forwarding*. Quando la topologia cambia, gli switch ricalcolano lo Spanning Tree.
Quando la LAN ha ottenuto la convergenza e si è creato l'albero gerarchico (FIGURA 4), si hanno i seguenti elementi:

- un root bridge per LAN;
- una root port per i non root bridge;
- una designated port per segmento;
- porte non usate.

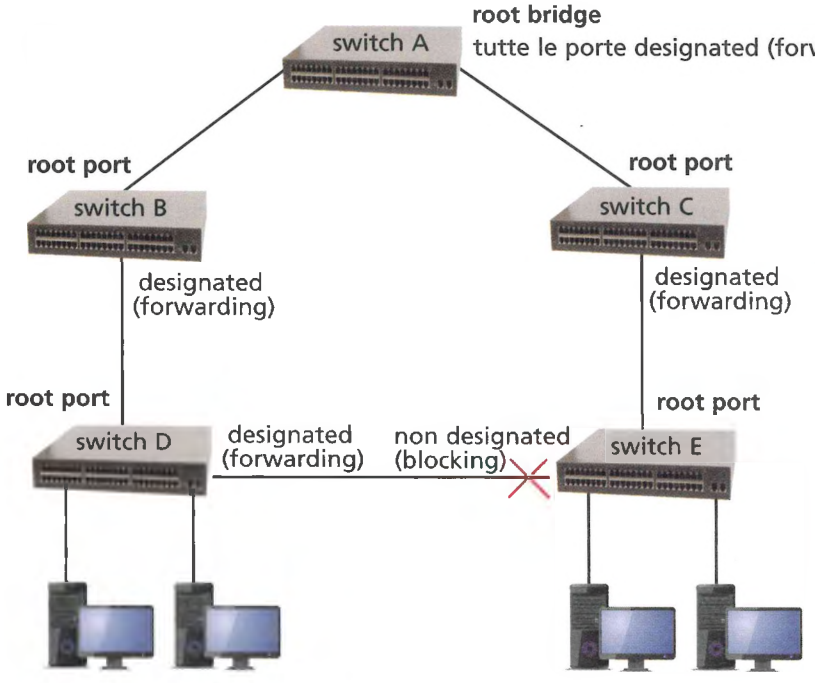


FIGURA 4 Esempio di gerarchia creata con STP

Ogni porta dello switch in STP si può quindi trovare in uno dei seguenti stati:

- **blocking**: può solo ricevere le BPDU, scarta i frame e non è in grado di apprendere nessun indirizzo fisico;
- **listening**: sta costruendo la topologia "attiva" della rete, ossia lo switch determina se ci sono altri percorsi verso il root bridge;
- **learning**: sta costruendo la tabella di bridging, quindi è in grado di apprendere gli indirizzi fisici, ma non invia né riceve dati;
- **forwarding**: può inviare e ricevere dati e in generale è in grado di svolgere tutte le funzioni possibili;
- **disabled**: è stata disabilitata (cioè resa *down*) dall'amministratore.

#techwords

In generale, il **tempo di convergenza** della rete è il tempo che la rete stessa impiega ad aggiornare i percorsi in seguito a una modifica (per esempio, il guasto o l'aggiunta di un nodo, l'attivazione dell'algoritmo Spanning Tree).

Nelle reti attuali un **#tempo di convergenza** di 30-50 secondi risulta inadeguato alle velocità elevate delle LAN, di conseguenza molti produttori hanno sviluppato delle modifiche, proprietarie, al protocollo STP standard al fine di ottenere tempi di convergenza inferiori.
Un'altra modifica è quella di permettere all'amministratore di configurare manualmente le porte alle quali è connesso un computer (e non un altro switch), così da evitare che la porta transiti attraverso tutti gli stati previsti dal protocollo, ma passi direttamente da *blocked/disabled* a *forwarding*.
Tutte queste migliorie hanno consentito di abbassare il tempo di convergenza, ma, nonostante ciò, sui link a elevata velocità che necessitano di ridondanza, gli switch di livello 2 sono sostituiti da apparati di livello superiore, chiamati **MultiLayer Switch**.

1.3 Evoluzione del protocollo Spanning Tree: RSTP

Negli anni STP ha subito varie evoluzioni: sul sito di IEEE (*www.ieee.org*) è possibile avere informazioni sugli sviluppi in corso che riguardano STP.
Nel 2001 IEEE definì il nuovo protocollo **Rapid Spanning Tree Protocol** (RSTP), identificato dalla sigla IEEE 802.1w, allo scopo di rendere più veloce la convergenza dell'algoritmo Spanning Tree a fronte di cambiamenti della topologia.
Infatti, RSTP è in grado di intervenire entro: 3 · *Hello time*, dove *Hello time* è un intervallo di tempo usato da RSTP in vari ambiti; il suo valore di default è 2 secondi.
Nel 2004 è stata emessa una nuova specifica dello standard, denominata IEEE Std 802.1D™-2004, che include il nuovo protocollo RSTP e rende obsoleto STP.
Pur mantenendo la struttura di STP, con un root bridge da cui parte lo Spanning Tree e un path costituito dagli switch, RSTP calcola un percorso alternativo definendo le porte che lo costituiscono *alternate*; eventuali porte da cui partono altri percorsi con costo maggiore rimangono in stato *blocking*. Quando una porta in *forwarding* smette di ricevere i frame di *Hello* e i timer scadono, viene subito attivato un altro percorso aprendo le porte *alternate*, velocizzando notevolmente il processo di convergenza.
Quando uno switch ha due porte in un stesso segmento, quella a costo più alto viene definita in un nuovo modo: *backup*. Quando la porta in *forwarding* non funziona più, quella in *backup* prende il suo posto. Anche in questo caso la convergenza è molto veloce.
Da sottolineare che RSTP non migliora la convergenza nei link condivisi, infatti lo standard è stato sviluppato pensando alle reti moderne che non usano più hub ma switch e che lavorano in full-duplex.

FISSA LE CONOSCENZE

- Che cosa significa "segmentare" una rete locale?
- Che cosa si intende con dominio di collisione?
- Che differenza c'è tra una LAN segmentata usando uno switch e una segmentata usando un router?
- Quali problemi può creare l'operazione di rendere ridondante la rete?
- Spiega il protocollo Spanning Tree Protocol.
- Quali sono gli stati in cui si può trovare una porta di uno switch in cui è attivo STP?

2 LE RETI LOCALI VIRTUALI (VLAN)

2.1 Dominio di broadcast

Nella Lezione precedente si è visto come l'impiego di switch in una LAN consenta di segmentare la rete in domini di collisione separati. Oltre a ciò, è utile avere anche domini di broadcast separati, in modo da poter implementare tra i diversi segmenti di rete funzioni tipiche del livello Network, come la sicurezza o la qualità del servizio.

Il **dominio di broadcast** di una rete è un insieme di computer che riceve un messaggio di broadcast trasmesso da uno di essi.
La TABELLA 1 mostra come l'impiego di apparati di rete diversi (hub, switch o router) comporti un diverso rapporto con i domini di collisione e di broadcast.

apparato di rete	dominio di collisione	dominio di broadcast
hub	uno per tutte le porte	uno per tutte le porte
switch	uno per ogni porta	uno per tutte le porte
router	uno per ogni porta	uno per ogni porta

TABELLA 1 Descrizione dei domini per tipo di apparato

La tipica configurazione di uno switch prevede quindi che tutti gli host collegati a esso siano parte dello stesso dominio di broadcast, mentre vi possono essere molti domini di collisione. Infatti una coppia di host che comunica tramite lo switch forma un singolo dominio di collisione, di conseguenza con gli switch non si eliminano del tutto le collisioni (se due host vogliono inviare l'uno all'altro un messaggio esattamente nel medesimo istante, si avrà ancora una collisione).
Se quindi le collisioni non sono più un problema nelle reti che usano switch, il fatto che questi inoltrino su tutte le porte un messaggio di broadcast può generare molto traffico su reti con centinaia di host.

Per ovviare a questo problema, gli switch attuali offrono due diverse tecnologie:

1. **Virtual LAN (VLAN)**: si creano delle sottoreti nella rete locale che, in realtà, esistono solo sugli switch. La rete rimane configurata con la stessa topologia fisica, mentre cambia la topologia logica; quando un computer su una data sottorete invia un messaggio broadcast, esso verrà trasmesso solo ai computer appartenenti a quella sottorete e non a tutta la rete locale;
2. **Layer 3 switching**: quando un host su una VLAN deve comunicare con un host su un'altra VLAN, è necessaria la presenza di un router che interconnette le due VLAN, dopo di che intervengono i rispettivi switch (questo processo viene anche detto: *route once, switch many*). Se invece si usano switch con funzionalità di routing, detti **switch Layer-3** (il riferimento è al livello 3 del modello OSI che si occupa dell'instradamento dei pacchetti), non è più necessario avere un router, in quanto questi switch sono in grado di leggere l'indirizzo di rete contenuto nel pacchetto e individuare verso quale switch inviare i pacchetti. In questo modo viene minimizzata l'attività di routing tra VLAN, effettuandola solo quando è assolutamente necessario.

2.2 Vantaggi e svantaggi delle VLAN

La segmentazione e l'isolamento del traffico che si realizzano con le VLAN consentono di ridurre il traffico non necessario, migliorando notevolmente le prestazioni di rete. Questo importante vantaggio compensa la difficoltà nel configurare le VLAN, attività che richiede un notevole lavoro di pianificazione e realizzazione.

Con le VLAN, infatti:

- è semplice aggiungere, cambiare o spostare gli host sulla rete;
- si definiscono più domini di broadcast, di dimensioni ridotte, all'interno di una stessa rete locale switched, e questo implica un miglioramento delle prestazioni della rete;
- migliora la sicurezza della rete;
- riduce i costi relativi agli apparati di rete impiegati.

Le VLAN non sono da considerarsi una soluzione alternativa alle reti con router per realizzare la comunicazione tra reti differenti (internetworking).

2.3 Creazione di una VLAN

#prendinota

Quando si configura una VLAN, la topologia logica è indipendente da quella fisica.

Una **Virtual Local Area Network** (VLAN) è un insieme di computer, stampanti, server o altri device di rete che sono trattati come se fossero collegati a una singola rete, mentre, in realtà, si trovano su LAN fisiche diverse.
La tecnica di realizzazione delle VLAN permette di raggruppare, per esempio, una o più porte di uno switch in modo da considerarle parte di una stessa rete virtuale alla quale possono essere aggiunte porte di altri switch.
A ogni host della LAN può essere assegnato un numero identificativo (**VLAN ID**) per identificare la VLAN di appartenenza (FIGURA 5). Host con lo stesso VLAN ID si comportano come se si trovassero nella stessa rete fisica.

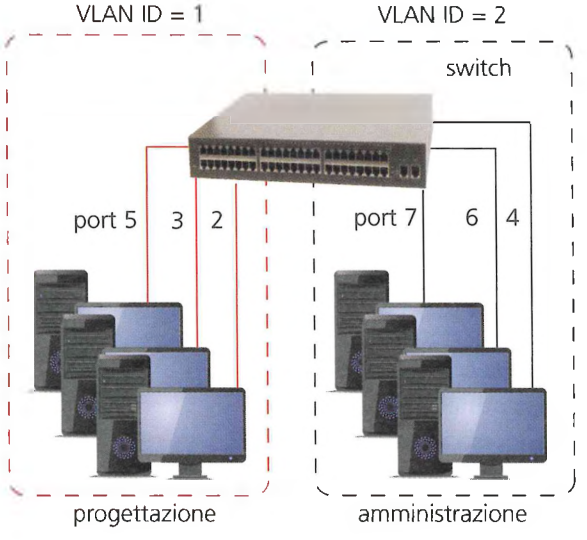


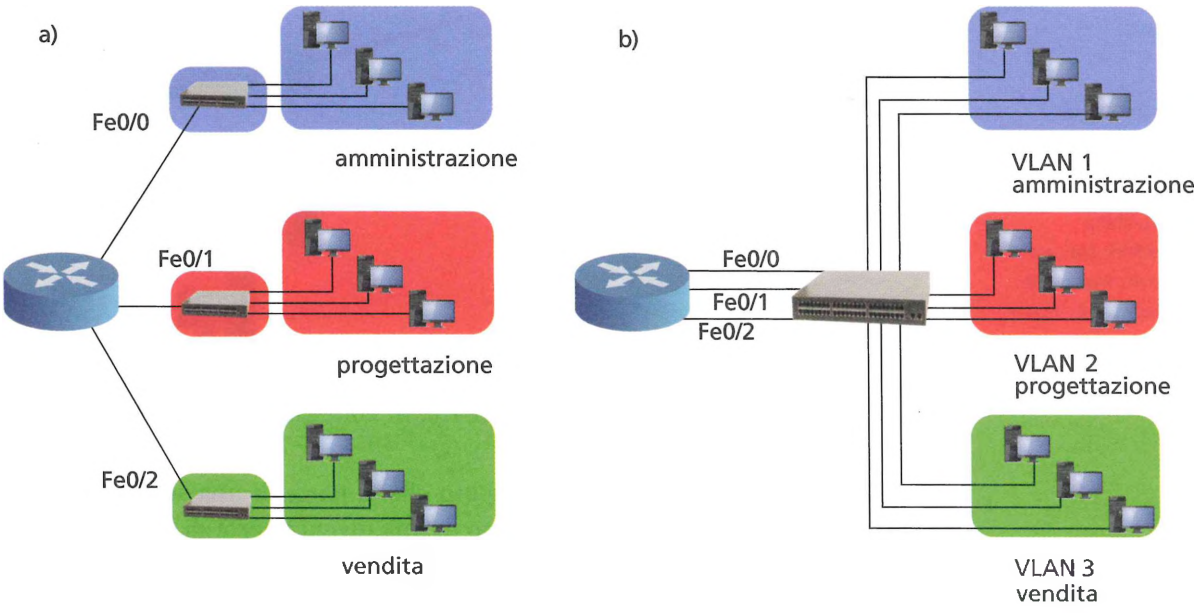
FIGURA 5 Esempio di realizzazione di 2 VLAN per gruppi di porte

Una VLAN può essere creata in più modi:

- per **gruppi di porte**, a questo scopo si utilizza l'identificativo della porta; è la modalità più comune ed è tipica delle LAN che utilizzano un indirizzamento dinamico a livello Network (per esempio tramite il protocollo DHCP, Dynamic Host Configuration Protocol, per l'assegnazione degli indirizzi IP);
- per **utenti**, tramite l'indirizzo fisico (MAC) dell'host; questa modalità è poco usata in quanto più difficile da gestire;
- per **protocolli**, la modalità è simile alla precedente, ma invece di indirizzi fisici usa indirizzi logici (per esempio l'indirizzo IP); da quando si è diffuso l'uso del DHCP per assegnare gli indirizzi IP non è più comunemente usata.

Vediamo con un esempio cosa significa che le VLAN permettono di raggruppare dispositivi indipendentemente dalla loro locazione fisica.
Supponiamo di dover suddividere una rete LAN in 3 aree distinte che corrispondono a 3 diversi gruppi di utenti: gli amministrativi, i progettisti e i venditori.

La FIGURA 6 mostra due diverse soluzioni per realizzare la segmentazione di rete richiesta da questo scenario:



a) la LAN è divisa in 3 segmenti di rete realizzati tramite l'impiego di 3 switch;
b) la LAN è divisa in 3 segmenti di rete realizzati tramite la configurazione software di 3 VLAN.

FIGURA 6 (a) Rete locale segmentata con 3 switch; (b) rete locale con uno switch e 3 VLAN

Si noti che affinché un membro del personale di vendita della VLAN 3 possa condividere delle risorse con il dipartimento della progettazione della VLAN 2, è necessario introdurre un router o scegliere uno switch Layer-3.
Tra router e switch occorrono, però, tante linee quante sono le VLAN definite, quindi sul router deve essere configurata un'interfaccia per ogni VLAN. In questa modalità, il traffico fluisce attraverso il router come se si usassero LAN fisiche e non virtuali. Dal momento che un router deve effettuare maggiori elaborazioni sui pacchetti rispetto a uno switch, le prestazioni che offre questa realizzazione dipendono da quanto traffico rimane all'interno di una singola VLAN e quanto deve essere instradato verso altre VLAN.

Inoltre, dedicare un'interfaccia per ogni VLAN realizzata richiede di riservare un certo numero di porte sia sullo switch che sul router; spesso però i router di fascia bassa non hanno un elevato numero di porte Ethernet, quindi si dovrebbe scegliere un router più costoso.
Un'alternativa a questa realizzazione è quella di usare un trunk.

2.4 VLAN Trunking

Un metodo per permettere la comunicazione tra host collocati in VLAN diverse è di realizzare tra switch e router, oppure tra switch e switch, un canale comune, detto **trunk**, sul quale far transitare le comunicazioni tra VLAN diverse (FIGURA 7).
Di norma per realizzare questo collegamento si sceglie la porta più veloce disponibile sull'apparato di rete, in quanto sarà usato per trasportare grossi volumi di traffico.

#prendinota

Il concetto di **trunk** ha origine nella tecnologia radio, dove rappresenta una linea di comunicazione che trasporta più canali con segnali radio.

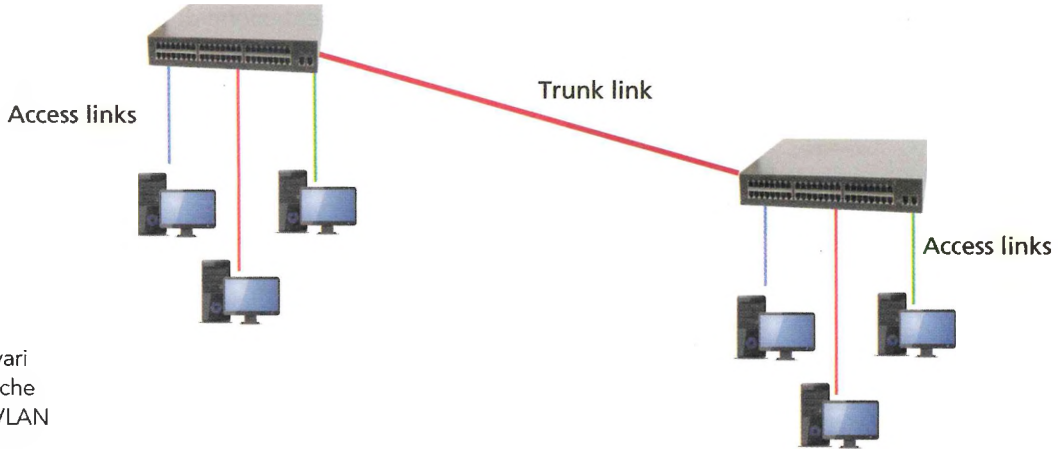


FIGURA 7 Le VLAN si possono estendere tra vari switch utilizzando trunk che convogliano traffico di VLAN diverse

Nella Figura 7 vengono evidenziati i due tipi di collegamento presenti nelle reti VLAN:

- **access link**: si tratta di un collegamento che fa parte di una sola VLAN; un computer collegato tramite questo tipo di link diventa parte di un dominio di broadcast e può comunicare solo con gli altri computer di questo dominio, a meno che il pacchetto da trasmettere sia inoltrato verso un router; il computer non è consapevole di appartenere a una VLAN, in quanto lo switch rimuove ogni informazione a essa relativa prima di inviargli il pacchetto;
- **trunk link**: è un collegamento punto-punto sul quale transita il traffico appartenente a VLAN diverse (fino a 4096); può essere usato tra due switch, tra uno switch e un server o anche tra uno switch e un router.

La FIGURA 8 visualizza un trunk attraverso il quale transitano le comunicazioni relative a 3 diverse VLAN.

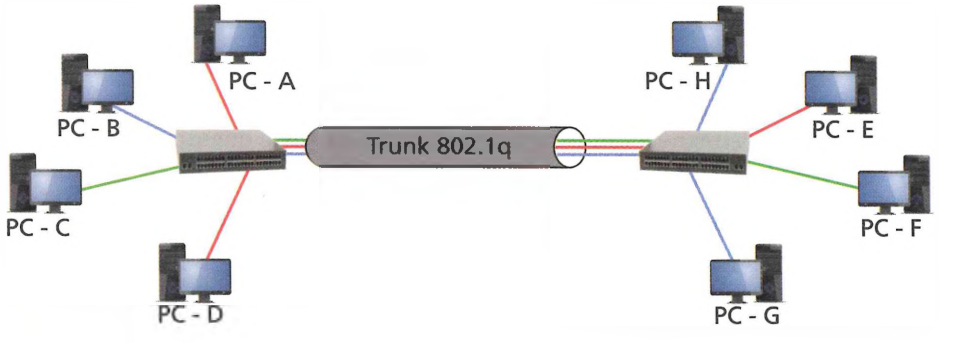


FIGURA 8 Rappresentazione di un trunk usato per mettere in comunicazione 3 diverse VLAN

#prendinota

Affinché uno switch possa inoltrare il messaggio al destinatario tramite un trunk, esso deve contenere un riferimento alla VLAN di appartenenza del computer di destinazione; la tecnica usata prevede l'uso di un **tag** e viene detta **VLAN tagging**.

Il frame Ethernet non prevede un campo per effettuare il **tagging delle VLAN** (le VLAN sono state inventate successivamente), esistono quindi vari metodi per associare un tag ai messaggi (frame) inviati sul trunk; per esempio, Cisco ha definito, per alcuni suoi switch, il protocollo Inter-Switch Link (ISL) e 3COM il protocollo Virtual LAN Trunk (VLT).
Attualmente, però, si tende ad abbandonare i protocolli proprietari, preferendo a questi degli standard internazionali.
Lo standard definito a livello internazionale, quindi protocollo non proprietario, è: **IEEE 802.1q**.

IEEE 802.1Q

Questo standard prevede di inserire un campo di 4 byte per la gestione del tag (FIGURA 9), suddiviso come di seguito indicato.

- **Tag Protocol ID** (TPID), 2 byte, usato per identificare il frame come un frame IEEE 802.1q (il valore è 0x8100).
- **Tag Control Information** (TCI), 2 byte, così suddiviso:
  - **User Priority**, 3 bit, indica il livello di priorità del frame; va da 1, bassa priorità, a 7, alta priorità. Lo zero indica nessuna priorità (best effort).
  - **Canonical Format Indicator** (CFI), 1 bit, usato in passato per indicare se gli indirizzi nel frame erano in forma canonica, ora è chiamato **Drop Eligible Indicator** (DEI) e, usato insieme a User Priority, segnala i frame da scartare (drop) in caso di congestione in rete;
  - **VLAN ID**, 12 bit, indica a quale VLAN appartiene il frame (ID = 0 e ID = 4096 sono riservati).

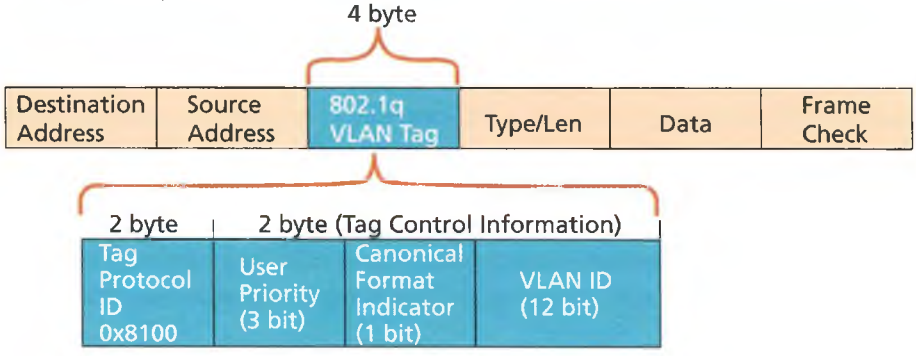


FIGURA 9 Frame Ethernet modificato con l'inserimento del campo per il tagging delle VLAN

VLAN TRUNKING PROTOCOL (VTP)

In reti complesse, la gestione delle VLAN richiede molto tempo e si possono commettere facilmente errori. Una soluzione a questo problema è l'utilizzo del protocollo **VTP** (VLAN Trunking Protocol), proprietario Cisco, che permette di gestire centralmente su uno switch i nomi e i membri di una VLAN e poi distribuire in automatico la configurazione sugli altri switch.

Dal punto di vista del protocollo VTP, gli switch si suddividono in:

- **VTP server**: switch sui quali si effettuano le modifiche di configurazione delle VLAN;
- **VTP client**: switch ai quali sono propagati i cambiamenti effettuati sui VTP server;
- **VTP transparent**: switch che ricevono e inoltrano gli aggiornamenti, ma non li applicano alla propria configurazione; eventuali modifiche su questi switch dovranno essere fatte manualmente.

Nella Lezione 7 vedremo come realizzare delle VLAN con trunk e come STP risolva i loop mediante un'esercitazione con Cisco Packet Tracer.

FISSA LE CONOSCENZE

- Che cos'è una VLAN?
- In quale standard si trovano le specifiche per le VLAN?
- In che modo è possibile comunicare tra VLAN?
- Spiega l'uso di trunk con le VLAN.

Case study
Progettazione di una rete con 3 VLAN

3 IL FIREWALL E LE ACL

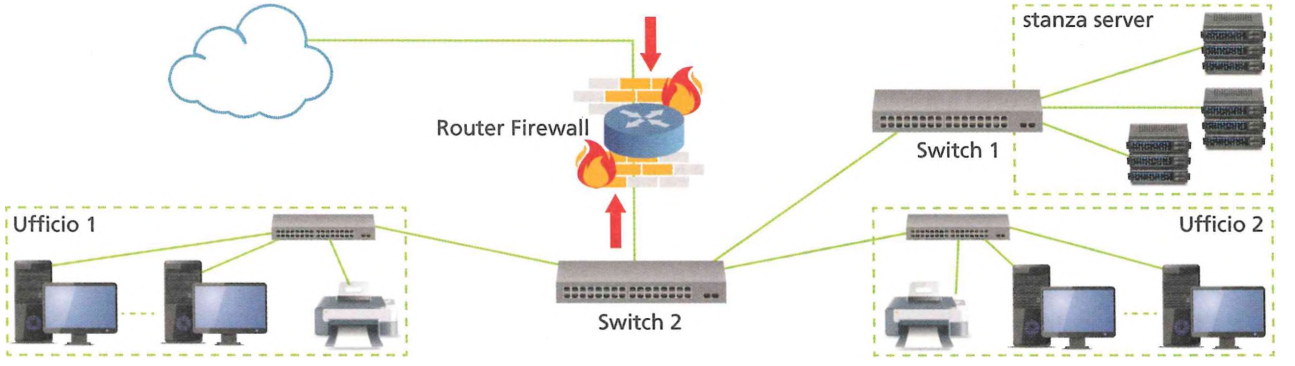
3.1 Firewall

Il **firewall** (letteralmente: muro tagliafuoco) è una linea di difesa indispensabile contro le intrusioni di rete poiché agisce come sentinella alla porta di collegamento del computer con una rete esterna come Internet. In pratica separa la LAN aziendale dalla WAN pubblica.

> Il firewall filtra tutti i **pacchetti entranti** e **uscenti**, da e verso una rete o un computer, secondo regole prestabilite (policy) che contribuiscono alla sicurezza della rete stessa.

Un firewall può essere realizzato con un computer (con almeno due schede di rete, una per l'input e l'altra per l'output) e il software apposito.
Nelle LAN aziendali viene realizzato attraverso una funzionalità logica (software) **inclusa nel router** oppure può essere implementato su un apparato **hardware dedicato**.
La sicurezza di tutta una rete aziendale connessa a Internet viene ricondotta quindi alla sicurezza di un ristrettissimo numero di nodi, generalmente uno. Solo il nodo costituito dal firewall risulta essere direttamente collegato a Internet e dunque solo su di esso occorre effettuare le operazioni di controllo degli accessi, contro i tentativi di intrusione nella rete, e delle uscite, per bloccare richieste contrarie alla policy aziendale (FIGURA 10).

FIGURA 10 Router firewall: le frecce indicano la direzione del filtraggio



Non disporre di un firewall significa essere esposti a numerosi attacchi e tentativi di intrusione.
Nel caso di un semplice sistema casalingo, il danno può essere minimo, ma nel caso di un'azienda, una perdita di dati può risultare un danno considerevole soprattutto in termini di costi e affidabilità.
Il firewall diventa così uno degli strumenti più efficaci per la gestione della sicurezza delle reti, con la possibilità di gestirne le regole e definire meccanismi di controllo degli accessi.
Un firewall è configurabile e i filtri possono essere aggiunti o rimossi quando serve. È possibile decidere quali programmi o quali host possono avere accesso a Internet da una rete e quali no.

#prendinota

Esistono anche i cosiddetti firewall personali, cioè programmi installati sui normali elaboratori client, che filtrano solamente i pacchetti che entrano ed escono da quel computer.

Per esempio, grazie a una regola del firewall si può stabilire che solo un computer in una rete può accedere a Internet, oppure un solo computer può usare il protocollo FTP o ricevere e mandare email.
Funzioni di sicurezza di alto livello mettono al sicuro la rete da attacchi provenienti dall'esterno ma anche dall'interno. Attacchi di tipo ARP spoofing, port scanning, DoS, Worm.Blaster, Worm.Sasser, SQL slammer, per citare solo i più comuni, sono identificati, intercettati e resi inoffensivi.

3.2 Categorie di firewall

I firewall si possono distinguere sostanzialmente in 3 categorie in base al livello dello stack TCP/IP in cui operano.

1. **Application Level Firewall**: intercetta le trasmissioni a livello Application dello stack TCP/IP. In altre parole, valuta il contenuto applicativo dei pacchetti, per esempio riconoscendo e bloccando i dati appartenenti a virus o worm noti in una sessione HTTP o SMTP. A questa categoria appartengono i **proxy**. Utilizzando un proxy, la configurazione della LAN privata non consente connessioni dirette verso l'esterno: il proxy è connesso sia alla rete privata sia alla rete pubblica e permette alcune connessioni in modo selettivo. In pratica, mediante regole prestabilite dall'amministratore, vengono gestite le applicazioni che hanno accesso a Internet. Lavorando a livello Application, questo tipo di firewall riconosce comandi specifici delle applicazioni e offre un alto livello di protezione a scapito però della velocità della rete.

2. **Packet Filter Firewall**: lavora a livello Network e a livello Transport. Il Packet Filter Firewall è molto più veloce dell'Application Level Firewall in quanto il controllo viene effettuato sui pochi byte di header (20, escluse le opzioni) senza preoccuparsi dell'applicazione (di livello superiore) che ha generato il pacchetto. D'altra parte, questo firewall non ha la possibilità di gestire i dati all'interno del pacchetto. Per esempio, una email contenente un virus può tranquillamente passare attraverso il firewall, se è consentito il traffico POP/SMTP. Questo implica anche che non si possono filtrare le informazioni che passano dai computer interni verso l'esterno. Grazie a questa superficialità nel controllo, però, la connessione di rete non subisce rallentamenti.

   Se collocato alla fonte della connessione a Internet può essere configurato per funzionare su tutta la LAN (router firewall). I parametri che il Packet Filter Firewall controlla nell'header del pacchetto possono essere:

   – l'indirizzo IP di origine e destinazione (header IP);
   – il numero della porta TCP/UDP di origine e destinazione (header TCP/UDP);
   – il protocollo di livello superiore usato (header IP).

3. **Stateful Packet Inspection Firewall:** agisce a livello Transport e permette, oltre al controllo dell'header del pacchetto dati, anche di analizzarne il contenuto per catturare più informazioni rispetto ai semplici indirizzi di origine e destinazione. Un firewall che utilizza questo tipo di tecnologia può controllare lo stato della connessione TCP e compilare le informazioni ottenute su una tabella. In questo modo le operazioni di filtraggio dei pacchetti risulteranno basate sia su impostazioni definite dall'amministratore, sia sulla base di regole adottate per pacchetti simili già scansionati dal firewall. Nel complesso pregi e difetti sono sostanzialmente gli stessi del Packet Filter Firewall.

3.3 Le ACL

La sintassi della configurazione di un firewall in molti casi è basata su un meccanismo di **lista di controllo degli accessi ACL (Access Control List)**.
Le ACL possono essere modificabili tramite configurazione esplicita da parte dell'amministratore di sistema o possono variare in base allo stato interno del sistema.

Le ACL sono un elenco di istruzioni da applicare alle interfacce di un router allo scopo di gestire il traffico, filtrando i pacchetti in entrata e in uscita.

Esistono varie ragioni per decidere di utilizzare le ACL:
- fornire un livello base di sicurezza: si può per esempio restringere gli accessi a una determinata rete o sottorete;
- limitare il traffico e aumentare la performance della rete: si può, infatti, decidere che alcuni pacchetti vengano processati prima di altri;
- decidere quale tipo di traffico può essere trasmesso: si può per esempio permettere l'invio di email e impedire allo stesso tempo il Telnet.

#prendinota

Tra le tecniche di filtraggio più usate vi sono quelle che si basano sulle *whitelist* oppure sulle *blacklist*: le prime elencano in una tabella i soli indirizzi verso cui consentono il passaggio dei pacchetti, bloccando tutti gli altri; le seconde, viceversa, elencano le destinazioni bloccate, consentendo il passaggio dei pacchetti verso tutte le destinazioni non elencate.

Le ACL vengono elaborate dal router in maniera sequenziale in base all'ordine in cui sono state inserite le varie clausole. Appena un pacchetto soddisfa una delle condizioni, la valutazione si interrompe e il resto delle ACL non viene preso in considerazione. Il pacchetto viene quindi inoltrato o eliminato secondo l'istruzione eseguita. Se il pacchetto non soddisfa nessuna delle condizioni viene scartato (si considera cha alla fine di una ACL non vuota ci sia l'istruzione deny any ovvero **nega tutto**). L'ordine con cui sono scritte le ACL è importante: essendo eseguite in sequenza, è necessario inserire le condizioni più restrittive all'inizio.

ACL è quindi un meccanismo usato per esprimere regole complesse che determinano l'accesso o meno ad alcune risorse di un sistema informatico da parte dei suoi utenti.
Le ACL possono essere standard, **Standard ACL**, oppure estese, **Extended ACL**.
Le prime specificano delle limitazioni ai pacchetti guardando esclusivamente l'indirizzo della sorgente e vanno posizionate sull'interfaccia del router il più possibile vicino alla destinazione finale.
Le seconde, invece, pongono le limitazioni ai pacchetti in base a molte specifiche, come il protocollo usato, l'indirizzo di sorgente, l'indirizzo di destinazione e la porta a cui è indirizzato il pacchetto.
La Lezione 8 sarà interamente dedicata alla creazione di ACL standard ed estese mediante Cisco Packet Tracer.

FISSA LE CONOSCENZE

- A che cosa serve il firewall?
- Quali sono le 3 categorie di firewall distinte in base al livello TCP/IP in cui operano?
- Che cosa sono le ACL?
- Quali sono i principali motivi per cui si decide di utilizzare le ACL?
- Perché è importante l'ordine in cui sono scritte le ACL?
- Che differenza c'è tra le ACL standard e quelle estese?

4 IL PROXY SERVER

4.1 I compiti del Proxy Server

Un **proxy** è un programma (in esecuzione su un semplice computer o su un apparato hardware) che si interpone tra un client e un server facendo da tramite. Il client si collega al proxy, invece che al server, e gli invia la richiesta. Il proxy, a sua volta, si collega al server a cui inoltra la richiesta del client. Infine il proxy, ricevuta la risposta, la inoltra al client. I proxy, nella maggior parte dei casi, lavorano a livello Application. Il loro compito principale è garantire la **connettività** e il **caching** ai client a loro collegati ai fini dell'efficienza della rete (FIGURA 11).

Collocare il proxy in una posizione prossima ai client permette un miglioramento delle prestazioni e una riduzione del consumo di banda. Un Proxy Server può essere usato per molti compiti, alcuni già visti nell'Unità 8 del volume del quarto anno affrontando i proxy HTTP (Proxy Web). Nel complesso, le configurazioni del Proxy Server permettono loro di svolgere alcuni compiti che ricordiamo:

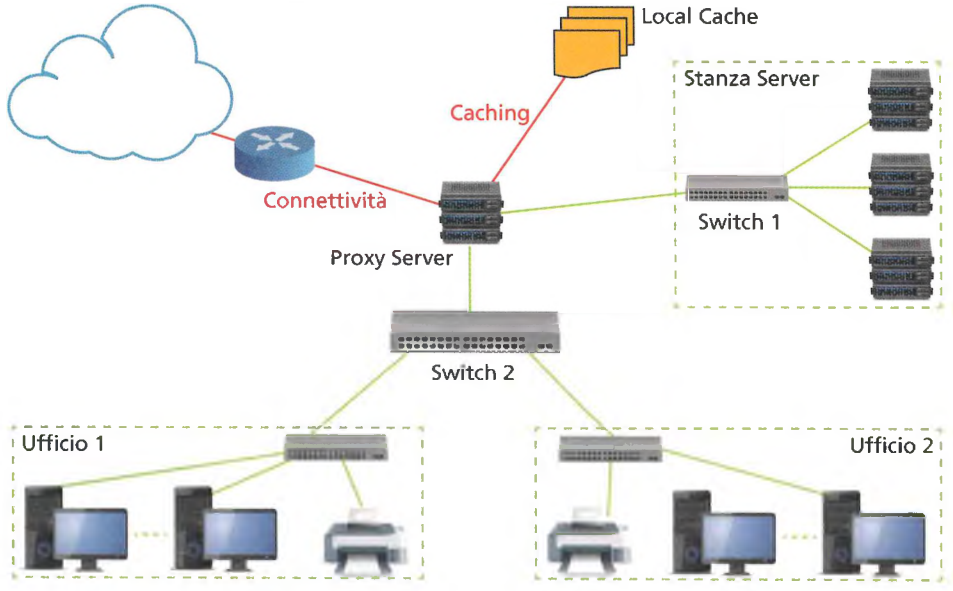


FIGURA 11 Collocazione del Proxy Server ai fini dell'efficienza della rete

- **connettività**: permettere a una intera rete privata di accedere a Internet attraverso un unico computer;
- **privacy**: mascherare il vero indirizzo IP del client in modo che il server remoto non venga a conoscenza di chi ha effettuato la richiesta. Questo compito verrà approfondito nella prossima Lezione 5, dove parleremo del Network Address Translation (NAT);
- **caching**: immagazzinare per un certo tempo i risultati delle richieste di un client e, se un altro client effettua le stesse richieste, rispondere senza dover consultare il server originale;
- **monitoraggio**: tenere traccia di tutte le operazioni effettuate (per esempio, tutte le pagine web visitate), consentendo statistiche e osservazioni dell'utilizzo della rete;
- **amministrazione**: applicare regole definite dall'amministratore di sistema per determinare quali richieste inoltrare e quali rifiutare, oppure limitare l'ampiezza di banda utilizzata dai client, oppure filtrare le pagine web in transito, per esempio bloccando quelle il cui contenuto è ritenuto offensivo in base a determinate regole;
- **filtraggio**: svolgere funzioni di firewall a livello Application, garantendo un alto grado di protezione a scapito della velocità della rete;

- **restrizioni**: creare una zona neutra (*terza zona*), non appartenente né alla LAN aziendale, né alla WAN, ma dove il traffico LAN e WAN è fortemente limitato e controllato. Questo processo verrà approfondito nella Lezione 6 dove parleremo della DeMilitarized Zone (DMZ).

4.2 Tipi di proxy

I Proxy Server, in particolare quelli che incorporano funzioni di firewall, possono essere diversamente collocati in base alle esigenze dell'azienda. Si possono individuare 3 categorie di utilizzo prevalenti.

1. **Single Proxy Topology**: risulta essere la scelta più semplice in quanto utilizza un singolo Proxy Server per servire l'intera rete (FIGURA 12). Questa configurazione è sufficiente però solo per un piccolo gruppo di client: la performance sarà compromessa appena aumenta il numero di client che richiedono pacchetti.

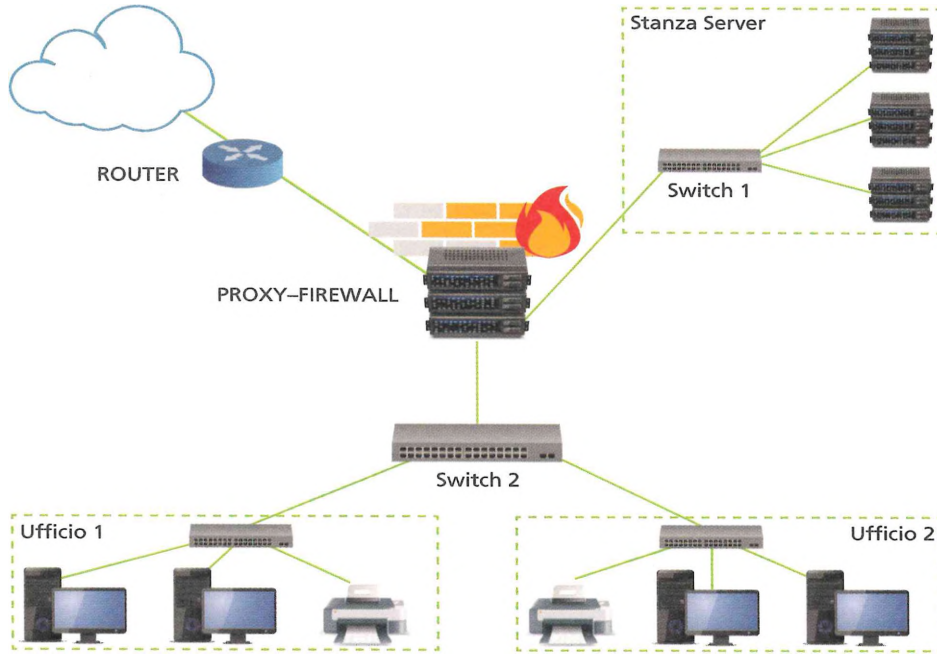


FIGURA 12 Single Proxy Topology

2. **Multiple Proxy Vertically Topology**: nel caso di reti medio-grandi è preferibile configurare più proxy, per esempio uno per ogni subnet, stabilendo un **proxy primario** a cui gli altri si connettono (FIGURA 13). I **proxy secondari** agiscono come client del primario. Questa tecnica *verticale* consente a qualsiasi client di avere il filtraggio dei pacchetti personalizzato. Il proxy secondario semplicemente guarda nel suo **repository** per vedere se è in grado di risolvere il pacchetto in transito. Se non lo risolve, inoltra il pacchetto al livello superiore, cioè verso il proxy primario. Questa configurazione fa sì che i proxy secondari dipendano dal primario per gli aggiornamenti, così come per i pacchetti personalizzati.
3. **Multiple Proxy Horizontally Topology**: consente di bilanciare il carico tra i server in base alle richieste dei client. In tale caso, le informazioni sul trattamento dei pacchetti personalizzati si distribuiscono ai server di pari livello, in modo da garantirne la risoluzione in locale (FIGURA 14). Lo svantaggio sta nella necessità di sincronizzare il repository di ogni proxy con quello degli altri.

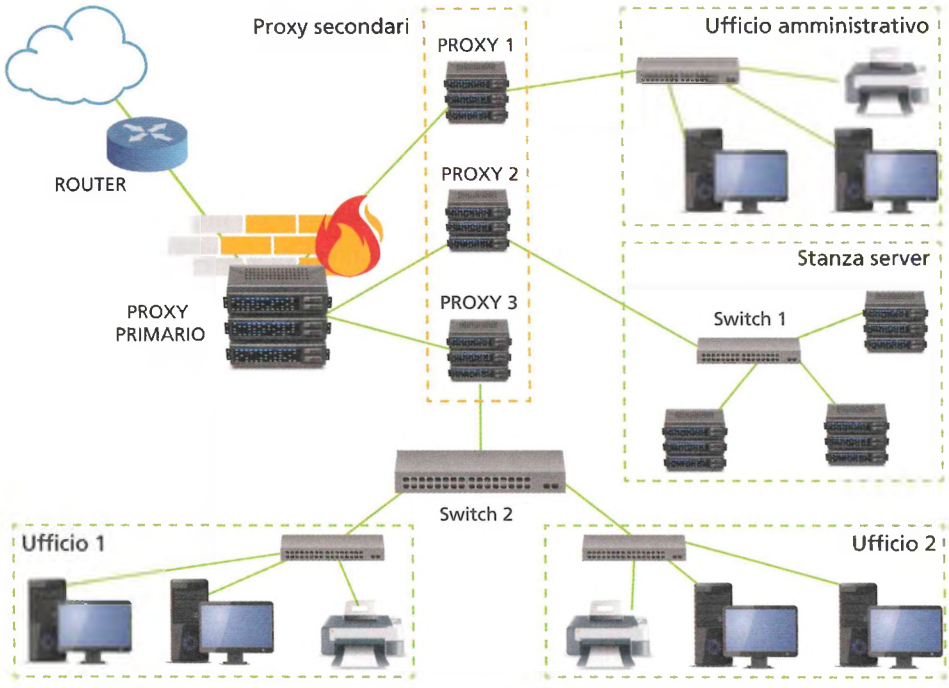


FIGURA 13 Multiple Proxy Vertically Topology

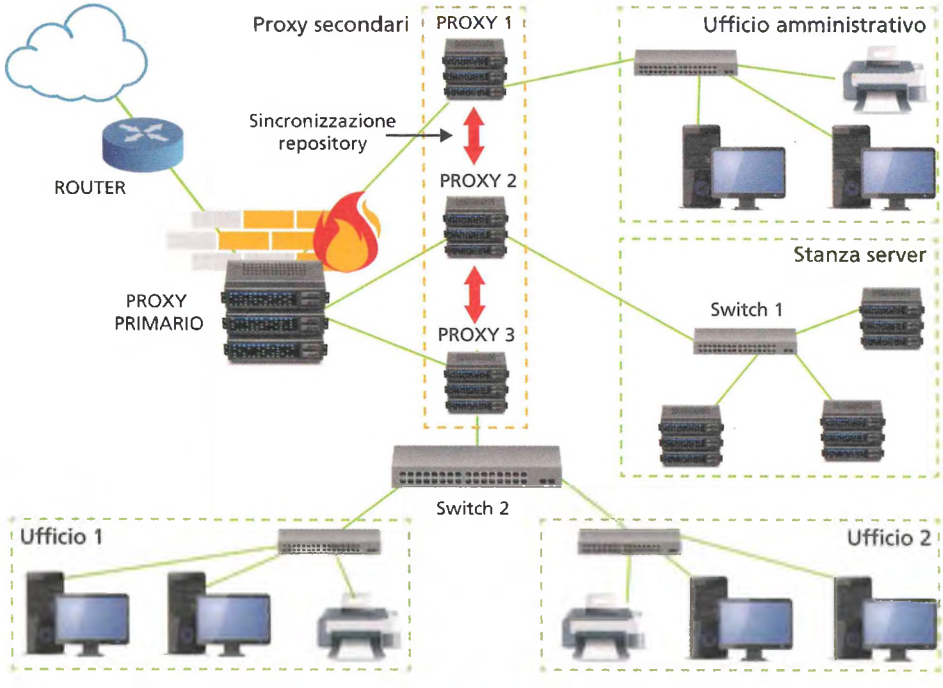


FIGURA 14 Multiple Proxy Horizontally Topology

FISSA LE CONOSCENZE

- Che cos'è un Proxy Server?
- Quali sono i compiti che un Proxy Server può svolgere?
- Quali sono le 3 categorie principali di Proxy Server?

5 LE TECNICHE NAT E PAT

5.1 NAT (Network Address Translation)

NAT è una tecnica attuata dal router che, nell'intestazione di un pacchetto IP, sostituisce l'indirizzo IP, sorgente o destinazione, con un altro indirizzo. NAT, nel suo impiego più diffuso, viene usato per permettere a una rete locale, che usa una classe di indirizzi privata, di accedere a Internet usando un solo indirizzo pubblico fornito dall'Internet Service Provider (ISP).
Si tratta dunque di condividere Internet su una LAN usando un solo punto di accesso (un solo indirizzo IP pubblico).
Dal punto di vista della sicurezza, anche se non efficace come un firewall, un NAT offre già buone garanzie, proprio perché nasconde gli host interni e non indirizza loro il traffico generico proveniente dall'esterno.

> NAT usa una **tabella** contenente la corrispondenza tra le socket interne ed esterne in uso. Le **socket** non sono altro che l'insieme di protocollo, indirizzo IP e porta di comunicazione usati da mittente e destinatario.

Quando un client richiede una pagina web a un server esterno, il suo indirizzo e la sua porta di origine vengono **traslati** e la corrispondenza viene registrata nella tabella. Quando arriva la risposta dal server esterno, la tabella permette di capire chi voleva quei dati, quindi effettua la traslazione inversa e manda i pacchetti al client richiedente. Tutte le comunicazioni provenienti dall'esterno che non sono state registrate nella tabella vengono eliminate.
Vediamo in FIGURA 15 un esempio in cui supponiamo sia utilizzato il protocollo TCP per tutte le trasmissioni dei pacchetti e che le socket siano limitate a indirizzo IP e numero di porta.

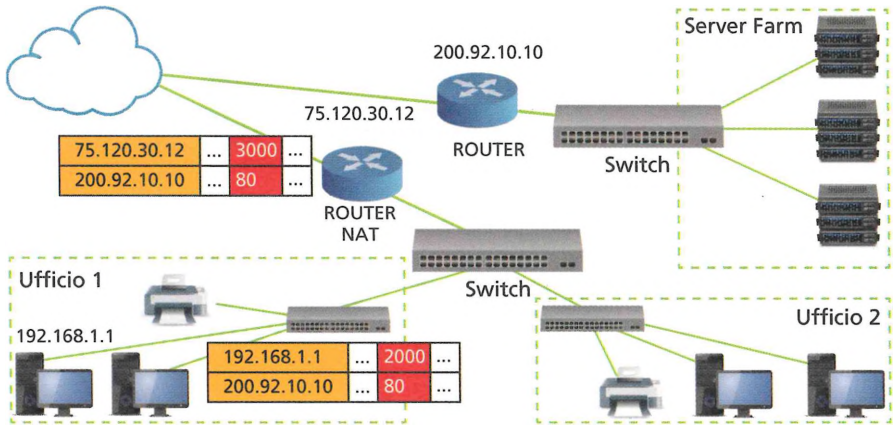


FIGURA 15 Router con funzionalità NAT

Il client con indirizzo privato 192.168.1.1 utilizza la porta 2000 per chiedere una pagina web residente presso una server farm, la quale risponde all'indirizzo pubblico 200.92.10.10 sulla porta 80 (Well Known Port per HTTP). Il router NAT (75.120.30.12) della LAN riceve la richiesta del client e, prima di inoltrare i pacchetti in rete sulla sua porta 3000, modifica l'intestazione dei pacchetti in modo che risultino generati

dal router NAT stesso (**traslazione dell'indirizzo**). Contestualmente, inserisce nella tabella contenente la corrispondenza tra le socket, la relativa corrispondenza:

CLIENT		ROUTER NAT		SERVER DESTINAZIONE
192.168.1.1:2000	↔	75.120.30.12:3000	↔	200.92.10.10:80

La destinazione finale riceverà i pacchetti dal router NAT e restituirà la pagina web richiesta. A quel punto, al router NAT non resterà che consultare la tabella con la corrispondenza delle socket, ripristinare l'indirizzo originario (effettuando un'**altra traslazione** dell'indirizzo) e inoltrare i pacchetti al client della sua LAN che aveva effettuato la richiesta.
Il limite del NAT è che può traslare un solo indirizzo IP per volta, dovendo traslare indirizzo IP e porta abbinati. Quindi se arriva una seconda richiesta per lo stesso server di destinazione, il router NAT non può gestirla avendo già mappato la connessione con quel server sulla porta 3000 dell'esempio ed essendo questa già in uso. È come se si fosse creata una seconda riga, priva di senso, nella tabella di corrispondenza:

CLIENT		ROUTER NAT		SERVER DESTINAZIONE
192.168.1.1:2000	↔	75.120.30.12:3000	↔	200.92.10.10:80
192.168.2.1:2000	↔	75.120.30.12:3000	↔	200.92.10.10:80

In questo caso vale la regola del **rapporto 1:1** tra indirizzo IP server destinazione e indirizzo IP client.
Il router NAT, cioè, non è in grado di distinguere a quale dei due client locali sono destinati, di volta in volta, i pacchetti in arrivo dallo stesso server remoto.
La tecnica PAT supera questa limitazione.

La funzione NAT presenta diversi vantaggi:
- limita il numero di indirizzi IP pubblici necessari per collegare una LAN a Internet;
- mantiene inalterata la configurazione degli host;
- non modifica il funzionamento dei protocolli e delle applicazioni della rete intranet;
- offre una flessibilità elevata grazie allo spazio molto esteso per gli indirizzi privati;
- riduce i costi di accesso a Internet (gli indirizzi pubblici sono concessi a pagamento);
- garantisce maggior sicurezza per i computer della rete locale (dall'esterno non si conosce l'indirizzo IP privato di un host).

Il NAT presenta 3 funzionalità:
- Static NAT;
- Dynamic NAT;
- Port Address Translation (PAT).

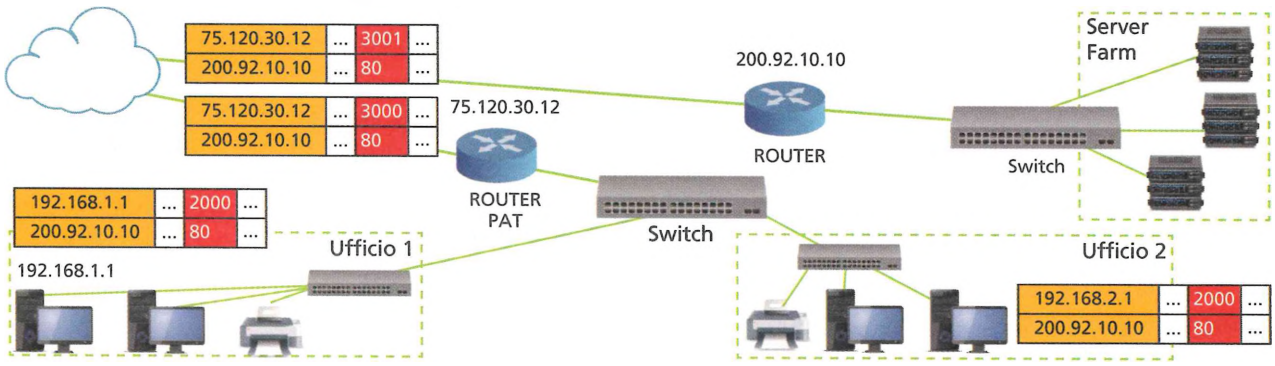
La prima ha a disposizione un solo indirizzo pubblico (IP statico) e a qualunque pacchetto in uscita assegnerà tale indirizzo.
La seconda ha a disposizione un insieme di indirizzi pubblici tra cui sceglierne uno da assegnare ai pacchetti in uscita.
La terza traduce in modo dinamico l'indirizzo delle porte, ovvero guarda alla porta di trasmissione e non agli indirizzi IP degli host. Quest'ultima funzionalità può essere usata in coppia con una della precedenti per ottenere la traslazione dell'indirizzo IP e della porta su ogni pacchetto.

Nella Lezione 9 vedremo nello specifico come realizzare le funzionalità di **NAT statico** e **NAT dinamico**, mediante due esercitazioni con Cisco Packet Tracer.

5.2 PAT (Port Address Translation)

La tecnica PAT consente al router di utilizzare un singolo indirizzo IP per gestire oltre 64.000 connessioni private contemporaneamente (per la precisione, 2^{16} = 65.536 porte diverse indirizzabili). Questo significa che può traslare più indirizzi IP client per un medesimo indirizzo IP destinazione cambiando solo la porta (FIGURA 16). Per il PAT vale la regola del **rapporto 1:N** tra indirizzo IP server destinazione e indirizzo IP client.

FIGURA 16 Router con funzionalità PAT



In questo caso la seconda riga della tabella di corrispondenza permette al router PAT di distinguere a quale client inoltrare i pacchetti in arrivo dal server di destinazione sulle due connessioni aperte rispettivamente sulle porte 3000 e 3001:

CLIENT		ROUTER PAT		SERVER DESTINAZIONE
192.168.1.1:2000	↔	75.120.30.12:3000	↔	200.92.10.10:80
192.168.2.1:2000	↔	75.120.30.12:3001	↔	200.92.10.10:80

5.3 NAT per IPv6

Anche IPv6 implementa una forma di NAT con scopi del tutto diversi dal NAT per IPv4. Con IPv6 non serve più "risparmiare" indirizzi pubblici ma serve mettere in comunicazione reti IPv6 con reti IPv4.

Per la fase di transizione da IPv4 a IPv6, IETF ha ipotizzato 3 meccanismi di possibile convivenza:

- **dual-stack**: i dispositivi di rete sono in grado di inoltrare pacchetti IPv4 e pacchetti IPv6;
- **conversion**: è considerato il NAT per IPv6 realizzato con il protocollo **NAT-PT** (Network Address Translation - Protocol Translator) che permette la comunicazione tra reti IPv6 e reti IPv4;
- **tunneling per IPv6**: incapsula un pacchetto IPv6 in un pacchetto IPv4, permettendone il trasporto in reti IPv4.

La tecnica del **dual-stack** prevede l'utilizzo del doppio stack IP (FIGURA 17) nella pila di protocolli TCP/IP.

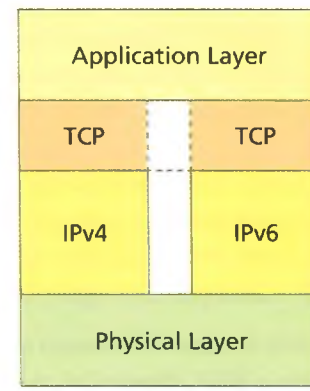


FIGURA 17 Dual-stack

Questo doppio stack permette di interpretare entrambe le versioni del protocollo IP e quindi di smistare ai livelli superiori il contenuto del pacchetto senza che questi sappiano da quale protocollo IP derivi.

Il dual-stack è senza dubbio una delle tecniche più semplici da implementare, ma presenta alcuni svantaggi. Innanzitutto aumenta la complessità della rete: router e switch devono essere multiprotocollo per funzionare sia con IPv4 che con IPv6 e devono interpretare più istanze dello stesso protocollo. Inoltre non risolve il problema della scarsità degli indirizzi IPv4 poiché secondo la tecnica del dual-stack un'interfaccia dev'essere sempre e comunque dotata dei due indirizzi IPv4 e IPv6. Infine i due indirizzi devono essere entrambi annunciati in Internet e ciò complica e rallenta il routing.

La **conversion** con NAT-PT è un sistema che sfrutta i concetti introdotti dalla tecnologia NAT: infatti esso opera una **conversione** dell'indirizzo IPv6 in indirizzo IPv4 e viceversa secondo le tecniche di un NAT IPv4, permettendo in questo modo a due reti con protocolli IP diversi di poter comunicare tra di loro.
NAT-PT consente quindi la comunicazione diretta tra reti solo IPv6 e reti solo IPv4 come mostrato in FIGURA 18.

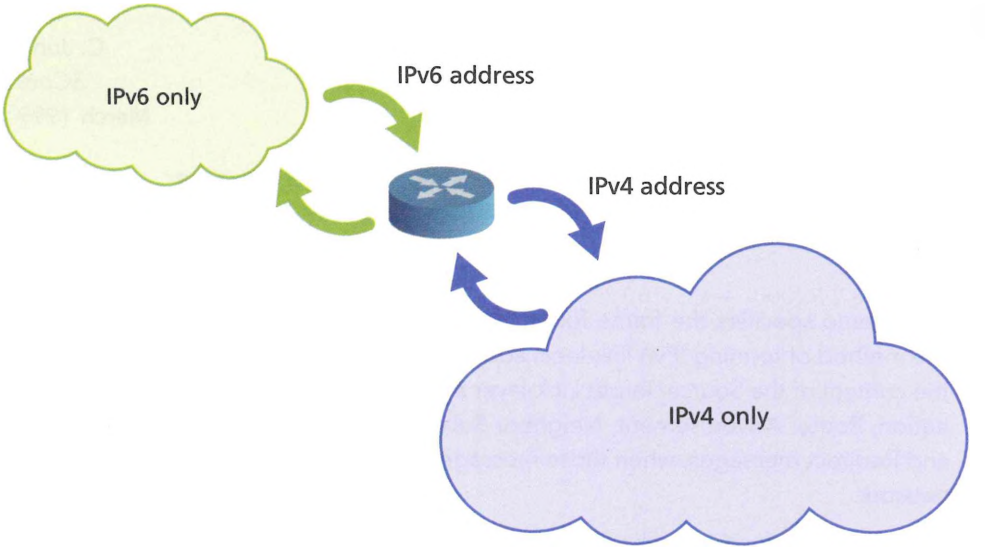


FIGURA 18 Comunicazione diretta IPv4-IPv6

È consigliabile non utilizzare NAT-PT per comunicare tra un host dual-stack e un host solo IPv6 o solo IPv4.
Allo stesso modo è meglio evitare l'uso di NAT-PT in uno scenario in cui una rete solo IPv6 tenta di comunicare con un'altra rete solo IPv6 tramite un backbone IPv4 o viceversa, perché NAT-PT richiede una doppia traduzione degli indirizzi IP.
In presenza di tali scenari è più conveniente utilizzare tecniche di tunneling.

> Tuttavia, se si dispone di una rete interamente IPv6 e ci si connette a un provider IPv6, il NAT non ha senso perché non serve, tranne per il fatto che è possibile eseguire il tunneling tra reti IPv4 su reti IPv6.

La tecnica del **tunneling** è quella più utilizzata per far fronte ai problemi di incompatibilità tra le reti IPv4 e IPv6. Con il tunneling si stabilisce un collegamento point-to-point tra due host.

4to6

Nel tunneling IPv4 di un pacchetto IPv6, i pacchetti IPv6 vengono incapsulati dall'host sorgente in pacchetti IPv4, inviati nel tunnel IPv4 (FIGURA 19) e, una volta giunti a destinazione, l'host ricevente li decapsula per riottenere l'indirizzo in IPv6.

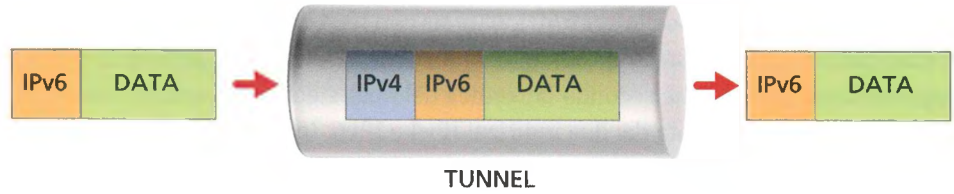


FIGURA 19 Tunnel IPv4 per pacchetti IPv6

Il tunneling IPv4 è di tipo multicast, consentendo ai nodi IPv6 di vedere tutto il resto della rete a cui sono connessi come un'unica rete LAN IPv6 virtuale. Questa tecnica è descritta nella RFC 2529.

IN ENGLISH PLEASE

Network Working Group
Request for Comments: 2529
Category: Standards Track

B. Carpenter
IBM
C. Jung
3Com
March 1999

Transmission of IPv6 over IPv4 Domains without Explicit Tunnels

Abstract

This memo specifies the frame format for transmission of IPv6 [IPV6] packets and the method of forming IPv6 link-local addresses over IPv4 domains. It also specifies the content of the Source/Target Link-layer Address option used in the Router Solicitation, Router Advertisement, Neighbor Solicitation, and Neighbor Advertisement and Redirect messages, when those messages are transmitted on an IPv4 multicast network.

The motivation for this method is to allow isolated IPv6 hosts, located on a physical link which has no directly connected IPv6 router, to become fully functional IPv6 hosts by using an IPv4 domain that supports IPv4 multicast as their virtual local link. It uses IPv4 multicast as a "virtual Ethernet".

6to4

Viceversa, il tunneling IPv6 su IPv4 è di difficile realizzazione sulle reti globali per le complicazioni che introduce a livello di routing e quindi il suo utilizzo è limitato ad applicazioni e comunicazioni in reti locali più o meno grosse.

È una tecnica di tunnel automatico, descritta dalla RFC 3056 successivamente ampliata dalla RFC 6343. Essa integra nell'indirizzo IPv6 l'indirizzo IPv4 dell'host destinazione. Il modello parte dall'assunto che un dispositivo utilizza nativamente un indirizzo IPv6 ma opera in un ambiente, per esempio Internet, in cui il fornitore di servizi utilizza IPv4.

IN ENGLISH PLEASE

Internet Engineering Task Force (IETF)
Request for Comments: 6343
Category: Informational
ISSN: 2070-1721

B. Carpenter
Univ. of Auckland

August 2011

Advisory Guidelines for 6to4 Deployment

Abstract

This document provides advice to network operators about deployment of the 6to4 technique for automatic tunneling of IPv6 over IPv4. It is principally addressed to Internet Service Providers (ISPs), including those that do not yet support IPv6, and to Content Providers. Some advice to implementers is also included. The intention of the advice is to minimize both user dissatisfaction and help-desk calls.

Usando un tunnel IPv6, viene generato un indirizzo IPv6 composto nel seguente modo (0 indica il bit più significativo):

- bit 0-15: prefisso 6to4 al valore esadecimale fisso 2002;
- bit 16-47: indirizzo IPv4 espresso in notazione esadecimale; per esempio: 160.1.1.32 diventa A001:0120;
- bit 48-63: identificativo delle sottoreti;
- bit 64-127: identificativo dell'interfaccia fisica.

Il pacchetto così generato viene inviato tramite il tunnel al router di destinazione che è in grado di interpretarlo e preparare un pacchetto IPv4 per l'host cui era indirizzato. Con questa tecnica, un singolo indirizzo IPv4 corrisponde a un indirizzo IPv6 con maschera /48: per esempio, l'indirizzo IPv4 160.1.1.32 equivale al range di indirizzi IPv6 2002: A001:0120::/48.

FISSA LE CONOSCENZE

- In che cosa consiste la tecnica NAT attuata dai router?
- Quali sono le 3 funzionalità del NAT e che caratteristiche hanno?
- In che cosa consiste la tecnica PAT attuata dai router?
- Quali sono i 3 meccanismi per la possibile convivenza di IPv4 e IPv6?
- Che cosa consente di fare NAT-PT?
- In quale caso il NAT su un host IPv6 non serve?
- Che cosa si intende rispettivamente per 4to6 e per 6to4?

6 LA DEMILITARIZED ZONE (DMZ)

6.1 La terza zona

La sicurezza perimetrale si occupa di proteggere una rete nei punti in cui essa è a contatto con il mondo esterno. Dividere la rete in zone è una tecnica che aumenta notevolmente la sicurezza: in base al tipo di traffico e alla funzione si identificano diverse zone.
Nei casi più semplici, le uniche due zone, LAN e WAN, sono attestate sui due lati del firewall.

La **zona LAN** è il segmento privato e protetto: comprende tutti gli host e i server i cui servizi sono riservati all'uso interno.
La **zona WAN** è la parte esterna a cui appartengono gli apparati di routing che sostengono il traffico da e per rete locale, Internet e sedi remote dell'azienda.
In molti casi, però, si rende necessaria la creazione di una terza zona.

> Questa terza zona è detta **DMZ, DeMilitarized Zone**. Si tratta di un'area in cui sia il traffico WAN sia quello LAN sono fortemente limitati e controllati.
> Tale configurazione viene normalmente utilizzata per permettere ai server posizionati sulla DMZ di fornire servizi all'esterno senza compromettere la sicurezza della rete aziendale interna.

Nel caso più comune si colloca nella DMZ la **posta elettronica**: l'installazione di un server mail all'interno della rete aziendale comporta la pubblicazione del servizio SMTP. In pratica, il server che pubblica il servizio SMTP viene collocato in DMZ ed eventualmente anche la webmail, l'antispam e l'antivirus; in LAN restano il server che ospita il database delle caselle e gli altri servizi.
Altro caso tipico sono gli **Application Server**, che isolano un database residente in LAN ma ne offrono un'interfaccia verso l'esterno.

Generalmente in DMZ si installano i server detti **front-end**, a cui corrispondono i relativi **back-end** in LAN. In genere un server di front-end comunica solo con il suo back-end, e solo con le porte TCP e/o UDP strettamente necessarie.
Nel malaugurato caso in cui un servizio in LAN sia compromesso in seguito a una vulnerabilità, l'aggressore potrebbe raggiungere anche gli altri host della rete, dato che in LAN non esiste isolamento tra il server e gli altri nodi.

Se lo stesso problema si verificasse in DMZ, l'aggressore avrebbe grosse difficoltà a raggiungere la LAN, poiché il traffico tra i server front-end e back-end è fortemente limitato dal firewall.

6.2 Tipi di DMZ

Una DMZ, per esporre all'esterno i servizi di un'azienda, può essere realizzata in due modi:

- **vicolo cieco**: realizzato mediante un firewall con due porte, una verso la LAN e una verso la DMZ, oltre naturalmente alla porta verso la WAN.

La Figura 12 della Lezione 4 ne illustra un esempio: il firewall separa la stanza server (DMZ) dagli uffici (LAN). L'idea è quella di consentire l'accesso dall'esterno (ma anche dall'interno) alla DMZ, garantendo che, una volta raggiunta la DMZ, non si possa accedere alla LAN, cioè agli uffici. Si è cioè entrati in un vicolo cieco da cui si esce solo attraversando la stessa via da cui si è entrati. Dunque, un utente potrà accedere ai servizi che l'azienda rende accessibili dall'esterno (per esempio da Internet) nella DMZ senza mettere in pericolo la sicurezza dei dati presenti nella zona LAN;

- **zona cuscinetto**: creata aggiungendo un secondo firewall, come nella FIGURA 20. L'**external firewall** separa la rete pubblica dalla DMZ; l'**internal firewall** separa la DMZ dalla zona LAN vera e propria. Questo garantisce una sicurezza ancora maggiore dei database presenti in LAN. Chi dall'esterno approda alla DMZ, per attaccare i dati in LAN dovrà superare un secondo firewall dedicato.

Ricapitolando, la DMZ è un'area pubblica protetta, dove il traffico è strettamente regolato da entrambi i lati ed è utile per pubblicare servizi verso l'esterno minimizzando i rischi per la rete interna. La DMZ è una *sottorete* della rete aziendale accessibile dai dipendenti tramite LAN e da utenti esterni tramite Internet. Architetture più complesse possono implicare la presenza di più zone DMZ distinte, ognuna con la sua policy e con il relativo controllo del traffico su tutti i lati. Laddove la sicurezza è vitale, la DMZ è stratificata, cioè sono presenti più di due firewall.

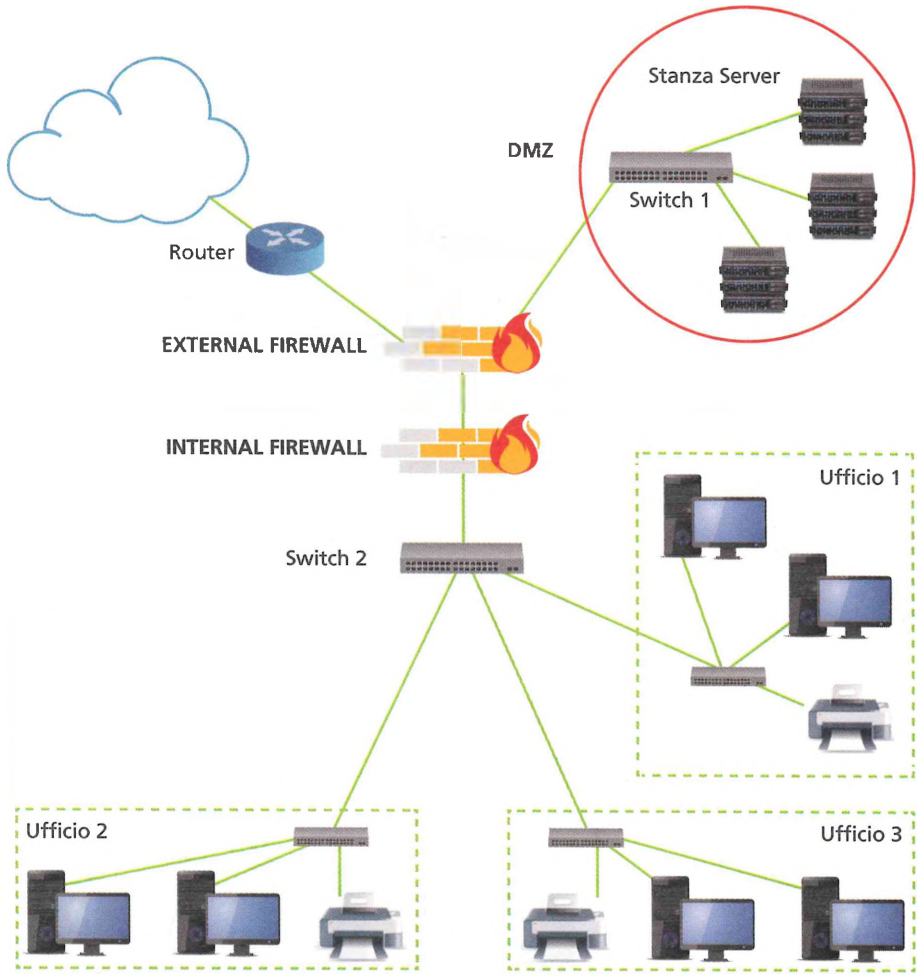


FIGURA 20 DMZ con modalità a zona cuscinetto

FISSA LE CONOSCENZE

- Perché la DMZ è detta terza zona?
- Quali sono i due modi in cui si può realizzare una DMZ e in che cosa differiscono?
- Per che cosa viene normalmente utilizzata la DMZ?

7 PACKET TRACER: CONFIGURARE LE VLAN E VERIFICARE STP

In questa esercitazione di laboratorio realizzeremo con il simulatore Packet Tracer la segmentazione di una LAN in più VLAN mediante l'assegnazione statica alle porte degli switch.

esercizio

File sorgenti
Scarica il file

→ PROBLEMA

Data una rete LAN aziendale, segmentarla in 3 distinte reti più piccole, indipendenti, una per ciascun dipartimento: amministrazione (AMM), vendite (VEN) e progettazione (PROG).

→ ANALISI DEL PROBLEMA

Per realizzare la segmentazione della rete non vogliamo aggiungere dei router per creare delle reti fisicamente separate. Vogliamo invece usare gli switch già presenti per creare reti virtualmente separate, realizzando 3 distinti domini di broadcast mediante la configurazione di altrettante VLAN.

→ SVOLGIMENTO

Si consideri lo scenario mostrato in FIGURA 21.

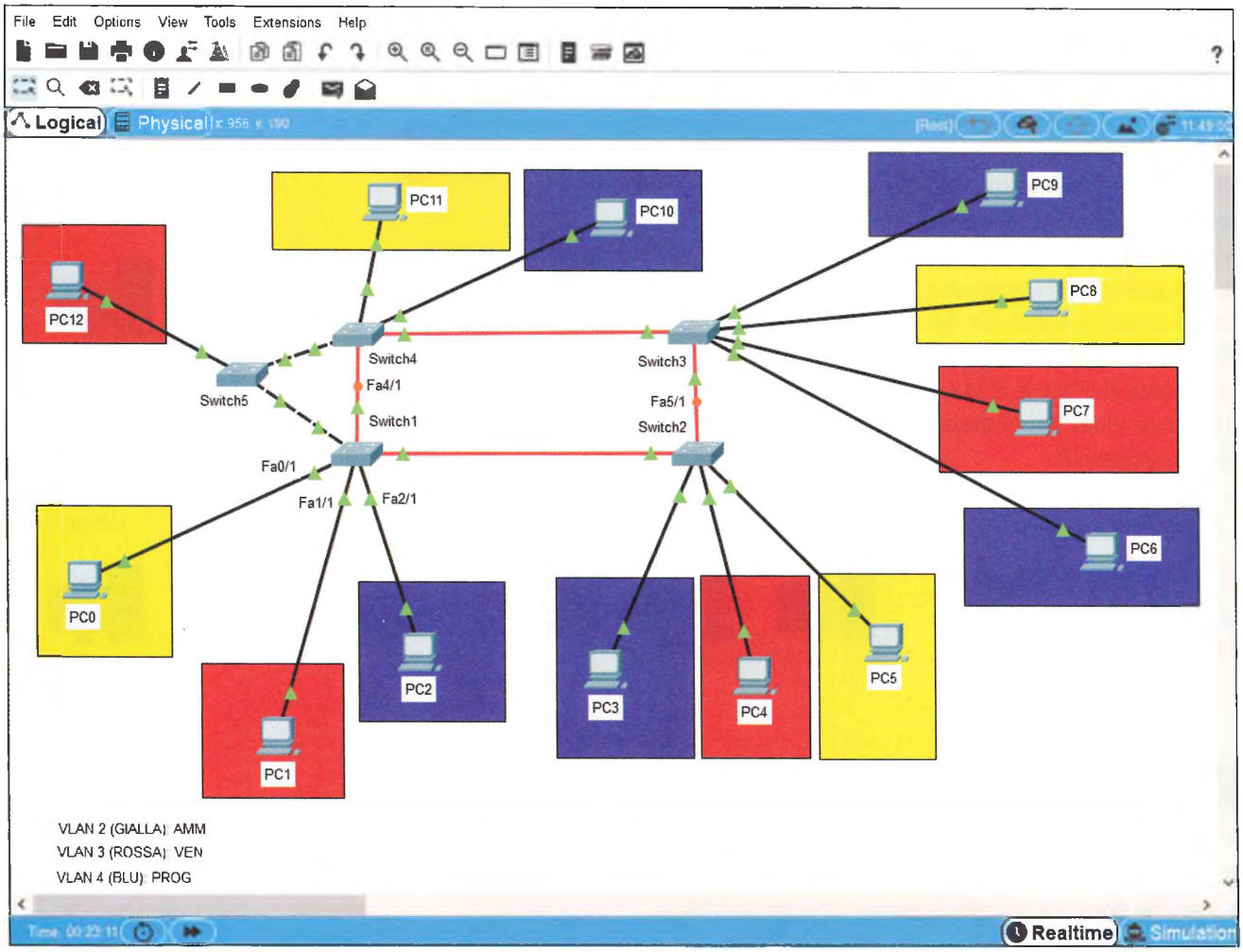


FIGURA 21 Scenario LAN segmentata in 3 VLAN

Per realizzare e verificare quanto richiesto procediamo in 5 passi:
d) creazione delle VLAN sugli switch;
e) assegnazione delle porte degli switch alle VLAN create;
f) configurazione dei trunk tra gli switch;
g) test di connettività tra i PC;
h) verifica del protocollo STP.

a. Creazione delle VLAN sugli switch

Per configurare le VLAN sugli switch occorre innanzitutto cliccare sullo switch e dalla scheda **Config** selezionare **VLAN Database**. Di seguito introdurre il **VLAN Number** e la **VLAN Name** di ogni VLAN che si vuole configurare e con **ADD** aggiungerla all'elenco. La FIGURA 22 mostra l'operazione svolta sullo Switch1.

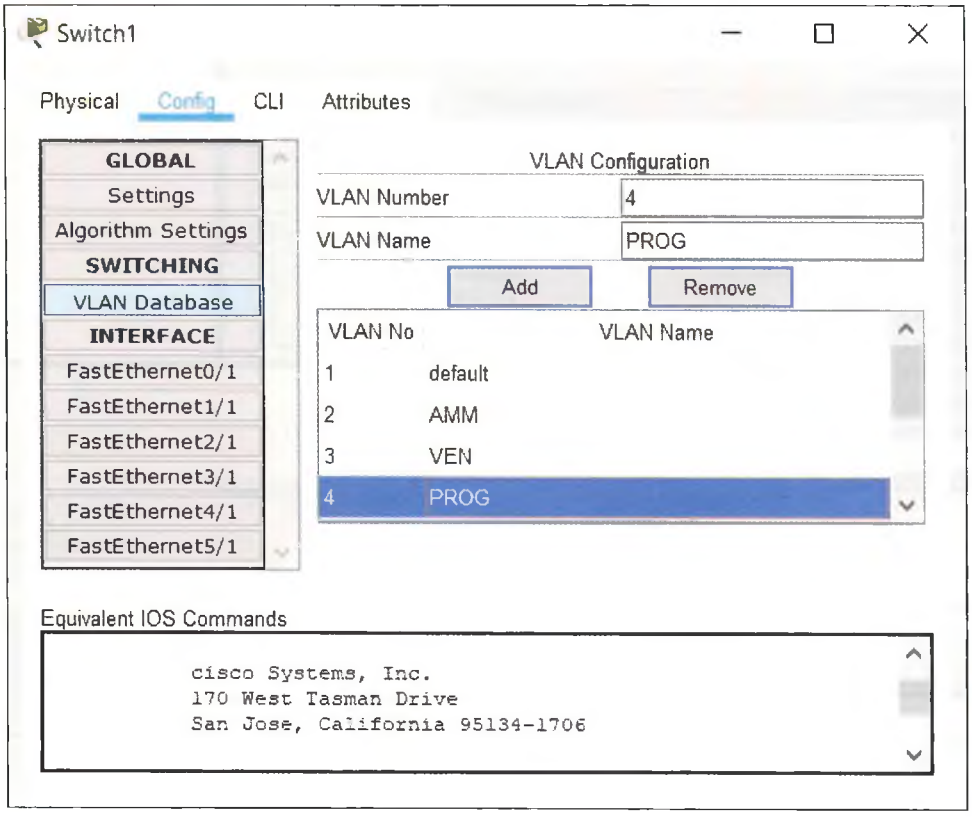


FIGURA 22 VLAN Configuration del VLAN Database dello Switch1

#prendinota

Per default, sugli switch della Cisco tutte le porte appartengono alla VLAN1.

b. Assegnazione delle porte degli switch alle VLAN create

Sullo stesso switch andiamo ora a configurare le porte Ethernet verso i PC a esso collegati.
Sempre dalla scheda Config dello switch, selezioniamo la porta Ethernet che ci interessa e le assegniamo in modalità **Access** la VLAN cui appartiene. La FIGURA 23 mostra l'operazione svolta sullo Switch1 nel rispetto dello scenario proposto in Figura 21 e riassunto nella seguente tabella.

PORTA	VLAN Number	VLAN Name	PC
FastEthernet0/1	2	AMM	PC0
FastEthernet1/1	3	VEN	PC1
FastEthernet2/1	4	PROG	PC2

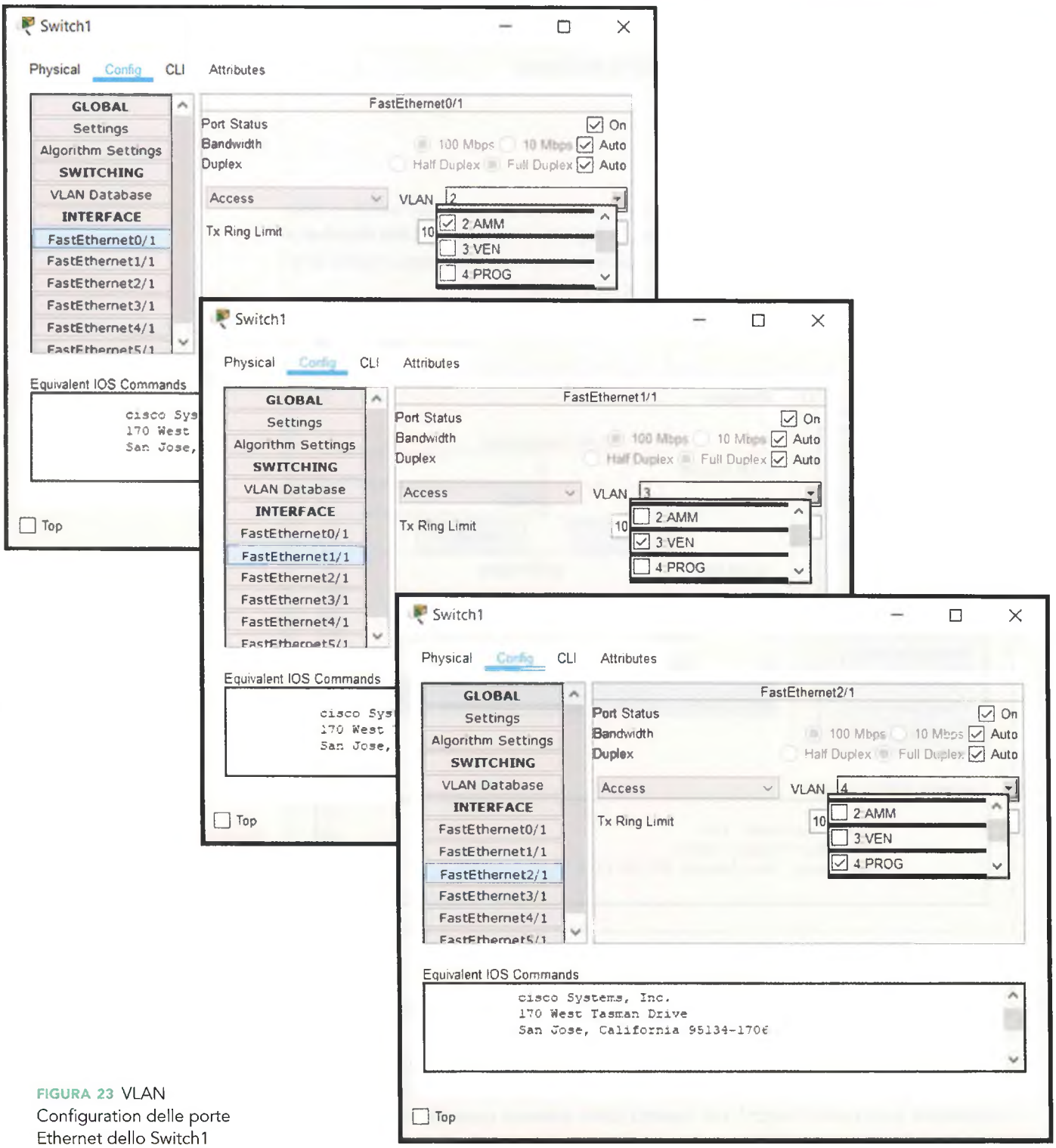


FIGURA 23 VLAN Configuration delle porte Ethernet dello Switch1

#prendinota

Per default, sugli switch della Cisco tutte le porte che appartengono alla stessa VLAN sono **Access port**.

Identica operazione va svolta su tutti gli switch della LAN. Al termine della configurazione è possibile controllare le VLAN configurate sulle porte mediante il comando nella CLI:

```
Switch#show vlan brief
```

il cui risultato per lo Switch1 è mostrato in FIGURA 24.

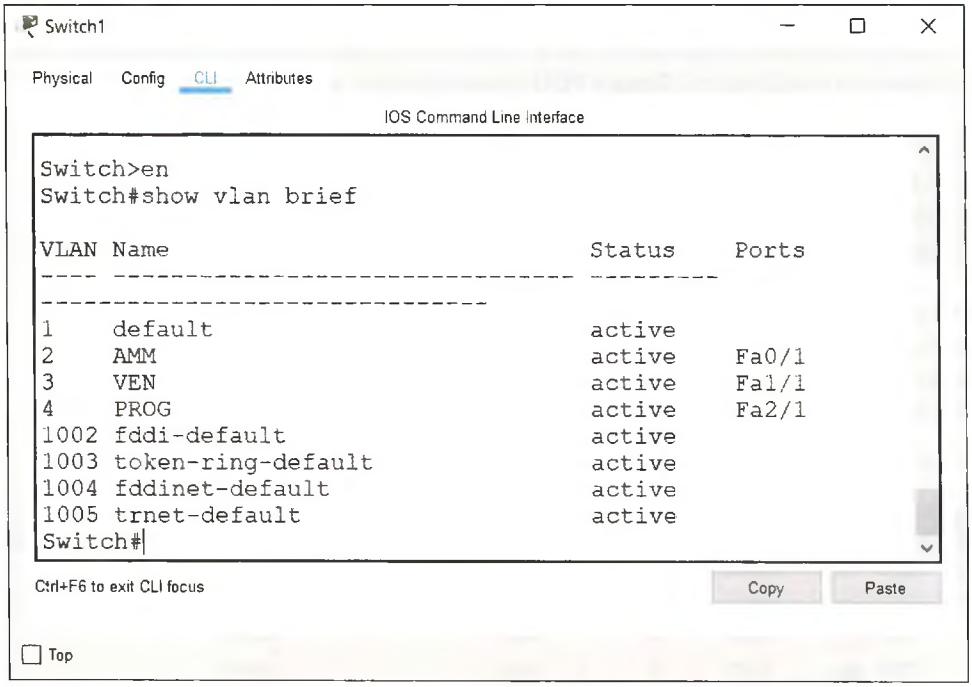


FIGURA 24 Controllo da CLI dell'assegnazione delle VLAN alle porte Ethernet dello Switch1

c. Configurazione dei trunk tra gli switch

Per configurare i link in modalità **trunk** al fine di consentire il passaggio delle informazioni tra VLAN che si estendono su diversi switch, selezioniamo dalla scheda **Config** la porta Ethernet che ci interessa e le assegniamo in modalità **Trunk** le 3 VLAN create.

La FIGURA 25 mostra l'operazione svolta sullo Switch1 alla porta FastEthernet3/1 nel rispetto dello scenario proposto in Figura 21.

Identica operazione va svolta sulle altre porte dello Switch1 che lo collegano ad altri switch e su tutti gli altri switch della LAN.

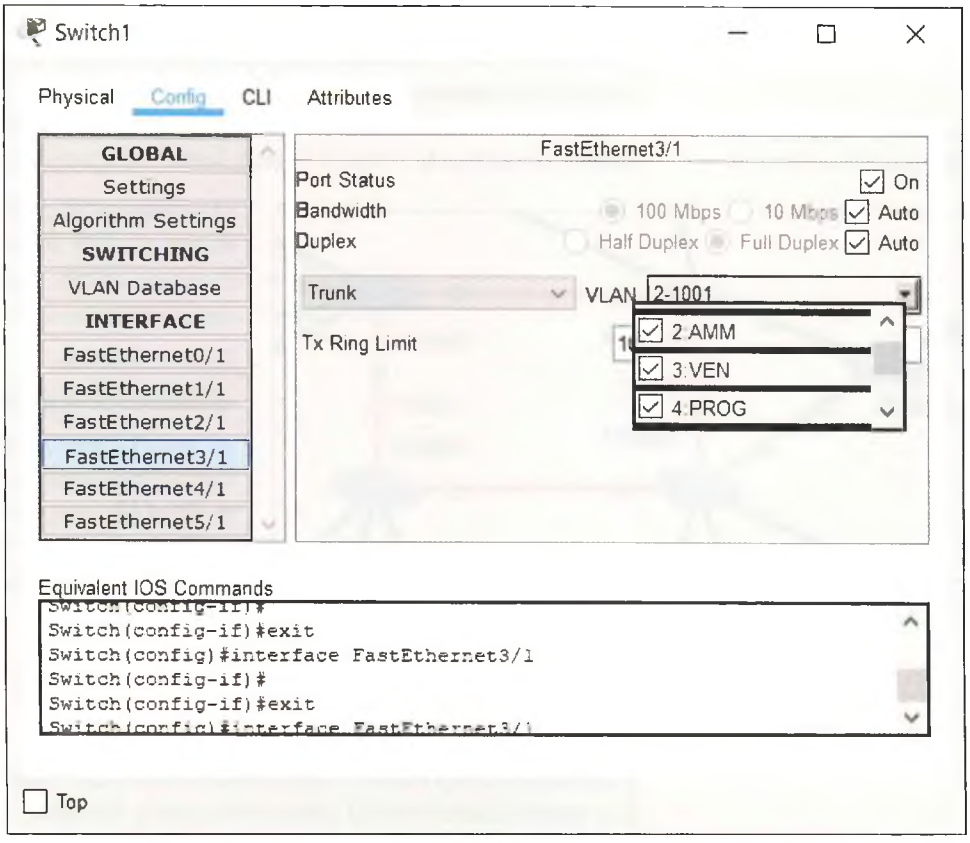


FIGURA 25 Configurazione del link trunk su FastEthernet3/1 di Switch1

d. Test di connettività tra i PC

A questo punto la configurazione delle VLAN è conclusa e possiamo verificarne il funzionamento mediante dei **Simple PDU** (comando ping, protocollo ICMP) tra i vari PC.

> Per utilizzare questo comando è necessario che ai computer sia stato assegnato un indirizzo IP, manualmente o automaticamente tramite DHCP. Se optiamo per il DHCP, non essendo presente nel nostro scenario un router o un server, il DHCP assegnerà indirizzi APIPA.

Proviamo tre ping:

- tra PC0 e PC1 (stesso switch ma VLAN diverse);
- tra PC0 e PC5 (stessa VLAN ma switch diversi);
- tra PC6 e PC9 (stessa VLAN e stesso switch).

La FIGURA 26 mostra il risultato dei 3 ping.

FIGURA 26 Risultato dei ping per la verifica della connettività

Realtime Simulation

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Failed	PC0	PC1	ICMP		0.000	N	0	(edit)	(delete)
	Successful	PC0	PC5	ICMP		0.000	N	1	(edit)	(delete)
	Successful	PC6	PC9	ICMP		0.000	N	2	(edit)	(delete)

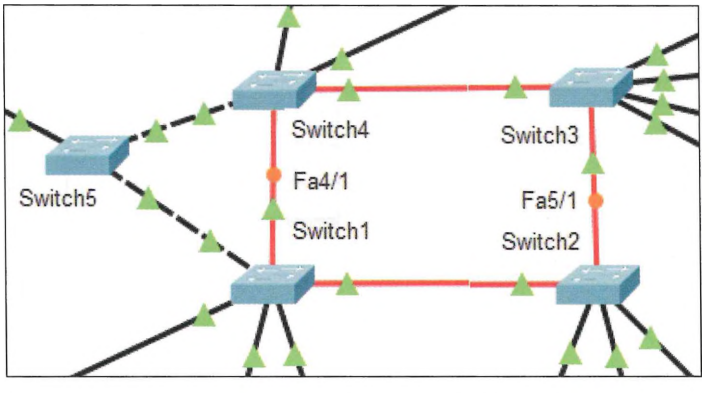
Dalla figura si può notare che solo i ping tra PC che stanno sulla stessa VLAN hanno successo, mentre il ping tra PC appartenenti a VLAN diverse falliscono anche se i PC sono collegati allo stesso switch.

e. Verifica del protocollo STP

Lo scenario proposto in Figura 21 presenta dei loop fisici tra gli switch. Questo implica l'intervento del protocollo STP che a livello logico blocca le porte degli switch che introducono percorsi ridondanti che possono generare dei loop.

Nella FIGURA 27, che riporta gli switch dello scenario, si possono notare due **pallini arancioni**: uno sul trunk di Switch4 verso Switch1 e uno sul trunk di Switch2 verso Switch3.

FIGURA 27 Risultato dello Spanning Tree Protocol



La presenza dei pallini arancioni su un link sta a indicare che STP è intervenuto e ha bloccato la porta di uno switch. Risultano bloccate la porta Fa5/1 dello Switch2 e la porta Fa4/1 dello Switch4.

Con il comando:

```
Switch#show spanning-tree
```

gli switch Cisco consentono di visualizzare le porte che STP ha eletto come:

- **Root ID**: root dell'intera LAN
- **Bridge ID**: root di uno switch

e lo stato delle porte collegate.

Sono previsti 3 stati:

- **Root FWD**: porta eletta per l'inoltro verso la root;
- **Desg FWD**: porta eletta per l'inoltro su un segmento;
- **Altn BLK**: porta bloccata.

> Ogni porta di ogni switch, rispetto a una data VLAN, deve essere o forward o blocked. Lo switch eletto Root ID avrà tutte le porte forward.

La FIGURA 28 mostra il risultato del comando sullo Switch2. Si può notare come la porta **Fa5/1** risulti in stato blocked su tutte e 4 le VLAN, quella di default e le 3 che abbiamo creato.

FIGURA 28 Comando Switch#show spanning-tree sullo Switch2

#prendinota

Nello scenario proposto, è lo Switch5 a essere eletto Root ID. Di conseguenza lo Switch5 sarà l'unico ad avere **Root ID = Bridge ID**. Tutti gli altri switch avranno come Root ID la Root ID dello Switch5 e come Bridge ID una propria porta.

FISSA LE CONOSCENZE

- Cosa va inserito nel VLAN Database di ogni switch per creare le VLAN?
- Quali porte di uno switch vanno configurate Access e quali Trunk?
- Quali sono i 3 stati che possono assumere le porte di uno switch in una VLAN?
- Quante Root ID ci sono in una LAN e quanti Bridge ID?

8 PACKET TRACER: ACL STANDARD E ACL ESTESE

In questa Lezione realizzeremo con il simulatore Packet Tracer una serie di ACL, standard o estese, allo scopo di filtrare diversi tipi di traffico in 3 scenari LAN diversi.

esercizio

File sorgenti
Scarica il file

→ PROBLEMA

Facendo riferimento allo scenario in FIGURA 29, creare una ACL che blocchi il traffico tra PC0 della LAN 1 e tutti i PC della LAN 2, consentendo invece il traffico tra PC1 e PC2 della LAN 1 e tutti i PC della LAN 2.
Ai PC della LAN 3 è invece consentito inviare e ricevere pacchetti con tutti i PC delle altre 2 LAN.

→ ANALISI DEL PROBLEMA

Per realizzare quanto richiesto configureremo una ACL sulla porta FastEthernet0/1 del RouterA che collega la LAN 2, in modo che filtri tutti i pacchetti in entrata e in uscita ma blocchi solo quelli che riguardano PC0 (deny) e permetta quelli che riguardano PC1 e PC2 (permit).
Poiché il problema chiede di applicare il blocco solo in base alla **sorgente** (PC0, PC1 e PC2 della LAN 1), serve una ACL **standard**.

→ SVOLGIMENTO

Si consideri lo scenario mostrato in Figura 29.

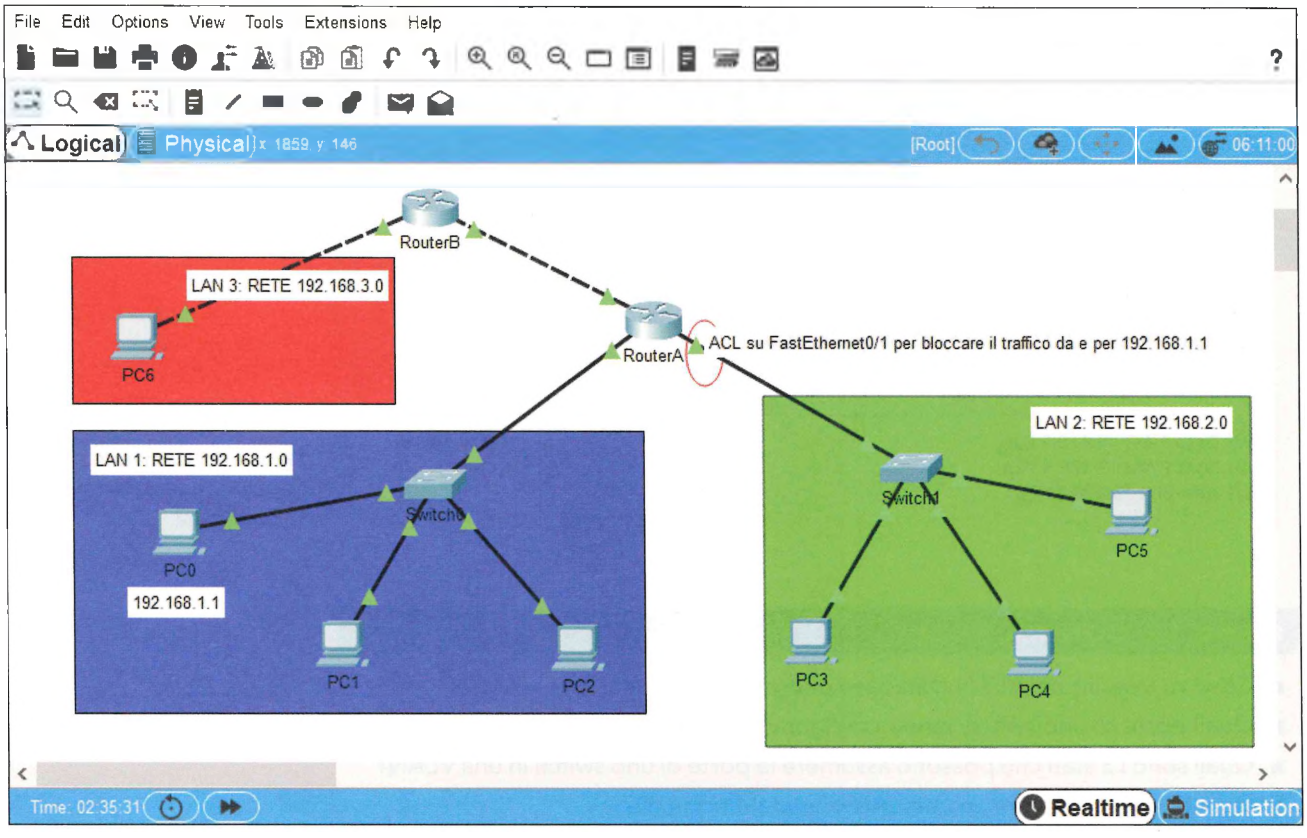


FIGURA 29 Scenario con ACL sulla porta FastEthernet0/1 del RouterA

La sintassi del comando per definire una ACL sui router Cisco è:

```
Router(config)#access-list access-list-number {permit|deny} source [source wildcard] [log]
```

Il significato dei parametri presenti nel comando è descritto nella TABELLA 2.

TABELLA 2 Parametri del comando di definizione di una ACL sui router Cisco

Parametro	Descrizione
access-list-number	Indica il nome e il tipo di ACL.
permit	Permette l'accesso se le condizioni sono soddisfatte.
deny	Nega l'accesso se le condizioni sono soddisfatte.
source	Introduce l'indirizzo sorgente del pacchetto.
source wildcard	Indica la wildcard mask che deve essere applicata all'indirizzo sorgente (opzionale).
log	Attiva i messaggi di log che comprendono l'indirizzo sorgente, il numero di pacchetti e l'esito del controllo (permit o deny). I log vengono generati a intervalli di 5 minuti (opzionale).

Le ACL standard, che specificano solo la sorgente del traffico, andranno applicate a interfacce **vicine alla destinazione**, per almeno due motivi: innanzitutto, per non bloccare in partenza anche il traffico verso destinazioni autorizzate, in secondo luogo perché, non conoscendo il percorso che fanno i pacchetti su una rete magliata, conviene proteggere la rete destinazione posizionandosi al suo ingresso.

#prendinota

Sui router della Cisco, ogni ACL è identificata da un **access-list-number**, cioè da un numero univoco che ne definisce il tipo: da 1 a 99 sono quelle standard riferite al protocollo IP, da 100 a 199 sono quelle estese, sempre riferite a IP.

Nel nostro caso conviene quindi applicare la ACL sulla porta FastEthernet0/1 che fa da porta destinazione per la LAN 2. La sintassi del comando da usare è:

```
Router(config-if)#ip access-group access-list-number {in|out}
```

Per capire quando scegliere **in** e quando **out**, occorre mettersi dal punto di vista della porta del router.
Per applicare una ACL su un host **all'interno della LAN si sceglie in**, mentre se è una ACL su un host **fuori dalla LAN si sceglie out**.
Nel nostro caso, dal punto di vista del RouterA, l'host che blocchiamo è fuori dalla LAN 2 collegata alla porta FastEthernet0/1, quindi l'ACL va definita out.

La sequenza di comandi da scrivere nella CLI del RouterA diventa quindi:

```
Router>enable
Router#configure terminal
Router(config)#access-list 1 deny 192.168.1.1 0.0.0.0     ACL 1 con regola per bloccare la destinazione PC0 mediante wildcard.
Router(config)#access-list 1 permit any                   ACL 1 con regola per consentire tutte le altre destinazioni.
Router(config)#interface fastEthernet0/1                  Apre l'interfaccia verso LAN 2.
Router(config-if)#ip access-group 1 out                   Assegna le regole dell'ACL 1 all'interfaccia in modalità out.
Router(config-if)#^Z
```

A questo punto la ACL è applicata e possiamo verificarne il funzionamento mediante dei **Simple PDU** (comando ping, protocollo ICMP) tra i vari PC.

Per utilizzare questo comando è necessario che sui due router sia stato configurato il RIP e ai computer sia stato assegnato l'opportuno indirizzo IP come da Figura 29.

Proviamo 3 ping:

- tra PC0 e PC3 (bloccato);
- tra PC1 e PC3 (non bloccato);
- tra PC0 e PC6 (non bloccato).

La FIGURA 30 mostra il risultato dei 3 ping.

FIGURA 30 Risultato dei ping per la verifica della ACL

Realtime Simulation

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Failed	PC0	PC3	ICMP		0.000	N	0	(edit)	(delete)
	Successful	PC1	PC3	ICMP		0.000	N	1	(edit)	(delete)
	Successful	PC0	PC6	ICMP		0.000	N	2	(edit)	(delete)

Lo stesso risultato lo si ottiene con i ping in direzione opposta.

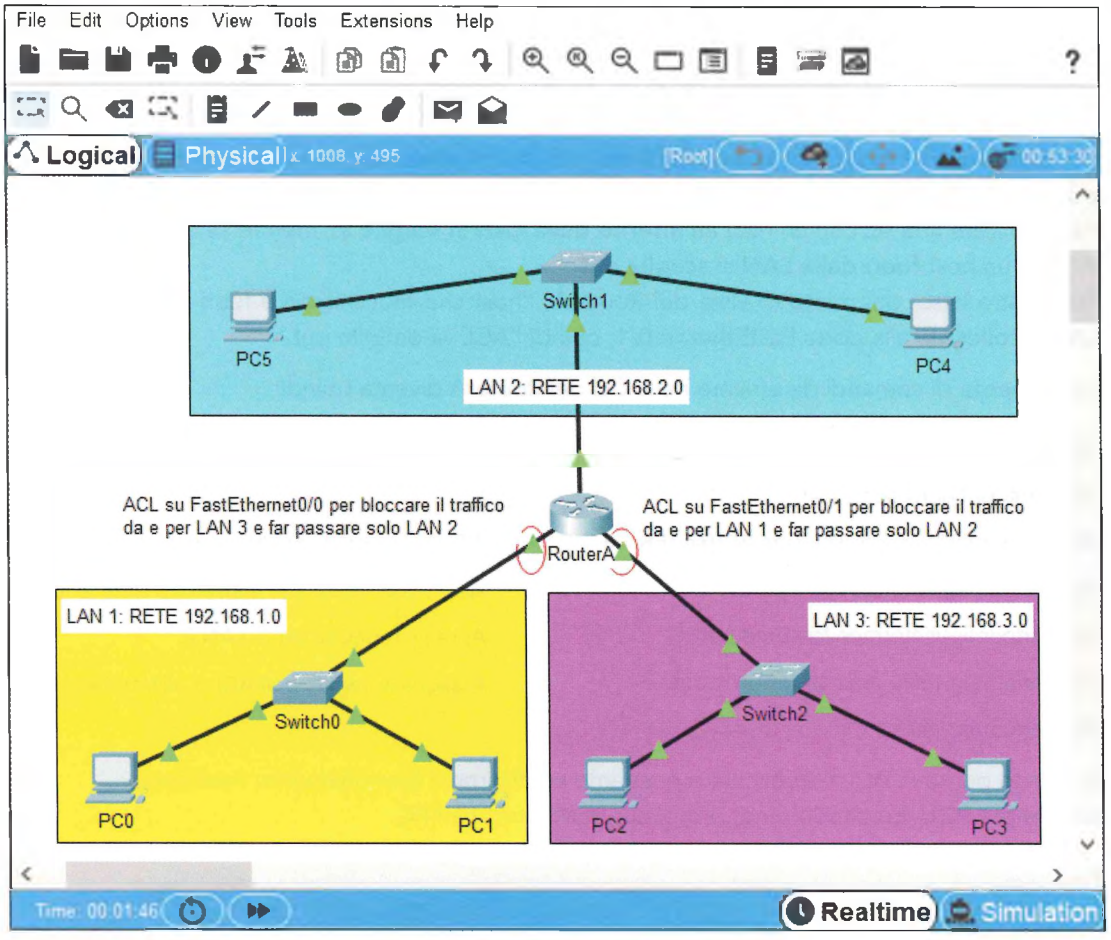
esercizio

File sorgenti
Scarica il file

→ PROBLEMA

Facendo riferimento allo scenario in FIGURA 31, creare una ACL che blocchi il traffico tra tutti i PC della LAN 1 e tutti i PC della LAN 3, consentendo invece tutto il traffico della LAN 2 con le altre LAN.

FIGURA 31
Scenario con ACL sulle porte FastEthernet0/0 e 0/1 del RouterA



→ ANALISI DEL PROBLEMA

Per realizzare quanto richiesto dovremo configurare una ACL che:

- permetta (permit) il traffico della LAN 2 con le altre LAN;
- blocchi (deny) il traffico sorgente della LAN 1 con la LAN 3;
- blocchi (deny) il traffico sorgente della LAN 3 con la LAN 1.

Poiché il problema chiede di applicare il blocco solo in base alla **sorgente** (LAN 1 o LAN 3), serve una ACL **standard**.

→ SVOLGIMENTO

Si consideri lo scenario mostrato in Figura 31.

Affinché vengano applicate le regole della ACL, il RouterA va programmato sulle 2 interfacce FastEthernet verso LAN 1 e LAN 3.
La sequenza di comandi da scrivere nella CLI del RouterA diventa quindi:

Router>enable	
Router#configure terminal	
Router(config)#access-list 1 permit 192.168.2.0 0.0.0.255	ACL 1 con regola per permettere a LAN 2 di comunicare con tutti.
Router(config)#access-list 1 deny any	ACL 1 con regola per negare l'accesso.
Router(config)#interface fastEthernet0/0	Apre l'interfaccia verso LAN 1.
Router(config-if)#ip access-group 1 out	Assegna le regole dell'ACL 1 all'interfaccia in modalità output.
Router(config-if)#exit	Termina la configurazione dell'interfaccia.
Router(config)#interface fastEthernet0/1	Apre l'interfaccia verso LAN 3.
Router(config-if)#ip access-group 1 out	Assegna le regole dell'ACL 1 all'interfaccia in modalità output.
Router(config-if)#^Z	

A questo punto la ACL è applicata e possiamo verificarne il funzionamento mediante dei **Simple PDU** (comando ping, protocollo ICMP) tra i vari PC.

> Per utilizzare questo comando è necessario che ai computer sia stato assegnato l'opportuno indirizzo IP come da Figura 31.

Proviamo 3 ping:

- tra PC0 e PC2 (bloccato);
- tra PC3 e PC1 (bloccato);
- tra PC0 e PC5 (non bloccato).

La FIGURA 32 mostra il risultato dei 3 ping.

FIGURA 32 Risultato dei ping per la verifica della ACL

Realtime | Simulation

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Failed	PC0	PC2	ICMP		0.000	N	0	(edit)	(delete)
	Failed	PC3	PC1	ICMP		0.000	N	1	(edit)	(delete)
	Successful	PC0	PC5	ICMP		0.000	N	2	(edit)	(delete)

Lo stesso risultato lo si ottiene con i ping in direzione opposta.

esercizio

File sorgenti
Scarica il file

→ PROBLEMA

Facendo riferimento allo scenario in FIGURA 33, creare una ACL che blocchi l'accesso al Web Server installato nella LAN 1 da parte dei PC della LAN 2, tranne che per PC2. La ACL dovrà bloccare inoltre tutti gli altri tipi di pacchetto.

→ ANALISI DEL PROBLEMA

Per realizzare quanto richiesto dovremo configurare una ACL che agisca sulla porta 80, quella di HTTP, al fine di bloccare l'accesso al Web Server (che funge da sorgente del traffico HTTP). Siamo quindi di fronte alla richiesta di filtrare un **protocollo**, serve una ACL **estesa**. Per il PC2 bisognerà fare in modo che passino solo i pacchetti HTTP (incapsulati in pacchetti TCP) e non altri pacchetti: il ping (ICMP) per esempio non deve passare.

→ SVOLGIMENTO

Si consideri lo scenario mostrato in Figura 33.

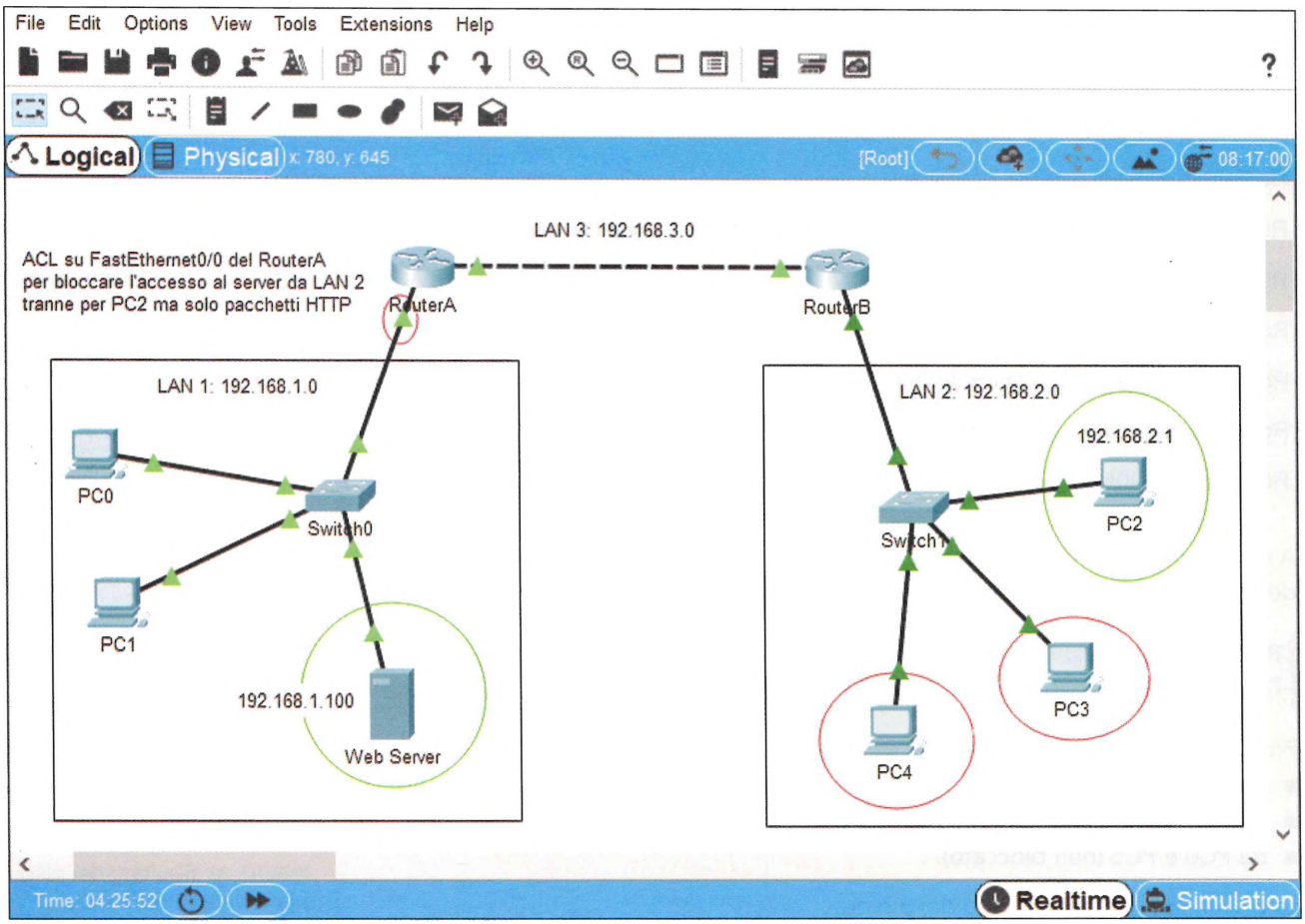


FIGURA 33 Scenario con ACL sul Web Server

PC2 della LAN 2 (cerchiato in verde) deve poter accedere al Web Server (anch'esso cerchiato in verde) mentre PC3 e PC4 (cerchiati in rosso), vanno bloccati.
Per filtrare i pacchetti relativi al Web Server occorre programmare il RouterA sulla sua porta FastEthernet0/0 che collega la LAN 1.

> Le ACL estese poiché indicano sia la sorgente sia la destinazione, si possono applicare a interfacce **vicine alla sorgente**, riducendo così anche il traffico inutile in rete.

La sequenza di comandi da scrivere nella CLI del RouterA diventa quindi:

```
Router>enable
Router#configure terminal
Router(config)#access-list 110 permit tcp host 192.168.2.1 host 192.168.1.100 eq 80
Router(config)#access-list 110 deny ip any any
Router(config)#interface fastEthernet0/0
Router(config-if)#ip access-group 110 out
Router(config-if)#^Z
```

ACL 110 con regola per permettere il traffico tra PC2 e il Web Server sulla porta 80 (HTTP).

ACL 110 con regola per bloccare tutto il resto del traffico.

Apre l'interfaccia verso LAN 1.

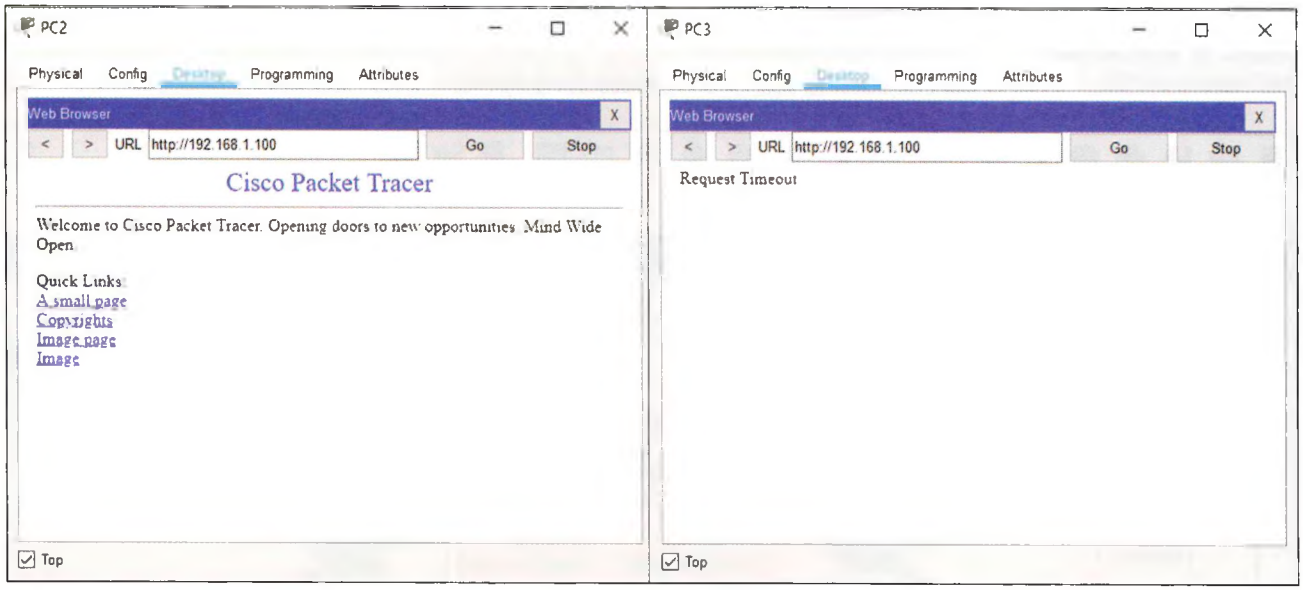
Assegna le regole dell'ACL 110 all'interfaccia in modalità output.

A questo punto la ACL è applicata e possiamo verificarne il funzionamento aprendo la scheda Desktop di PC2, selezionando **Web Browser** e inserendo nella barra dell'URL l'IP address del Web Server (192.168.1.100).
La stessa operazione può essere ripetuta su PC3 o su PC4 per verificarne il risultato opposto.

Per poter fare queste operazioni è necessario che sui due router sia stato configurato il RIP e ai computer sia stato assegnato l'opportuno indirizzo IP come da Figura 33.

La FIGURA 34 mostra il risultato ottenuto per PC2 (il Web Server ha risposto) e per PC3 (nessuna risposta).

FIGURA 34 Risultato della richiesta HTTP per la verifica della ACL



FISSA LE CONOSCENZE

- Quali ACL conviene applicare a interfacce vicine alla destinazione?
- Quali ACL conviene applicare a interfacce vicine alla sorgente?
- A che cosa serve l'access-list-number sui router Cisco?
- Che differenza c'è tra mettere *in* e mettere *out* nel comando *ip access-group*?

9 PACKET TRACER: NAT STATICO E NAT DINAMICO

In questa Lezione realizzeremo con il simulatore Packet Tracer due tipi di NAT: statico e dinamico. Il primo ha a disposizione un solo indirizzo pubblico (IP statico) e a qualunque pacchetto in uscita assegnerà tale indirizzo. Il secondo ha a disposizione un insieme (pool) di indirizzi pubblici tra cui sceglierne uno dinamicamente da assegnare ai pacchetti in uscita.

esercizio

File sorgenti
Scarica il file

➜ PROBLEMA

Impostare il **NAT statico** su un router in modo da traslare, su tutti i pacchetti di un PC in uscita da una LAN, l'indirizzo privato del PC in un indirizzo pubblico prestabilito. Verificarne poi l'effettivo funzionamento mediante l'invio di un Simple PDU.

➜ ANALISI DEL PROBLEMA

Per realizzare quanto richiesto occorre impostare il NAT sulle interfacce del router in modo tale che i pacchetti del PC preso in considerazione, nell'attraversamento del router, subiscano la traslazione dell'indirizzo IP.
La traslazione dell'indirizzo invece non deve esserci per gli altri PC della LAN e quando un PC comunica con un altro PC appartenente alla stessa LAN. Solo l'uscita dalla rete provoca il NAT sull'indirizzo IP e solo sul PC considerato.

➜ SVOLGIMENTO

Si consideri lo scenario mostrato in FIGURA 35.

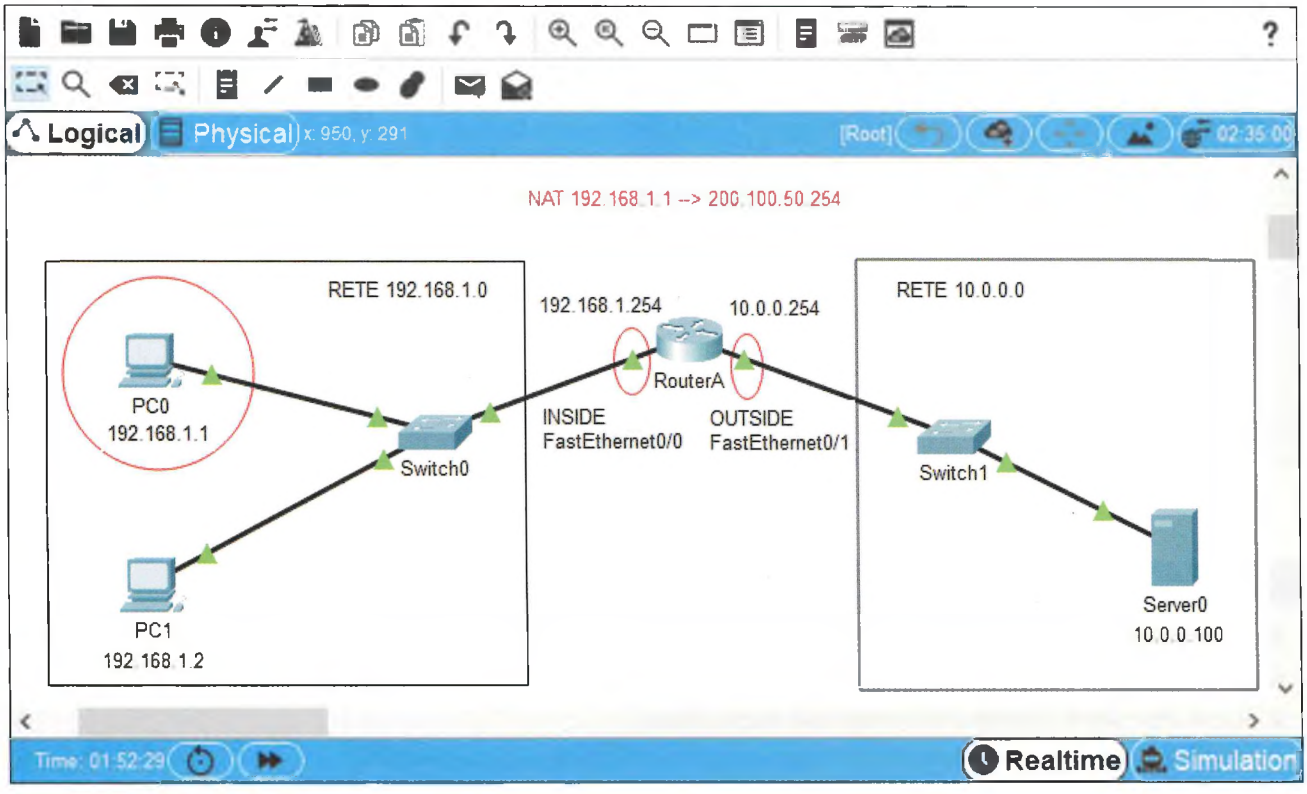


FIGURA 35 Scenario per il NAT statico di PC0

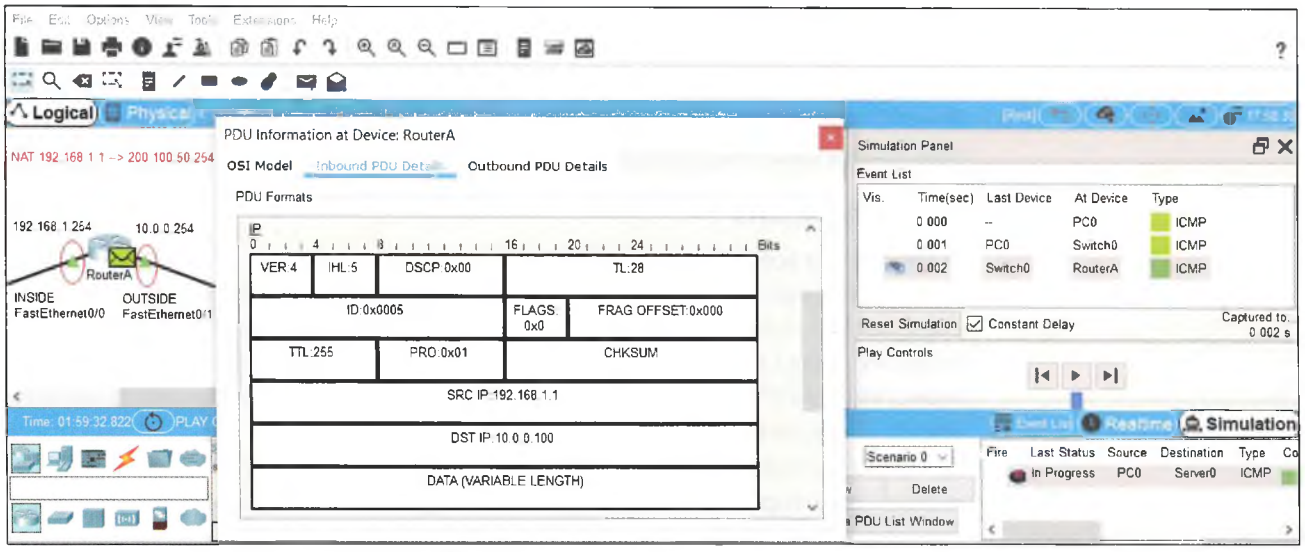
Prendiamo come indirizzo privato da traslare quello di PC0 (192.168.1.1) e stabiliamo che l'indirizzo pubblico che ne prenderà il posto sia 200.100.50.254. Nel momento in cui PC0 comunica con Server0, i pacchetti di PC0 in uscita dalla LAN devono avere l'indirizzo IP modificato dal RouterA.
Per realizzare questo sui router Cisco, occorre che l'indirizzo IP privato del PC da *nattare* sia impostato come **inside**, mentre l'indirizzo IP pubblico che lo sostituisce sia impostato come **outside**. La sequenza di comandi da scrivere nella CLI del RouterA per effettuare il NAT tra i due indirizzi diventa quindi:

```
Router>enable
Router#configure terminal
Router(config)#interface fastEthernet0/0          Apre l'interfaccia verso LAN INSIDE.
Router(config-if)#ip nat inside                   Assegna le impostazioni NAT INSIDE.
Router(config-if)#no shutdown                     Attiva l'interfaccia.
Router(config-if)#exit
Router(config)#interface fastEthernet0/1          Apre l'interfaccia verso LAN OUTSIDE.
Router(config-if)#ip nat outside                  Apre l'interfaccia verso LAN OUTSIDE.
Router(config-if)#no shutdown                     Attiva l'interfaccia.
Router(config-if)#ip nat inside source static 192.168.1.1 200.100.50.254   Imposta il NAT statico su PC0.
Router(config-if)#exit
Router(config)#do wr                              Applica la configurazione al router.
... building configuration ...
[OK]
Router(config)#exit
```

Per verificare che il NAT funzioni, inviamo un Simple PDU in modalità **Simulation** tra PC0 e Server0 e clicchiamo sul pacchetto quando è sul RouterA visualizzando le due schede di dettaglio **Inbound PDU Details** (FIGURA 36) e **Outbound PDU Details** (FIGURA 37).

Per utilizzare questo comando è necessario che ai computer e alle interfacce del router sia stato assegnato l'opportuno indirizzo IP come da Figura 35.

FIGURA 36 Inbound PDU Details



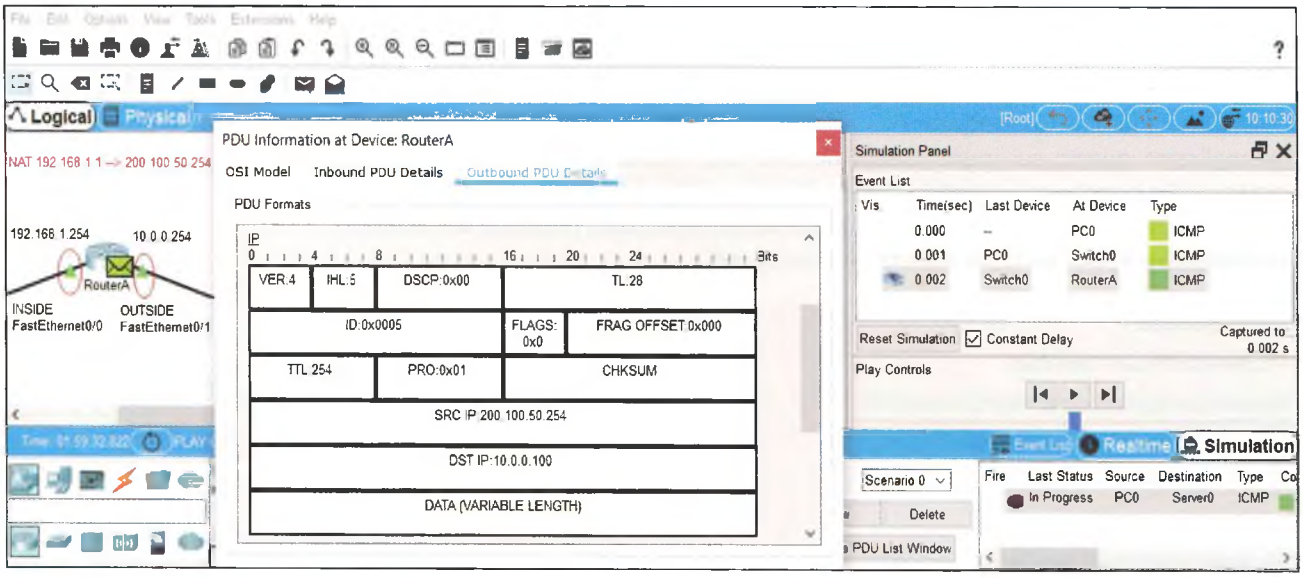


FIGURA 37 Outbound PDU Details

Confrontando i campi **SRC IP** delle due figure si può notare come il valore dell'indirizzo sorgente sia stato modificato a dimostrazione che il NAT ha funzionato. Il valore dell'indirizzo di destinazione, visibile nei campi **DST IP**, resta invece invariato.

La stessa operazione di invio di un Simple PDU da PC1 a Server0 non produrrà invece alcuna traslazione dell'indirizzo IP non essendo PC1 *nattato*.

esercizio

File sorgenti
Scarica il file

→ PROBLEMA

Impostare il **NAT dinamico** su un router in modo da traslare, su tutti i pacchetti in uscita da una LAN, gli indirizzi IP privati in indirizzi pubblici appartenenti a un pool di indirizzi prestabilito.
Verificarne poi l'effettivo funzionamento mediante l'invio di una serie di Simple PDU.

→ ANALISI DEL PROBLEMA

Per realizzare quanto richiesto occorre impostare il NAT sulle interfacce del router in modo tale che i pacchetti di ogni PC della LAN, nell'attraversamento del router, subiscano la traslazione dell'indirizzo IP.
La traslazione dell'indirizzo invece non deve esserci quando un PC comunica con un altro PC appartenente alla stessa LAN.
Solo l'uscita dalla rete provoca il NAT sull'indirizzo IP.

→ SVOLGIMENTO

Si consideri lo scenario mostrato in FIGURA 38.
Prendiamo come indirizzi privati da traslare quelli della LAN 192.168.1.0 e stabiliamo che il pool di indirizzi pubblici vada da 200.100.50.1 a 200.100.50.10. Nel momento in cui i PC della LAN comunicano con Server0, i pacchetti in uscita dalla LAN devono avere l'indirizzo IP privato modificato dal RouterA in un indirizzo IP pubblico appartenete al range prestabilito.
Per realizzare questo sui router Cisco, occorre che gli indirizzi IP privati dei PC da *nattare* siano impostati come **inside**, mentre gli indirizzi IP pubblici del pool siano impostati come **outside**.

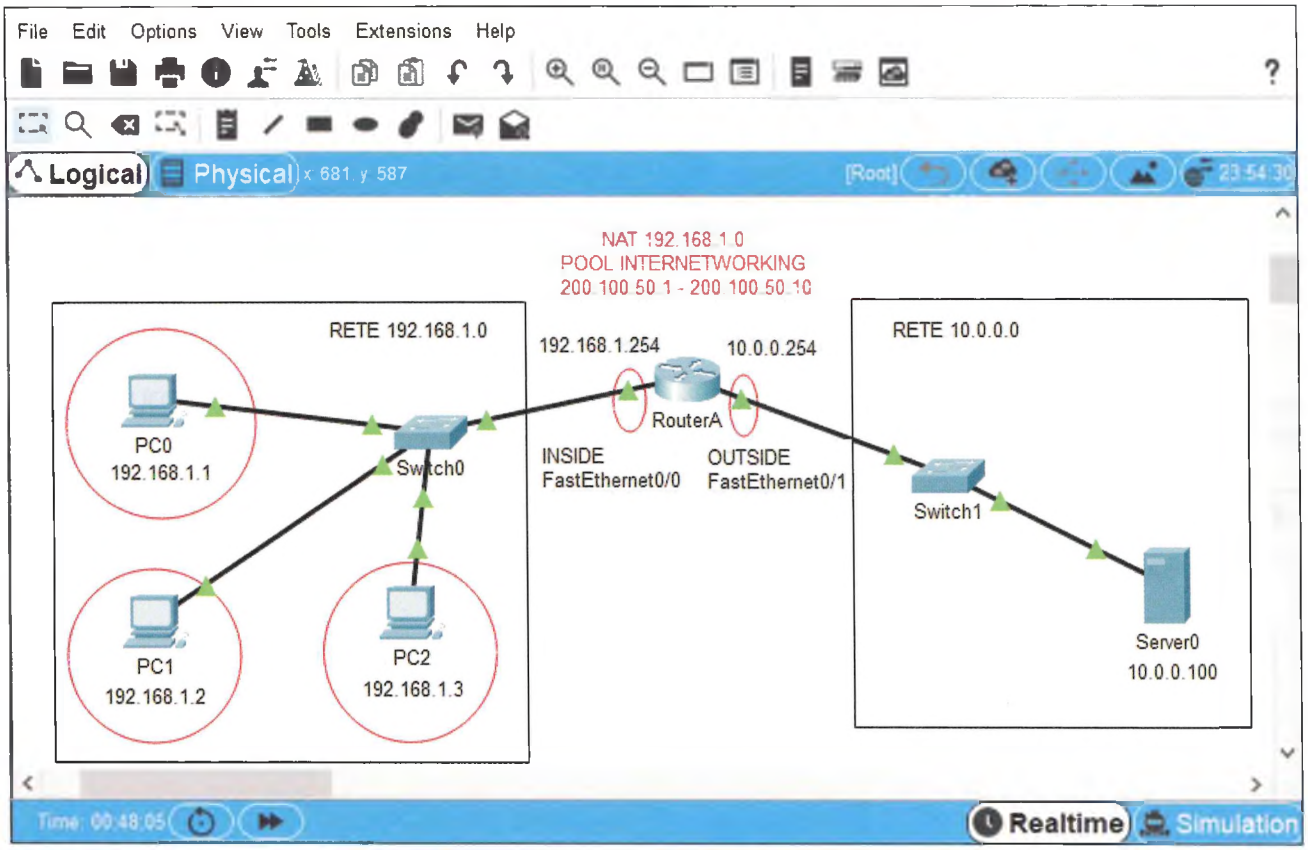


FIGURA 38 Scenario per il NAT dinamico della LAN 192.168.1.0

La sequenza di comandi da scrivere nella CLI del RouterA per effettuare il NAT tra gli indirizzi diventa quindi:

```
Router>enable
Router#configure terminal
Router(config)#ip nat pool internetworking 200.100.50.1 200.100.50.10 255.255.255.0
Router(config)#access-list 10 permit 192.168.1.0 0.0.0.255
Router(config)#ip nat inside source list 10 pool internetworking
Router(config)#interface fastEthernet0/0
Router(config-if)#ip nat inside
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#interface fastEthernet0/1
Router(config-if)#ip nat outside
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#do wr
... building ...
[OK]
Router(config)#exit
```

Crea il pool e gli assegna il nome internetworking.

ACL 10 per permettere alla LAN di comunicare con tutti.

Assegna il pool creato.

Apre l'interfaccia verso LAN INSIDE.

Assegna il NAT INSIDE.

Attiva l'interfaccia.

Apre l'interfaccia verso LAN OUTSIDE.

Assegna il NAT OUTSIDE.

Attiva l'interfaccia.

Applica la configurazione al router.

Per verificare il funzionamento del NAT, possiamo procedere come nell'esercizio precedente, inviando una serie di Simple PDU e controllando le due schede di dettaglio, Inbound PDU Details e Outbound PDU Details, sul pacchetto quando attraversa il router.

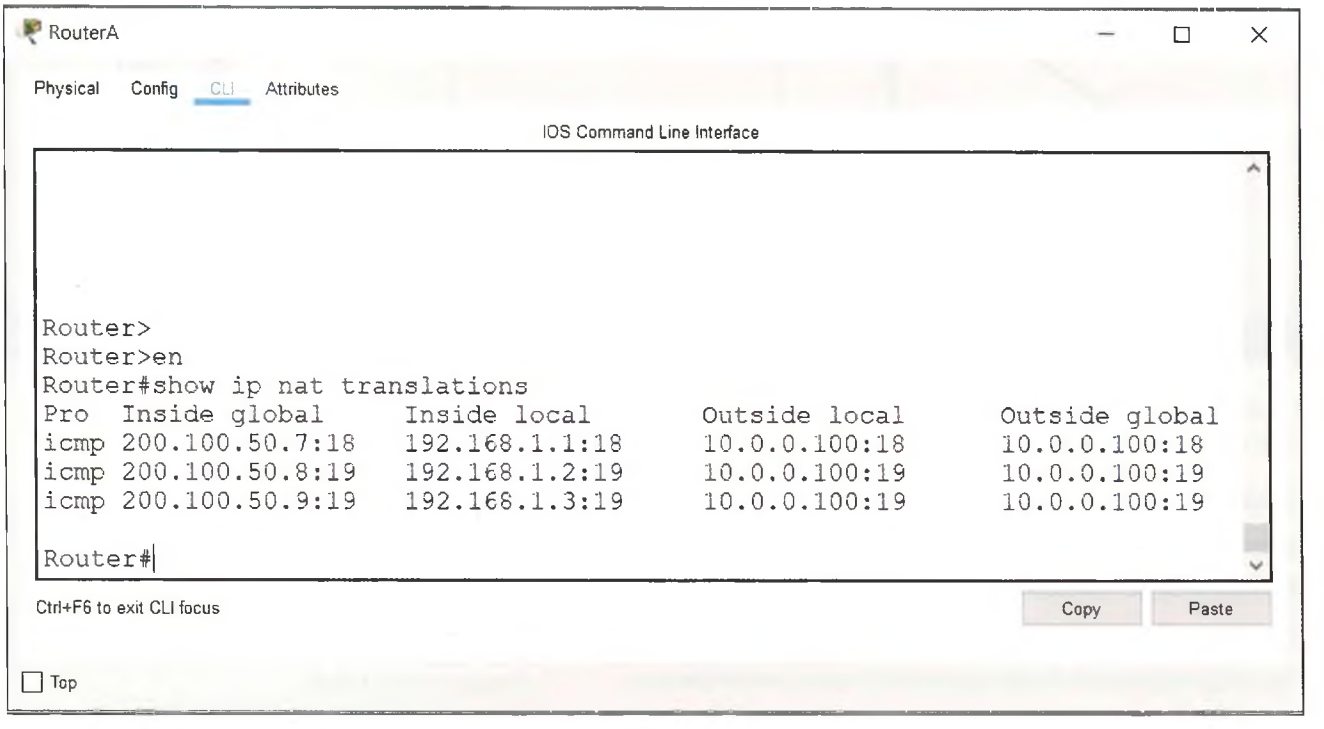
> Per utilizzare questo comando è necessario che ai computer e alle interfacce del router sia stato assegnato l'opportuno indirizzo IP come da Figura 38.

In alternativa possiamo, dalla CLI del router, usare il comando:

```
Router#show ip nat translations
```

In FIGURA 39 è mostrato l'esito del comando dopo l'invio di un Simple PDU da ciascun PC della LAN 192.168.1.0.

FIGURA 39 #Show ip nat translations sul RouterA



Si può notare che:

- l'indirizzo IP 192.168.1.1 è stato traslato in 200.100.50.7
- l'indirizzo IP 192.168.1.2 è stato traslato in 200.100.50.8
- l'indirizzo IP 192.168.1.3 è stato traslato in 200.100.50.9

FISSA LE CONOSCENZE

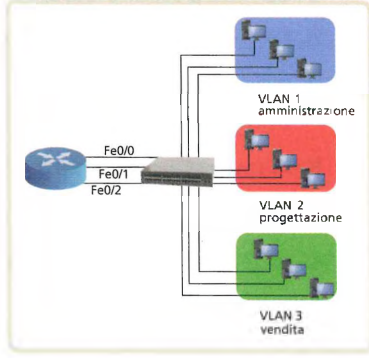
- Che differenza c'è tra NAT statico e NAT dinamico?
- Quale indirizzo IP va impostato come inside?
- Quale indirizzo IP va impostato come outside?
- Come si può verificare il funzionamento del NAT sui router Cisco?

DIDATTICA INCLUSIVA

1 STP: il protocollo di comunicazione tra gli switch

Il protocollo STP ha lo scopo di impedire la formazione di loop nelle LAN. Il calcolo della topologia di una struttura di spanning è un percorso a più passaggi, al cui termine non ci saranno più loop nella rete. IEEE ha definito il nuovo protocollo RSTP adatto alle moderne reti con switch che riduce notevolmente i tempi di convergenza.

2 Le reti locali virtuali (VLAN)



Una rete locale virtuale (VLAN) è un gruppo di dispositivi di rete che si comportano come se si trovassero tutti nello stesso dominio di broadcast. Le VLAN definiscono domini di broadcast senza essere vincolate alla posizione fisica del device.

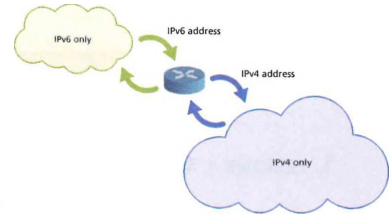
3 Il firewall e le ACL

Il firewall è posto a difesa della porta tra il computer e una rete esterna come Internet. I firewall sono classificati in base al livello dello stack TCP/IP in cui operano: Application Level Firewall, Packet Filter Firewall e Stateful Packet Inspection Firewall. La sintassi della configurazione di un firewall è basata su ACL (Access Control List) con cui si esprimono regole complesse per l'accesso al sistema.

4 Il Proxy Server

Un proxy è un programma che si interpone tra un client e un server facendo da tramite. I compiti principali sono garantire la connettività e il caching ai client collegati. Ci sono 3 topologie prevalenti: Single Proxy Topology, Multiple Proxy Vertically Topology e Multiple Proxy Horizontally Topology.

5 Le tecniche NAT e PAT



NAT (Network Address Translation) è una funzione del router che sostituisce l'indirizzo nell'intestazione di un pacchetto IP. NAT è spesso usato in reti locali per accedere a Internet usando un solo indirizzo pubblico. PAT (Port Address Translation) è un'evoluzione del NAT, in grado di traslare anche il numero della porta. Anche IPv6 implementa una forma di NAT non più per "risparmiare" indirizzi pubblici ma per mettere in comunicazione reti IPv6 con reti IPv4.

6 La DeMilitarized Zone (DMZ)

In una rete, oltre alle parti LAN e WAN, viene creata una terza zona: la DMZ (DeMilitarized Zone), in cui il traffico WAN e LAN è limitato e controllato. Una DMZ può essere realizzata a vicolo cieco o a cuscinetto.

VERIFICA DI FINE UNITÀ

Test
Svolgi il **test interattivo**

Quali delle seguenti affermazioni sono vere (V) e quali false (F)?

1. STP è il protocollo usato dagli switch per eliminare i loop nella rete. V F
2. Dispositivi che si trovano nella stessa VLAN comunicano tramite gli switch. V F
3. Dispositivi che si trovano in VLAN diverse comunicano tramite i router. V F
4. Il firewall filtra solo i pacchetti entranti in una rete. V F
5. Le ACL possono essere modificabili. V F
6. I Proxy Server garantiscono connettività e caching. V F
7. Il PAT consente al router di utilizzare un singolo indirizzo IP per gestire oltre 64.000 connessioni private contemporaneamente. V F
8. In una rete può essere presente un solo firewall. V F
9. I proxy si frappongono tra client e server. V F
10. La DMZ consente di creare una terza zona oltre la zona LAN e la zona WAN. V F

Domande a scelta multipla (una sola è la risposta esatta)

1. **In quale dei seguenti stati non può trovarsi una porta di uno switch su cui è abilitato STP?**
   - A Listening
   - B Incoming
   - C Forwarding
   - D Disabled

2. **Quali tra i seguenti non è compito del Proxy Server?**
   - A Caching
   - B Privacy
   - C Amministrazione
   - D Controllo degli errori

3. **Qual è la tecnica che consente a un gruppo di indirizzi IP privati di accedere a Internet con un solo indirizzo IP pubblico?**
   - A Firewall
   - B DMZ
   - C NAT o PAT
   - D Nessuna delle precedenti

4. **Qual è la tecnica che consente di dividere la rete in tre zone?**
   - A Firewall
   - B DMZ
   - C NAT
   - D PAT

Ascolta le **risposte**

PREPARATI PER IL COLLOQUIO ORALE

1. LEZIONE 1 **Qual è la finalità del protocollo STP?**
2. LEZIONE 1 **In quali stati si può trovare una porta di uno switch con STP?**
3. LEZIONE 2 **Da che cosa nasce l'esigenza di creare delle VLAN?**
4. LEZIONE 2 **Qual è il ruolo del router nelle reti locali con VLAN?**
5. LEZIONE 3 **Descrivi gli Application Level Firewall.**
6. LEZIONE 4 **Descrivi la Multiple Proxy Vertically Topology.**
7. LEZIONE 4 **Qual è il compito principale del Proxy Server?**
8. LEZIONE 5 **Qual è la differenza tra NAT e PAT?**
9. LEZIONE 5 **In che cosa consiste il NAT per IPv6?**
10. LEZIONE 6 **A che cosa serve la DMZ?**

IN ENGLISH, PLEASE

CLIL

Ascolta la **pronuncia del testo** e verifica la **traduzione**

ABSTRACT

Traffic filtering and LAN security

A firewall is a line of defense against network intruders. It is a special device that operates as a sentinel at the port connecting the computer to a public network, such as the Internet. A firewall allows a network administrator to control access between the outside world and internal resources by managing the traffic flow to and from these resources. Firewalls can be classified in three categories: traditional packet filters, stateful filters, and application level firewalls.
In packet filters, the firewall's rules are implemented in routers with Access Control Lists (ACL), with each router interface having its own list. ACLs are lists of instructions applied to the interfaces of a router in order to manage traffic by filtering incoming and outgoing packets. To have finer-level security, firewalls must combine packet filters with application gateways. Application gateways look beyond the IP/TCP/UDP headers and make policy decisions based on application data.
A way to hide the details of the internal network from the outside world is to use NAT-enabled routers. Frequently an enterprise network is partitioned into two regions: a high-security region, protected by a packet filter and an application gateway, and a lower-security region (referred to as the DeMilitarized Zone, DMZ) which is protected only by the packet filter. The DMZ usually includes the enterprise's servers that need to communicate with the outside world, such as its public Web Server.

EXERCISES

Use the appropriate number to match words and meanings.

...	Repository	1	Set of protocol, port and IP address.
...	Whitelist	2	If it occurs in a LAN, frames are constantly repeated
...	Socket	3	A state in which the switch does not process any frames, with the exception of STP messages
...	Caching	4	It is used to store information
...	PAT	5	It is provided by a Proxy Server
...	Loop	6	A common link among switches used to extend VLANs
...	Blocking	7	A type of network address translation
...	Trunk	8	In an ACL it is used to block accesses

GLOSSARY

ACL: Access Control List is a mechanism to implement access control for a system resource by listing the identities of the system entities that are permitted to access the resource.
DMZ: DeMilitarized Zone, or perimeter network, is a network area (a subnetwork) that sits between an organization's internal network and an external network, usually the Internet.
Firewall: special devices that operate as a sentinel at the port connecting the computer to a public network, such as the Internet.
NAT: Network Address Translation is used to share a small number of publicly routable IP addresses among a larger number of hosts. The hosts are assigned private IP addresses, which are then "translated" into one of the publicly routed IP addresses.
Proxy: a server that acts as an intermediary between a computer on the LAN and the Internet so that the enterprise can ensure security, administrative control, and caching service.
Segment: a partition of a LAN that is separated from the rest of the network by a bridge, router or switch.
STP (Spanning Tree Protocol): it provides path redundancy while preventing undesirable loops in the network.
VLAN (Virtual Local Area Network): it is a logical group within a LAN that is created through software rather than by physical cables. It combines computers and network devices into a single unit regardless of the physical LAN segment they are attached to.

LAVORARE PER COMPETENZE

COMPETENZE IN GIOCO

Competenze disciplinari

- Progettare sistemi in base ai requisiti di sicurezza di un'azienda.
- Scegliere dispositivi e strumenti in base alle loro caratteristiche funzionali.
- Descrivere e comparare il funzionamento di dispositivi e strumenti elettronici e di telecomunicazione.
- Gestire progetti secondo le procedure e gli standard previsti dai sistemi aziendali di gestione della qualità e della sicurezza.
- Utilizzare le reti e gli strumenti informatici nelle attività di studio, ricerca e approfondimento disciplinare.

Competenze chiave di cittadinanza

- Interpretare il testo.
- Risolvere problemi.
- Comunicare.
- Competenza digitale.

obiettivi formativi

- Stimolare l'approfondimento e la ricerca disciplinare.
- Consultare fonti Internet.
- Contestualizzare in un caso reale le nozioni teoriche acquisite studiando.
- Esporre i risultati della ricerca alla classe.

tempi

- Preparazione: 3 ore.
- Presentazione dei risultati e dibattito: 1 ora.
- Autovalutazione: 10 minuti.

strumenti

- Libro di testo.
- Dispositivo connesso a Internet.
- Software PowerPoint.
- Proiettore collegato al computer in classe o in laboratorio.

TEMA PROPOSTO

Un giornale locale negli anni Novanta realizzò una propria banca dati telematica per la distribuzione elettronica di un notiziario settimanale.
Il nuovo direttore del giornale desidera ora effettuare l'ammodernamento del sistema, realizzando una nuova rete locale per il collegamento dei computer e di altri dispositivi, la cui collocazione è la seguente:

- un computer e una stampante nell'ufficio del direttore;
- 30 computer distribuiti a due a due negli uffici dei giornalisti;
- 2 computer e una stampante professionale nell'ufficio dei redattori;
- altre apparecchiature mobili (smartphone, pc portatili, ecc.), che vengono usate all'occorrenza dai giornalisti o da collaboratori occasionali.

Inoltre, in un locale protetto, vi è un sistema su cui risiedono la banca dati e il web server. Il giornale ha un sito web contenente informazioni e una sintesi degli articoli pubblicati accessibili a tutti senza autenticazione; contiene inoltre una sezione riservata agli abbonati, i quali possono accedere agli articoli completi.

Dopo aver formulato eventuali ipotesi aggiuntive proporre:

1. un progetto, anche grafico, dell'infrastruttura di rete, indicando le risorse hardware e software necessarie, esaminandone in particolare l'architettura, gli apparati e le caratteristiche del collegamento della rete a Internet;
2. le possibili tecniche di protezione della rete locale e dei server interni dagli accessi esterni.

SVOLGIMENTO

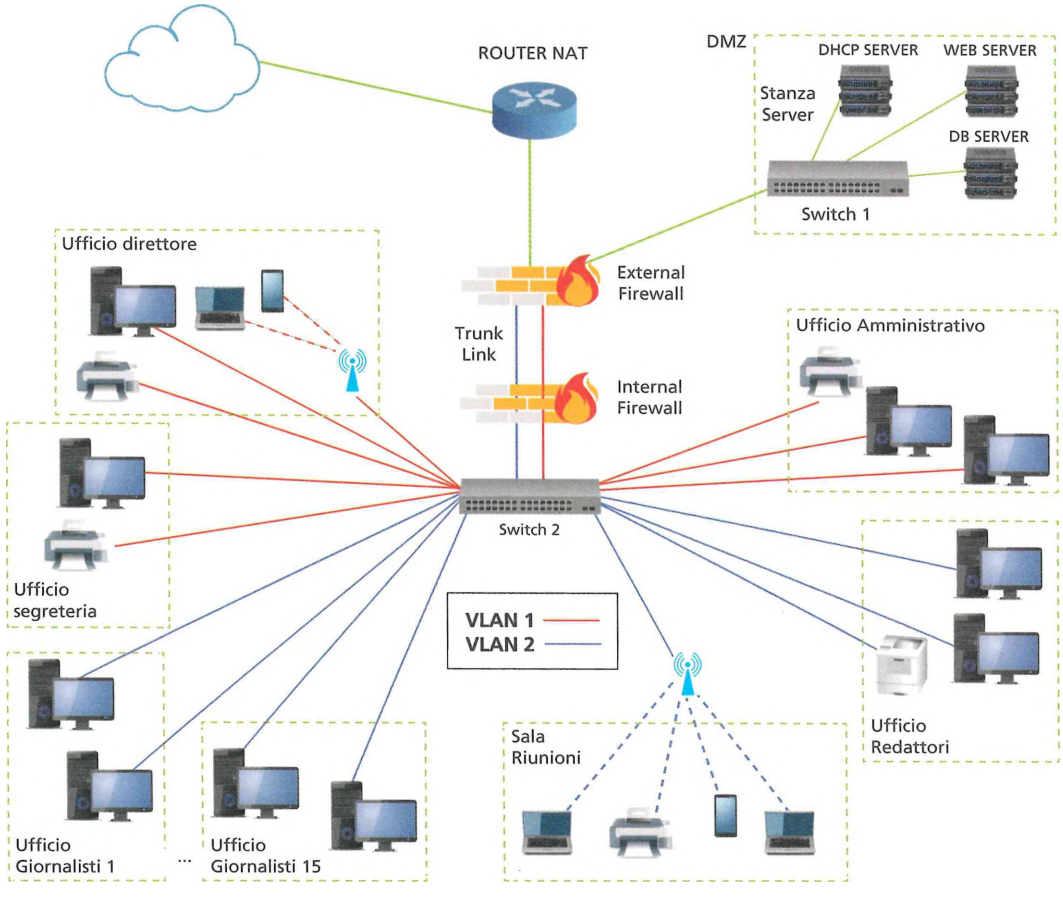
Ipotesi aggiuntive

- Poiché la rete preesistente risale agli anni Novanta del secolo scorso, supponiamo sia necessario progettarla da zero, su un unico piano di un edificio. Dal punto di vista fisico, realizziamo una WLAN (Wireless Local Area Network), con parte cablata e parte wireless, costituita da:
  - un open space per i 15 uffici dei giornalisti;
  - un ufficio per il direttore, uno di segreteria e un ufficio amministrativo;
  - una sala riunioni coperta dal Wi-Fi e dotata di lavagna interattiva;
  - una stanza server.
- Dal punto di vista logico, realizziamo 2 VLAN (Virtual Local Area Network) per separare il traffico degli uffici del direttore, della segreteria e amministrativo dal traffico di giornalisti, redattori e collaboratori.

Descrizione

- La topologia è a stella estesa con un centro stella primario (il router) e due centri stella secondari (i 2 switch).
- Il router, oltre a separare la WAN (Wide Area Network) dalla WLAN del giornale grazie alla funzionalità di firewall, segmenta fisicamente la rete locale in 2 parti: le VLAN e la DMZ.
- Lo Switch 1 connette la stanza dedicata ai server, mentre lo Switch 2, con funzionalità VLAN, permette di creare le 2 reti virtuali.
- Il trunk link consente di far passare su un'unica interfaccia del router (la più veloce) il traffico di entrambe le VLAN.
- I due Access Point garantiscono la copertura Wi-Fi della sala riunioni e dell'open space.

1. La figura seguente propone il progetto grafico della WLAN del giornale.



Elenco dei dispositivi di rete necessari con le rispettive caratteristiche:

- 1 router con funzionalità VLAN, firewall e NAT, dotato di 1 porta WAN per fibra ottica verso Internet e 2 porte GigaEthernet (1 Gbps) verso i 2 switch della WLAN interna;
- 1 switch a 8 porte GigaEthernet per la stanza server;
- 1 switch a 48 porte FastEthernet (100 Mbps) con funzionalità VLAN;
- 2 Access Point WLAN, standard Wi-Fi: 802.11ac (1.34 Gbps) con funzionalità di autenticazione, crittografia WPA-2 e DHCP;
- schede di rete 10/100/1000 Mbps su tutti i dispositivi cablati (PC Desk e stampanti);
- schede di rete Wi-Fi 802.ac su tutti i Wireless Terminal (smartphone, tablet e netbook).

2. Per proteggere la rete locale e i server interni è previsto l'utilizzo di un router NAT (eventualmente PAT), 2 firewall (uno Internal l'altro External) per la creazione di una DMZ (DeMilitarizated Zone) in modalità cuscinetto.

Di seguito si mostrano le modalità di protezione di rete locale e server interni.

- **Router NAT**: che protegge la privacy degli host della rete, sostituendo a tutti i pacchetti in uscita il proprio indirizzo IP pubblico. Siccome sono previsti numerosi accessi contemporanei alla rete pubblica, conviene predisporre un NAT dinamico con un pool di indirizzi IP a disposizione.
  Un router PAT, in grado di gestire 2^{16} connessioni contemporaneamente, risulterebbe sovradimensionato rispetto alle necessità della rete del giornale locale e non aggiungerebbe nulla in termini di sicurezza.
- **Firewall**: ne servono 2. Uno (internal) per filtrare i pacchetti in entrata contro i tentativi di intrusione e gli attacchi dall'esterno, con opportune ACL legate alla policy aziendale che impediscono a pacchetti con provenienza indesiderata di arrivare al Web Server o agli host interni della rete. Un secondo firewall (external) sarà utilizzato per proteggere la rete dagli attacchi interni e creare una DMZ, poiché il giornale prevede di offrire un servizio di consultazione degli articoli online a utenti e abbonati tramite i propri server, e un solo firewall non permette di separare e filtrare il traffico tra la LAN interna e i server e tra la WAN esterna e i server.
- **DMZ in modalità cuscinetto**: creata dai 2 firewall con funzione di DMZ. Il firewall external separa la rete pubblica dalla DMZ mentre il firewall internal separa la DMZ dalla LAN vera e propria. Tale configurazione permette la consultazione dall'esterno dei server posizionati sulla DMZ senza compromettere la sicurezza aziendale interna.

A CASA

- Effettua una ricerca in Internet sui più recenti e noti attacchi informatici (per esempio a Enti pubblici o grandi aziende); esaminando i diversi casi trovati concentrati su:
  – tipo di attacco;
  – conseguenze sul sistema;
  – misure di sicurezza: prima dell'attacco e approntate successivamente.
- Leggi l'esempio di svolgimento proposto per verificare se qualcuno dei casi trovati si adatta a quello presentato e se la trattazione proposta risulta completa nell'ottica dei risultati della tua ricerca.
- Raccogli i tuoi risultati in una presentazione in PowerPoint (massimo 5 slide) evidenziando i casi trovati, la relazione con il contesto proposto, eventuali modifiche o aggiunte da effettuare alla rete proposta nell'esempio di svolgimento.

IN CLASSE

- Condividi la presentazione dei tuoi risultati con i compagni.
- Confrontate e discutete i casi che sono stati presentati stabilendo quale rappresenta l'esempio migliore per completezza e realisticità nell'ottica della realizzazione della richiesta del tema.
- Procedi con l'autovalutazione.

AUTOVALUTAZIONE

ATTIVITÀ	LIVELLO			
	INIZIALE	BASE	INTERMEDIO	AVANZATO
Ho compreso senza difficoltà le richieste dell'attività proposta?	Ho compreso solo alcune delle richieste aiutato dal docente. ☐	Con la guida del docente e la collaborazione dei compagni ho compreso quasi tutte le richieste. ☐	Ho compreso le richieste e in parte le ho svolte autonomamente. ☐	Ho identificato le richieste e le ho svolte senza difficoltà. ☐
Ho reperito le informazioni in rete senza difficoltà?	Ho reperito solo alcune delle informazioni utili aiutato dal docente. ☐	Con la guida del docente e la collaborazione dei compagni ho reperito quasi tutte le informazioni. ☐	Ho reperito le informazioni utili autonomamente e le ho elaborate. ☐	Ho identificato le informazioni utili e le ho elaborate senza difficoltà. ☐
La ricerca in Internet mi ha permesso di definire modifiche e miglioramenti allo svolgimento proposto?	A partire dalla mia analisi, non sono stato in grado di individuare nessun punto critico nello svolgimento proposto. ☐	A partire dalla mia analisi, sono stato in grado di individuare alcuni punti critici nello svolgimento proposto con l'aiuto del docente. ☐	A partire dalla mia analisi, sono stato in grado di individuare i punti critici e alcune modifiche apportabili nello svolgimento proposto con l'aiuto del docente. ☐	A partire dalla mia analisi, sono stato in grado di individuare i punti critici e definire le modifiche apportabili in modo dettagliato e completo. ☐

UNITÀ 3

LE RETI PRIVATE VIRTUALI (VPN)

Guarda la **presentazione** dell'unità

IN QUESTA UNITÀ

Didattica Digitale Integrata Plus

conoscenze	abilità	competenze
Conoscere i tipi di reti private in commercio e i dispositivi che le implementano. Conoscere protocolli propri delle reti VPN. Conoscere le caratteristiche delle VPN in termini di sicurezza, affidabilità e prestazioni.	Saper distinguere le diverse tecnologie e le diverse componenti necessarie alla realizzazione di reti VPN. Saper scegliere l'opportuna tecnologia in base ai diversi scenari d'utilizzo. Comprendere le problematiche relative alla sicurezza in ambito geografico.	Scegliere dispositivi e strumenti in base alle loro caratteristiche funzionali.

FLIPPED CLASSROOM

A casa

- Leggi la Lezione 5 di questa Unità;
- ricerca in Internet i software più utilizzati per la realizzazione di una VPN per la tutela della privacy da parte di privati cittadini;
- confronta le funzionalità e i servizi offerti dai software e raccogli le valutazioni in una tabella comparativa.

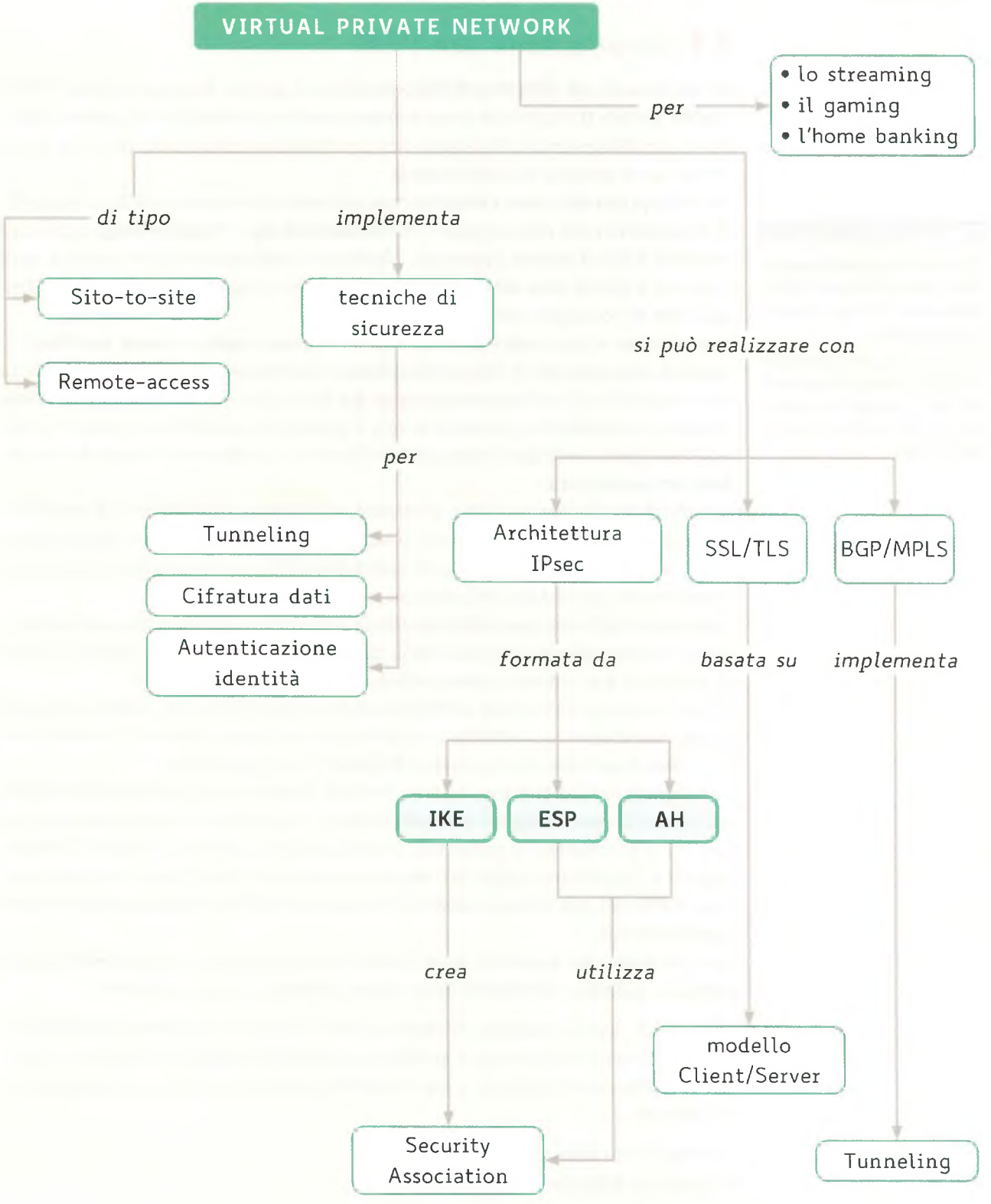
In classe

- Confrontate i risultati e le valutazioni;
- stabilite, con una discussione, quale tra le soluzioni trovate meglio risponde alle esigenze di tutela della privacy dei cittadini.

MAPPA CONCETTUALE

DIDATTICA INCLUSIVA

Mappa modificabile



1 LE CARATTERISTICHE DI UNA VIRTUAL PRIVATE NETWORK

1.1 Introduzione alle VPN

Per un'azienda con diverse sedi, dislocate anche a grande distanza tra loro, l'ideale sarebbe poterle trattare tutte come un'unica rete locale aziendale. In pratica, estendere in ambito geografico la propria rete LAN privata, realizzando, cioè, una WAN privata per il business di tutta l'azienda.

Gli sviluppi possibili sono molteplici: non solo sedi dislocate, ma anche la possibilità di includere nella rete postazioni di **#homeworking** e **#teleworking**, come pure eventuali LAN di partner consociati. Mediante la realizzazione di reti private, ogni LAN non è più un'isola nell'oceano (Internet) ma si collega con le altre in un arcipelago (WAN) con regole comuni e condivise.

In particolare si sta sempre più diffondendo il **lavoro agile** (o **smart working**). Si tratta di una modalità di lavoro subordinato caratterizzato dall'assenza di vincoli orari o spaziali e da un lavoro organizzato per fasi, cicli e obiettivi, stabiliti mediante accordo tra dipendente e datore di lavoro. È quindi una modalità che mira ad aiutare il lavoratore a conciliare i tempi di vita e lavoro e, al contempo, favorire la crescita della sua produttività.

La definizione di smart working, contenuta nella Legge n. 81/2017 art. 18, pone l'accento sulla flessibilità organizzativa, sulla volontarietà delle parti che sottoscrivono l'accordo individuale e sull'utilizzo di strumentazioni che consentano di lavorare da remoto (come per esempio: PC portatili, tablet e smartphone).

Ai lavoratori agili viene garantita la parità di trattamento – economico e normativo – rispetto ai loro colleghi che eseguono la prestazione con modalità ordinarie. È, quindi, prevista la loro tutela in caso di infortuni e malattie professionali.

Fino a poco tempo fa lo smart working era messo in atto soprattutto dalle aziende più grandi e strutturate, già attrezzate con un'opportuna infrastruttura IT e organizzate in termini di gestione del personale e dispositivi per i dipendenti.

Con l'emergenza Coronavirus lo smart working ha subito un'impennata, diventando una modalità quasi obbligata per molte aziende nei periodi di lockdown istituiti dal Governo per contenere la pandemia. Tutto questo ha costretto le aziende a dotarsi nel giro di pochissimo tempo dei mezzi necessari per il lavoro agile, è quindi molto probabile che resterà una modalità di lavoro molto diffusa anche quando avremo superato la crisi.

Come vedremo nel seguito di questa Unità però, in Italia non molte aziende hanno pensato a realizzare un'infrastruttura di rete veramente sicura e protetta.

#techwords

L'**homeworking** è la tipologia di lavoro svolta da casa (ufficio domestico), collegandosi alla rete aziendale.

Il **teleworking** è la tipologia di lavoro svolta collegandosi alla rete aziendale da qualsiasi luogo col proprio dispositivo mobile.

Tra le LAN private, esistono reti private vere e proprie e reti private virtuali. Le reti private vere e proprie sono quelle che collegano più sedi in una rete aziendale attraverso canali dedicati, a uso esclusivo, pagandone l'affitto al proprietario o al gestore.

I vantaggi sono molti:

- larghezza di banda sempre disponibile;
- nessun problema di accesso;

- nessuna congestione del traffico (almeno non a livello di rete);
- prestazioni garantite;
- sicurezza garantita.

Gli svantaggi tuttavia non mancano:

- alti costi di installazione;
- costi ricorrenti di manutenzione;
- tempi lunghi per la configurazione e la riconfigurazione;
- mancanza di scalabilità;
- rischio di blocco della rete in caso di grave guasto su un canale (non c'è ridondanza).

Si può dire che le reti private sono ottimizzate per cercare di ottenere le migliori prestazioni, ma non per garantire l'efficienza della rete e un buon rapporto tra costi e benefici. Per ottenere ciò si ricorre alle reti private virtuali (FIGURA 1).

Una **VPN** (Virtual Private Network) è una rete privata creata all'interno di un'infrastruttura di rete pubblica, per esempio Internet.

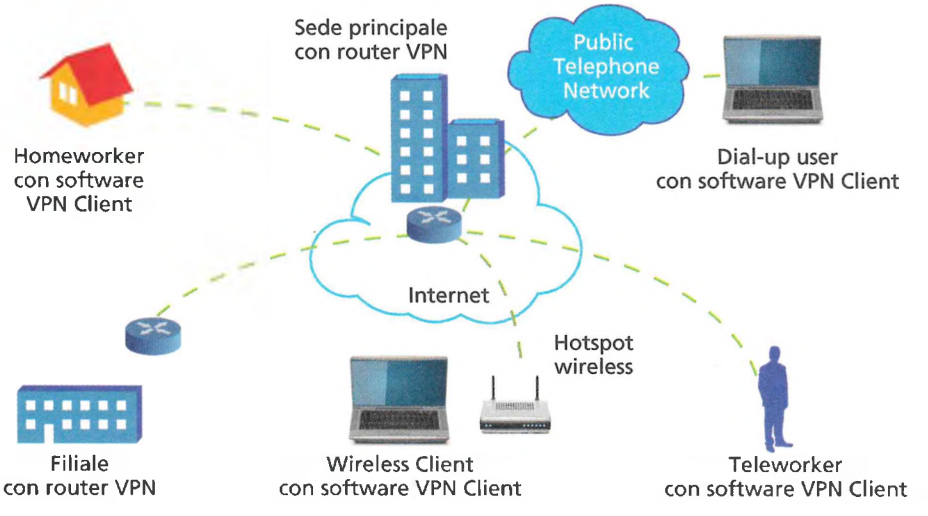


FIGURA 1 Esempio di struttura di una VPN

Rispetto a una normale rete privata, le VPN sono configurabili e riconfigurabili facilmente, sono scalabili e offrono un valido rapporto tra costi e funzionalità.
Dal momento che una VPN utilizza una rete pubblica, l'alto grado di ridondanza è garantito e dunque il rischio di blocco della rete è pressoché nullo.

La sua natura condivisa implica però il dover affrontare 3 grossi problemi:

- la variabilità del tempo di trasferimento (traffico, congestione, latenza, velocità variabili, jitter, perdita di pacchetti, ecc.);
- il controllo degli accessi (autenticazione);
- la sicurezza delle trasmissioni (cifratura e tunneling).

Il primo problema è stato ampiamente affrontato nelle Unità 8 del volume del terzo anno, quando si è parlato delle reti geografiche (WAN) e della qualità del servizio (QoS).

Il secondo e il terzo problema, nel contesto attuale delle reti VPN basate su Internet, vengono affrontati impiegando una combinazione di 3 fattori: **autenticazione**, **cifratura** e **tunneling**. Dei protocolli e delle tecniche che realizzano tali fattori parleremo nella prossima Lezione.

1.2 Tipi di VPN

#prendinota

Il termine VPN è un termine generico e non un marchio. Non esiste alcun ente che regoli la denominazione di un prodotto come VPN.

Esistono due principali tipi di VPN in commercio:

- **Remote-access VPN**: porta qualsiasi applicazione dati, voce o video al desktop remoto, emulando il desktop dell'ufficio principale;
- **Site-to-site VPN**: è l'alternativa alle WAN e consente alle aziende di ampliare le risorse di rete alle filiali, agli uffici domestici e alle sedi di partner.

REMOTE-ACCESS VPN

Una **Remote-access VPN** (FIGURA 2) consente ai singoli utenti di stabilire connessioni sicure con la LAN aziendale remota. Gli utenti possono accedere alle risorse protette della rete locale, come se fossero direttamente collegati ai server della rete. Un tipico esempio è quello di un'azienda produttrice con centinaia di punti vendita sul territorio.

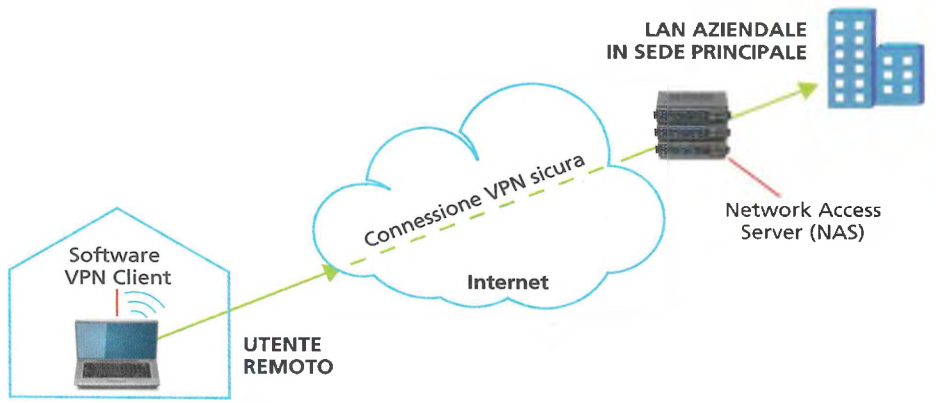


FIGURA 2 Schema di una remote-access VPN

Ci sono due componenti indispensabili per realizzare un accesso remoto VPN.
La prima è un server di accesso alla rete, ovvero un **NAS** (Network Access Server, colloquialmente Nazz).
Un NAS può essere un server dedicato oppure un'applicazione software in esecuzione su un server condiviso. Attraverso un NAS, un utente si connette a Internet e può utilizzare una VPN. Il NAS richiede all'utente di fornire credenziali valide per accedere alla VPN. Per autenticare le credenziali dell'utente, il NAS utilizza il proprio processo di autenticazione o, in alternativa, si avvale di un server di autenticazione separato in esecuzione sulla rete, come per esempio un **RADIUS AAA Server**.

#prendinota

RADIUS (Remote Authentication Dial In User Service) è un protocollo AAA molto diffuso, standardizzato da IETF, che si basa sul modello Client/Server.
IETF ha standardizzato inoltre un secondo protocollo AAA, DIAMETER, di tipo peer-to-peer.

L'acronimo AAA indica i 3 servizi che il RADIUS fornisce: per ogni connessione VPN, il Server AAA conferma chi sei (**Authentication**), identifica ciò a cui ti è permesso accedere tramite la connessione (**Authorization**) e tiene traccia di ciò che fai mentre sei loggato (**Accounting**).
L'altra componente indispensabile è un **software VPN Client**. La maggior parte dei sistemi operativi oggi sono dotati di software in grado di connettersi alle reti Remote-access VPN, anche se alcune VPN potrebbero richiedere agli utenti di installare un'applicazione specifica. Inoltre è necessario anche un **firewall**, che fornisce una barriera tra la LAN privata e Internet.

Le grandi aziende, o le aziende con personale IT esperto, in genere scelgono di acquistare, implementare e gestire in proprio la VPN ad accesso remoto. Viceversa, le imprese possono anche scegliere di esternalizzare (**outsourcing**) i propri servizi di accesso remoto VPN tramite un **provider di servizi enterprise** (ESP, **Enterprise Service Provider**). L'ESP configura un NAS per il business aziendale e ne garantisce il funzionamento.

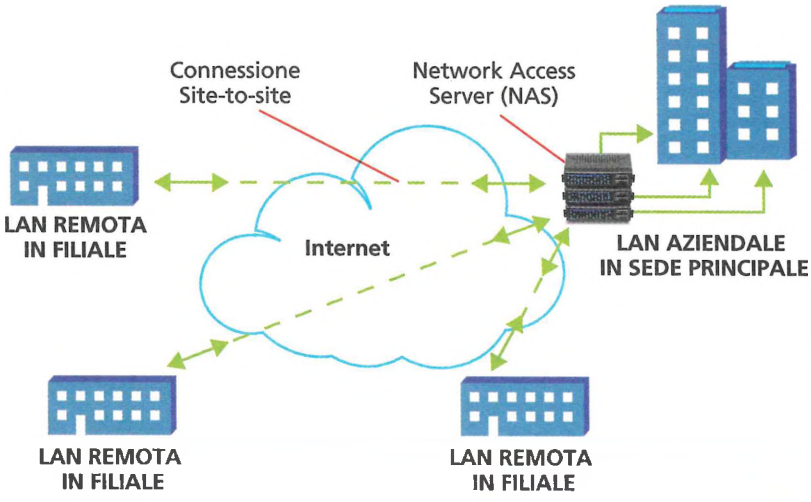
Una **Remote-access VPN** è adatta per i singoli dipendenti/utenti o per aziende con filiali costituite da piccoli uffici.

In caso di aziende con filiali grandi e con centinaia di dipendenti occorre affidarsi a un altro tipo di VPN, utilizzate per mantenere le aziende collegate LAN-to-LAN.

SITE-TO-SITE VPN

Una **Site-to-site VPN** (FIGURA 3) permette di stabilire connessioni sicure attraverso una rete pubblica, come Internet, anche ad aziende con tante sedi, ognuna con una sua LAN, creando quindi collegamenti LAN-to-LAN. La Site-to-site VPN realizza, meglio di ogni altra rete, il concetto di WAN come insieme di LAN. Questa estende la rete aziendale, rendendo disponibili le risorse della sede principale alle altre sedi.

FIGURA 3 Schema di una Site-to-site VPN



Ci sono due tipi di Site-to-site VPN:

- **#Intranet-based**: se una società desidera unire le reti delle sedi remote in un'unica rete privata, può creare una **VPN intranet** per collegare ogni LAN separata in una singola rete WAN;
- **#Extranet-based**: se una società ha un rapporto stretto con un'altra società (per esempio un partner fornitore o un'azienda cliente), può costruire una **VPN extranet** che collega le LAN di queste imprese. La VPN extranet permette alle aziende di lavorare insieme in un ambiente sicuro, condividendo le risorse e senza l'accesso preventivo alla propria intranet.

Anche se lo scopo di una Site-to-site VPN è diverso da quello di una Remote-access VPN, i due tipi di VPN potrebbero utilizzare parte dello stesso software e gli stessi dispositivi. Idealmente, però, una Site-to-site VPN dovrebbe eliminare la necessità di eseguire il software VPN Client come se l'host fosse su una Remote-access VPN.

#techwords

La rete **intranet** è una rete interna aziendale (LAN), che impiega le tecnologie e i protocolli di Internet).

La rete **extranet** impiega le tecnologie e i protocolli di Internet per collegare un'azienda ai propri fornitori o clienti o ad aziende consociate.

FISSA LE CONOSCENZE

- Che cosa sono l'homeworking e il teleworking?
- Quali sono i vantaggi e gli svantaggi delle reti private vere e proprie?
- Quali sono i due tipi di VPN in commercio e che cosa le distingue?
- Qual è il compito del NAS (Network Access Server)?

2 LA SICUREZZA NELLE VPN

I FATTORI DI SICUREZZA

Il fatto che le reti VPN abbiano ambito geografico (WAN) e utilizzino la rete pubblica (Internet) obbliga ad affrontare seri problemi legati alla sicurezza dei dati e alla riservatezza delle trasmissioni.
Come già accennato nella precedente Lezione i fattori su cui occorre concentrare l'attenzione sono 3: autenticazione, cifratura e tunneling.

AUTENTICAZIONE DELL'IDENTITÀ

Le reti VPN sono reti private, dunque chiuse al pubblico. Per potervi accedere occorre prima essere autenticati.

#prendinota

Attenzione: autenticità dei dati è diverso da autenticazione dell'identità.

Si definisce **autenticazione dell'identità** il processo con cui un sistema informatico, un applicativo o un utente verifica la corretta identità di un altro sistema informatico, applicativo o utente che vuole comunicare attraverso una connessione, per poi concedergli l'autorizzazione a usufruire dei relativi servizi associati.

Come detto nella Lezione precedente, la porta di accesso di un client alla sua VPN risulta essere un server NAS dotato di processo di autenticazione o un server dedicato all'autenticazione come il server AAA.
Al fine di connettersi alla VPN desiderata occorre dunque prima autenticarsi. Questa procedura è nota come **MultiFactor Authentication** (MFA). Per esempio, dopo aver effettuato il login con username e password, viene chiesto di immettere un codice generato tramite una chiave elettronica (**key fob**) che cambia ogni volta. Questa modalità attualmente è superata dall'uso di applicazioni per smartphone che alla generazione di sequenze di caratteri da usare una volta sola (**one-time password**) associano altri fattori quali: l'impronta di un dito (**fingerprint**) oppure la lettura di un **QR code** che compare nella pagina web di autenticazione.
Solo dopo aver superato la fase di autenticazione si viene autorizzati ad accedere ai servizi della rete. Affinchè la VPN funzioni come la LAN aziendale, l'amministratore dovrà definire, per ciascun utente, le opportune autorizzazioni per l'accesso ai servizi della rete (policy di servizio). Per esempio, la condivisione di risorse (dischi, stampanti, ecc.) può essere autorizzata solo per il personale dell'azienda, mentre ai client VPN esterni si consente di accedere a servizi di navigazione Internet o posta elettronica.

IN ENGLISH PLEASE

MultiFactor Authentication (MFA) is a security technology that takes something that end users possess, such as a security token (e.g., a key fob, fingerprint, software on a smartphone), and pairs it with a standard username/password login to prove users are who they claim to be.

La maggior parte dei protocolli per la sicurezza nelle VPN garantisce anche l'**integrità** e l'**autenticità** dei dati, cioè che i pacchetti ricevuti non siano stati modificati durante la trasmissione e che provengano da fonte certa, mediante i meccanismi di firma digitale e certificato digitale.
Per controllare che non siano state effettuate azioni indesiderate e non autorizzate, occorre prevedere meccanismi di accounting.

Con **accounting** si intendono tutte le azioni volte a misurare e documentare le risorse concesse a un utente durante un accesso.

Ciò può includere la durata della sessione di lavoro, oppure il quantitativo di traffico dati (inviati e ricevuti) in una sessione di lavoro.
Le informazioni ottenute dalla trascrizione delle attività (per esempio attraverso **file di log**) possono essere usate per applicare una tariffazione, per un controllo delle autorizzazioni, per una pianificazione della capacità della rete o per fini statistici (analisi dei trend). Dall'analisi delle richieste bloccate, un analizzatore della sicurezza può scoprire tentativi d'intrusione. In pratica, dall'analisi dell'accounting in un server AAA si possono trarre molte informazioni utili.
In termini di sicurezza spesso risulta fondamentale il rapporto fiduciario tra l'azienda che vuole creare una VPN e il fornitore di servizi Internet che gestisce l'infrastruttura pubblica. Il fornitore deve garantire la confidenzialità, cioè la protezione delle informazioni scambiate tra mittente e destinatario nei confronti di terze parti. Tale protezione deve essere realizzata a prescindere dalla sicurezza del sistema di comunicazione utilizzato.
Assume anzi particolare interesse il problema di assicurare la confidenzialità quando il sistema di comunicazione utilizzato è intrinsecamente insicuro (come per esempio la rete Internet).

CIFRATURA (O CRITTOGRAFIA)

Le VPN utilizzano un'ampia gamma di algoritmi di **crittografia** (3DES, CAST, IDEA, ecc.) per cifrare il traffico in rete. Sia l'algoritmo sia le chiavi segrete che l'algoritmo stesso utilizza sono concordate e scambiate tra mittente e destinatario attraverso protocolli di sicurezza.
Nello specifico caso delle reti VPN, viene soprattutto utilizzato il protocollo **Internet Key Exchange** (IKE), il cui compito principale è proprio implementare lo scambio delle chiavi per cifrare i pacchetti.
IKE automatizza la gestione delle chiavi. Il servizio IKE sostituisce l'assegnazione e l'aggiornamento manuale delle chiavi nelle reti IPv4. Permette inoltre all'amministratore di gestire un maggior numero di reti sicure.
Di IKE parleremo diffusamente affrontando il protocollo IPsec (IP security) nella prossima Lezione.

TUNNELING

> Lo scopo dei protocolli di tunneling è aggiungere un livello di sicurezza al fine di proteggere ogni pacchetto nel suo viaggio su Internet. Le VPN possono essere protette in **modalità trasporto** o in **modalità tunnel** (**#tunneling**).

Nel caso di modalità trasporto hanno un ruolo fondamentale i **software** impiegati. Immaginiamo un lavoratore mobile (teleworker) che deve collegarsi alla sede centrale attraverso l'unico carrier disponibile in qualsiasi punto del mondo, ovvero Internet. Il suo dispositivo (notebook, tablet, ecc.) dovrà dotarsi di software per VPN. Il collegamento potrà essere effettuato con qualsiasi ISP in quanto cifratura e decifratura dei dati verranno garantite dal software installato sul dispositivo e dagli apparati riceventi presso la sede centrale. Internet lascerà in chiaro solamente le informazioni di instradamento IP (header e trailers dei pacchetti).

Nel caso di modalità tunneling hanno un ruolo fondamentale gli **apparati** e, in particolar modo, router e firewall. È la tecnologia tipica di un collegamento tra una

#techwords

Il termine **tunneling** si riferisce a un insieme di tecniche per cui un protocollo viene incapsulato in un protocollo dello stesso livello o di livello superiore.

#prendinota

Il tunneling ha notevoli vantaggi in tema di sicurezza, tanto che alcuni lo considerano come elemento essenziale di una VPN e lo includono nella sua definizione.

filiale e la sede centrale (Site-to-site VPN). Gli apparati sono preposti a trasformare e codificare tutto il traffico tra gli end-point. Per gli utenti finali non vi è alcuna percezione della protezione applicata.

In questa modalità un intero pacchetto viene posto all'interno di un altro pacchetto prima di essere trasportato su Internet. Il pacchetto esterno protegge il contenuto dalla vista del pubblico e assicura che il pacchetto passeggero si muova all'interno di un tunnel virtuale.

Tale stratificazione di pacchetti viene chiamata **incapsulamento**. Gli host o i dispositivi di rete su entrambe le estremità del tunnel (**tunnel interface**), possono incapsulare i pacchetti in uscita e riaprire i pacchetti in entrata. Gli utenti (a una estremità del tunnel) e il personale IT (a una o entrambe le estremità del tunnel) dovranno configurare le interfacce di cui sono responsabili per utilizzare il protocollo di tunneling, chiamato anche protocollo di incapsulamento.

La FIGURA 4 mostra un esempio di tunneling dove IPv6 è il **passenger protocol**, IPsec (di cui parleremo nella prossima Lezione) è il **tunneling protocol** e IPv4 è il **carrier protocol**.

I due router sono in grado di comunicare sia con IPv6 sia con IPv4 (**dual-stack**); l'interfaccia verso la rete IPv4 è la **tunnel interface**. Da sottolineare che solitamente i dati che transitano nel tunnel vengono cifrati, garantendo così un trasferimento sicuro.

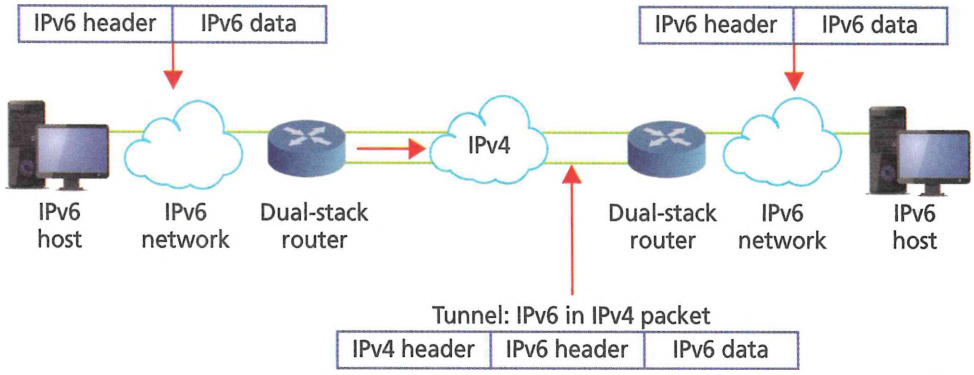


FIGURA 4 Esempio di tunneling: pacchetto IPv6 incapsulato in IPv4

Il pacchetto è in viaggio con lo stesso protocollo di trasporto (**carrier protocol**) che avrebbe utilizzato senza il tunnel VPN.

Per capire meglio le relazioni tra protocolli incapsulati facciamo un esempio (FIGURA 5). Supponiamo che un cliente abbia ordinato un televisore da un rivenditore e che gli verrà consegnato tramite corriere.

Il rivenditore predispone il televisore (passenger protocol) in una scatola d'imballaggio (tunneling protocol).

Gli addetti al magazzino del venditore quindi caricano l'imballo sul camion del corriere (carrier protocol).

Il corriere viaggia sulle autostrade (Internet) fino a casa del cliente e consegna l'imballo.

Il cliente apre l'imballo (tunneling protocol) e prende il televisore (passenger protocol).

Senza il tunnel, il televisore sarebbe stato ugualmente inviato col corriere, ma senza scatola d'imballaggio!

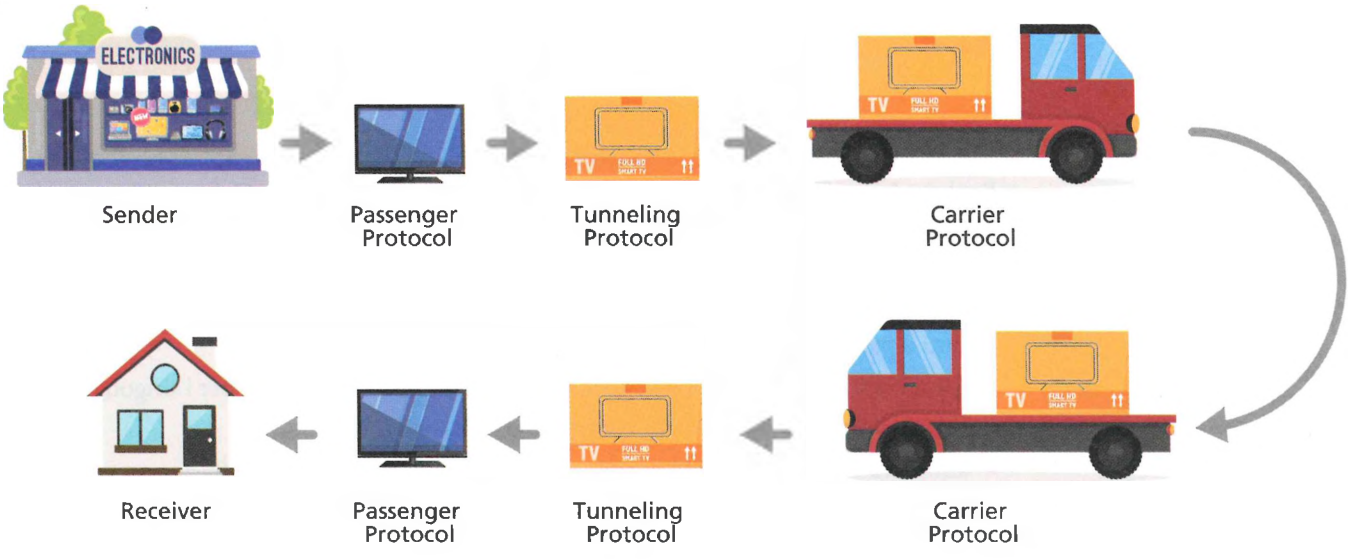


FIGURA 5 Protocolli incapsulati

I protocolli usati per il tunneling sono diversi:

- IPsec (IP security);
- SSL/TLS (Secure Sockets Layer/Transport Layer Security);
- BGP/MPLS (Border Gateway Protocol/Multiprotocol Label Switching);
- PPTP (Point-to-Point Tunneling Protocol);
- IEEE 802.1Q (Ethernet VLANs);
- SSH (Secure SHell);
- GRE (Generic Routing Encapsulation);
- L2TP (Layer 2 Tunneling Protocol).

Analizzeremo i principali tra questi protocolli nella prossima Lezione.

FISSA LE CONOSCENZE

- Quali sono i 3 i fattori necessari per garantire la sicurezza?
- Definisci l'autenticazione dell'identità.
- Che cosa si intende con accounting?
- Qual è il protocollo di cifratura più utilizzato delle VPN e quale compito svolge?
- Spiega in che cosa consiste il tunneling.
- Che cos'è il passenger protocol?

3 I PROTOCOLLI PER LA SICUREZZA NELLE VPN: SCENARI POSSIBILI

I principali protocolli per la sicurezza sono IPsec (IP security), SSL/TLS (Secure Sockets Layer/Transport Layer Security) e BGP/MPLS (Border Gateway Protocol/Multiprotocol Label Switching).

Una VPN IPsec-based, una VPN SSL/TLS-based e una VPN BGP/MPLS-based sono le soluzioni VPN scelte dalla maggior parte delle aziende per collegare uffici, utenti remoti e partner di business, in quanto:

- forniscono comunicazioni sicure con diritti di accesso su misura per i singoli utenti, che si tratti di dipendenti, consulenti o partner;
- aumentano la produttività ampliando rete e applicazioni aziendali;
- riducono i costi delle comunicazioni e accrescono la flessibilità.

#prendinota

Sono molti i documenti RFC relativi a IPsec; i due di riferimento sono: RFC 4301, che descrive l'architettura IP security, e RFC 6071, che fornisce una visione generale della IPsec protocol suite.

IPSEC VPN

IP security rappresenta la scelta adottata più frequentemente dalle aziende in quanto consente la realizzazione di diversi tipi di VPN, come mostrato in FIGURA 6. Il primo scenario rappresenta una VPN Site-to-site con topologia a maglia completa, mentre il secondo una VPN Remote-access con topologia a stella. Le righe verdi tratteggiate indicano i collegamenti VPN realizzati con IPsec.

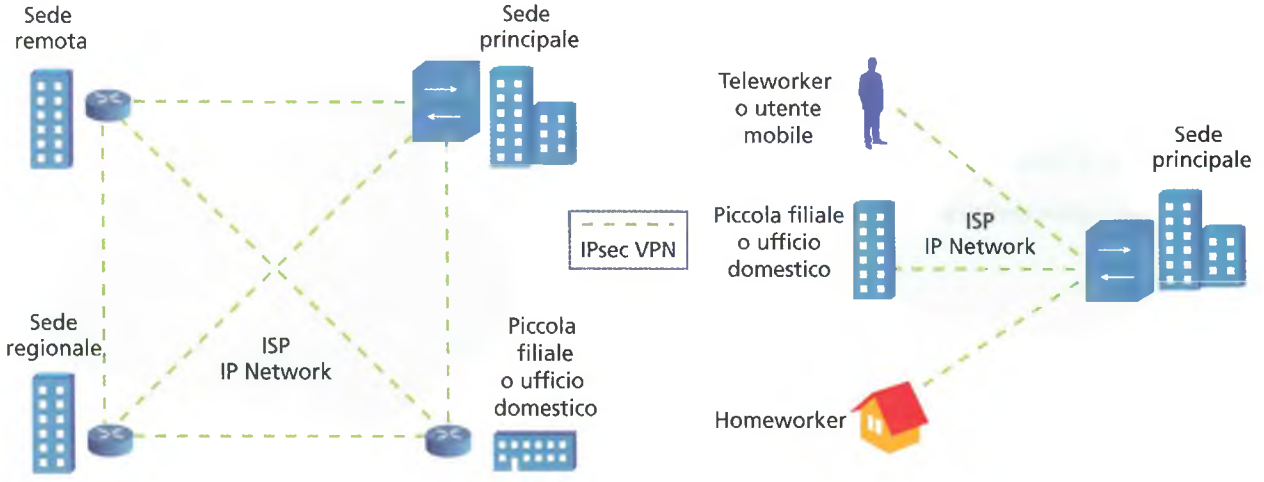


FIGURA 6 Due possibili scenari VPN IPsec-based

IPsec non è un singolo protocollo ma piuttosto un'architettura di sicurezza a livello Network, composta da vari protocolli e da altri elementi. I protocolli principali che costituiscono IPsec sono 3:

1. **Authentication Header (AH)**: garantisce l'autenticazione e l'integrità del messaggio ma non offre la confidenzialità; AHv3 è definito nell'RFC 4302.
2. **Encapsulating Security Payload (ESP)**: fornisce autenticazione, confidenzialità e integrità del messaggio; ESPv3 è definito nell'RFC 4303.
3. **Internet Key Exchange (IKE)**: implementa lo scambio delle chiavi per realizzare il flusso crittografato; IKEv2 è definito nell'RFC 7296.

#prendinota

IKEv2: si tratta di un protocollo sicuro e allo stesso tempo veloce e flessibile. Creato da Cisco e Microsoft, viene utilizzato su Windows dalla versione 7 alle successive. Ha il vantaggio di adattarsi bene ai dispositivi mobili.

Quando un host o un router invia un datagram con IPsec, lo fa usando o il protocollo AH o ESP. Dal momento che la confidenzialità è un fattore critico delle VPN, ESP è molto più diffuso di AH. Gli header AH e ESP in IPv4 hanno la forma dei tipici header di protocollo, mentre in IPv6 sono due extension header. IKE, in ambito sia IPv4 sia IPv6, è invece un protocollo di livello Application.

Sia AH sia ESP possono essere utilizzati in **modalità trasporto** oppure in **modalità tunnel**: nel primo caso (non utilizzabile tra #security gateway) si aggiungono gli header dei protocolli utilizzati (AH e/o ESP) tra l'header IP e l'header del protocollo di trasporto (TCP o UDP), mentre, nel secondo caso, il pacchetto IP originario viene interamente incapsulato, si effettua cioè il **tunneling**.

Nel momento in cui due host devono inviarsi dei dati tramite la VPN, usando il protocollo AH o ESP, è necessario instaurare prima una connessione logica tra loro, per condividere i meccanismi di sicurezza da utilizzare (l'algoritmo di crittografia, le chiavi, la modalità di verifica dell'integrità dei dati trasmessi, ecc.). Questa connessione logica, creata a livello Network, è detta **Security Association** (SA) e per stabilirla viene usato il protocollo IKE.

IKE usa UDP, però implementa un servizio affidabile (*reliable*); infatti, quando invia una richiesta per attivare una SA, la ritrasmette se non riceve risposta.

In generale, le chiavi associate alle SA devono essere usate per un tempo limitato e per proteggere una limitata quantità di dati. Nel caso servisse trasferire altri dati, si instaura una nuova SA.

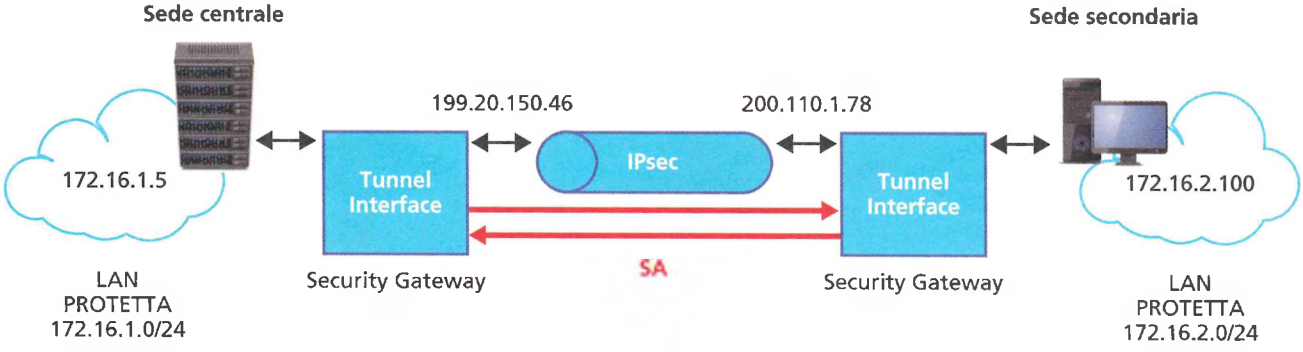
La FIGURA 7 mostra uno scenario di VPN Site-to-site al quale applicare IPsec.

Un PC della sede secondaria si deve collegare, tramite la VPN, a un server della sede centrale; su entrambi gli host non è implementato IPsec, così essi si affidano al tunnel gestito dai rispettivi **security gateway**.

#techwords

La presenza di un gateway a gestire le SA permette di lavorare in modalità tunnel. Tale gateway prende il nome di **security gateway**.

FIGURA 7 VPN Site-to-site con tunneling IPsec



In questo modo i due computer continuano a essere identificati con il loro indirizzo IP privato (172.16.1.5 e 172.16.2.100) e il routing nella rete pubblica avviene usando gli indirizzi IP contenuti nel nuovo header aggiunto al pacchetto originale (199.20.150.46 e 200.110.1.78, cioè le interfacce poste agli estremi del tunnel).

Le SA sono **unidirezionali**, per cui sono necessarie due SA per permettere a due host di comunicare tra loro. Tutte le Security Association attive su un host (o su un security gateway) sono contenute in un database detto **SAD** (Security Association Database), mentre esiste un altro database detto **SPD** (Security Policy Database) che contiene le politiche di sicurezza: è tramite queste che il sistema decide se un pacchetto IP debba essere scartato, lasciato passare in chiaro oppure elaborato tramite

IPsec, basandosi su parametri come l'indirizzo IP sorgente o destinazione, la porta sorgente o destinazione, il protocollo di trasporto.
Nell'analizzare l'elaborazione dei pacchetti IPsec, si distingue il traffico in uscita (*outbound*, ovvero diretto verso un'interfaccia di rete) dal traffico in entrata (*inbound*, ovvero proveniente da un'interfaccia di rete). Si noti che un security gateway può elaborare lo stesso pacchetto due volte: prima in entrata, proveniente da un'interfaccia, e poi in uscita, diretto verso un'altra interfaccia.
Per il **traffico in uscita**, bisogna innanzitutto cercare nel SPD un selettore applicabile al pacchetto. Se questo richiede un'elaborazione IPsec, bisogna associare il pacchetto a una SA esistente (cercandola nel SAD) oppure utilizzare IKE per crearne una nuova. Poi si esegue l'elaborazione necessaria (autenticazione, cifratura, incapsulamento del pacchetto in uno nuovo, che deve essere costruito, se è richiesta la modalità tunnel) e infine si passa il pacchetto al livello inferiore (FIGURA 8a).
Per il **traffico in ingresso**, bisogna innanzitutto ricomporre il datagramma IP nel caso sia stato frammentato, dopo di che si identificano i pacchetti che devono essere elaborati con IPsec tramite la presenza dei valori identificativi di ESP oppure di AH nel campo protocol dell'header IP (valore 50 per ESP, 51 per AH). Per i pacchetti IPsec, si identifica la SA relativa grazie al valore **SPI (Security Parameters Index)** presente nell'header AH o ESP, si applica l'elaborazione IPsec richiesta e si controlla l'SPD per accertarsi che le operazioni effettuate corrispondano alle politiche specificate. Infine, il pacchetto viene inoltrato verso la destinazione successiva oppure passato al livello superiore (FIGURA 8b).

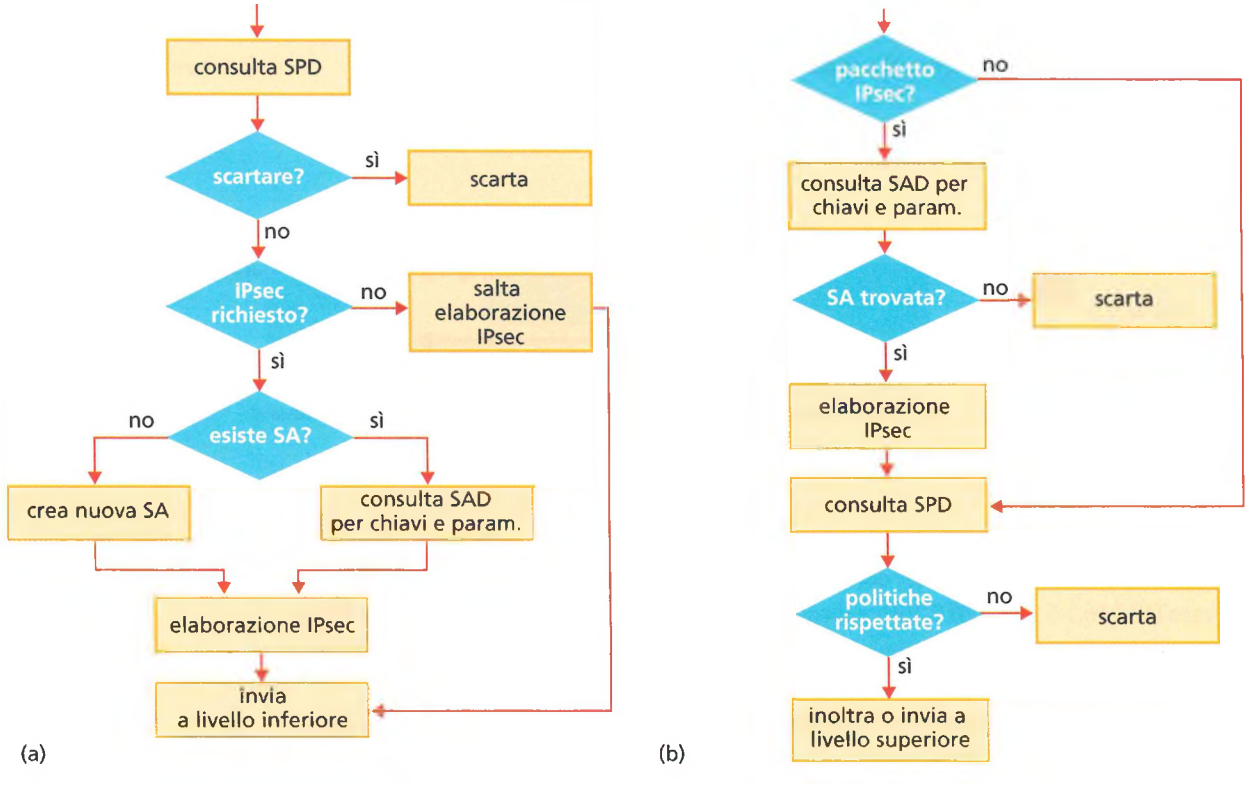


FIGURA 8 Elaborazione dei pacchetti IPsec: (a) traffico in uscita (outbound); (b) traffico in ingresso (inbound)

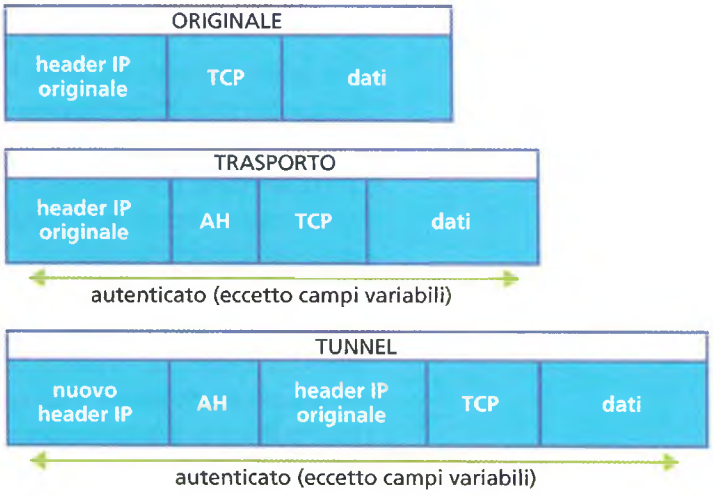
Le Security Association possono essere combinate tra loro, sia nel caso che i nodi terminali siano gli stessi sia nel caso siano diversi: per esempio, si potrebbero avere due SA in modalità trasporto tra due host (una per AH e una per ESP), oppure una SA in

modalità trasporto tra due host a cui si aggiunge una SA in modalità tunnel tra due security gateway che stanno tra i due host.
Vediamo i 3 protocolli (AH, ESP e IKE) nel dettaglio.

1. AH (Authentication Header)

Il protocollo AH fornisce servizi di autenticazione, integrità e protezione **da attacchi di tipo replay**, in cui un intruso immette nella rete un pacchetto autentico precedentemente intercettato. AH autentica l'intero pacchetto IP, a eccezione dei campi variabili dell'header IP originale (ovvero type of service, flags, fragment offset, time to live, header checksum, più alcune opzioni) che, essendo modificabili dai nodi intermedi, non possono essere autenticati. La posizione dell'header AH all'interno del pacchetto IP, nelle modalità trasporto e tunnel, è mostrata in FIGURA 9.

FIGURA 9 Posizionamento di AH all'interno del pacchetto IP

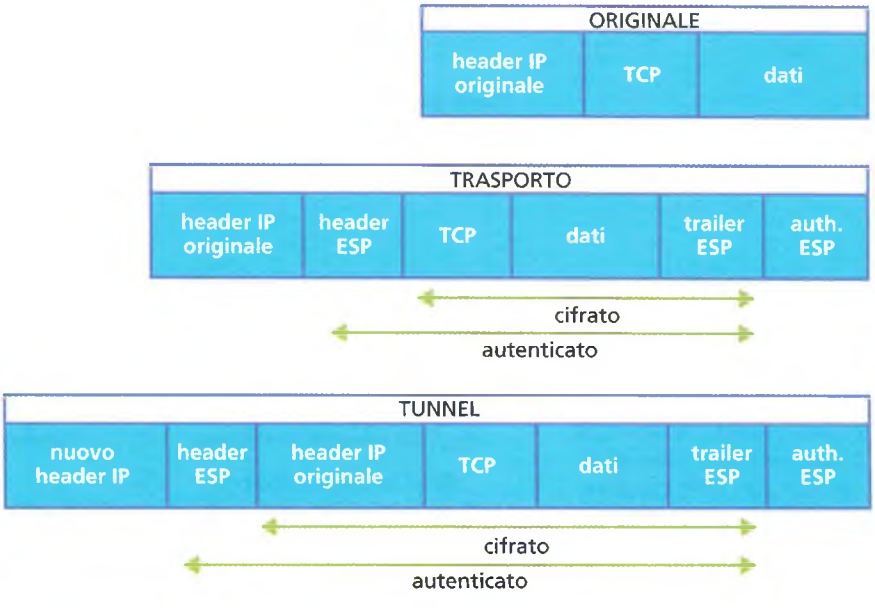


Il campo più interessante dell'header AH è il **Security Parameters Index** (SPI) che contiene un valore numerico che, insieme con l'indirizzo IP di destinazione e il protocollo (AH), identifica la Security Association utilizzata. Questo valore viene stabilito dal destinatario quando la SA viene negoziata. Nella modalità tunnel l'intero pacchetto originale (compreso l'header IP) viene incapsulato in un nuovo pacchetto e quindi è interamente autenticato.
Diverso è il comportamento di ESP.

2. ESP (Encapsulating Security Payload)

Il **protocollo ESP** fornisce servizi di confidenzialità, autenticazione, integrità e protezione da attacchi di tipo replay. È possibile utilizzare solo alcuni servizi (confidenzialità, autenticazione, integrità ed eventualmente anti-replay), oppure tutti i servizi insieme. Per quanto riguarda l'autenticazione, questa differisce da quella fornita dal protocollo AH in quanto non copre l'header IP esterno.

FIGURA 10 Posizionamento di ESP all'interno del pacchetto IP



La posizione di ESP all'interno del pacchetto IP nelle modalità tunnel e trasporto è mostrata in FIGURA 10: come si vede, ESP aggiunge sia un header sia un trailer, perché incapsula tutti i dati che protegge. ESP aggiunge anche un campo **authentication** (auth. ESP) che contiene i dati usati per autenticare il pacchetto.

Anche nell'header di ESP è presente il campo Security Parameters Index (SPI) che identifica la Security Association utilizzata.

#prendinota

IKE si occupa dell'autenticazione dell'identità dell'interlocutore, mentre AH e ESP dell'autenticazione della provenienza dei dati.
La prima è volta a garantire che l'interlocutore è chi effettivamente sostiene di essere, mentre la seconda è volta a garantire che i dati ricevuti provengano effettivamente dall'interlocutore identificato dalla prima.

3. IKE (Internet Key Exchange)

Nell'architettura di IPsec è centrale la Security Association, ma né AH né ESP si preoccupano della sua gestione. Le Security Association possono essere costruite anche manualmente; è chiaro però che una loro gestione manuale non è in genere praticabile se non in contesti molto limitati, per cui è necessario un meccanismo automatico: il protocollo IKE risolve questo problema.

Il protocollo IKE realizza un collegamento peer-to-peer in due fasi: nella prima i due host creano una Security Association per IKE stesso (IKE SA), ovvero un canale sicuro da utilizzare per i messaggi di IKE; nella seconda fase utilizzano la SA appena creata per negoziare Security Association per altri protocolli (IPsec SA).

SSL/TLS VPN

Una valida alternativa a IPsec è rappresentata dall'utilizzo dei **protocolli SSL/TLS** (Secure Sockets Layer/Transport Layer Security).

> Le **differenze** tra i due protocolli, SSL e TLS, sono poche e marginali, tuttavia sufficienti a renderli non compatibili. In generale vengono implementati entrambi rendendoli interoperabili.

Gli scenari consentiti risultano piuttosto semplici, come mostrato in FIGURA 11.
TLS è un protocollo di livello Session dello stack ISO/OSI. Opera quindi al di sopra del protocollo di livello Transport utilizzato (per esempio, TCP). È uno standard IETF (nella sua ultima versione è definito nella RFC 5246) e deriva dal protocollo SSL, originariamente proposto da Netscape Communication.

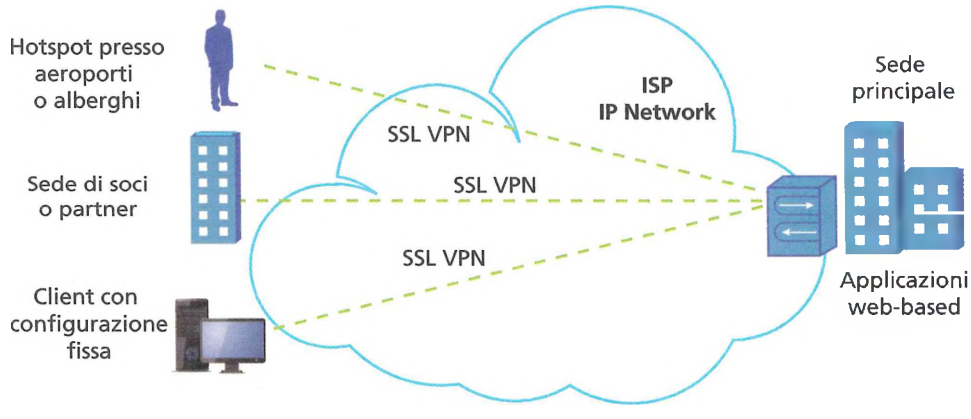


FIGURA 11 Possibile scenario VPN SSL/TLS-based

#prendinota

Diverse versioni del protocollo SSL/TLS sono ampiamente utilizzate in applicazioni come i browser, le email, la messaggistica istantanea e il voice over IP (VoIP). Un esempio di applicazione è nel protocollo HTTPS.

Il protocollo SSL/TLS è composto da due livelli: **Record Protocol** e **Handshake Protocol** (TABELLA 1).

HTTP/HTTPS	Application
SSL/TLS Handshake Protocol	Session
SSL/TLS Record Protocol	
TCP	Transport
IP	Network

TABELLA 1 Esempio di stack con i livelli inferiori e superiori di SSL/TLS

Il primo rappresenta il livello inferiore, opera subito sopra un protocollo di livello Transport affidabile (come TCP) ed è utilizzato per incapsulare protocolli di livello superiore.
Il secondo rappresenta il livello superiore e si occupa della fase di negoziazione in cui si autentica l'interlocutore e si stabilisce la crittografia comune.
La realizzazione di una VPN SSL/TLS-based passa innanzitutto attraverso l'uso del protocollo SSL/TLS, al posto di IKE dell'IPsec, per la fase di autenticazione degli estremi del tunnel e la creazione delle chiavi.

> **SSL/TSL** è un semplice protocollo Client/Server che ha lo scopo di autenticare il server da parte del client e, opzionalmente, anche il client da parte del server, e di creare un canale cifrato, sicuro, di comunicazione tra i due.

L'autenticazione è basata sui certificati digitali riconosciuti da una Certification Authority (CA). Il server invia il proprio certificato firmato dalla CA al client che ne verifica la validità confrontandone la **firma digitale** con quella della CA a lui nota. Se la firma digitale è valida, accetta il certificato e autentica il server.
Analogamente il server può chiedere il certificato del client per verificarne la validità e procedere all'autenticazione, a quel punto reciproca.
I passi necessari per stabilire una connessione sicura sono:

1. **Client → Server**: il client invia al server la richiesta di connessione includendo la lista degli algoritmi di crittografia supportati e un valore random (casuale) necessario a creare la cosiddetta **pre-master key**, che a sua volta servirà a generare la chiave privata di crittografia comune a entrambi;
2. **Server → Client**: il server invia al client il proprio certificato digitale, la scelta di algoritmi di crittografia, il proprio valore casuale per la pre-master key e la richiesta del certificato del client;
3. **Client → Server**: il client verifica il certificato del server e, se la verifica risulta negativa, il protocollo fallisce; altrimenti invia al server il proprio certificato digitale e la pre-master key cifrata con la chiave pubblica del server. Infine il client accoda la richiesta di passare a comunicazioni cifrate a partire dai pacchetti seguenti;
4. **Server → Client**: il server conferma al client di aver accettato il suo certificato digitale e passa alla fase di comunicazioni cifrate.

#prendinota

La pre-master key è l'ultimo parametro necessario a generare la chiave privata di crittografia, comune al client e al server, per la cifratura delle trasmissioni.

Dopo il punto 3 sia il client sia il server hanno tutte le informazioni necessarie per calcolare la chiave, comune a entrambi, e gli algoritmi a cui applicarla.

Confronto tra IPsec e SSL/TLS

Benché IPsec sia oggi il più diffuso protocollo per VPN, ritenuto sicuro e affidabile, si possono riscontrare alcune criticità come la complessità della fase di IKE per l'autenticazione degli estremi e lo scambio delle chiavi o il rischio di dover modificare il sistema operativo nel quale IPsec viene implementato (come successe con Windows XP service pack 2).
SSL/TLS sono singoli protocolli descritti da una RFC mentre IPsec, al contrario, ha un'architettura molto complessa e formata da elementi diversi (i protocolli AH, ESP e IKE e i database SPD e SAD).
IPsec offre diversi meccanismi di autenticazione mentre SSL/TLS consente solo l'uso dei certificati digitali.

D'altra parte SSL/TLS, essendo di tipo Client/Server, consente l'autenticazione asimmetrica, cioè permette di autenticare il server senza autenticare il client, mentre IKE di IPsec, essendo di tipo peer-to-peer, costringe all'autenticazione reciproca.
Diversa è poi la posizione dei due protocolli all'interno dello stack TCP/IP: SSL/TLS offre un canale sicuro tra due applicazioni proteggendo i dati fino alla consegna degli stessi all'applicazione interessata. I terminali della comunicazione tramite IPsec sono al contrario due macchine (host o security gateway). Quando i pacchetti arrivano all'host di destinazione, IPsec ha terminato il suo compito e i dati quindi non sono più protetti. IPsec protegge tutto ciò che sta sopra IP (come TCP, UDP, ICMP, ecc.), mentre SSL/TLS deve utilizzare un protocollo di trasporto affidabile e quindi funziona solo per proteggere il traffico TCP. Questo implica che le applicazioni basate su UDP sono escluse da SSL/TLS.

SSL/TLS è adatto a proteggere la comunicazione tra due applicazioni (autentica l'applicazione o l'utente), **IPsec** può facilmente rendere sicuro il traffico tra host o tra intere sottoreti (autentica la macchina).

La TABELLA 2 riassume le principali differenze tra i due protocolli.

TABELLA 2 Riassunto delle principali differenze tra i due protocolli

IPsec	SSL/TLS
Architettura complessa	Singoli protocolli
Peer-to-peer (IKE)	Client/Server
Livello Network	Livello Session
Canale tra due macchine	Canale tra due applicazioni
Protezione di tutto il traffico IP	Protezione solo del traffico TCP
Protezione di tutto ciò che segue l'header IP	Protezione dei dati del livello Application
Impatto maggiore sul sistema operativo	Impatto maggiore sulle applicazioni

BGP/MPLS VPN

#prendinota

MPLS (Unità 5 del volume del quarto anno) si basa sull'uso di una label al posto dell'indirizzo IP per muovere i pacchetti all'interno del suo dominio. Apposite *forwarding table* consentono di individuare il next hop.

In una rete MPLS (Multiprotocol Label Switching) è possibile utilizzare VPN con grande efficienza e affidabilità.
Le VPN basate su MPLS di solito sono offerte dai Service Provider come servizio gestito in ambito di reti IP e sono costituite da 3 elementi:

1. **CE** (**Customer Edge router**): è il router del sito aziendale che si interconnette con l'ISP fornitore del servizio VPN MPLS. Ha funzionalità di routing IP classiche e comunica con il Provider Edge (PE) router tramite BGP;
2. **PE** (**Provider Edge router**): è il router d'accesso della rete dell'ISP cui sono collegati uno o più CE;
3. **P** (**Provider core router**): Label Switched Router (LSR) che compongono il backbone MPLS dell'ISP.

Le VPN realizzate su reti MPLS usano un modello **peer-to-peer**, nel quale il router dell'azienda (CE) invia le proprie route al router del provider (PE). Solo un CE e un PE possono avere un rapporto di peering, che non può esserci invece tra CE. I router PE che fanno parte di una specifica VPN usano il protocollo **BGP** (**Border Gateway Protocol**) per scambiarsi le route relative a quella VPN. Con BGP/MPLS IP VPNs

(**RFC 4364**) viene garantita la separazione del traffico tra i diversi utilizzatori dei servizi, anche se i dati viaggiano sullo stesso backbone di rete.
Nella FIGURA 12 è mostrato un esempio di VPN tra 3 siti di una stessa azienda. La nuvoletta rappresenta la rete MPLS che andrà opportunamente configurata per collegare tra loro tutti i PE.
Per trasferire i pacchetti tra due siti di una VPN, il PE incapsulerà (tunneling) i pacchetti IP provenienti dal CE mittente e li inoltrerà nella rete MPLS verso il PE a servizio del CE destinatario. L'ultimo PE instraderà nuovamente su base IP.

#prendinota

BGP è un protocollo EGP (Exterior Gateway Protocol), di tipo Path Vector, evoluzione del Distance Vector, che elenca tutti gli Autonomous System da attraversare per giungere a destinazione.

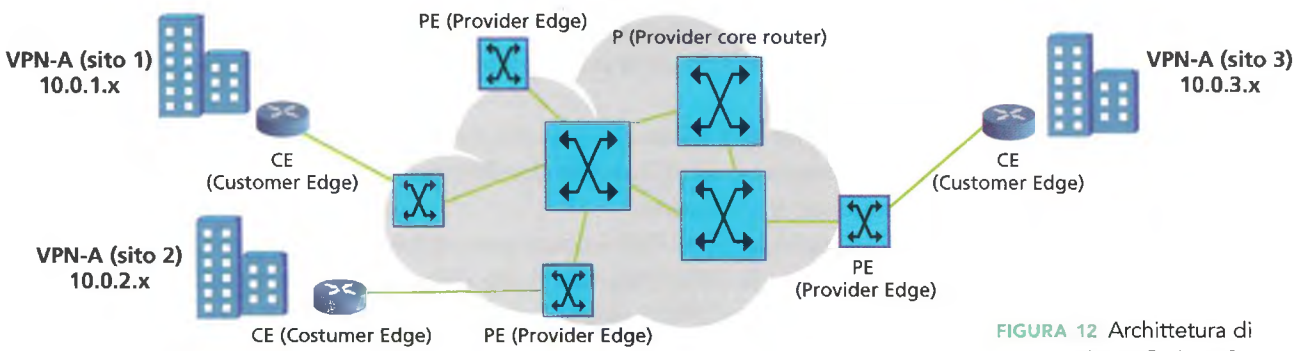
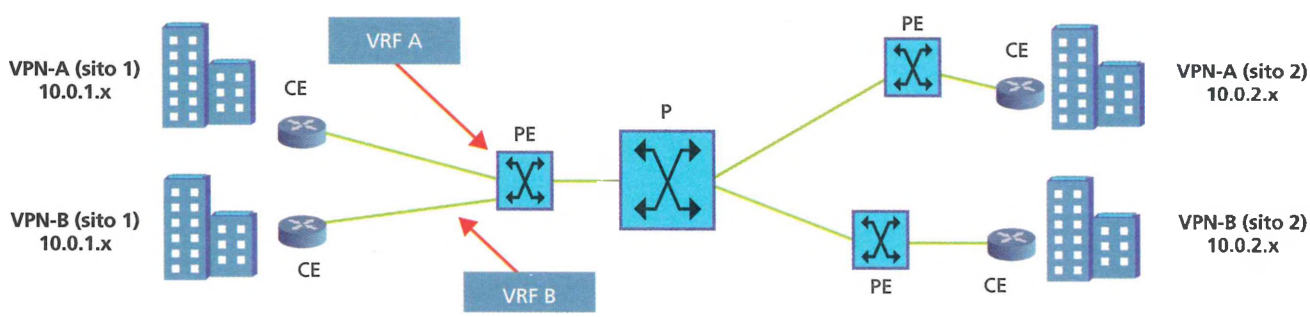


FIGURA 12 Architettura di servizio VPN BGP/MPLS

I PE si ritrovano a gestire più di una VPN e siccome l'indirizzamento non è coordinato potrebbe nascere il problema di due reti VPN con stessi indirizzi IP (FIGURA 13). Questo problema viene superato dal PE utilizzando un'interfaccia diversa per ogni VPN. Quando al PE arriva un pacchetto da un CE, lo instrada nella rete MPLS applicando le regole presenti nella **tabella di forwarding** della VPN (**VRF**, VPN Routing and Forwarding) a cui appartiene il CE. Il PE dovrà quindi gestire tante tabelle VRF quante sono le VPN a esso connesse.

FIGURA 13 2 reti VPN con stessi indirizzi IP in un'architettura VPN BGP/MPLS



Un PE possiede anche una **GFT** (**Global Forwarding Table**) che gli consente di indirizzare i pacchetti verso un altro PE.
La GFT è configurata dal provider durante le fasi di setup della VPN MPLS backbone.
Questo schema riproduce il meccanismo di instradamento all'interno di un dominio MPLS **utilizzando una label** anziché l'indirizzo IP del pacchetto da instradare. La label è costituita da due parti, una esterna e una interna:

- la parte **esterna**: servirà a indirizzare il pacchetto verso il next hop dentro la rete MPLS, cioè conterrà l'identificativo del primo PE che il pacchetto dovrà attraversare;
- la parte **interna**: servirà a identificare il nodo di uscita dalla rete MPLS, cioè l'interfaccia di uscita che deve usare il PE di destinazione.

La VPN BGP/MPLS dovrà dunque:

- isolare il traffico tra le VPN dei diversi clienti;
- connettere tra loro le sedi dei clienti;
- permettere l'uso di un indirizzamento privato indipendente per ogni cliente.

Confronto tra MPLS e IPsec

Innanzitutto, va detto che le due tecnologie non sono concorrenti ma complementari, perché garantiscono funzioni specifiche e differenti.

MPLS è stata progettata in particolare per garantire, tramite l'**instradamento per etichettatura** (**label**), un modo più efficiente e veloce di trasportare i pacchetti di dati in rete tramite schemi di routing Site-to-site (ideali per gestire le classi di servizio QoS).

IPsec invece, fin dall'inizio, è nato come protocollo di **massima sicurezza** idoneo a garantire integrità e confidenzialità dei dati trasportati da TCP/IP tramite l'utilizzo di autenticazione e cifratura.

Quindi in realtà le VPN MPLS-based non potrebbero diventare il nuovo standard VPN sostituendo le VPN IPsec-based, ma piuttosto potranno sostituire sempre più le vecchie tecnologie VPN Frame Relay e ATM.

Questo anche perché MPLS necessita della rete circoscritta di un service provider che ne fornisca l'infrastruttura, mentre IPsec è utilizzabile ovunque esista una normale connessione Internet ed è quindi ottimizzato per connessioni VPN mobile (client-to-site).

All'atto pratico, aziende e service provider possono utilizzare sia MPLS sia IPsec per creare un ambiente sicuro ideale, sfruttando i vantaggi di entrambe le tecnologie: alle aziende, l'implementazione convergente di un ambiente IPsec-MPLS integrato consente di creare una struttura intranet-extranet completa e protetta con funzionalità **VPN remote sicure**, mentre i service provider, ampliando l'offerta tecnologica, aumentano la propria competitività commerciale.

Esercizio commentato
Architettura VPN

FISSA LE CONOSCENZE

- Quali sono i 3 principali protocolli per la sicurezza in una VPN?
- Che cos'è una Security Association in ambito IPsec?
- Che differenza c'è tra la modalità trasporto e la modalità tunnel in ambito IPsec?
- Che cosa viene realizzato tramite il protocollo IKE?
- Quali sono i 2 livelli del protocollo SSL/TLS e di che cosa si occupano?
- Quali sono i passi per stabilire una connessione sicura in ambito SSL/TLS?
- Quali sono gli elementi di una VPN BGP/MPLS e quali compiti hanno?
- Che differenza c'è tra una VFR e una GFT in ambito VPN BGP/MPLS?

4 VPN DI FIDUCIA E VPN SICURE

CLASSIFICAZIONE DELLA VPN IN BASE ALLA SICUREZZA

Le reti VPN possono essere classificate in base ai protocolli che utilizzano e al grado di sicurezza che garantiscono, in 3 categorie:

- Trusted VPN
- Secure VPN
- Hybrid VPN

La prima si affida molto al proprio Internet Service Provider (ISP), la seconda ai protocolli per la sicurezza e la terza a entrambi.
Vediamo come.

TRUSTED VPN

Nelle **Trusted VPN** la riservatezza dei dati trasmessi attraverso Internet è controllata da un **Internet Service Provider** (**ISP**).

Queste non utilizzano i protocolli che permettono la cifratura e il conseguente tunneling dei dati trasmessi.
L'ISP assicura una qualità del servizio (QoS) attraverso l'utilizzo e il controllo di percorsi dedicati, garantendo che nessun altro possa usufruire del canale assegnato a una determinata VPN in un determinato momento.
L'azienda che si rivolge all'ISP ha quindi **fiducia** che i percorsi attraverso i quali i suoi dati si muovono siano mantenuti sicuri.

I protocolli e le tecnologie utilizzate dalle Trusted VPN sono:

- **Layer 2**:
  - circuiti di rete ATM;
  - trasporto del layer 2 su tecnologia MPLS.
- **Layer 3**:
  - MPLS con distribuzione limitata delle informazioni del percorso attraverso il BGP.

SECURE VPN

Le **Secure VPN** utilizzano protocolli che consentono la cifratura e il tunneling.

Per essere definita Secure VPN, una VPN deve garantire:

- la presenza di un sistema di autenticazione;
- che i dati viaggino criptati;
- che il livello di cifratura dei dati sia elevato e modificabile nel tempo.

I protocolli e le tecnologie utilizzate (standard IETF) dalle Secure VPN sono elencati di seguito.

- **IPsec (IP security)**:
  - Encapsulating Security Payload (ESP): fornisce autenticazione, confidenzialità e controllo di integrità del messaggio;
  - Authentication Header (AH): garantisce l'autenticazione e l'integrità del messaggio, ma non offre la confidenzialità;
  - Internet Key Exchange (IKE): implementa lo scambio delle chiavi per realizzare il flusso cifrato.
- **Secure Sockets Layer/Transport Layer Security (SSL/TLS)**:
  - garantisce confidenzialità e affidabilità delle comunicazioni su rete pubblica;
  - protegge da intrusioni, modifiche o falsificazioni.
- **PPTP (Point-To-Point Tunneling Protocol)**:
  - sviluppato da Microsoft, assicura autenticazione, cifratura e compressione dei dati;
  - opera insieme a **Generic Routing Encapsulation (GRE)**, un protocollo di trasporto usato per il tunneling;
  - non è considerato molto sicuro, pertanto è da usare occasionalmente.
- **SOCKS Protocol**:
  - standard IETF definito nella RFC 1928;
  - proxy trasparente che permette di effettuare connessioni TCP dirette tra computer su due reti IP differenti nei casi in cui un instradamento diretto (routing) non sia disponibile.
- **L2TP (Layer 2 Tunnelling Protocol)**:
  - è un protocollo di livello 5 (Session) che agisce però come un protocollo di livello 2 (Data link) usando pacchetti UDP per incapsulare i pacchetti L2TP e per mantenere una connessione point-to-point;
  - deve essere associato a un altro protocollo per implementare autenticazione, confidenzialità e integrità dei dati (solitamente IPSec).
- **L2TPv3 (Layer 2 Tunnelling Protocol version 3)**:
  - evoluzione di L2TP creato come alternativa a MPLS.
- **MPLS (Multiprotocol Label Switching)**:
  - utilizzato su reti a commutazione di pacchetto, tipicamente reti IP;
  - le decisioni di instradamento vengono prese in modo asincrono rispetto al trasporto del traffico e per una intera classe di destinazioni, che vengono associate a un'etichetta;
  - non può essere considerato un protocollo di rete, ma piuttosto una tecnologia che potenzia il trasporto del traffico all'interno delle reti;
  - in grado di instradare più tipi di traffico (dati, voce, video) sullo stesso canale, consentendo di differenziare la banda di trasmissione in base al tipo di traffico e di aggirare le zone congestionate e i collegamenti interrotti.

HYBRID VPN

Le Hybrid VPN rappresentano il tentativo di unire le caratteristiche delle Trusted VPN e delle Secure VPN.

Le **Secure VPN** assicurano la cifratura dei dati ma **non** assicurano i percorsi.
Le **Trusted VPN** assicurano le proprietà dei percorsi ma **non** garantiscono un alto livello di sicurezza.

Lo scenario tipico è quello di un'azienda che ha già una Trusted VPN e desidera sicurezza su una parte della VPN e dunque crea una Hybrid VPN.
In tale situazione una Secure VPN può essere adoperata come parte di una Trusted VPN, cioè la Secure VPN deve essere un sottoinsieme della Trusted VPN.

In merito ai protocolli e alle tecnologie utilizzate dalle Hybrid VPN si può affermare che ogni tecnologia supportata dalla Secure VPN si muove attraverso ogni tecnologia supportata dalla Trusted VPN.

L'emergenza Coronavirus ha provocato un boom nell'adozione delle VPN nelle principali economie mondiali. Ma nel nostro Paese si registra un aumento contenuto, pari a solo il 10,57%.
In FIGURA 14 è mostrato il grafico e la corrispondente tabella della crescita della base di utenti VPN per Paese, effettuata nella primavera 2020 a firma NordVPN Teams (una tra le più grandi reti di server VPN al mondo).

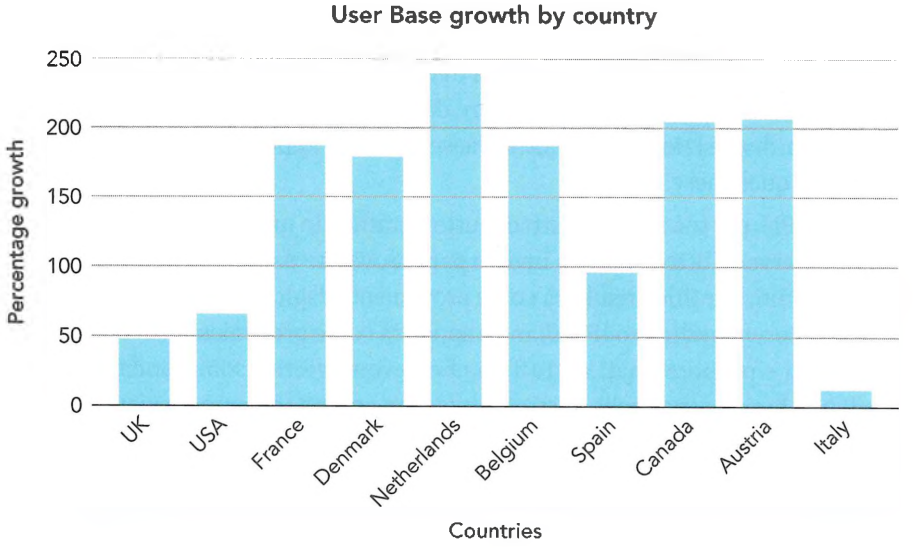


FIGURA 14 Crescita utenti VPN

Country	Growth, %
UK	48.1%
USA	65.93%
France	187.71%
Denmark	180.35%
Netherlands	240.49%
Belgium	187.76%
Spain	95.89%
Canada	206.29%
Austria	207.86%
Italy	10.57%

L'Italia, si legge nel report, è il Paese che ha registrato il tasso di crescita più basso nell'uso delle VPN. Nel nostro Paese, inoltre, il ricorso alla modalità desktop per lo smart working vanta una quota dell'85,89% contro un risicato 10,87% di quella mobile.

FISSA LE CONOSCENZE

- Qual è il ruolo dell'ISP in una Trusted VPN?
- Che cosa differenzia le Secure VPN dalle Trusted VPN?
- Che cosa deve garantire una VPN per essere definita una Secure VPN?
- Come può essere modificata una Trusted VPN per diventare una Hybrid VPN?

5 LE VPN PER LO STREAMING, IL GAMING E L'HOME BANKING

5.1 Le VPN per lo streaming

Nelle precedenti Lezioni di questa Unità sono state descritte le caratteristiche e i vantaggi delle VPN in ambito aziendale. Esiste però anche la possibilità di usare le VPN per la tutela della privacy da parte di privati cittadini e per poter quindi usare servizi altrimenti rischiosi.
Le connessioni sicure garantite dalla crittografia proteggono infatti da eventuali attacchi hacker, una caratteristica sempre più utile considerato il numero crescente di persone che si trova a lavorare o a studiare in remoto. Altri utenti, invece, si affidano alle VPN per poter usare applicazioni senza rivelare il proprio indirizzo IP. O magari per evitare, in alcuni Paesi, ingerenze da parte delle autorità governative.
Il fatto che le migliori VPN permettano di far apparire un indirizzo IP diverso da quello reale rende il loro impiego molto esteso e flessibile. Questa caratteristica può tornare molto utile per chi guarda contenuti video in streaming, permettendo di accedere a versioni di piattaforme di altri Paesi altrimenti non accessibili.

Servizi di streaming come Netflix o Spotify, il cui catalogo varia in base all'area geografica, consentono solitamente di avere a disposizione solo l'offerta confezionata per il proprio Paese. Per poter invece usufruire dell'offerta più ampia che eventualmente viene messa a disposizione in un altro Paese, occorre appoggiarsi a server dell'area geografica di quel Paese.

Un servizio VPN, per sua natura, instrada tutto il traffico in una connessione protetta fra un client e il server. Tutto il traffico inviato pare provenire dal server, quindi se il server è negli Stati Uniti, il traffico risulterà come proveniente dagli Stati Uniti. Se il server è in Italia, il traffico avrà indirizzo IP italiano e apparirà come proveniente dal nostro Paese. I server veloci e proporzionati al traffico che devono gestire sono fondamentali per godere di una buona esperienza di streaming. Non serve a nulla un servizio VPN a pagamento che fa vedere i contenuti a singhiozzo o che fa soffrire di continui buffering.

5.2 Le VPN per il gaming

Il gaming presenta a volte restrizioni geografiche che, come per lo streaming, possono essere aggirate utilizzando, mediante una VPN, dei server di Paesi in cui le restrizioni non ci sono.
Le VPN possono anche consentire di accedere ai nuovi giochi con un certo anticipo. Poniamo ci sia un multiplayer online che annuncia la data di uscita di un nuovo videogame. Probabilmente sarà inizialmente disponibile solo in Giappone o negli USA. Quindi solo con un indirizzo IP giapponese o statunitense sarà possibile provare il gioco in anteprima come un cittadino di quei Paesi.

Le VPN risultano ancora più importanti quando si parla di protezione. Oggigiorno online si possono trovare tanti giochi seri e competitivi, e questo comporta il rischio di hackeraggio. È assai pericoloso avere pubblicamente esposti il proprio indirizzo IP autentico e ulteriori informazioni personali sensibili. Con una VPN è possibile tenere tutto ciò nascosto dietro la protezione di una connessione criptata.

#prendinota

Le VPN forniscono anche la variabilità della posizione virtuale. Ogni volta che ci si connette a Internet viene assegnato un indirizzo IP e gli indirizzi IP possono anche essere usati per identificare la posizione dell'utente e persino rintracciare i contenuti, tramite l'account presso il proprio ISP, eliminando all'istante qualsiasi forma di privacy

Sempre in tema di connessioni, una VPN protegge anche dagli attacchi DDoS (variante degli attacchi DoS), un problema che ha afflitto a lungo il gioco online competitivo. Il DoS, cioè Denial of Service, è un'azione il cui obiettivo è ingolfare le risorse di un sistema informatico che fornisce un determinato servizio ai computer connessi. Ci riesce prendendo di mira server, reti di distribuzione o data center che vengono inondati di false richieste di accesso a cui non riescono a far fronte. Il risultato è che viene saturata la banda di comunicazione e i siti web o i naviganti che cercano di raggiungere quella determinata risorsa online hanno difficoltà o non ci riescono del tutto.
I DDoS funzionano allo stesso modo, ma avvengono su scala molto più ampia. Nel caso dei DoS, infatti, bisogna difendersi da una sola sorgente di traffico informatico: per esempio, un numero elevato di email in arrivo contemporaneamente. Durante gli attacchi DDoS le domande fasulle arrivano nello stesso momento da più fonti. Tutto ciò determina una maggiore efficacia dell'attacco.
In definitiva, le caratteristiche che dovrebbe offrire una VPN per il gioco online sono:

- **velocità**: bisogna assicurarsi che il servizio offra velocità eccellenti e costanti, in modo da poter mantenere sempre il gioco a livelli performanti;
- **parco server**: di solito più server si hanno a disposizione meglio è;
- **interfaccia semplice**: una buona VPN non si deve concentrare solo sulla tecnologia, ma deve investire anche nell'usabilità;
- **assistenza clienti reattiva**: è importante utilizzare VPN dotate di un supporto clienti efficiente in grado di risolvere velocemente eventuali problemi.

5.3 Le VPN per l'home banking

Le VPN sono perfette per l'uso quotidiano, ma sono particolarmente utili per oscurare informazioni sensibili come numeri di carte di credito, dettagli bancari del proprio conto corrente o dei propri investimenti.
Le banche hanno sempre fatto largo uso di sportelli per i propri clienti. Eseguire un pagamento, un deposito o ricevere una consulenza, costringeva a trovare una filiale e aspettare in fila. Con il passare degli anni la tecnologia web ha guadagnato terreno in ogni campo, l'attività bancaria online ha così iniziato a prendere piede. I dispositivi mobili e l'accesso all'account basato su browser o app sono diventati rapidamente il modo preferito per interagire con la banca. Adesso per fare un bonifico, per effettuare il pagamento di una bolletta o per visualizzare il saldo del conto corrente, è sufficiente accedere al proprio account bancario online. Sebbene le banche dispongano di una serie di forti misure di sicurezza per proteggere i dati, non possono proteggere da ogni minaccia. È qui che entrano in gioco le VPN. Utilizzare una VPN per gestire il conto online può bloccare molti tipi di attacchi, compresi i tentativi di furto d'identità.

FISSA LE CONOSCENZE

- Come fanno le VPN a tutelare la privacy del privato cittadino?
- Quali caratteristiche dovrebbe offrire una VPN per il gioco online?

6 PACKET TRACER: CREAZIONE DI UN TUNNEL IPsec VPN

In questa esercitazione di laboratorio realizzeremo con il simulatore Packet Tracer una VPN Site-to-site.

esercizio

File sorgenti
Scarica il file

→ PROBLEMA

Realizzare una rete VPN aziendale di tipo Site-to-site configurando un tunnel IPsec tra 2 router per avere comunicazioni sicure tra gli host di 2 sedi aziendali.

→ ANALISI DEL PROBLEMA

Per simulare e verificare il funzionamento di un tunnel IPsec Site-to-site ipotizziamo 3 Site in WAN e ne colleghiamo due tra loro mediante un tunnel.

→ SVOLGIMENTO

Si consideri lo scenario mostrato in FIGURA 15. I router 2 e 3 non sono collegati direttamente tra loro, ma tramite il router 1, il quale non è a conoscenza dell'esistenza della VPN.

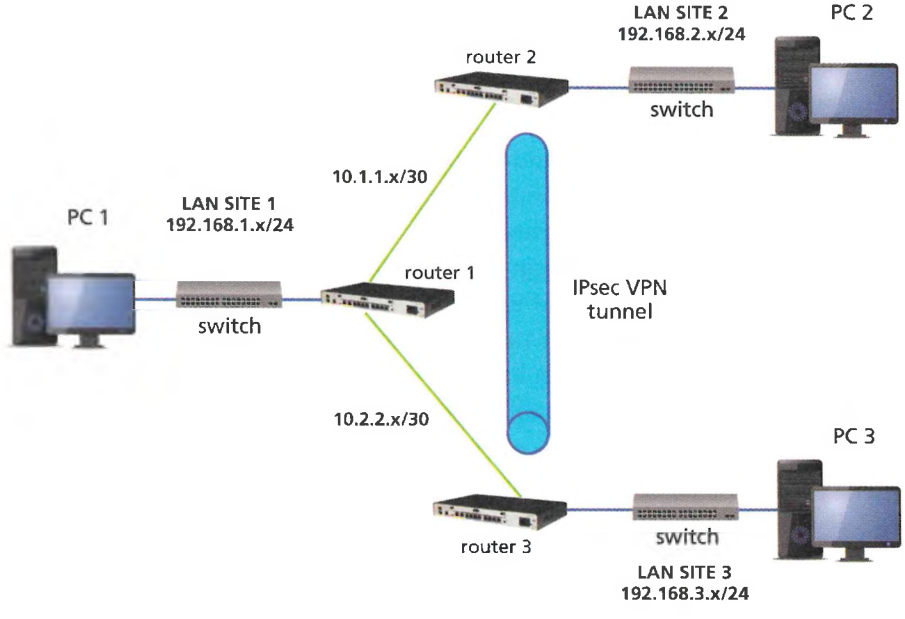


FIGURA 15 VPN Site-to-site con tunneling IPsec

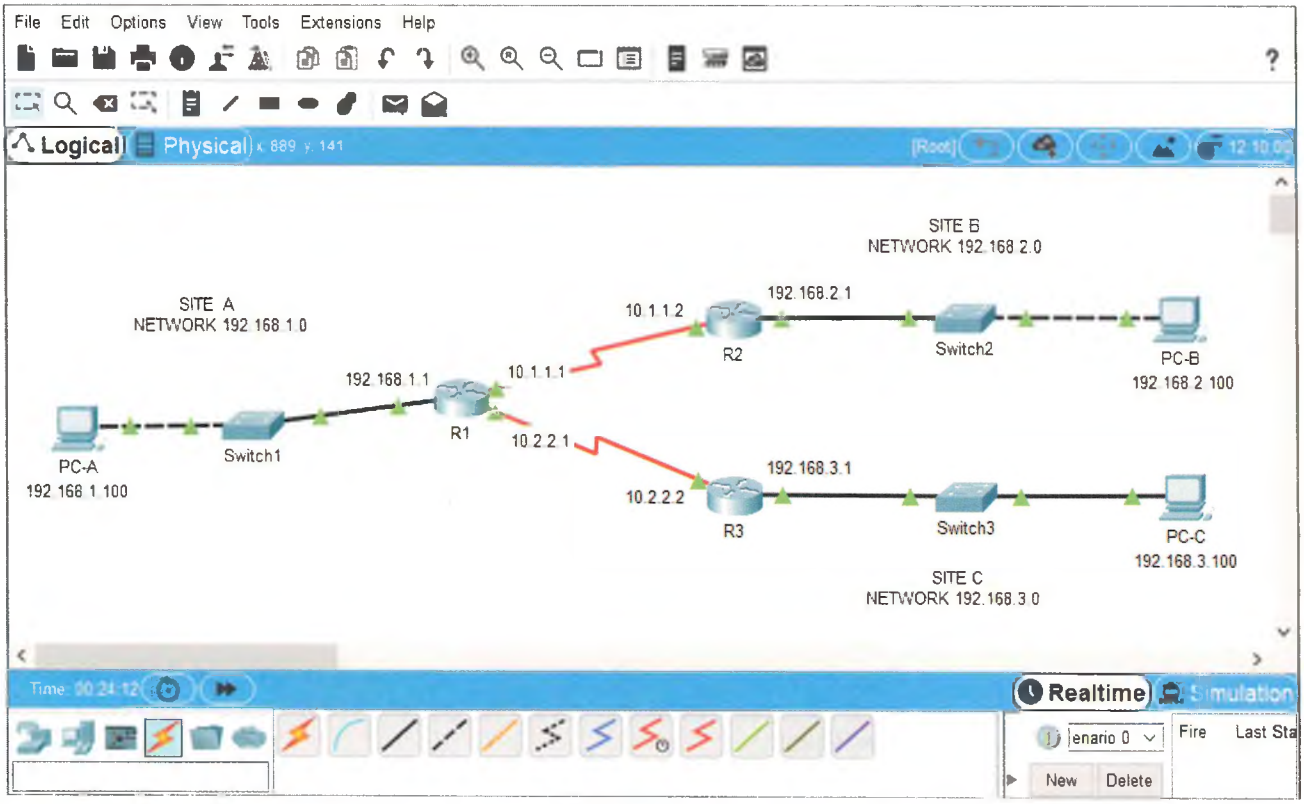
Definizioni

- ISAKMP (Internet Security Association and Key Management Protocol) è il protocollo IKE usato per creare le Security Association (SA) e per lo scambio delle chiavi.
- ACL (Access Control List): definiscono il traffico che dovrà essere trattato con IPsec.
- Confidenzialità: per proteggere i dati si usano gli algoritmi di crittografia DES, 3DES, AES, SEAL.
- Integrità: per garantire che il pacchetto non sia stato modificato si usano gli algoritmi di hash MD5, SHA.
- Autenticazione: per garantire l'identità dei 2 peer si usano gli algoritmi PSK, RSA.

- Scambio sicuro delle chiavi: si basa sull'algoritmo Diffie-Hellman (DH1, DH2, DH5, ..., DH21, DH24).
- Transform-set: è una combinazione di diversi protocolli per la sicurezza e di algoritmi.
- Crypto map: è il comando usato per creare una nuova entry ogni volta che si crea una SA; contiene i parametri di sicurezza negoziati tra i 2 peer coinvolti nella comunicazione IPsec.

La FIGURA 16 mostra lo scenario di rete Site-to-site con 3 sedi aziendali collegate in WAN tramite 3 router.

FIGURA 16 Scenario di rete con 3 sedi aziendali



La configurazione delle interfacce di rete è riassunta nel piano di indirizzamento in TABELLA 3.

Apparato	Interfaccia	Indirizzo IP	Subnet Mask	Default Gateway
R1	FE0/0	192.168.1.1	255.255.255.0	N/A
	S0/0/0	10.1.1.1	255.255.255.252	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
R2	FE0/0	192.168.2.1	255.255.255.0	N/A
	S0/0/0 (DCE)	10.1.1.2	255.255.255.252	N/A
R3	FE0/0	192.168.3.1	255.255.255.0	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A
PC-A	NIC	192.168.1.100	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.2.100	255.255.255.0	192.168.2.1
PC-C	NIC	192.168.3.100	255.255.255.0	192.168.3.1

TABELLA 3 Piano di indirizzamento

#prendinota

Ai 3 router 1841 è stato aggiunto il modulo **HWIC2T** dotato di 2 porte seriali High-Speed WAN per simulare il collegamento in WAN tra le 3 sedi aziendali. Per inserire il modulo ricordarsi di spegnere prima il router, effettuare l'inserimento del modulo e infine riaccendere il router.

Nella Lezione 3 abbiamo visto che le **Security Association** (**SA**) sono unidirezionali, quindi sarà necessario definirne una sul router 2 e una sul router 3.

Prima di iniziare la fase di creazione del tunnel, effettuare il test di connettività della rete creata; in particolare si deve poter inviare con successo un **ping da PC2 a PC3 e viceversa**. Per conoscere quali policy ISAKMP sono state definite su un router, si usa il seguente comando:

```
R2#show crypto isakmp default policy
```

Se non sono state configurate manualmente delle nuove policy ISAKMP nè ne sono state cancellate, questo comando fornirà in output l'elenco delle policy di default supportate dal sistema operativo (IOS) del router.

1) Configurazione dei parametri IPsec su R2

- Verificare con il comando show version se è abilitato il package Security Technology, e in caso contrario abilitarlo:

```
R2#config t
R2(config)#license boot module c1900 technology-package securityk9
```

  – rispondere yes alla richiesta sulla licenza e terminare:

```
R2(config)#end
```

  – salvare la running-config ed effettuare un reload del router per abilitare la licenza:

```
R2#copy running-config startup-config
R2#reload
```

  – verificare l'abilitazione del package Security Technology dando il seguente comando:

- Creare una ACL per definire la VPN Site-to-site con R3, poiché il default è *deny all*, tutto quello che si vuol far transitare deve essere espressamente specificato:

  – configurare ACL 120 per identificare il traffico dalla LAN SITE2 alla LAN SITE3 da trattare con IPsec:

```
R2#config t
R2(config)#access-list 120 permit ip 192.168.2.0  0.0.0.255 192.168.3.0
0.0.0.255
```

- Definire i parametri da usare per configurare una nuova ISAKMP policy:

  – configurare i parametri per la policy 1 relativi all'algoritmo di cifratura (AES 256), al metodo di autenticazione (pre-share) e di scambio delle chiavi (DH 5), gli altri parametri sono già impostati (protocollo ISAKMP, algoritmo di hash SHA-1 e tempo di vita della SA):

```
R2(config)#crypto isakmp policy 1
R2(config-isakmp)#encryption aes 256
R2(config-isakmp)#authentication pre-share
R2(config-isakmp)#group 5
R2(config-isakmp)#exit
```

  – configurare la chiave di crittografia condivisa con R3 (Pre-Shared Key):

```
R2(config)#crypto isakmp key vpnpw1 address 10.2.2.2
```

- Configurare i parametri di policy per la IPsec SA:
  - definire il transform-set VPN-SET che utilizza protocollo ESP con gli algoritmi di cifratura AES e di autenticazione SHA:

```
R2(config)#crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
```

  - creare quindi una nuova crypto map, VPN-MAP, avente numero di sequenza pari a 10, indicando che sarà usato il protocollo IKE (ipsec-isakmp) per creare la SA:

```
R2(config)#crypto map VPN-MAP 10 ipsec-isakmp
R2(config-crypto-map)#description VPN connection to R3
R2(config-crypto-map)#set peer 10.2.2.2
R2(config-crypto-map)#set transform-set VPN-SET
R2(config-crypto-map)#match address 120
R2(config-crypto-map)#exit
```

- Applicare la crypto map VPN-MAP all'interfaccia di uscita di R2 (Serial 0/0/0):

```
R2(config)#interface s0/0/0
R2(config-if)#crypto map VPN-MAP
R2(config-if)#end
```

- Verificare la policy ISAKMP e la crypto map create:

```
R2#show crypto isakmp policy
R2#show crypto map
```

2) Configurazione dei parametri IPsec su R3

- Verificare con il comando show version se è abilitato il package Security Technology, e in caso contrario abilitarlo seguendo la stessa procedura indicata per R2;
- Creare una ACL per definire la VPN Site-to-site con R2:

```
R3#config t
R3(config)#access-list 120 permit ip 192.168.3.0  0.0.0.255 192.168.2.0  0.0.0.255
```

- Definire i parametri da usare per configurare una nuova ISAKMP policy:
  - configurare i parametri per la policy 1 in modo analogo a quanto fatto per R2:

```
R3(config)#crypto isakmp policy 1
R3(config-isakmp)#encryption aes 256
R3(config-isakmp)#authentication pre-share
R3(config-isakmp)#group 5
R3(config-isakmp)#exit
```

  - configurare la chiave di crittografia condivisa «vpnpw1»:

```
R3(config)#crypto isakmp key vpnpw1 address 10.1.1.2
```

- Configurare i parametri di policy per la IPsec SA:
  - definire il transform-set VPN-SET:

```
R3(config)#crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
```

– creare la crypto map VPN-MAP

```
R3(config)#crypto map VPN-MAP 10 ipsec-isakmp
R3(config-crypto-map)#description VPN connection to R2
R3(config-crypto-map)#set peer 10.1.1.2
R3(config-crypto-map)#set transform-set VPN-SET
R3(config-crypto-map)#match address 120
R3(config-crypto-map)#exit
```

- Applicare la crypto map (VPN-MAP) all'interfaccia di uscita di R3 (Serial 0/0/1):

```
R3(config)#interface s0/0/1
R3(config-if)#crypto map VPN-MAP
R3(config-if)#end
```

- Verificare la policy ISAKMP e la crypto map create:

```
R3#show crypto isakmp policy
R3#show crypto map
```

3) Verifica del Tunnel IPsec VPN

Verifichiamo ora il funzionamento del tunnel IPsec VPN creato tra R2 e R3.
Faremo inviare dei dati da R2 verso R3 che dovranno essere trattati con i meccanismi di sicurezza di IPsec. Il protocollo utilizzato è ESP.

- Per verificare se c'è stato traffico in ingresso e in uscita da un router gestito con IPsec dare il seguente comando (la prima volta i contatori saranno tutti a zero):

```
R2#show crypto ipsec sa
```

- Creare traffico da PC-B verso PC-C e controllare i contatori della VPN, questa volta saranno diversi da zero:

```
R2#ping ip 192.168.3.100 source 192.168.2.100
R2#show crypto ipsec sa
```

- Creare traffico che non coinvolge IPsec, per esempio da PC-B verso PC-A e controllare nuovamente i contatori della VPN; i valori non sono cambiati, a conferma che questo traffico non è cifrato:

```
R2#ping ip 192.168.1.100 source 192.168.2.100
R2#show crypto ipsec sa
```

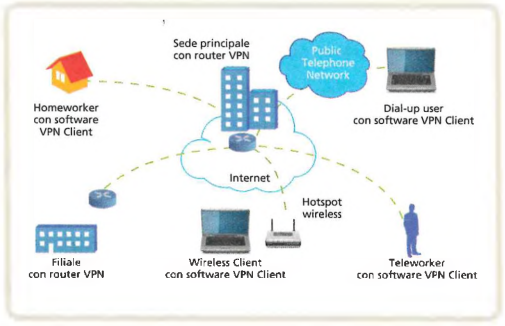
FISSA LE CONOSCENZE

- Quali algoritmi di cifratura e di autenticazione sono usati per configurare un tunnel IPsec in PT?
- Qual è lo scopo della ACL creata durante la configurazione del tunnel?
- Spiega il comando crypto map.
- Come si può controllare che il traffico di interesse è stato cifrato?

DIDATTICA INCLUSIVA

1 Le caratteristiche di una Virtual Private Network

Esistono reti private vere e proprie, che collegano più siti di una rete aziendale attraverso canali dedicati, a uso esclusivo, pagandone l'affitto al proprietario o al gestore, e reti private virtuali. Una Virtual Private Network (VPN) è una rete privata creata all'interno di un'infrastruttura di rete pubblica, per esempio Internet.

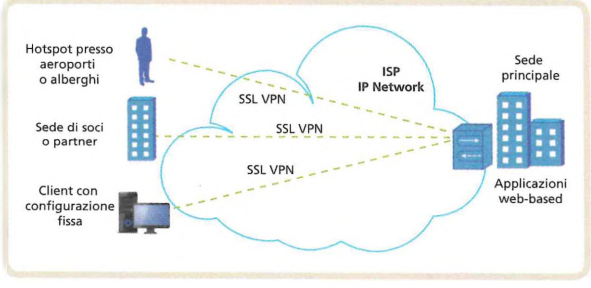


2 La sicurezza nelle VPN

Le reti VPN con ambito geografico (WAN) che utilizzano Internet garantiscono sicurezza dei dati e riservatezza delle trasmissioni attraverso: autenticazione, cifratura e tunneling.

3 I protocolli per la sicurezza nelle VPN: scenari possibili

I principali protocolli per la sicurezza sono IPsec, SSL/TLS e BGP/MPLS. Tali protocolli, in modo diverso, forniscono comunicazioni sicure con diritti di accesso su misura per i singoli utenti, che si tratti di dipendenti, consulenti o partner. IPsec non è un singolo protocollo ma un'architettura di sicurezza a livello Network, composta da vari protocolli e da altri elementi.



SSL/TSL è un semplice protocollo Client/Server avente lo scopo di autenticare il server da parte del client e, opzionalmente, anche il client da parte del server, e di creare un canale cifrato e sicuro di comunicazione tra i due.

4 VPN di fiducia e VPN sicure

Le reti VPN possono essere classificate in 3 categorie, in base ai protocolli che utilizzano e al grado di sicurezza che garantiscono: Trusted VPN, Secure VPN e Hybrid VPN. La prima si affida al proprio Internet Service Provider (ISP), la seconda ai protocolli per la sicurezza e la terza a entrambi.

5 Le VPN per lo streaming, il gaming e l'home banking

Il fatto che le VPN permettano di far apparire un indirizzo IP diverso da quello reale e di crittografare le trasmissioni rende il loro impiego molto esteso e flessibile. Per esempio consentono di guardare contenuti video in streaming o di provare videogame in anteprima accedendo a piattaforme di altri Paesi altrimenti non accessibili. Anche l'home banking risulta più sicuro grazie alle VPN.

VERIFICA DI FINE UNITÀ

Test
Svolgi il **test interattivo**

Quali delle seguenti affermazioni sono vere (V) e quali false (F)?

1. Il teleworker svolge il proprio lavoro da casa. V F
2. Il protocollo Internet Key Exchange (IKE) implementa lo scambio delle chiavi per realizzare il flusso crittografato. V F
3. All'interno di una stessa VPN non vi possono essere due indirizzi uguali. V F
4. Le Trusted VPN garantiscono i percorsi e un alto livello di sicurezza. V F
5. MPLS è stata progettata per garantire l'instradamento tramite indirizzo IP. V F
6. I protocolli SSL e TLS non sono compatibili ma interoperabili. V F
7. Il protocollo AH in modalità Transport introduce nel pacchetto un nuovo header IP. V F
8. Le Security Association (SA) previste in IPsec sono unidirezionali. V F

Domande a scelta multipla (una sola è la risposta esatta)

1. Quale di questi fattori non rappresenta una VPN?

A La variabilità del tempo di trasferimento
B Il controllo degli accessi
C Il blocco della rete
D La sicurezza delle trasmissioni

2. Quale tra i seguenti protocolli non è usato per il tunneling?

A IPsec (IP security)
B PPP (Point-to-Point Protocol)
C SSL/TLS (Secure Sockets Layer/Transport Layer Security)
D SSH (Secure SHell)

3. Tra gli elementi di una VPN BGP/MPLS-based c'è il CE (Customer Edge) che rappresenta:

A il router d'accesso della rete dell'ISP
B uno dei router del backbone MPLS dell'ISP
C il router del sito aziendale che si interconnette con l'ISP
D un qualsiasi router

4. Le Secure VPN garantiscono:

A la cifratura dei dati e i percorsi
B la cifratura dei dati ma non i percorsi
C i percorsi ma non la cifratura dei dati
D né i percorsi né la cifratura dei dati

Ascolta le **risposte**

PREPARATI PER IL COLLOQUIO ORALE

1. LEZIONE 1 **All'interno di una stessa VPN l'indirizzamento deve essere univoco o si possono avere due indirizzi privati uguali? Perché?**
2. LEZIONE 1 **Quali sono i vantaggi e gli svantaggi delle reti private virtuali (VPN)?**
3. LEZIONE 1 **Descrivi i due tipi di Site-to-site VPN.**
4. LEZIONE 2 **In cosa consistono rispettivamente l'integrità e l'autenticità dei dati?**
5. LEZIONE 2 **Nella sicurezza informatica che cosa si intende per confidenzialità (o riservatezza)?**
6. LEZIONE 2 **Descrivi le differenze tra la modalità trasporto e la modalità tunnel.**
7. LEZIONE 3 **Elenca le principali caratteristiche del protocollo IPsec.**
8. LEZIONE 3 **Descrivi i compiti dei protocolli AH (Authentication Header) ed ESP (Encapsulating Security Payload) di IPsec.**
9. LEZIONE 3 **Elenca le principali caratteristiche del protocollo SSL/TLS.**
10. LEZIONE 3 **Descrivi quali sono le differenze tra IPsec e BGP/MPLS.**
11. LEZIONE 4 **Perché nelle Trusted VPN occorre avere fiducia nell'ISP?**

IN ENGLISH, PLEASE

CLIL

Ascolta la **pronuncia del testo** e verifica la **traduzione**

ABSTRACT

VPN (Virtual Private Network)

A Virtual Private Network (VPN) is a private network created within a public network infrastructure, such as the Internet. It is used to connect a LAN to other workers at home (homeworkers) and employees (teleworkers), who connect to the corporate office over the public network. Using a public network requires three issues to be addressed: authentication, encryption and tunneling. Authentication allows the user to be identified and resources allocated to them according to specific criteria. Tunneling is a set of techniques whereby a protocol is encapsulated in a protocol of the same or higher level, and allows a set of data to be encapsulated. Encryption is applied using different protocols depending on the flexibility and level of security required. VPNs can be classified into three categories according to the protocols they use and the degree of security they provide: Trusted VPN, Secure VPN and Hybrid VPN.

EXERCISES

Use the appropriate number to match words and meanings.

...	Accounting	1	Process of confirming user identity
...	Teleworker	2	Encapsulated protocol
...	Tunneling	3	Worker connected to a VPN at home
...	User authentication	4	Gathering data about network resources utilisation
...	Homeworker	5	A single point of access to remote protected resource
...	NAS	6	Worker connected to a VPN by mobile devices
...	Secure VPN	7	The ISP ensures the paths
...	Trusted VPN	8	It uses protocols for encryption and tunneling

GLOSSARY

AAA server: a server program that provides authentication, authorization and accounting services.

Extranet: a network that, using the same structures as the Internet, connects only subjects linked by privileged relationships (such as a company and its branches).

Hybrid VPN: enables to designate which traffic is to be routed through a secure VPN server and which connects directly to the Internet.

IKE (Internet Key Exchange): a protocol that establishes the rules for encryption keys exchange.

Intranet: it is the internal company network that uses Internet browsers, servers and communication protocols, to which, however, only recognized users can have access.

IPsec (IP security): a suite of protocols for securing IP communications at Network Level.

SA (Security Association): a contract that specifies what security mechanisms to use and with what keys.

SAD (Security Association Database): a database that contains the parameters of each active SA. It is populated by IKE when an SA is established.

Secure VPN: a VPN that uses protocols for encryption and tunneling.

Smart working: a new way of working remotly, including mobile working, coworking or generally speaking a more flexible way of working.

SPD (Security Policy Database): a database that stores the security requirements for an SA to be established. It is used during both inbound and outbound packet processing.

SSL (Secure Sockets Layer): a simple Client/Server protocol used by the client to authenticate the server and to create an encrypted, secure communication channel between the two.

Transport mode: it inserts the IPsec header information into an existing packet between the IP header and the IP data.

Trusted VPN: a VPN that does not use cryptographic tunneling; instead it relies on the security of a single provider's network to protect the traffic.

Tunnel mode: it creates a new IP packet and IPsec header, then places the entire original packet into the data section of the new packet.

LAVORARE PER COMPETENZE

COMPETENZE IN GIOCO

Competenze disciplinari

- Saper progettare reti private in ambito geografico.
- Scegliere gli standard tecnici adeguati in base alle richieste.
- Saper descrivere e documentare le soluzioni adottate.
- Utilizzare le reti e gli strumenti informatici nelle attività di studio, ricerca e approfondimento disciplinare.

Competenze chiave di cittadinanza

- Interpretare il testo.
- Risolvere problemi.
- Comunicare.
- Competenza digitale.

obiettivi formativi

- Stimolare azioni di ricerca e approfondimento disciplinare.
- Consultare fonti Internet.
- Contestualizzare in un caso reale le nozioni teoriche acquisite studiando.
- Esporre i risultati della ricerca alla classe.

tempi

- Preparazione: 2 ore.
- Presentazione dei risultati e dibattito: 1 ora.
- Autovalutazione: 10 minuti.

strumenti

- Libro di testo.
- Dispositivo connesso a Internet.
- Foglio di carta.
- Software PowerPoint.
- Proiettore collegato al computer in classe o in laboratorio.

TEMA PROPOSTO

Una scuola superiore con 1500 studenti è ospitata in una serie di edifici della città in cui è situata.
La scuola ha esigenze crescenti di servizi di rete, sia per quanto riguarda l'attività amministrativa (che sempre più viene svolta su portali esterni ministeriali e privati come per il registro elettronico), sia per quanto riguarda la didattica innovativa e multimediale.

Inoltre, essendo la scuola distribuita su più edifici distanti tra loro, ha necessità di tecnologie idonee a uno scambio dati in tempo reale ma al tempo stesso sicuro.

Bisognerà quindi garantire l'autenticazione degli utenti (studenti, docenti, impiegati, dirigenza) e assegnare le opportune autorizzazioni a ciascuno attraverso la creazione di una rete privata.

Servirà che le trasmissioni siano crittografate poiché si comunicano dati sensibili tra le varie sedi della scuola.

L'amministratore della rete dovrà provvedere alla creazione degli account e al monitoraggio del traffico.

Dopo aver formulato eventuali ipotesi aggiuntive, analizzare le possibili soluzioni tecnologiche che rispondono a questo tipo di esigenze, discutendone in dettaglio le caratteristiche a livello di protocolli.

SVOLGIMENTO

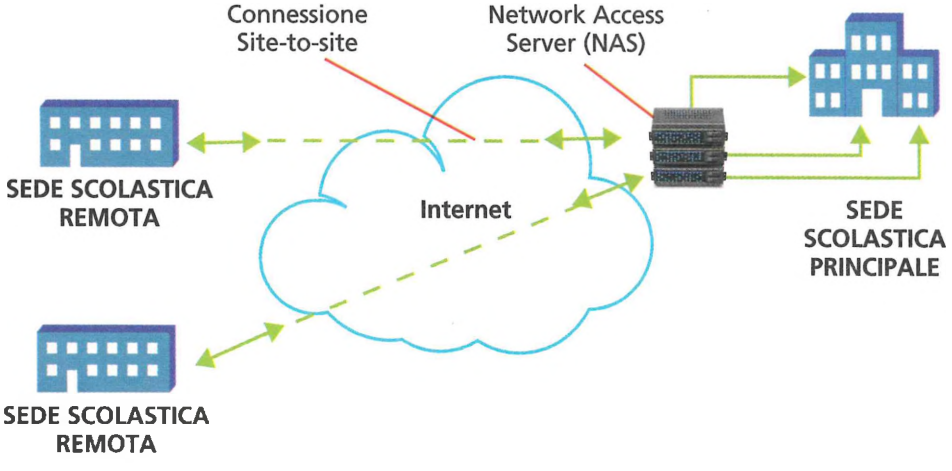
Ipotesi aggiuntive

Per adeguarci allo scenario proposto ipotizziamo che la scuola, invece di essere in un singolo edificio, sia distribuita tra più sedi sparse nei quartieri di una grande città o sparse tra piccoli comuni limitrofi.
In altre parole immaginiamo la scuola come una piccola azienda con filiali distribuite sul territorio.
Supponiamo inoltre che la scuola abbia un amministratore della rete scolastica.

Descrizione

Se ipotizziamo che la scuola sia suddivisa in più plessi (sedi distanti tra loro), può rendersi necessario uno scambio di dati sicuro e protetto, tra i singoli plessi.
Pensiamo per esempio alla necessità di condividere dati sensibili tra le diverse segreterie amministrative o alla necessità del Dirigente Scolastico di trasmettere ordini di servizio dal suo ufficio alle varie sedi.
La tecnologia che oggi rende possibile questo è la VPN (Virtual Private Network).
Le VPN realizzano una rete privata sfruttando i canali condivisi della rete Internet. Sarebbe troppo costoso realizzare una rete privata con canali a uso esclusivo.
L'uso condiviso dei canali comporta però rischi per la sicurezza.

Per garantire la sicurezza su un canale condiviso, le VPN creano un tunnel mediante l'incapsulamento dei pacchetti in transito in altri pacchetti con protocollo di pari livello o superiore.
Quello che si ottiene è che il pacchetto esterno protegge il contenuto del pacchetto interno e assicura che il pacchetto passeggero si muova all'interno di un tunnel virtuale.
Nel caso di più edifici in zone diverse serve in particolare la Site-to-site VPN (rappresentata nella figura seguente) che consente di aprire un tunnel cifrato tra la sede principale e quelle sparse sul territorio, cui accedere autenticandosi.



La cifratura garantisce la riservatezza della trasmissione, l'autenticazione protegge dalle intrusioni.

Le reti VPN sono reti private, dunque chiuse al pubblico. Per potervi accedere occorre prima essere autenticati.

La porta di accesso di un client alla sua VPN è il server NAS (Network Access Server) dotato di un processo di autenticazione o un server dedicato all'autenticazione come il server AAA (Authentication, Authorization and Accounting). Per esempio, dopo aver effettuato il login con username e password, viene chiesto di immettere un codice generato tramite una chiave elettronica (key fob) che cambia ogni volta. Oppure mediante l'uso di applicazioni che alla generazione di sequenze di caratteri da usare una volta sola (one-time password) associano altri fattori quali l'impronta (fingerprint) oppure la lettura di un QR code che compare nella pagina web di autenticazione.

Si occuperà dell'accounting l'amministratore della rete scolastica, il quale dovrà, per ogni utente (dirigente, impiegato, docente, ecc.), stabilire le autorizzazioni e le limitazioni cui è soggetto.
Suo sarà anche il compito di monitorare la VPN scolastica, controllandone i flussi al fine di prevenire congestioni e guasti.

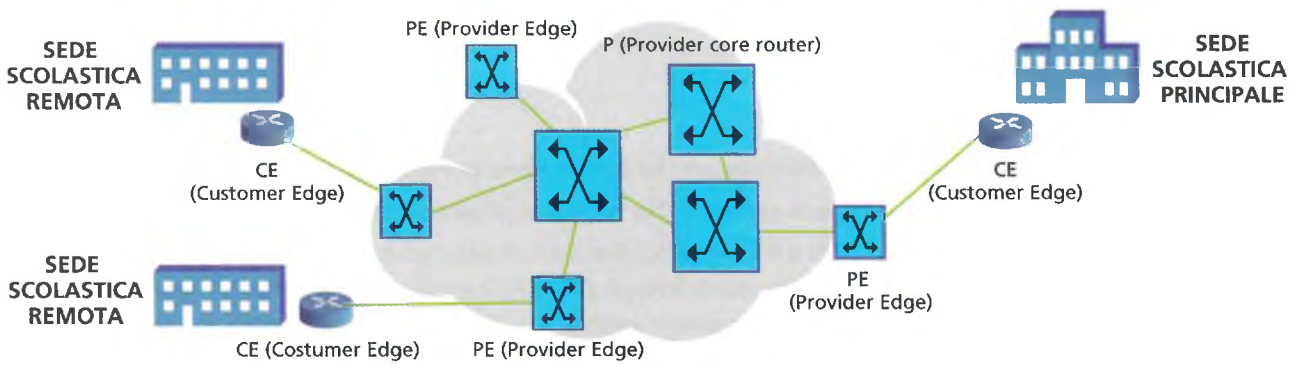
Le VPN utilizzano un'ampia gamma di algoritmi di crittografia (3DES, CAST, IDEA, ecc.) per cifrare il traffico in rete. Sia l'algoritmo sia le chiavi segrete che l'algoritmo stesso utilizza sono concordate e scambiate tra mittente e destinatario attraverso protocolli di sicurezza.
I principali protocolli per la sicurezza sono IPsec (IP security), SSL/TLS (Secure Sockets Layer/Transport Layer Security) e MPLS (Multiprotocol Label Switching).
Questi realizzano comunicazioni sicure con diritti di accesso su misura per i singoli utenti, che si tratti di dipendenti, consulenti o soci.

IPsec rappresenta la scelta adottata più frequentemente dalle aziende.
Si tratta di un'architettura di sicurezza a livello Network, composta da 3 protocolli principali:

- Authentication Header (AH): che garantisce l'autenticazione e l'integrità del messaggio ma non offre la confidenzialità;
- Encapsulating Security Payload (ESP): fornisce autenticazione, confidenzialità e integrità del messaggio;
- Internet Key Exchange (IKE): implementa lo scambio delle chiavi per realizzare il flusso crittografato.

Una valida alternativa a IPsec è rappresentata dall'utilizzo dei protocolli SSL/TLS di tipo Client/Server, che hanno lo scopo di autenticare il server da parte del client (opzionalmente viceversa) e di creare un canale cifrato, sicuro, di comunicazione tra i due. Infatti, SSL/TLS consente l'autenticazione asimmetrica, cioè consente di autenticare il server senza autenticare il client – mentre IKE di IPsec, essendo di tipo peer-to-peer, costringe all'autenticazione reciproca.
SSL/TLS è quindi adatto a proteggere la comunicazione tra due applicazioni, mentre IPsec invece può facilmente rendere sicuro il traffico tra host o tra intere sottoreti (autentica la macchina).

Infine, le VPN basate su MPLS di solito sono offerte dagli ISP come servizio gestito in ambito di reti IP. Questo perché MPLS necessita della rete circoscritta di un service provider che ne fornisca l'infrastruttura, mentre IPsec è utilizzabile ovunque esista una normale connessione Internet.
Va detto che le tecnologie IPsec e MPLS non sono concorrenti ma complementari, perché garantiscono funzioni specifiche e differenti.
MPLS è stata progettata in particolare per garantire, tramite l'instradamento per etichettatura (label), un modo più efficiente e veloce di trasportare i pacchetti di dati in rete.



MPLS VPN

A CASA

- Effettua una ricerca in Internet sulle reti private con sedi remote; esaminando i diversi casi trovati concentrati su:
  - tipologie possibili;
  - protocolli utilizzati;
  - caratteristiche di sicurezza.
- Individua quali, tra i casi trovati, risulta affine al contesto illustrato nel tema proposto.
- Leggi l'esempio di svolgimento proposto per verificare se le tue ipotesi si adattano al caso preso in esame e se la trattazione proposta risulta completa nell'ottica dei risultati della tua ricerca.
- Raccogli i tuoi risultati in una presentazione in PowerPoint (massimo 5 slide) evidenziando i casi trovati, la relazione con il contesto proposto, eventuali modifiche o aggiunte da effettuare alla soluzione proposta nell'esempio di svolgimento.

IN CLASSE

- Condividi la presentazione dei tuoi risultati con i compagni.
- Confronta e discuti con i compagni i casi che sono stati presentati.
- Stabilite quale caso rappresenta l'esempio migliore per completezza e realisticità nell'ottica della realizzazione delle tecnologie richieste dal problema.
- Procedi con l'autovalutazione.

AUTOVALUTAZIONE

ATTIVITÀ	LIVELLO			
	INIZIALE	BASE	INTERMEDIO	AVANZATO
Ho compreso senza difficoltà le richieste dell'attività proposta?	Ho compreso solo alcune delle richieste aiutato dal docente. ☐	Con la guida del docente e la collaborazione dei compagni ho compreso quasi tutte le richieste. ☐	Ho compreso le richieste e in parte le ho svolte autonomamente. ☐	Ho identificato le richieste e le ho svolte senza difficoltà. ☐
Ho reperito le informazioni in rete senza difficoltà?	Ho reperito solo alcune delle informazioni utili aiutato dal docente. ☐	Con la guida del docente e dei compagni ho reperito quasi tutte le informazioni. ☐	Ho reperito le informazioni utili autonomamente e le ho elaborate. ☐	Ho identificato le informazioni utili e le ho elaborate senza difficoltà. ☐
L'analisi dello scenario mi ha permesso di definire modifiche e miglioramenti allo svolgimento proposto?	A partire dalla mia analisi, non sono stato in grado di individuare nessun punto critico nello svolgimento proposto. ☐	A partire dalla mia analisi, sono stato in grado di individuare alcuni punti critici nello svolgimento proposto con l'aiuto del docente. ☐	A partire dalla mia analisi, sono stato in grado di individuare i punti critici e alcune modifiche apportabili nello svolgimento proposto con l'aiuto del docente. ☐	A partire dalla mia analisi, sono stato in grado di individuare i punti critici e definire le modifiche apportabili in modo dettagliato e completo. ☐

UNITÀ

4 LE RETI WIRELESS

Guarda la **presentazione** dell'unità

IN QUESTA UNITÀ

conoscenze	abilità	competenze
Conoscere le componenti, le specifiche e gli standard dei sistemi wireless. Comprendere la configurazione dei sistemi wireless. Conoscere lo stato dell'arte e la normativa sul Wi-Fi.	Saper distinguere le diverse tecnologie e le diverse componenti necessarie alla realizzazione di reti wireless. Saper configurare una LAN wireless. Comprendere le problematiche relative alla sicurezza wireless.	Saper utilizzare le tecnologie wireless e scegliere gli opportuni dispositivi mobili in base alle esigenze di progettazione.

DDI+ Didattica Digitale Integrata Plus

FLIPPED CLASSROOM

A casa

- Leggi la Lezione 2 di questa Unità;
- leggi il Case study *Sicurezza delle reti wireless*;
- indica in un report (massimo 1 pagina) quali soluzioni tra quelle proposte nel Case study sono efficaci per proteggere l'azienda anche da attacchi diversi da quello presentato.

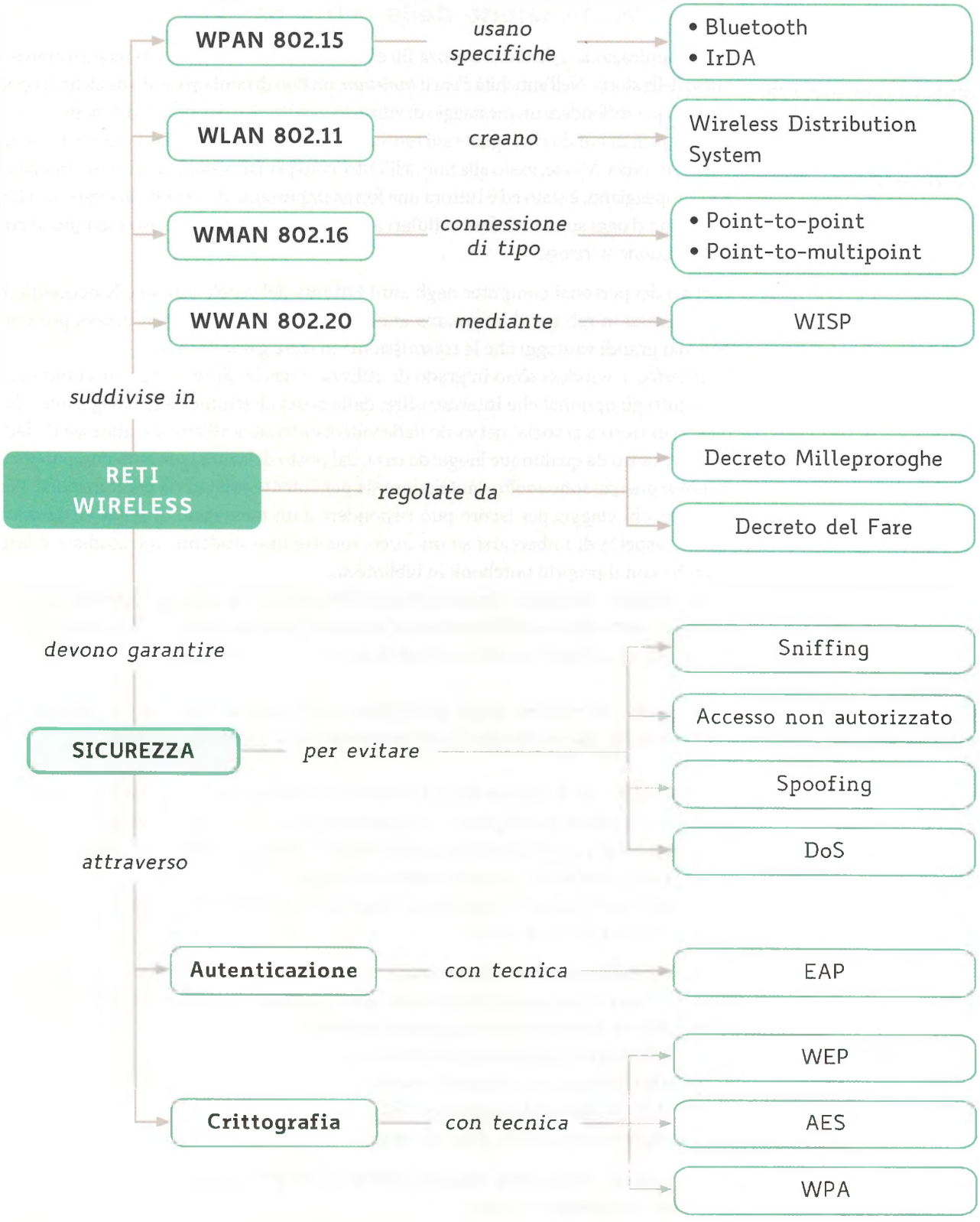
In classe

- Confrontate i vari report e discutete l'efficacia delle soluzioni proposte;
- individuate e descrivete le soluzioni aggiuntive approntabili per la protezione dell'azienda;
- raccogliete i risultati della discussione in uno schema riassuntivo.

MAPPA CONCETTUALE

DIDATTICA INCLUSIVA

Mappa modificabile



1 SCENARI DI RETI SENZA FILI

1.1 Classificazione delle reti senza fili

#prendinota

Una rete wireless permette alle persone di comunicare e di accedere ad applicazioni e informazioni senza l'utilizzo di connessioni via cavo.

La comunicazione a distanza e senza fili è stata realizzata dall'uomo in molte forme nel corso della storia. Nell'antichità c'era il *tam-tam*, un tipo di tamburo usato da alcuni popoli africani per diffondere un messaggio di villaggio in villaggio. Gli indiani d'America utilizzavano pelli di bufalo che, agitate sul fuoco, inviavano segnali di fumo a grandi distanze. Anche il codice Morse, usato alla fine dell'Ottocento per far comunicare le navi mediante luci lampeggianti, è stato ed è tuttora una forma importante di comunicazione senza fili. Al giorno d'oggi sono i telefoni cellulari a rappresentare il più diffuso esempio di comunicazione wireless.

L'arrivo dei personal computer negli anni Ottanta del secolo scorso e la necessità di organizzarsi in reti per il lavoro, ma anche per il divertimento, non poteva prescindere dai grandi vantaggi che le trasmissioni via *etere* garantiscono.
Le interfacce wireless sono in grado di utilizzare servizi di rete che consentono l'uso di tutti gli optional che Internet offre: dalla posta elettronica alla navigazione, dai motori di ricerca ai social network, dalle videoconferenze all'accesso alle basi di dati. E tutto questo da qualunque luogo: da casa, dal posto di lavoro o da ambienti pubblici.
Le conseguenze sono molto vantaggiose sia per l'utente privato sia per le aziende. Per esempio: chi viaggia per lavoro può rispondere a un messaggio di posta elettronica mentre aspetta di imbarcarsi su un aereo, mentre uno studente può studiare e fare ricerche con il proprio notebook in biblioteca.
Ma il maggior vantaggio consiste nella facilità con cui si possono estendere le reti aziendali senza dovere effettuare nuovi e costosi cablaggi. Inoltre c'è la comodità di non dover più allestire postazioni fisse di lavoro.

> Grazie alle reti wireless, non è più l'utente che si sposta laddove c'è il sistema di elaborazione, ma è il sistema di elaborazione che si sposta con l'utente.

Esistono molti tipi di sistemi di comunicazione wireless, ma la caratteristica comune è la comunicazione tra dispositivi computerizzati, cioè dispositivi dotati di capacità di elaborazione, memorizzazione e input/output. Questi dispositivi includono: tablet, smartphone, notebook, netbook, router e stampanti.
La maggior parte dei produttori ormai integra nei dispositivi di elaborazione la scheda di rete wireless e l'antenna.

Le reti wireless possono utilizzare onde radio o segnali infrarossi per comunicare attraverso l'etere e, così come le reti wired, possono essere classificate in base all'estensione dell'area fisica che sono in grado di coprire:

- **WPAN** (Wireless Personal Area Network)
- **WLAN** (Wireless Local Area Network)
- **WMAN** (Wireless Metropolitan Area Network)
- **WWAN** (Wireless Wide Area Network)

La distinzione non è netta, ma solo indicativa dei principali ambiti d'applicazione delle varie tecnologie (FIGURA 1).

1.2 WPAN

Le reti **PAN wireless** coprono il campo d'azione di una persona (10-15 metri) e sono adatte per reti domestiche o per piccoli uffici. Una WPAN, per esempio, potrebbe consentire di sincronizzare in modo wireless il proprio tablet o smartphone con un computer portatile per uno scambio di dati. Oppure l'installazione di periferiche come una stampante.

Uno dei campi nei quali più si vanno diffondendo le WPAN è la domotica.
Il termine **domotica** (anche nota come *home automation*), indica la disciplina che si occupa delle tecnologie atte a migliorare la qualità della vita nelle case, creando le cosiddette **case intelligenti**.
L'obbiettivo è l'integrazione dei dispositivi di controllo e trasduzione e dei sistemi di interconnessione (*sensor networking*) che si trovano nelle abitazioni.

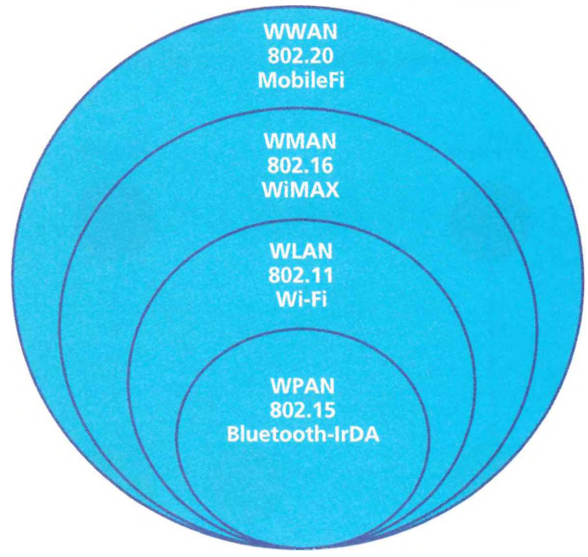


FIGURA 1 Classificazione delle wireless network

BLUETOOTH

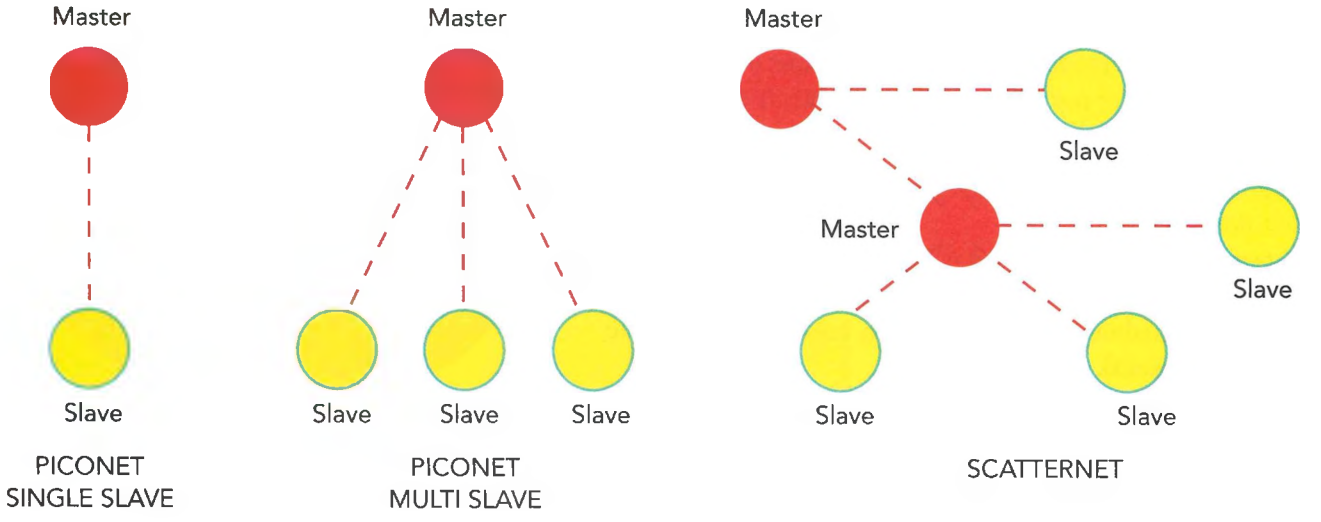
La maggior parte delle WPAN utilizza le **onde radio** per trasferire le informazioni attraverso l'etere. Per esempio, la specifica **Bluetooth** (FIGURA 2) definisce una PAN wireless nella banda di frequenza libera **ISM** (frequenze radio assegnate per scopi industriali, scientifici e medici) a 2.4 GHz e una velocità di trasmissione massima di 2 Mbps.

FIGURA 2 Logo Bluetooth

Questa tecnologia nasce alla fine degli anni Novanta del secolo scorso a opera di un consorzio guidato dalla Ericsson.
Bluetooth è adatto ai dispositivi di piccole dimensioni, a corto raggio, a basso consumo e poco costosi e la sua specifica è nello standard IEEE 802.15 per le WPAN.
I dispositivi compatibili che rispettano gli standard del Bluetooth possono, in qualità di Short Range Devices (SRD), operare **senza restrizioni a livello mondiale** in questa banda di frequenze.
Una connessione può essere avviata da qualunque dispositivo che assume il ruolo di **Master** (padrone) rispetto a uno **Slave** (schiavo, ossia i dispositivi connessi), creando una cosiddetta rete Bluetooth **piconet**. I dispositivi che vogliono collegarsi a una piconet ascoltano, a intervalli di 2,56 secondi, il segnale del Master. La connessione viene generalmente stabilita nel giro di 1,28 secondi. La connessione di due o più dispositivi tramite Bluetooth viene chiamata anche **pairing** (accoppiamento).
L'accoppiamento avviene, a seconda del dispositivo, tramite un software specifico, attivato da una casella di controllo o un pulsante, contraddistinti dal simbolo del Bluetooth. La connessione deve in seguito essere autorizzata mediante un **PIN** che viene visualizzato sullo schermo del dispositivo Slave o è riportato nel rispettivo manuale.
Il dispositivo accoppiato viene salvato in una lista e si connette automaticamente non appena entra nel raggio della piconet, purché il Bluetooth sia attivato.
La piconet è costituita da un massimo di **8 dispositivi Bluetooth attivi** (FIGURA 3). Un dispositivo Bluetooth può partecipare contemporaneamente a più piconet in qualità di Slave, ma solo in una come Master. Fino a **10 piconet** formano una cosiddetta

scatternet. Tutti i dispositivi all'interno di questa rete possono entrare in contatto con gli altri, tuttavia ne risente la velocità di trasmissione dei dati.

FIGURA 3 Piconet e scatternet



Per comunicare attraverso il Bluetooth, un dispositivo deve disporre di un **software specifico di controllo del trasferimento dati** e un particolare **chip Bluetooth** dotato di un'unità trasmittente e una ricevente installate nei componenti hardware. Tra i produttori più conosciuti di questi chip figurano Atheros, Nordic Semiconductor e Toshiba.

Bluetooth 5.0 (seguita dalle release 5.1 e 5.2) è l'ultima versione dello standard di comunicazione wireless Bluetooth. Viene comunemente utilizzato per cuffie wireless e altri dispositivi audio, oltre a tastiere, mouse e controller wireless. Il Bluetooth viene anche utilizzato per la comunicazione tra vari dispositivi di casa smart e Internet of Things (IoT).
I principali vantaggi di Bluetooth 5.0 sono una maggiore velocità e una maggiore portata.
Con Bluetooth 5.0, i dispositivi possono utilizzare velocità di trasferimento dati fino a 2 Mbps, il doppio rispetto a Bluetooth 4.2. I dispositivi possono anche comunicare su distanze fino a 240 metri, ovvero 4 volte i 60 metri consentiti da Bluetooth 4.2. Questi miglioramenti si applicano a Bluetooth Low Energy, garantendo che i dispositivi possano trarne vantaggio mentre risparmiano energia.

IrDA

Altre WPAN utilizzano **segnali infrarossi** invece che onde radio per trasferire le informazioni da un dispositivo a un altro.
IrDA (**Infra**red **D**ata **A**ssociation) è una organizzazione no-profit di produttori elettronici, costituita nel 1994, che definisce le specifiche fisiche dei protocolli di comunicazione che fanno uso della radiazione infrarossa per la trasmissione wireless a breve distanza dei dati.
La specifica **IrDA** definisce una tecnologia di interconnessione dati tramite infrarossi, di tipo bidirezionale, point-to-point, tra dispositivi posizionati in visibilità reciproca **LoS** (Line of Sight), con range ridotto (1-2 metri).

Nei dispositivi più lenti, la connessione avviene a 9.600 bps. Nei notebook è possibile avere normalmente 115.200 bps (modalità IrDA *base*) ottimizzabile fino a 4 Mbps (modalità IrDA *fast*). Quando la comunicazione avviene tra due dispositivi con diversa velocità massima, lo standard prevede che la velocità effettiva venga negoziata direttamente tra gli apparecchi all'inizio della connessione, sincronizzandola su quella inferiore.

Il vantaggio degli infrarossi è la mancanza di interferenze radio. Per contro, la necessità del contatto visivo tra i dispositivi limita le possibilità di posizionamento dei dispositivi stessi. Un pannello divisorio di un ufficio, per esempio, è sufficiente a bloccare il segnale. Per questo motivo, i raggi infrarossi vengono soprattutto utilizzati per connettere via etere tastiere e mouse con personal computer.
Il Bluetooth, che come detto è uno standard di trasmissione a onde radio, ha sostituito la trasmissione a infrarossi su diversi dispositivi.

1.3 WLAN

Le **LAN wireless** sono simili alle tradizionali LAN Ethernet cablate sia per prestazioni e costi sia per funzionamento e componenti utilizzate. Di fatto, anche i protocolli LAN wireless sono analoghi ai protocolli LAN Ethernet e soprattutto i formati sono completamente compatibili tra loro. Questo rende facile estendere una rete cablata preesistente con componenti wireless.
Lo standard più diffuso per le WLAN è l'IEEE 802.11. Le ultime versioni in commercio sono la 802.11g (a 2,4 GHz), la 802.11n (a 2,4 GHz e a 5 GHz) e la 802.11ac (a 5 GHz).
La FIGURA 4 riassume le velocità (teoriche) dei 3 standard.

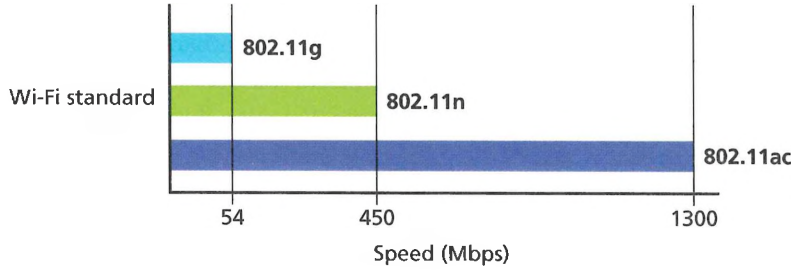


FIGURA 4 Confronto tra le velocità degli standard 802.11

LABORATORIO ONLINE

WINDOWS: CONFIGURARE UNA WIRELESS DOMESTICA

In questo Laboratorio viene spiegato come configurare una WLAN domestica che consenta di mettere in rete tutti i dispositivi di casa.

Ricordiamo che i dispositivi che costituiscono le reti LAN wireless sono:

- i **Wireless Terminal** (WT): sono dispositivi mobili (notebook, smartphone, tablet, ecc.) dotati di interfaccia 802.11, integrata o su schede PCMCIA o USB, oppure fissi (PC) con schede PCI o adattatori USB;
- gli **Access Point** (AP): hanno un doppio uso, possono essere bridge che collegano la parte cablata (wired) con la parte wireless oppure consentire ai WT di collegarsi alla rete wireless (e agire quindi da gateway).

#prendinota

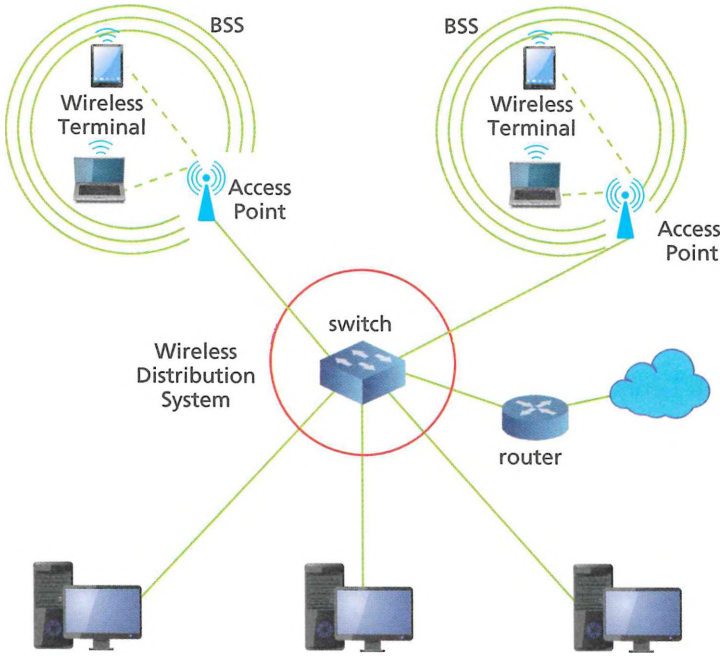
Nella maggior parte delle configurazioni, gli access point hanno un lato cablato che li collega agli switch e quindi al router della LAN aziendale per la connessione a Internet.

L'insieme formato dall'access point e dalle stazioni poste nella sua zona di copertura è detto **Basic Service Set (BSS)**, ovvero **insieme di servizi di base**, e costituisce una **cella**. Ogni BSS è identificato da un BSS-ID, un identificativo di 6 byte (48 bit). Nella cosiddetta modalità **infrastruttura** (di default dallo standard 802.11b in poi), nella quale i client senza fili sono connessi a un punto di accesso, il BSS-ID corrisponde all'indirizzo MAC del punto di accesso.

È possibile inoltre collegare più AP alla rete cablata o tra loro (*roaming*) creando un **Wireless Distribution System**. Gli AP in questi casi funzionano come un bridge tra BSS e Wireless Distribution System.
Due o più BSS collegati tra loro da un Wireless Distribution System costituiscono un **ESS (Extended Service Set)**. L'ESS appare come una unica WLAN (FIGURA 5).

All'interno di un ESS, i diversi BSS fisicamente possono essere posizionati secondo diversi criteri:

FIGURA 5 Rete WLAN aziendale (ESS) con parte cablata e infrastruttura wireless



- **BSS parzialmente sovrapposti**: permettono di fornire una copertura continua;
- **BSS fisicamente disgiunti**;
- **BSS co-locati** (diversi BSS nella stessa area): possono fornire una ridondanza alla rete o permettere prestazioni superiori.

La sempre maggior diffusione dei dispositivi mobili collegati in reti wireless ha posto il problema di come consentire la permanenza della connessione a fronte di spostamenti che portano il dispositivo fuori dal raggio d'azione di un access point. Lo standard 802.11 gestisce la mobilità delle stazioni distinguendo 3 tipi di transizioni:

- **transizione statica**: la stazione è immobile o si sposta solo entro l'area di un singolo BSS;
- **transizione tra BSS**: la stazione si sposta tra due diversi BSS, parzialmente sovrapposti, appartenenti allo stesso ESS (la connessione resta attiva e non c'è cambiamento di indirizzo IP);
- **transizione tra ESS**: la stazione si sposta tra BSS appartenenti a due ESS diversi.

In quest'ultimo caso la connessione attiva viene chiusa in quanto ci troviamo di fronte al passaggio da una WLAN a un'altra. Appena entrati nel raggio d'azione della nuova WLAN occorrerà aprire una nuova connessione con conseguente assegnazione di un nuovo indirizzo IP.
Nelle reti domestiche, l'access point funge anche da router-switch, spesso dotato anche di funzionalità firewall, e viene collegato a una connessione Internet a banda larga, per esempio ADSL. La normale portata di un router WLAN è sufficiente a coprire un appartamento, una casa (anche su due piani) o un ufficio.

Un altro scenario importante è quello rappresentato da ospedali, magazzini o ristoranti che vogliano offrire l'accesso a un database centrale ai propri dipendenti mediante dispositivi mobili come palmari o tablet: un magazziniere potrà aggiornare l'inventario ed effettuare un nuovo ordine direttamente dal magazzino e un cameriere potrà trasmettere le ordinazioni in cucina riducendo il tempo di attesa dei clienti. Un medico può richiedere un prelievo al laboratorio tramite un dispositivo mobile e, da questo, vedere il referto appena pronto. Una rete wireless connessa al database contenente le informazioni mediche dei pazienti aumenta la velocità e l'efficacia dell'assistenza sanitaria.

L'utilizzo di una periferica mobile che trasmetta i dati raccolti, attraverso una connessione wireless, a un database centralizzato garantisce tempestività e assicura maggior precisione.

La configurazione di un access point in una rete aziendale (Figura 5) o domestica (FIGURA 6) prevede l'impostazione di una serie di parametri.

- **SSID** (Service Set Identifier): serve ad assegnare un nome alla WLAN affinché gli utenti possano identificarla. L'access point può essere configurato per trasmettere in broadcast e in continuazione con l'SSID attraverso un frame periodico detto **beacon**. In questo modo, i wireless terminal sono in grado di rilevare l'elenco delle reti wireless esistenti nel loro raggio d'azione. Non c'è una corrispondenza biunivoca tra access point e SSID: è normale che più access point condividano lo stesso SSID se forniscono accesso alla stessa rete (tipico delle reti aziendali come in figura 4), ma è anche possibile che uno stesso access point si presenti con più SSID, se fornisce accesso a diverse reti. Disabilitando il broadcast di un SSID, è possibile nascondere una rete, cioè far sì che il suo nome non appaia negli elenchi delle reti disponibili. La rete resta comunque individuabile.
- **Potenza**: la normativa tecnica ETS 300-328 dell'**#ETSI** impone di irradiare segnali con una **EIRP** (Effective Isotropic Radiated Power) non superiore a 100 mW per la banda a 2,4 GHz e 1 W per la banda a 5 GHz. La EIRP è la potenza isotropica effettiva irradiata (isotropica significa uguale in tutte le direzioni), ovvero la potenza effettivamente emessa dall'antenna, somma della potenza dell'access point e del **guadagno dell'antenna**.
- **Canale**: si può impostare l'access point affinché lavori su uno qualsiasi dei canali disponibili compresi tra 1 e 13. Quando si installa un solo access point, il canale scelto non ha importanza. Se invece si installano più access point in una WLAN o se due WLAN vicine hanno una portata che sovrappone i rispettivi raggi d'azione, allora bisogna applicare la **regola del 5** che impone di selezionare canali distanti 5 (per esempio 1-6-11).
- **Crittografia**: lo standard di crittografia e di autenticazione di 802.11 è la WEP (Wired Equivalent Privacy). È necessario attivarla come livello minimo di sicurezza (al problema fondamentale della sicurezza nelle reti wireless sarà interamente dedicata la Lezione 3). Si deve assegnare una chiave di crittografia a ogni utente per collegarsi all'access point con dati crittografati. Le chiavi standard sono da 10 cifre esadecimali (40 bit) o da 26 cifre esadecimali (104 bit) corrispondenti alla crittografia rispettivamente a 64 o 128 bit per via dell'aggiunta, in entrambi i casi, di un vettore d'inizializzazione a 24 bit.
- **Incapsulamento**: se l'access point è anche router, occorre settare il protocollo per il trasporto dei frame. Gli standard più usati sono PPPoA (Point-to-Point Protocol over ATM - RFC 2364) e PPPoE (Point-to-Point Protocol over Ethernet - RFC 2516). Oggi quasi tutti gli apparati dei gestori dei servizi Internet (ISP) sono configurati in modalità *autosense* così da riconoscere automaticamente il metodo di incapsulamento impostato sul modem/router dell'utente.
- **NAT** e **DHCP**: sempre in caso di access point che sia anche router-switch, occorre attivare la funzione NAT ed eventualmente il protocollo DHCP.

#techwords

L'**ETSI** (European Telecommunications Standards Institute) è un organismo internazionale, indipendente e senza fini di lucro, ufficialmente responsabile della definizione e dell'emissione di standard nel campo delle telecomunicazioni in Europa.

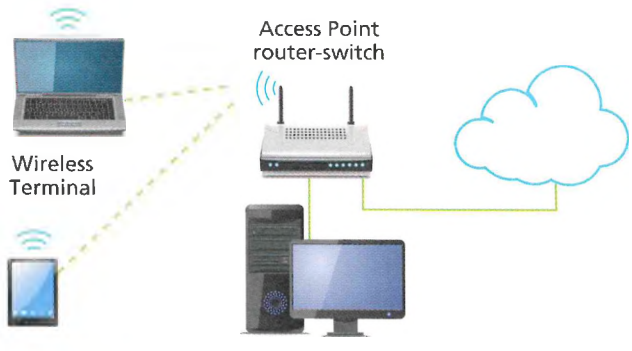


FIGURA 6 Rete WLAN domestica con parte cablata e parte wireless

#prendinota

Un'altra tecnologia WLAN è la HIPERLAN (*HIgh PErformance Radio LAN*). Si tratta di uno standard sviluppato dalla ETSI che funziona alla velocità massima di 54Mbps nella banda a 5GHz. Rappresenta la risposta europea allo standard americano IEEE 802.11. I prodotti presenti sul mercato con questa tecnologia hanno generalmente costi superiori a quelli Wi-Fi e la loro diffusione risulta piuttosto limitata.

Dal punto di vista della sicurezza, anche se non efficace come un firewall, un NAT nasconde gli host interni e non indirizza loro il traffico generico proveniente dall'esterno. Il DHCP (Dynamic Host Configuration Protocol), è un protocollo che prevede un'assegnazione centralizzata degli indirizzi IP, del gateway e dei DNS. L'access point che funge da router diventa un server DHCP, col compito di fornire gli indirizzi IP ai nodi che ne fanno richiesta e che sono definiti come client DHCP.

Oltre a WLAN aziendali e domestiche, esistono anche le **WLAN ad hoc**, note anche come **MANET** (Mobile Ad hoc NETwork). Si tratta di reti wireless realizzate in situazioni in cui non è possibile installare un access point. La modalità ad hoc consente alla scheda di rete 802.11 di operare in quello che lo standard definisce una configurazione di rete **Independent Basic Service Set (IBSS)**.
In modalità IBSS non ci sono access point e le varie schede di rete comunicano direttamente tra loro in modalità peer-to-peer (FIGURA 7).

FIGURA 7 WLAN ad hoc

Alcuni esempi applicativi delle WLAN ad hoc sono:
- operazioni di acquisizione dati su terreno inospitale;
- interventi militari in territorio nemico;
- pronto intervento in situazioni di emergenza (uragani, terremoti, ecc.).

1.4 WMAN

Un altro dominio di applicazione è quello delle **MAN wireless**, che consente di distribuire dati su di un agglomerato di case tramite una potente antenna. Questa soluzione fornisce un'alternativa al costoso *cablaggio dell'ultimo miglio*. Il gruppo di lavoro **IEEE 802.16** si occupa di questa architettura.
Solitamente le WMAN forniscono interconnessioni tra utenti fissi. Per esempio, un'azienda può collegare la sede centrale con un vicino centro di distribuzione utilizzando componenti wireless quando vi sono limitazioni del diritto d'accesso che vietano la posa dei cavi, o quando affittare linee esistenti risulta troppo costoso.

I **Wireless Internet Service Providers** (**WISP**) talvolta mettono a disposizione MAN wireless nelle città e nelle aree rurali.
La connessione può essere **point-to-point** o **point-to-multipoint**.
- Il collegamento **point-to-point** viene realizzato mediante una coppia di dispositivi che supportano la connettività fissa da un punto all'altro. Tale coppia di dispositivi è solitamente rappresentata da due bridge wireless. I bridge wireless hanno una porta cablata che li collega alla rete aziendale e una porta wireless che li collega a un'*antenna direzionale*.
- Il collegamento **point-to-multipoint** prevede invece un'*antenna centralizzata omnidirezionale* (per esempio posta in un edificio ubicato nel centro di una città) e una serie di antenne direzionali puntate verso l'antenna centrale (per esempio da una serie di edifici decentrati) come mostrato in FIGURA 8.

FIGURA 8 WMAN point-to-multipoint

Dallo standard IEEE 802.16 è nato il progetto **WiMAX Forum**, FIGURA 9 (WiMAX è acronimo di Worldwide Interoperability for Microwave Access): consorzio di imprese, con ruolo simile alla Wi-Fi Alliance per IEEE 802.11.
La trasmissione dei dati può avvenire secondo due differenti modalità. **Non-line-of-sight** su frequenze basse utilizzata in ambienti urbani, dove il segnale ha un'alta probabilità di essere schermato; il range va dai 2 GHz agli 11 GHz e il computer si connette alla rete WiMAX tramite piccole antenne (*dongle*) portatili da collegare direttamente al computer.
La seconda modalità operativa è **line-of-sight** su frequenze molto più alte, utilizzata in aree dove la probabilità che il segnale venga schermato sono molto basse; questa funziona con frequenze vicine ai 60 Ghz ed è ideale per coprire aree molto estese (una singola antenna può diffondere il proprio segnale fino a 50 km di distanza, per una copertura d'area di quasi 8.000 km^2) assicurandovi una velocità di circa 70 Mbps.

FIGURA 9 Logo del WiMAX Forum

1.5 WWAN

Le **WAN wireless** offrono applicazioni mobili che coprono vaste aree, come uno stato o un continente. La necessità di garantire una copertura ampia implica l'utilizzo di tecnologie diverse da quelle utilizzate per le altre reti. Queste tecnologie sono offerte a livello regionale e nazionale dai Wireless Internet Service Providers (WISP) che garantiscono la realizzazione di infrastrutture WWAN per fornire la connettività a grande raggio. Accordi di roaming tra gli operatori di telecomunicazioni permettono poi la connettività anche a livello globale. Pagando un solo provider, un utente può accedere a servizi Internet su una WWAN da qualsiasi luogo. I costi delle infrastrutture, benché piuttosto alti, possono essere suddivisi tra molti utenti garantendo costi di abbonamento relativamente bassi.
Lo svantaggio delle WWAN è la limitata disponibilità dello spettro in frequenza, che implica basse prestazioni e sicurezza limitata. La velocità di trasmissione è inferiore al Wi-Fi e si avvicina al WiMAX, siamo quindi nell'ordine dei Mbps. Le prestazioni aumentano utilizzando tecnologie di telefonia mobile.
Il vantaggio della WWAN è invece quello di consentire, per esempio, di controllare la posta elettronica mentre si è in viaggio, senza dover aspettare di arrivare in albergo per poter utilizzare la WLAN dall'hotspot Wi-Fi dell'albergo stesso.
Gli hotspot che offrono la connessione in Italia sono alcune migliaia. Uno dei più aggiornati motori di ricerca per hotspot è *http://www.hotspots-wifi.it*.
Nel 2017 nasce **WiFi·Italia·It** (FIGURA 10) l'applicazione per navigare gratuitamente sulle reti Wi-Fi italiane. Il progetto WiFi·Italia·It ha come obiettivo principale quello di permettere a cittadini e turisti, italiani e stranieri, di connettersi gratuitamente e in modo semplice a una rete wireless libera e diffusa su tutto il territorio nazionale.

#prendinota

La Wi-Fi Alliance è stata formata nel 1999 per guidare l'adozione di un unico standard per la banda larga senza fili nel mondo. Wi-Fi Alliance è inoltre proprietaria del trademark Wi-Fi che certifica l'interoperabilità di un dispositivo con lo standard wireless IEEE 802.11.

FIGURA 10 Logo di WiFi·Italia·It

FISSA LE CONOSCENZE

- Quali tipi di segnali utilizzano le reti wireless?
- Come si possono classificare le reti wireless in base all'estensione?
- Descrivi una ESS con parte cablata e infrastruttura wireless.
- Descrivi la modalità a infrastruttura e la modalità ad hoc.
- Quali sono i principali parametri che occorre configurare in un access point?
- Descrivi le connessioni point-to-point e point-to-multipoint.
- Che cos'è il progetto WiMAX?

2 LA SICUREZZA NELLE RETI WIRELESS

2.1 I principali rischi per la sicurezza

Garantire la sicurezza nelle reti wireless è di fondamentale importanza soprattutto perché i segnali si propagano attraverso un mezzo impossibile da isolare come l'aria. È quindi necessario che chi utilizza le reti wireless sia consapevole dei problemi e delle contromisure necessarie. In questa Lezione affronteremo i **rischi** a cui sono sottoposte le reti wireless e le tecniche per rafforzare la sicurezza mediante **crittografia** e **autenticazione**.

LEZIONE ONLINE

LA NORMATIVA SUL WIRELESS

Nel corso degli anni le norme per l'utilizzo del Wi-Fi nei locali pubblici (alberghi, stazioni, internet point, ecc.) hanno subito molte modifiche.
È necessario disporre di un sistema in grado di garantire l'inviolabilità della rete, preservare l'integrità dei dati personali raccolti e assicurare che i titolari della struttura pubblica non siano in alcun modo responsabili delle attività dei clienti.

SNIFFING

Si definisce sniffing l'attività di intercettazione passiva dei dati che transitano in una rete. Un hacker esperto, ma anche un intruso occasionale, può facilmente monitorare i pacchetti di dati wireless non protetti tramite appositi applicativi, detti **sniffer**, che oltre a intercettare e memorizzare il traffico offrono funzionalità di analisi del traffico stesso.
Lo sniffing può essere svolto sia per scopi legittimi (per esempio l'analisi e l'individuazione di congestioni su tratti di rete o di tentativi d'intrusione) sia per scopi illeciti (intercettazione fraudolenta di password, numeri di carte di credito o altre informazioni sensibili). Gli sniffer intercettano i singoli pacchetti, decodificano gli header dei vari livelli e ricostruiscono lo scambio di dati tra le applicazioni. Solo l'utilizzo di efficaci meccanismi di crittografia consente di mantenere la segretezza dei dati.

#techwords

Il **wardriving** è un'attività che consiste nell'intercettare reti Wi-Fi, girando in automobile, in bicicletta o a piedi, con un laptop, solitamente abbinato a un ricevitore GPS per individuare l'esatta posizione della rete trovata ed eventualmente pubblicarne le coordinate geografiche su un sito web.
I wardriver operano in maniera lecita se si limitano a trovare un access point e a registrarne la posizione.

ACCESSO NON AUTORIZZATO

Secondo la normativa italiana è illegale procurarsi l'accesso a una rete privata senza aver ottenuto esplicita autorizzazione. Alcuni **#wardriver** (che girano per le strade con attrezzatura minima) infrangono le scarse misure di sicurezza delle reti private, soprattutto quelle domestiche, per navigare gratis ad alta velocità. Se con un portatile si riesce a connettersi a una rete wireless, diventa possibile esplorare le risorse di qualsiasi altro portatile collegato alla medesima rete.
La tecnica più utilizzata (e più efficace) per accedere a una rete aziendale wireless senza autorizzazione è quella di servirsi di un **Access Point Rogue (APR)**, cioè un access point non autorizzato sulla rete. Per esempio, un dipendente che acquisti e installi un access point non autorizzato, privo di adeguata tecnica di crittografia, renderebbe la connessione alla rete aziendale non protetta rispetto a un hacker dotato di dispositivo wireless (FIGURA 11).

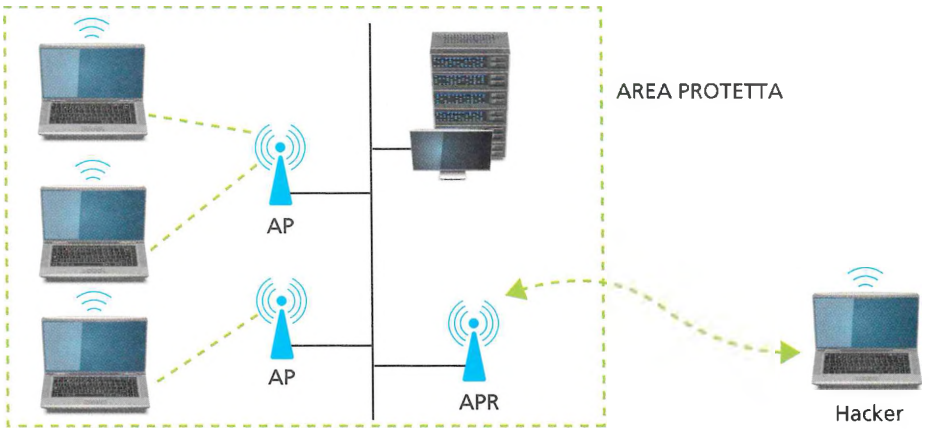


FIGURA 11 Rete aziendale con intrusione tramite APR

Il problema degli APR non riguarda solo le reti wireless. È infatti possibile collegare un APR a qualsiasi rete Ethernet cablata e rendere facile l'accesso dall'esterno alla rete aziendale. Per questo motivo ogni società deve verificare costantemente l'eventuale presenza di APR nella propria rete.
Per ostacolare l'accesso non autorizzato, è opportuno prevedere un meccanismo di autenticazione reciproca tra i wireless terminal e gli access point della rete.
Inoltre, gli access point devono eseguire l'autenticazione con gli switch, in modo da impedire la connessione di un APR.

SOSTITUZIONE DEL SID (SECURITY IDENTIFIER): SPOOFING

Nell'ambito di una rete, a ogni account utente viene assegnato un **identificativo SID univoco** a cui vengono associate, dall'amministratore della rete, autorizzazioni ben precise. Per un hacker è possibile effettuare la sostituzione del SID posizionando un **dispositivo intermedio WTR** (Wireless Terminal Rogue) tra un utente della rete wireless e un access point della medesima rete (FIGURA 12). Questo tipo di attacco, per esempio, può sfruttare il protocollo ARP mettendo in atto lo **spoofing ARP**.

#techwords

Lo **spoofing** è un tipo di attacco informatico in cui si realizza la falsificazione dell'identità (spoof). Lo spoofing può avvenire in qualunque livello della pila ISO/OSI.

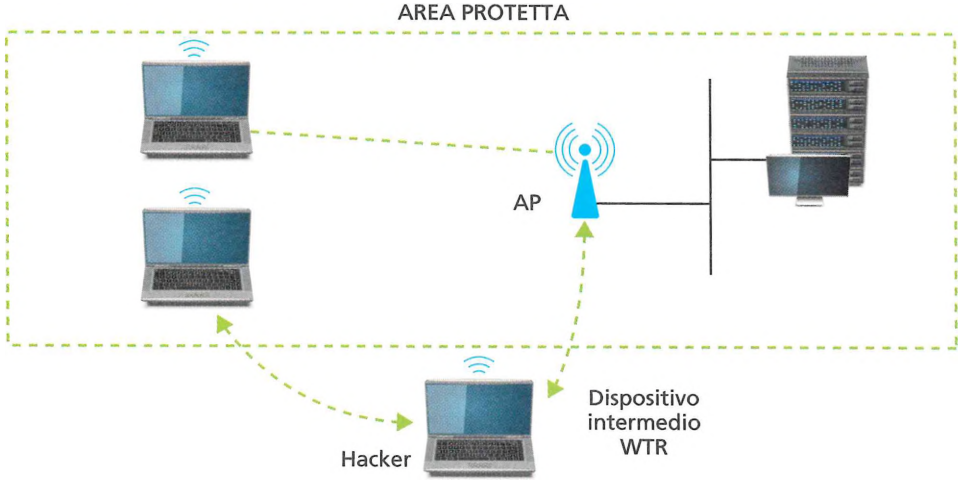


FIGURA 12 Rete aziendale con intrusione tramite dispositivo intermedio WTR

Per effettuare lo **spoofing** ARP, è sufficiente che un dispositivo rogue invii all'AP della rete un pacchetto ARP contenente il proprio indirizzo MAC e l'indirizzo IP del wireless terminal a cui vuole sostituirsi.

Questo fa sì che tutte le stazioni della rete aggiornino automaticamente le loro cache ARP con la mappatura fasulla. Il risultato sarà che tali stazioni invieranno tranquillamente i loro pacchetti al rogue credendo di inviarli a un nodo sicuro della rete.

Per evitare questi tipi di attacchi in una rete wireless si può usare il protocollo **SARP** (**Secure ARP**), che fornisce un tunnel protetto tra ogni client e l'access point o router wireless.
Questo protocollo permette all'access point posto a un'estremità del tunnel di ignorare ogni risposta non associata al client posto esattamente all'altra estremità del tunnel. In pratica, solo le risposte mediante pacchetti ARP autorizzati consentono di modificare la cache ARP del destinatario.

L'utilizzo di SARP libera dallo spoofing ma, necessitando dell'installazione di software particolari su ogni client, non è adatto agli hotspot pubblici. Le aziende, invece, possono facilmente installare SARP.

ATTACCO DOS (DENIAL OF SERVICE)

#prendinota

In generale il DoS è un attacco di tipo *brute force* (forza bruta) in cui un numero elevatissimo di pacchetti viene inviato, per esempio, a un server web, FTP o di posta elettronica con lo scopo di impedire agli utenti l'accesso e l'utilizzo di quei servizi. Per rendere più efficace l'attacco, vengono utilizzati molti computer inconsapevoli, detti zombie, sui quali precedentemente è stato caricato un programma appositamente creato e che si attiva a un comando del cracker creatore.

Si tratta di un attacco in grado di paralizzare o disattivare una rete wireless, rendendola indisponibile per un periodo di tempo indeterminato.
Nel caso delle reti wireless, oltre i comuni attacchi **brute force**, possono essere utilizzati dei forti segnali radio che sovrapponendosi ai segnali trasmessi rendono inutilizzabili gli AP e i wireless terminal. I protocolli IEEE 802.11 permettono al segnale dell'attacco DoS di accedere al supporto senza limiti di tempo.
Per contro, un simile tipo di attacco è piuttosto rischioso per chi lo mette in atto poiché la fonte è di facile identificazione, utilizzando gli strumenti di rilevazione forniti con gli analizzatori di rete.
In generale è possibile proteggere una LAN wireless dagli attacchi DoS proteggendo l'edificio dai segnali radio esterni mediante una serie di accorgimenti:

- verificare che le travi metalliche nelle pareti interne siano state messe a terra;
- montare finestre con isolamento termico basato su film in rame o metallici;
- utilizzare vetri oscurati al posto di veneziane o tende;
- utilizzare vernici a base metallica per le pareti interne ed esterne;
- indirizzare le antenne direzionali degli AP verso l'interno;
- regolare la potenza dei trasmettitori allo scopo di limitare la dispersione.

Un attacco DoS può, in certi casi, essere **non intenzionale**. Per esempio, una rete wireless con standard 802.11g, funzionando in uno spettro radio piuttosto affollato (cellulari, microonde e Bluetooth), può essere soggetta a interferenze tanto forti da impedire il funzionamento della rete stessa.

Come abbiamo detto, per proteggersi dai rischi per la sicurezza occorre mettere in campo tecniche crittografiche e di autenticazione. Tali tecniche non sono esclusiva delle reti wireless, ma nelle reti wireless rappresentano un requisito imprescindibile. Vediamo le tecniche più utilizzate nelle reti wireless.

2.2 Crittografia

WEP (WIRED EQUIVALENT PRIVACY)

Il nome indica che questa tecnologia garantisce un livello di riservatezza pari a quello di una rete cablata. WEP è la tecnica di crittografia (a chiave simmetrica a flusso) e autenticazione di default dello standard 802.11, implementata a livello MAC, e viene supportata dalla maggior parte dei dispositivi mobili e access point in commercio.

Quando la WEP è attivata, viene crittografato il payload del frame da trasmettere utilizzando l'algoritmo di cifratura a flusso, a chiave simmetrica, **RC4** (Rivest Cipher, Cifratore di Rivest).

RC4 genera un flusso di bit pseudocasuali (**keystream**) mediante una S-box di 256 byte e due indici da 8 bit, generalmente identificati con le lettere *i* e *j* (FIGURA 13).

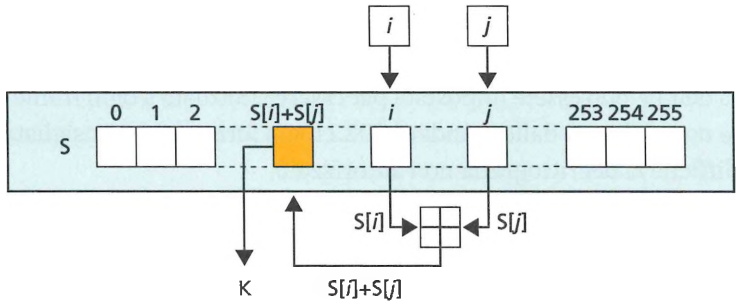


FIGURA 13 Algoritmo RC4

La chiave di cifratura è generalmente lunga da 40 a 256 bit ed è utilizzata per inizializzare l'S-box mediante una funzione di *scheduling* della chiave.
Il wireless terminal ricevente o l'access point, eseguono la decrittografia all'arrivo del frame, di conseguenza il segnale viaggia crittografato solo tra due nodi wireless 802.11. Quando entra nella parte cablata della rete, WEP non si applica più.
WEP si basa su una chiave di crittografia assegnata a ogni utente per collegarsi all'access point con dati crittografati. Le chiavi sono da 10 cifre esadecimali (40 bit) o da 26 esadecimali (104 bit) corrispondenti alla crittografia rispettivamente a 64 o 128 bit per via dell'aggiunta, in entrambi i casi, di un vettore d'inizializzazione (IV, Initialization Vector) a 24 bit.
WEP, essendo a **chiave simmetrica**, utilizza la **stessa chiave** per crittografare e decrittografare, di conseguenza ogni WT e ogni AP deve essere configurato con la stessa chiave.
La tecnica WEP con RC4 agisce in 5 passi (FIGURA 14).

1. L'IV a 24 bit, generato in modo casuale, verrà trasmesso in chiaro (non crittografato) nei primi byte del frame.
2. L'IV viene combinato con la chiave di cifratura segreta dell'utente creando una sequenza di chiavi.
3. Mediante tale sequenza, RC4 crea un flusso di bit pseudocasuali della stessa lunghezza del payload.
4. Il payload viene composto con il testo in chiaro e l'aggiunta dei bit di check calcolati con CRC-32 (Cyclic Redundancy Code a 32 bit).
5. Viene eseguita un'operazione di XOR tra keystream e payload ottenendo il frame crittografato da inviare.

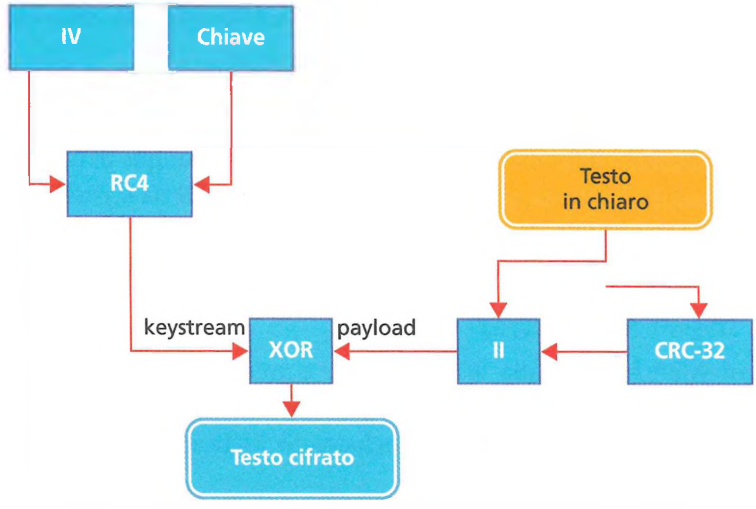


FIGURA 14 Tecnica WEP con algoritmo RC4

Essendo XOR simmetrico e l'IV in chiaro, il destinatario potrà procedere nello stesso modo per l'operazione di decrittografia.
La modifica dell'IV può essere impostata per essere effettuata a ogni frame trasmesso (operazione non richiesta dallo standard 802.11, ma fortemente consigliata) e questo rende più difficile la decrittografia non autorizzata.
La chiave di crittografia resta invece uguale per lunghi periodi (a volte addirittura anni) salvo interventi da parte dell'amministratore di rete. Il protocollo di per sé non ne prevede la modifica.

#prendinota

Nel 2005 è stato trovato un modo per violare una connessione wireless protetta con WEP in meno di un minuto!

La dimensione relativamente piccola dell'IV, la forte correlazione tra keystream e chiave e le chiavi statiche rendono WEP particolarmente vulnerabile.
In definitiva, WEP rappresenta il livello minimo di sicurezza, adeguato per reti domestiche o piccoli uffici.

TKIP (TEMPORAL KEY INTEGRITY PROTOCOL)

Si tratta di un'evoluzione del WEP (nota infatti anche come WEP2), volta a migliorarne il livello di vulnerabilità e standardizzata dall'IEEE 802.11i.
TKIP utilizza ancora l'RC4 per eseguire la crittografia, ma parte con una **chiave temporale** a 128 bit condivisa tra wireless terminal e access point, dunque ancora simmetrica. TKIP combina la chiave temporale con l'indirizzo MAC del wireless terminal e aggiunge un IV di altri 128 bit per creare la chiave di crittografia dei dati. La chiave temporale viene rigenerata a ogni pacchetto o a ogni burst (raffica) di pacchetti inviati. Si ha quindi quella che si definisce una **distribuzione dinamica** delle chiavi.
TKIP è più robusto di WEP, cioè più difficile da violare, sia per la temporalità della chiave, sia per la maggior lunghezza dell'IV.
Il passaggio da WEP a TKIP è facilmente realizzabile attraverso semplici patch del firmware dei wireless terminal e degli access point. Inoltre, dispositivi WEP possono comunque dialogare con dispositivi TKIP.

AES (ADVANCED ENCRYPTION STANDARD)

Oltre al protocollo TKIP, l'802.11i include lo standard AES come opzione alternativa che garantisce una crittografia molto più sicura: la maggior parte dei crittografi ritiene l'AES praticamente **indecifrabile** (uncrackable) grazie all'utilizzo dell'algoritmo di crittografia a blocchi **Rijndael** (dal nome degli ideatori Vincent Rijmen e Joan Daemen) al posto dell'RC4.
Il Ministero per il Commercio USA ha approvato l'utilizzo di AES come standard ufficiale del governo nel maggio 2002.
Lo svantaggio di AES è che richiede una grande capacità di elaborazione, capacità che non tutti gli access point in commercio possono supportare. In pratica, per funzionare AES necessita della presenza di un coprocessore, dunque di un hardware aggiuntivo. Quindi sia l'installazione di nuovi dispositivi AES sia il passaggio da WEP ad AES risulta essere parecchio costoso.
AES ha sostituito il famosissimo e usatissimo **DES** che abbiamo visto nell'Unità 1.

WPA (WI-FI PROTECTED ACCESS)

Lo standard WPA fornito dalla Wi-Fi Alliance è un aggiornamento WEP dotato di distribuzione dinamica delle chiavi e autenticazione reciproca.
La distribuzione dinamica è realizzata includendo TKIP in WPA e prende il nome di **WPA1**.

WPA2-Personal e **WPA2-Enterprise** sono due nuove versioni introdotte da Wi-Fi Alliance.
I WPA2-Personal utilizzano una PSK (passphrase key) di autenticazione condivisa mentre i WPA2-Enterprise utilizzano un server di autenticazione.
Nel luglio 2018 la Wi-Fi Alliance ha introdotto un programma di certificazione per il **WPA3**, con l'obbiettivo di fornire miglioramenti e nuove funzionalità di sicurezza tra cui il blocco degli attacchi basati su **#KRACK** (Key Reinstallation Attacks) a cui il protocollo WPA2 è risultato vulnerabile.

La Wi-Fi Alliance ha previsto due versioni anche di WPA3.

1. **WPA3-Personal** è ottimizzato per reti piccole (tipo reti domestiche) garantendo la sicurezza tramite il protocollo **SAE** (**Simultaneous Authentication of Equals**) che prevede una tecnica di scambio della password peer-to-peer (quindi diretta tra i dispositivi e non delegata a una certification authority) in grado di garantire una sicurezza equivalente a quella di una crittografia tramite certificato. Questo nuovo sistema di sicurezza sarà inoltre immune da attacchi brute force che tentano tutte le combinazioni di parole note. WPA3 personal è quindi sicuro anche se la password dell'utente risultasse essere troppo debole.
2. **WPA3-Enterprise** è invece pensato per grandi installazioni Wi-Fi e permette la cifratura a 192 bit, allineata alla suite CNSA (Commercial National Security Algorithm), che soddisferà le esigenze di tutela delle reti in ambito governativo, industriale e nel settore della difesa.

Il nuovo standard, pensato per durare anni, è chiaramente rivolto anche al futuro e al mondo dei dispositivi della Internet of Things (IoT). Per questo motivo è stato introdotto **Wi-Fi Easy Connect**, un nuovo protocollo di connessione per reti WPA2 e WPA3, che semplifica la connessione dei dispositivi molto essenziali, in particolar modo quelli senza display. Easy Connect utilizza un dispositivo terzo dotato di un'interfaccia più completa (come potrebbe essere uno smartphone o un tablet) per scannerizzare un codice di sicurezza **QR**.

La FIGURA 15 mostra la sequenza di passi per collegare al Wi-Fi svariati dispositivi mediante uno smartphone che funge da **configuratore**:

1. il configuratore effettua la registrazione alla rete Wi-Fi mediante la scannerizzazione del QR code dell'access point;
2. il configuratore effettua la registrazione e il **#provisioning** dei dispositivi client mediante la scannerizzazione del QR code di ciascuno;
3. i dispositivi si connettono senza difficoltà alla rete.

#techwords

KRACK: chi effettua questo attacco, si intromette, con una tecnica *man in the middle* (cioè si interpone nello scambio di messaggi), forzando a generare una chiave composta di soli 0. Questo rende facile decrittare i dati in arrivo e in partenza. E non importa come siano crittografati i dati una volta che viaggiano in rete, perché l'attacco li prende di mira prima che partano (nel caso il dispositivo mobile li trasmetta) o dopo il loro arrivo (nel caso il dispositivo mobile li riceva).

#techwords

Provisioning: processo mediante il quale un amministratore di sistema assegna risorse e privilegi agli utenti di una rete.

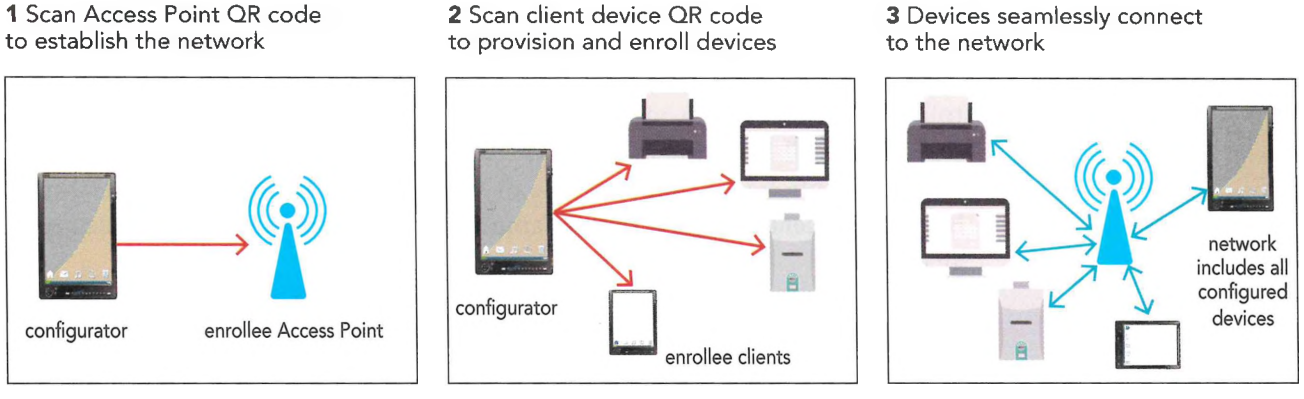


FIGURA 15 La sequenza Wi-Fi Easy Connect

Molte aziende hanno già annunciato pieno supporto al nuovo standard WPA3 per tutti i router e gli access point marchiati Wi-Fi CERTIFIED. Tra queste ci sono Cisco, HP, Broadcom e Qualcomm.

2.3 Autenticazione

L'autenticazione reciproca, tipica delle reti wireless, può risolvere parecchi problemi legati alla sicurezza, come per esempio gli attacchi DoS. È importante che l'autenticazione sia reciproca e non unilaterale per rendere più difficili le operazioni di intrusione.

> Ciò che si richiede per l'**autenticazione reciproca** è che il client riconosca la rete wireless come quella di appartenenza e che la rete riconosca il client come parte della rete stessa.

La prima e più semplice forma di riconoscimento è realizzata tramite l'SSID (Service Set Identifier) inviato in broadcast e in chiaro dall'access point.

L'access point consente l'accesso alla rete wireless solo ai wireless terminal client il cui SSID coincide con quello inviato dall'access point stesso. Ovviamente il fatto che l'SSID sia in chiaro rende facile il lavoro degli sniffer. Una volta scoperto l'SSID, diventa automatico potersi collegare alla rete, se non vi sono altri accorgimenti. Infatti, lo standard 802.11 applica di default una forma di autenticazione detta **OSA** (Open Systems Authentication) che fa sì che l'access point accolga qualunque richiesta che disponga dell'SSID corretto. Tutto ciò implica che affidarsi solo all'SSID non è assolutamente sufficiente.
Lo standard 802.11 consente anche un processo di autenticazione facoltativo più avanzato. Lo descriviamo in 4 passi:

1. il client invia un frame di richiesta di autenticazione;
2. l'access point risponde con un frame particolare detto challenge;
3. il client crittografa il challenge con chiave WEP comune che poi restituisce all'AP;
4. l'access point decrittografa il frame ricevuto sempre tramite la chiave comune e, se risulta uguale al challenge da lui stesso inviato, autentica il client.

Tutto ciò, però, prova solo che il client dispone della WEP corretta.
Un'altra forma di autenticazione prevede che l'amministratore della rete autorizzi l'accesso alla rete a un elenco di indirizzi MAC. Gli AP rifiuteranno i frame con un indirizzo MAC non in elenco. Il problema di questa tecnica è che la crittografia WEP non crittografa il campo del frame dedicato all'indirizzo MAC. Questo consente a uno sniffer che analizzi il traffico di individuare gli indirizzi MAC validi e di sostituirsi a un client quando questi non è collegato.
Il problema della vulnerabilità di tipo MAC è risolvibile mediante la protezione delle porte. L'autenticazione tramite elenco di MAC non è adatta a reti i cui utenti cambiano di frequente perché costringe l'amministratore al continuo aggiornamento degli elenchi.
Un miglioramento lo si ha utilizzando come metodo di autenticazione la WPA Enterprise, che come abbiamo visto nel paragrafo precedente, aggiunge un server di autenticazione per il riconoscimento dei wireless terminal.

La miglior forma di autenticazione possibile è ottenuta utilizzando lo standard **IEEE 802.1x**, il quale definisce uno schema architetturale nel quale possono essere usate varie metodologie; per questo una delle sue caratteristiche fondamentali è la **versatilità**. La metodologia più diffusa è quella che implementa il protocollo **EAP** (Extensible Authentication Protocol) su entrambi i supporti di rete: parte wireless e parte cablata. Con l'EAP, al wireless terminal che cerca di utilizzare la rete viene consentito solo il passaggio dei pacchetti **EAP**. Tale processo si avvale di un server di autenticazione, posizionato nella parte cablata della rete (FIGURA 16) come, per esempio, il **RADIUS** (Remote Authentication Dial-In User), per eseguire l'autenticazione.

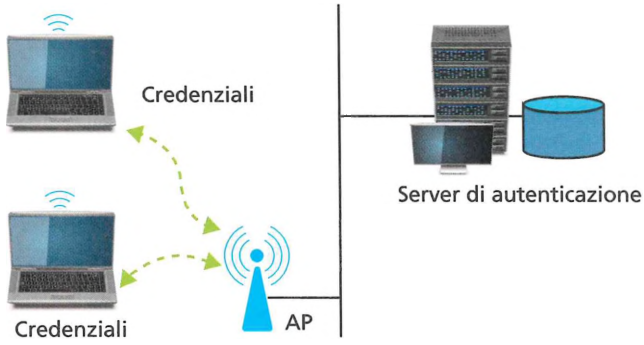


FIGURA 16 Rete aziendale con server di autenticazione

Ad autenticazione avvenuta, viene consentito il passaggio del traffico di rete.
Il server di autenticazione utilizza un algoritmo di autenticazione specifico per verificare l'identità del client.

Tale algoritmo non è espressamente definito dallo standard 802.1x. Occorre scegliere un tipo di EAP, come per esempio:

- EAP-TSL (Transport Layer Security)
- EAP-TTSL (Tunneled Transport Layer Security)
- LEAP (LigtweightEAP della Cisco)

Il software che supporta il tipo di EAP specifico si trova sul server di autenticazione e nel sistema operativo o in apposito software sui dispositivi client.

FISSA LE CONOSCENZE

- Quali sono i principali rischi per la sicurezza?
- Che cos'è un Access Point Rogue?
- Che cos'è lo spoofing?
- Quali sono le principali caratteristiche della crittografia WEP?
- Come si sviluppa un attacco DoS?
- Quali sono le due versioni WPA3 e cosa le caratterizza?
- Descrivi la forma di autenticazione IEEE 802.1x con protocollo EAP.

Case study
Sicurezza delle reti wireless

3 PACKET TRACER: RETE WIRELESS CON ROUTER WI-FI E SERVER AAA

In questa esercitazione di laboratorio realizzeremo con il simulatore Packet Tracer una rete wireless utilizzando un router Wi-Fi e un server di autenticazione.

esercizio

File sorgenti
Scarica il file

→ PROBLEMA

Realizzare una rete LAN wireless utilizzando diversi dispositivi Wi-Fi con protezione WPA2-Enterprise e configurando il servizio di autenticazione AAA (Authentication, Authorization, Accounting) su un server di rete.

→ ANALISI DEL PROBLEMA

Per realizzare la rete richiesta ci serviamo di un router Wi-Fi a cui collegare smartphone, tablet, laptop, PC e stampanti. Per garantire la riservatezza delle trasmissioni impostiamo la protezione WPA2-Enterprise dotata di distribuzione dinamica delle chiavi e autenticazione reciproca e che protegge gli accessi mediante la registrazione degli utenti su un server RADIUS (Remote Authentication Dial-In User Service) di autenticazione.

Serviranno quindi 3 passi:

- configurazione del router Wi-Fi;
- configurazione del servizio AAA su un server;
- configurazione dei dispositivi Wi-Fi con WPA2.

→ SVOLGIMENTO

Nella FIGURA 17 è mostrato un possibile scenario LAN wireless con 5 dispositivi mobili di vario tipo, un router wireless e un server per l'autenticazione.

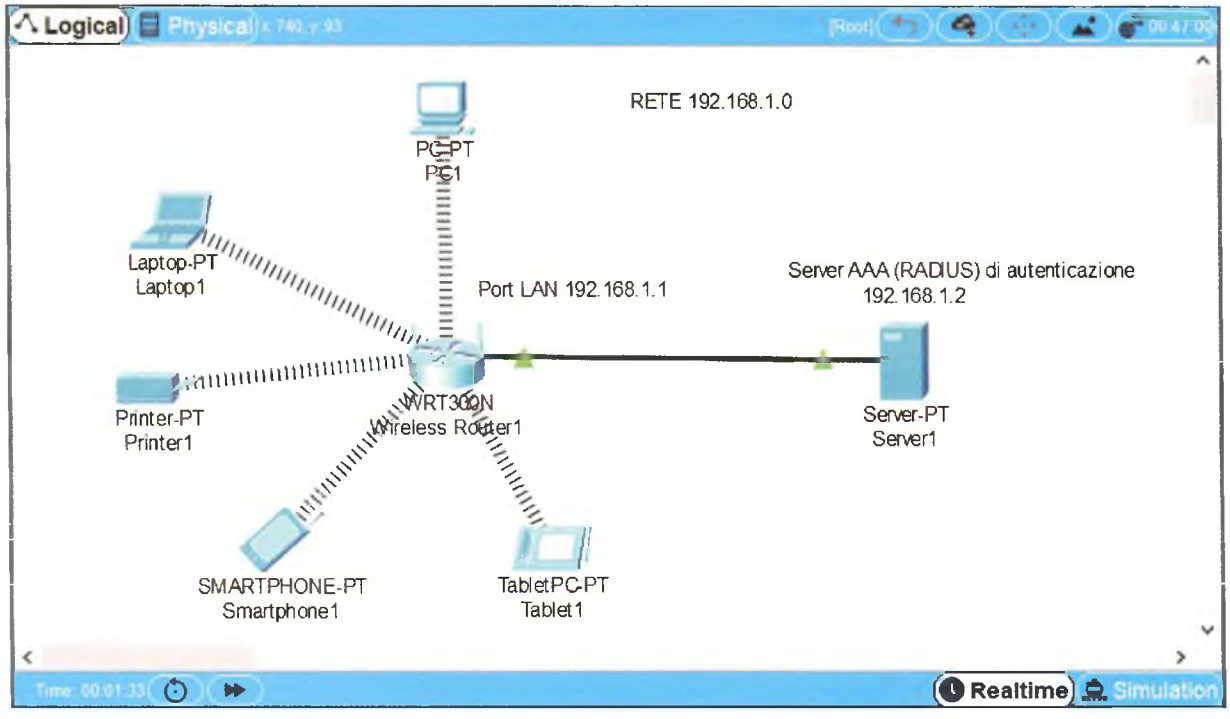


FIGURA 17 Scenario con router Wi-Fi e server AAA

PRIMO PASSO: configurazione del router Wi-Fi

Scegliamo il router **WRT300N** in grado di dialogare con PC, laptop e stampanti dotati di scheda della serie **300N**.
Clicchiamo sul router e selezioniamo la GUI (Graphic User Interface) che ci consente facilmente l'inserimento dei parametri e l'attivazione dei servizi necessari. In questa esercitazione ci occupiamo del lato LAN, quindi nella scheda **Setup → Basic Setup** tralasciamo l'Internet Setup e configuriamo l'interfaccia per il **Network Setup**.
Settiamo l'IP Address a **192.168.1.1** e abilitiamo il DHCP che di default è impostato al range **192.168.1.100 – 149**, quindi per un massimo di 50 utenti (FIGURA 18).

L'IP addressdel router wireless fungerà da Default Gateway per i dispositivi mobili collegati.

Terminato il setup, salvare la configurazione col bottone **Save Settings** in fondo alla scheda Setup.
Nella Figura 18 si possono vedere i valori di IPv4 e Subnet Mask assegnati al router Wi-Fi e l'abilitazione del servizio DHCP indispensabile per l'assegnamento degli IP ai dispositivi mobili.

#prendinota

Tutte le impostazioni del router vanno sempre salvate col **Save Settings** in fondo a ogni scheda aperta.

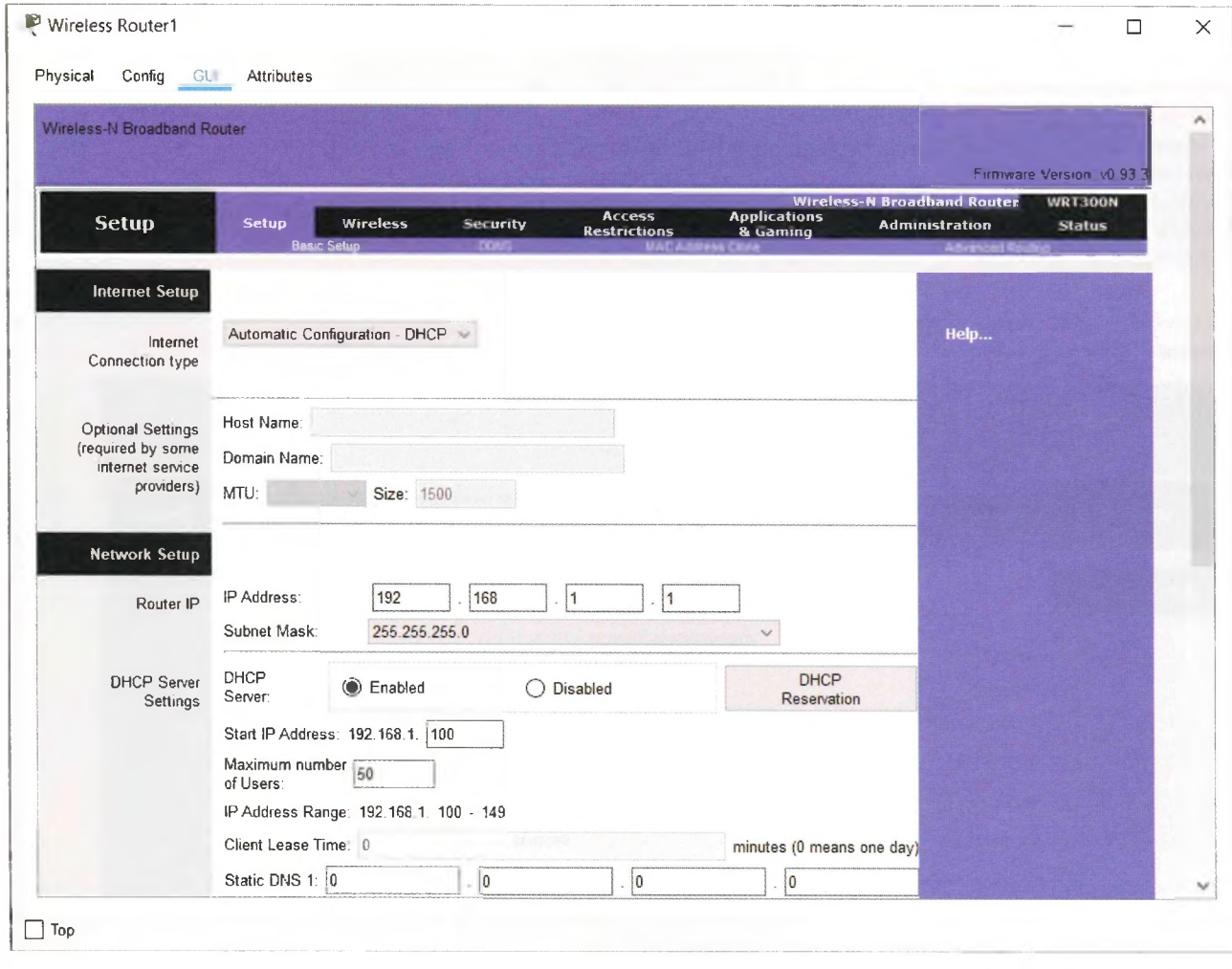


FIGURA 18 Setup LAN con DHCP sul Wireless Router1

Apriamo poi la scheda **Wireless → Basic Wireless Settings** impostando l'SSID con, per esempio, **Internetworking** (FIGURA 19) e salviamo con Save Settings.

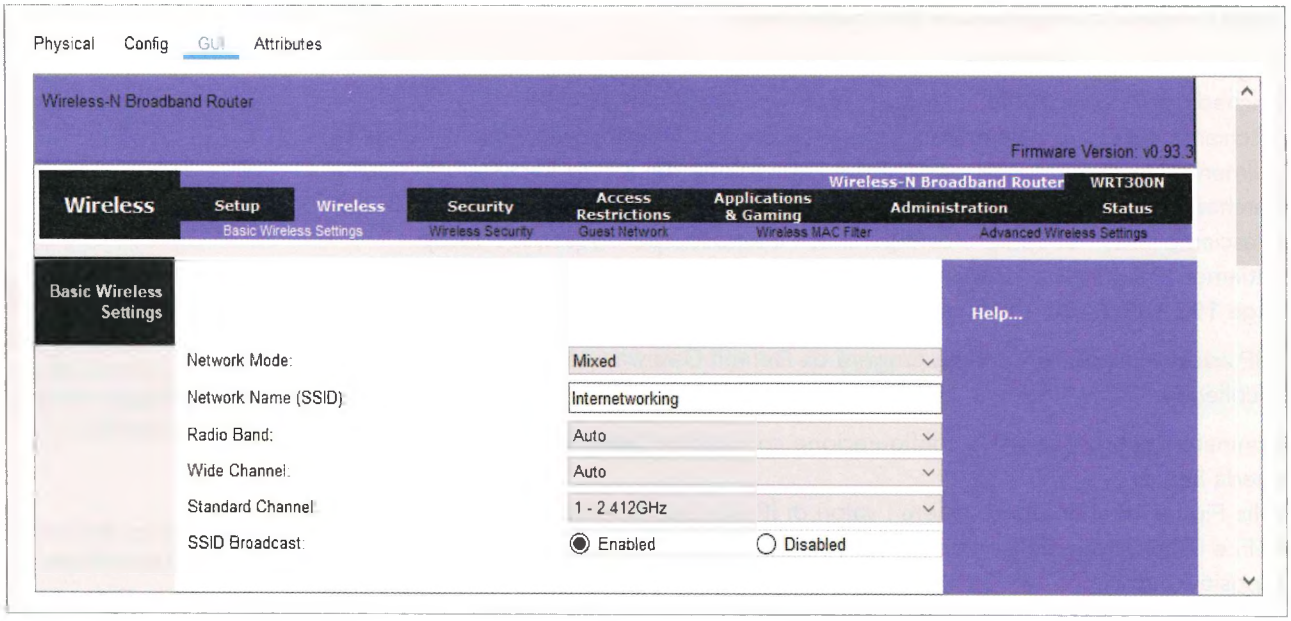


FIGURA 19 Configurazione dell'SSID sul Wireless Router1

#prendinota

La **Shared Secret** è la parola segreta che il router wireless condivide con il server RADIUS a garanzia dell'autenticazione degli accessi.

Apriamo poi la scheda **Wireless → Wireless Security** (FIGURA 20) impostando:

- la protezione **WPA2 Enterprise** con crittografia AES;
- l'indirizzo IP del server RADIUS: **192.168.1.2**;
- la Shared Secret con, per esempio, **ciscowpa2**.

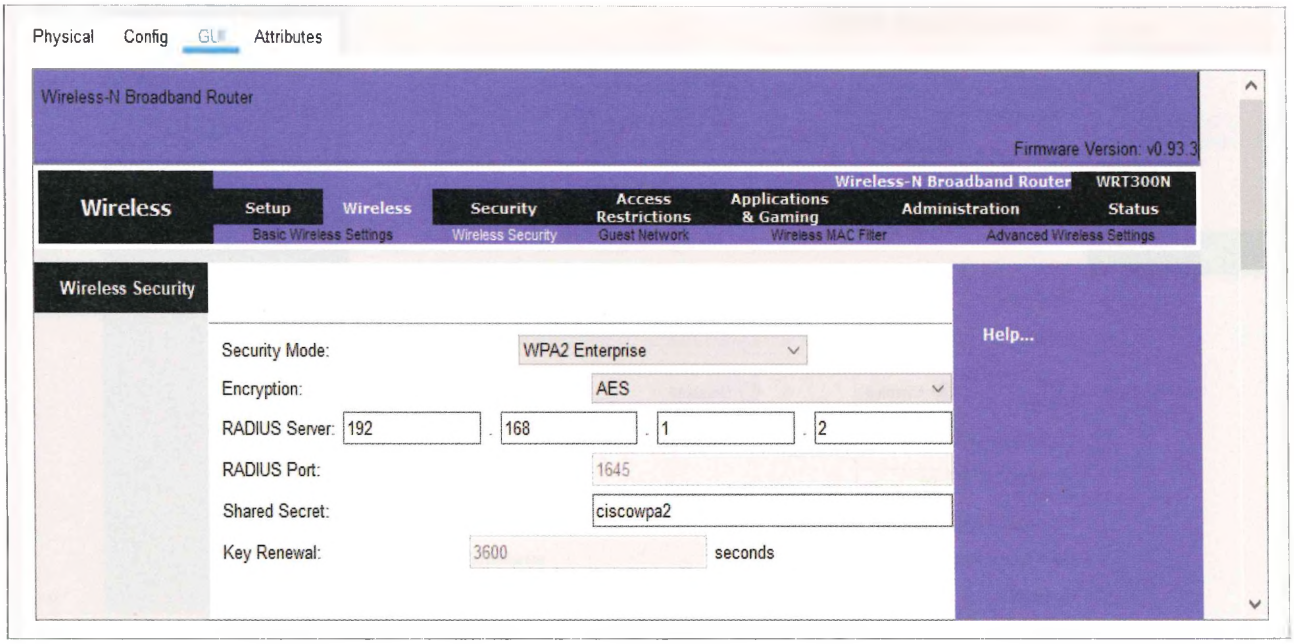


FIGURA 20 Configurazione del WPA2 Enterprise sul Wireless Router1

Dopo aver ancora una volta salvato con Save Settings, la configurazione del router è terminata.

SECONDO PASSO: configurazione del servizio AAA

Sul Server1 selezioniamo Services, il servizio AAA (FIGURA 21) e impostiamo nella **Network Configuration**:

- come Client Name l'SSID della rete wireless (**Internetworking**):
- come Client IP l'indirizzo IP del router wireless (**192.168.1.1**);
- come Secret la Shared Secret impostata sul router wireless (**ciscowpa2**);
- come Service Type selezioniamo RADIUS.

Con **ADD** aggiungiamo la configurazione creata.

Nella parte sottostante, **User Setup**, configuriamo le 5 utenze wireless previste. Per semplicità usiamo user1, user2, ..., user5 ripetuto sia come Username che come Password. Con **ADD** aggiungiamo le utenze create.

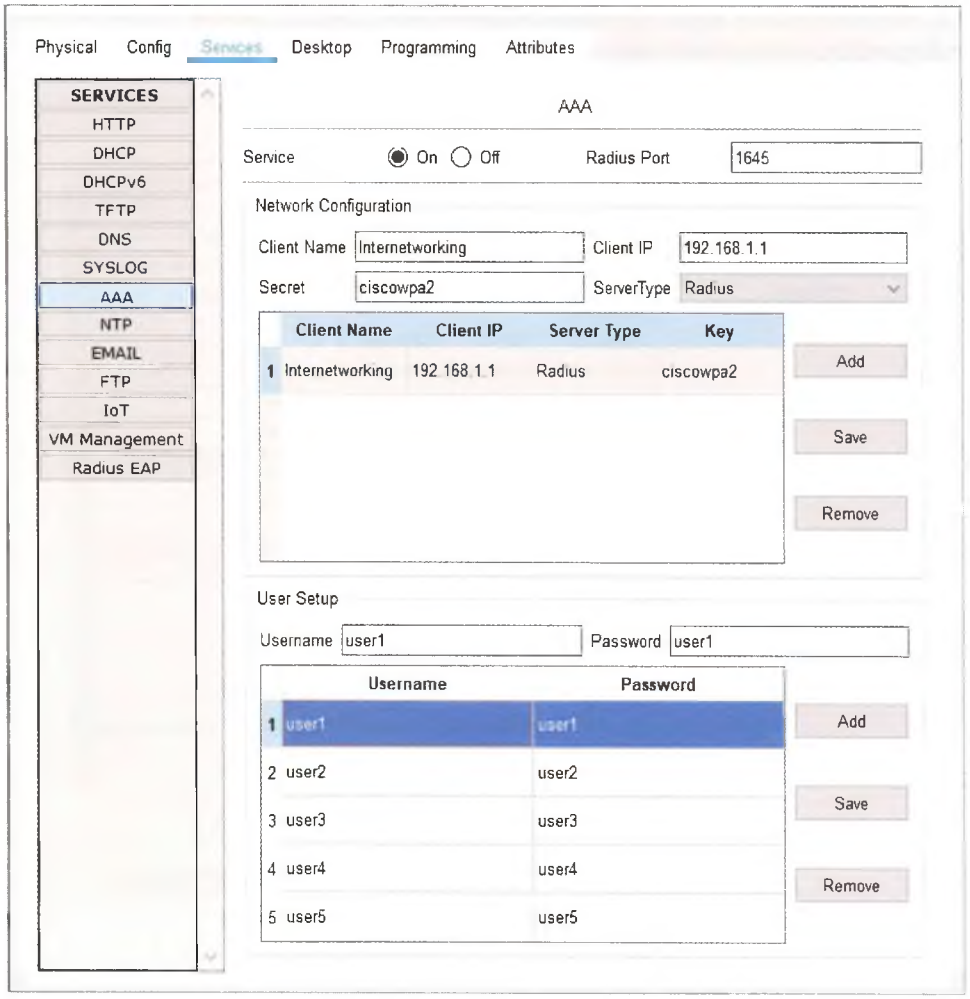


FIGURA 21 Configurazione del servizio AAA e delle utenze sul Server1

TERZO PASSO: configurazione dei dispositivi wireless

Dalla scheda Physical del PC1 spegniamo il dispositivo, quindi togliamo il modulo Ethernet e inseriamo il modulo wireless **WMP300N** per poi riaccendere PC1.

Questa operazione mette a disposizione la INTERFACE **Wireless0** al posto della FastEthernet0 nella scheda Config.

Selezioniamo l'interfaccia Wireless0 (FIGURA 22) e impostiamo:

- come SSID **Internetworking**;
- come metodo di Authentication la **WPA2** specificando User ID e Password dell'utente;
- come Encryption Type **AES**.

Nell'IP Configuration selezioniamo DHCP.

> Identiche operazioni vanno ripetute sul Laptop1 (inserendo il modulo WPC300N) e sulla Printer1 (inserendo il modulo WMP300N). Per gli smartphone e i tablet, già dotati di scheda wireless, si può passare subito alla configurazione.

Appena inserite le opportune credenziali di autenticazione sul dispositivo mobile, il router wireless (che fa da gateway) interrogherà il server AAA e in caso di risposta affermativa il collegamento Wi-Fi del dispositivo sarà attivato e protetto.
Per estendere la rete aggiungendogli una parte wired basterà cablare il router wireless collegandolo con qualsiasi apparato di rete (router, switch, ecc.).

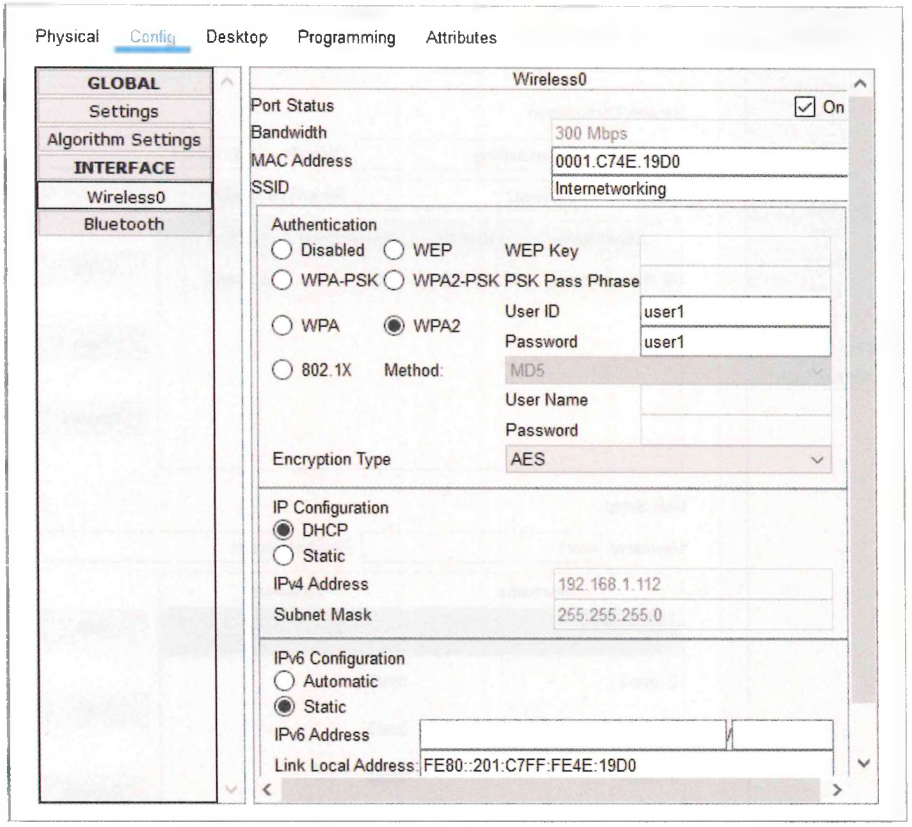


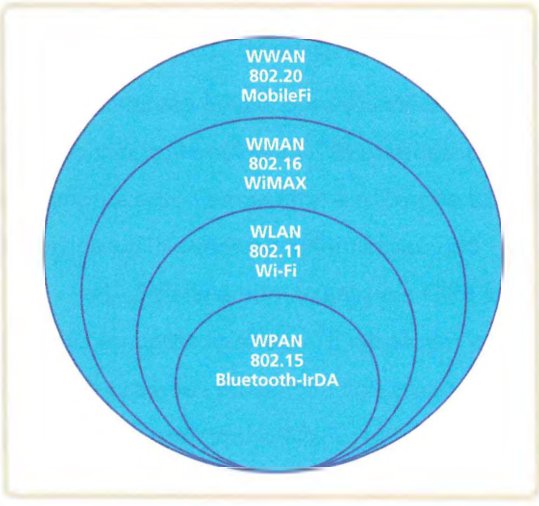
FIGURA 22 Configurazione del wireless sul PC1

FISSA LE CONOSCENZE

- Quali parametri vanno configurati sul router wireless?
- Come si configura il servizio AAA?
- Quali parametri vanno configurati sui dispositivi wireless?
- Quale modulo si può inserire per avere una porta wireless anziché una porta Ethernet?

DIDATTICA INCLUSIVA

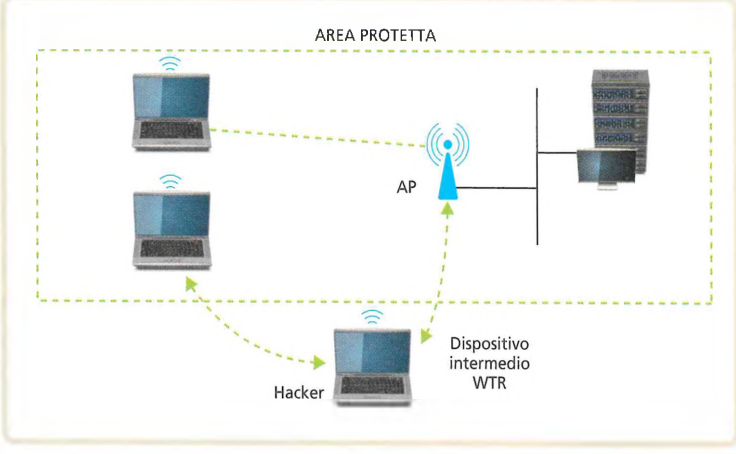
1 Scenari di reti senza fili



Le reti wireless, attraverso onde radio o segnali infrarossi, fanno comunicare dispositivi computerizzati, come notebook, tablet, smartphone, personal computer, router e stampanti.
La maggior parte dei produttori integra nei dispositivi schede di rete wireless e antenne.
Le reti wireless, come le reti cablate, sono classificate in base all'area fisica che possono coprire:

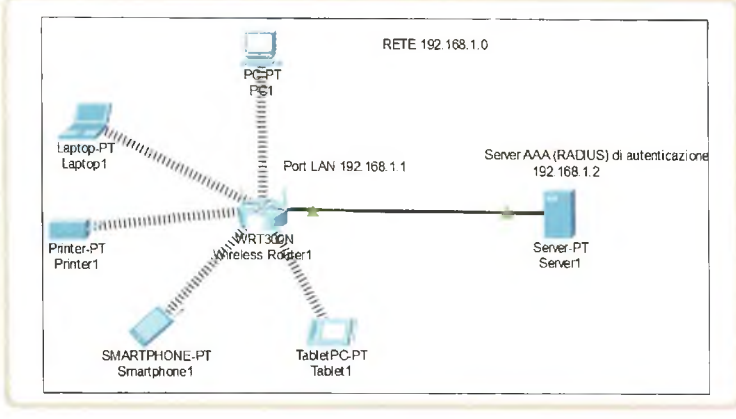
- WPAN (Wireless Personal Area Network);
- WLAN (Wireless Local Area Network);
- WMAN (Wireless Metropolitan Area Network);
- WWAN (Wireless Wide Area Network).

2 La sicurezza nelle reti wireless



Garantire la sicurezza nelle reti wireless è fondamentale soprattutto perché i segnali si propagano attraverso un mezzo impossibile da isolare e sono a disposizione di tutti.
I principali rischi per la sicurezza sono: sniffing, accesso non autorizzato, sostituzione del SID (Security IDentifier), attacco DoS (Denial of Service).
Le tecniche per rafforzare la sicurezza sono la crittografia e l'autenticazione.

3 Laboratorio Packet Tracer: reti wireless con router Wi-Fi e server AAA



In questa esercitazione di laboratorio abbiamo realizzato con il simulatore Packet Tracer una rete wireless utilizzando un router Wi-Fi e un server RADIUS per il servizio AAA di autenticazione con crittografia WPA2-Enterprise.

VERIFICA DI FINE UNITÀ

Test
Svolgi il **test interattivo**

Quali delle seguenti affermazioni sono vere (V) e quali false (F)?

1. Le WPAN coprono alcune centinaia di metri. V F
2. Lo standard 802.15 include la specifica Bluetooth. V F
3. La domotica è nota come home automation. V F
4. I BSS parzialmente sovrapposti garantiscono la copertura continua. V F
5. L'SSID assegna un nome alla WLAN. V F
6. La regola del 5 impone di scegliere canali distanti 5 tra i 13 a disposizione. V F
7. Un Acces Point consente l'accesso alla rete wireless a un solo dispositivo per volta. V F
8. Il WPA3-Personal è ottimizzato per reti piccole mentre il WPA3-Enterprise è pensato per grandi installazioni. V F

Domande a scelta multipla (una sola è la risposta esatta)

1. Lo sniffing è:
- A una tecnica di crittografia
- B un'attività di intercettazione
- C una falsificazione dell'identità
- D una tecnica di autenticazione

2. La WEP è:
- A una tecnica di crittografia
- B un'attività di intercettazione
- C una falsificazione dell'identità
- D una tecnica di autenticazione

3. Le reti wireless più estese sono:
- A WPAN
- B WLAN
- C WMAN
- D WWAN

4. Le bande ISM sono:
- A 2.4 GHz e 5 GHz
- B 24 GHz e 48 GHz
- C 100 GHz e 1.000 GHz
- D nessuna delle precedenti

5. Quale tra i seguenti è un parametro di configurazione di un access point?

A SSID B BSS C ESS D WISP

6. Quale tra i seguenti non è un rischio per la sicurezza?
- A Sniffing
- B Spoofing
- C DoS
- D Beacon

Ascolta le risposte

PREPARATI PER IL COLLOQUIO ORALE

1. LEZIONE 1 **Quali vantaggi offrono le reti wireless rispetto alle reti cablate?**
2. LEZIONE 1 **Cos'è una piconet? E una scatternet?**
3. LEZIONE 1 **Cos'è un BSS (Basic Service Set)? E un BSS-ID?**
4. LEZIONE 1 **Che cos'è l'IrDA e quale vantaggio hanno le trasmissioni a infrarossi?**
5. LEZIONE 2 **Che cosa occorre fare per rafforzare la sicurezza delle trasmissioni wireless?**
6. LEZIONE 2 **Descrivi lo sniffing.**
7. LEZIONE 2 **Descrivi i 5 passi della tecnica WEP con RC4.**
8. LEZIONE 2 **Che cosa si intende per autenticazione reciproca?**

IN ENGLISH, PLEASE

CLIL

Ascolta la **pronuncia del testo** e verifica la **traduzione**

ABSTRACT

Wireless Networks

Wireless communication over distances has been accomplished in numerous forms in human history. Naturally, mobile telephones are nowadays the most widespread example of wireless communication. Wireless networks can use radio waves or infrared signals to communicate through the air. There are different types of wireless networks available: WPANs are used to convey information over short distances. WLANs allow users in a local area to form a network or gain access to the Internet. WMANs allow the connection of multiple networks in a metropolitan area. WWANs operate over large area, such as a city, via multiple antenna sites managed by an ISP. A wireless network implements techniques for preventing of unauthorized access. The most common is Wi-Fi Protected Access, the current standard is WPA2.

EXERCISES

Use the appropriate number to match words and meanings.

...	Wireless network	1	Organization whose purpose is to drive the adoption of a single standard for wireless broadband in the world
...	Piconet	2	Name assigned to the WLAN so that users can identify
...	Home automation	3	Wireless Personal Area Network standard
...	Wi-Fi Alliance	4	Two or more devices sharing a communication channel by using Bluetooth
...	WiMAX	5	A system attempting to illicitly impersonate another system
...	SSID	6	Network that does not use cable connections
...	Spoofing	7	Wireless communication standard based on IEEE 802.16
...	Bluetooth	8	Technologies to improve the quality of life at home

GLOSSARY

Access Point: a base station that plugs into an Ethernet hub, switch or server.
DoS: Denial of Service. Attack that could cripple or disable a wireless network.
Hotspot: a specific area in which an access point provides public wireless broadband network services to mobile visitors through a WLAN.
ISM band: Industrial, Scientific and Medical band. Unlicensed spectrum typically in the 900 MHz, 2.4 GHz and 5.7 GHz bands.
Rogue Access Point: an unauthorized access point either created by employees or attackers.
Wardriving: the act of searching for Wi-Fi wireless networks in a moving vehicle, using a laptop or a smartphone.
WEP (Wired Equivalent Privacy): a security algorithm for IEEE 802.11 wireless networks.
WPA (Wi-Fi Protected Access): a security standard for users of computing devices equipped with wireless internet connections.
Zombie PC: computer used to perform malicius attacks, whose owners are unaware that their device is used to do that.

LAVORARE PER COMPETENZE

COMPETENZE IN GIOCO

Competenze disciplinari

- Saper scegliere gli opportuni dispositivi mobili in base alle esigenze di progettazione.
- Saper descrivere e documentare le soluzioni adottate.
- Utilizzare le reti e gli strumenti informatici nelle attività di studio, ricerca e approfondimento disciplinare.

Competenze chiave di cittadinanza

- Interpretare il testo.
- Risolvere problemi.
- Comunicare.
- Competenza digitale.

obiettivi formativi

- Stimolare l'approfondimento e la ricerca disciplinare.
- Consultare fonti Internet.
- Contestualizzare in un caso reale le nozioni teoriche acquisite studiando.
- Esporre i risultati della ricerca alla classe.

tempi

- Preparazione: 3 ore.
- Presentazione dei risultati e dibattito: 1 ora.
- Autovalutazione: 10 minuti.

strumenti

- Libro di testo.
- Dispositivo connesso a Internet.
- Foglio di carta.
- Software PowerPoint.
- Proiettore collegato al computer in classe o in laboratorio.

TEMA PROPOSTO

Una scuola superiore con 1000 studenti è ospitata in un moderno edificio a due piani.
I computer presenti nei laboratori, le postazioni fisse a disposizione dei docenti e gli uffici e sono collegati tramite rete Ethernet cablata con apparati a 100/1000 Mbps.

La scuola intende ora sviluppare per le classi quinte una didattica basata sul principio del BYOD (Bring Your Own Device), che consiste nell'utilizzo in classe dei dispositivi mobili degli studenti (smartphone, tablet, PC portatili, ecc.) per la didattica ordinaria, con accesso a Internet.

Inoltre la scuola ha esigenze crescenti di servizi di rete, sia per quanto riguarda l'attività amministrativa (che sempre più viene svolta su portali esterni ministeriali e privati come per il registro elettronico), sia per quanto riguarda la didattica innovativa e multimediale.

La scuola deve quindi aggiornare la sua infrastruttura al fine di conseguire i seguenti obiettivi:

- avere una rete che copra l'intero istituto, aule comprese, per poter sviluppare la didattica BYOD nelle classi quinte;
- offrire una piattaforma interna per la didattica multimediale e per servizi in streaming, accessibile sia dalla rete locale interna alla scuola che tramite Internet;
- garantire la sicurezza della rete interna da possibili minacce, sia interne che esterne.

Dopo aver formulato eventuali ipotesi aggiuntive proporre:
a. l'hardware e i servizi necessari all'implementazione della nuova infrastruttura;
b. le modalità di limitazione dell'accesso a docenti e studenti delle quinte;
c. le problematiche che si potrebbero presentare e le possibili soluzioni.

SVOLGIMENTO

Ipotesi aggiuntive

Per poter effettuare una didattica BYOD (Bring Your Own Device, in italiano: porta il tuo dispositivo) che consenta di utilizzare i dispositivi mobili degli studenti in classe, occorre ipotizzare un wireless campus. Alla LAN cablata dei laboratori già esistente va integrata una LAN wireless per connettere anche le aule della scuola.

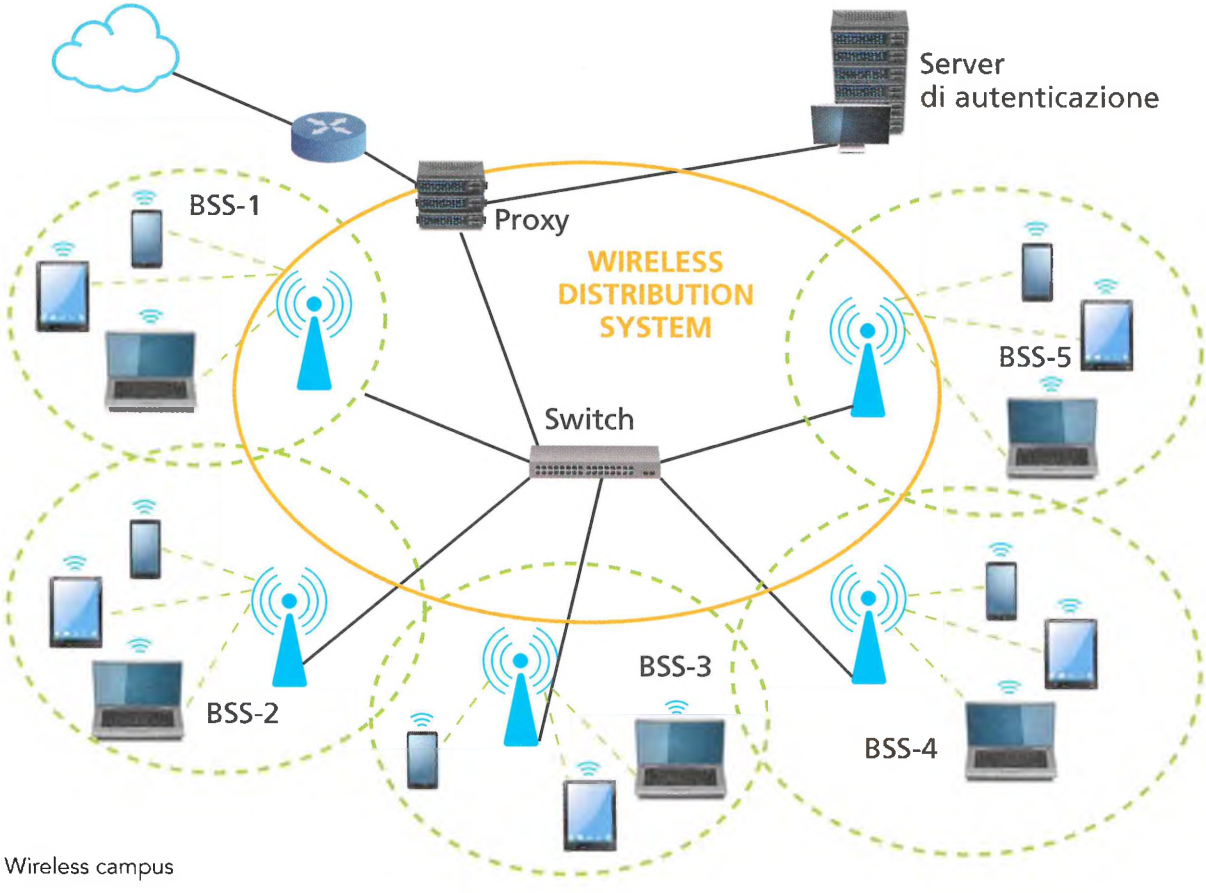
Descrizione

Molte sono le piattaforme che consentono di gestire classi virtuali (Edmodo è la più utilizzata, gratuita per docenti e studenti) per creare velocemente i gruppi classe, assegnare esercizi per casa, programmare verifiche, gestire i lavori di gruppo e altro ancora.

Al fine di poter utilizzare i dispositivi mobili degli studenti e dei docenti in tutti gli spazi della scuola, progettiamo una WLAN con specifiche Wi-Fi 802.11ac per la creazione di un wireless campus.

a. Un possibile schema logico dell'hardware necessario all'implementazione di tale infrastruttura è rappresentato nella figura seguente.

edmodo



Wireless campus

L'apparato che consente ai dispositivi mobili degli studenti e dei docenti di collegarsi alla rete Internet e in rete tra loro è l'Access Point (AP). Gli AP devono essere posizionati nei corridoi della scuola a distanza di qualche decina di metri l'uno dall'altro e cablati allo switch del piano (centro stella) a sua volta collegato al router della scuola.
Ogni AP, insieme ai dispositivi mobili che si muovono entro il suo raggio di copertura, rappresenta un Basic Service Set (BSS).
I BSS sono collegati tra loro da un Wireless Distribution System (l'intero sistema prende il nome di Extended Service Set, ESS).
La parziale sovrapposizione dei BSS garantisce la copertura continua: la connessione resta attiva e non c'è cambiamento di indirizzo IP per un dispositivo mobile che si sposta all'interno dell'intera WLAN.
La configurazione di un AP prevede l'impostazione di una serie di parametri:
– l'SSID (Service Set Identifier)
– la potenza del segnale
– il canale di trasmissione
– gli standard di crittografia e autenticazione
– la tecnica di incapsulamento
– l'abilitazione dei servizi di NAT o DHCP
Quest'ultimo, in particolare, provvederà ad attribuire un indirizzo IP dinamicamente a ogni smatphone o tablet che si connette alla rete.

b. Le modalità di accesso di docenti e studenti delle quinte è regolata da un processo di autenticazione.
La metodologia più diffusa è quella implementata dal protocollo EAP (Extensible Authentication Protocol) su entrambi i supporti di rete: parte wireless e parte cablata.
Con l'EAP, al dispositivo mobile che cerca di utilizzare la rete viene consentito il passaggio solo dei pacchetti EAP. Tale processo si avvale di un server di autenticazione, posizionato nella parte cablata della rete come, per esempio, il RADIUS (Remote Authentication Dial-In User) per eseguire l'autenticazione basandosi su username e password.
Questo significa che la scuola, attraverso il referente della rete, dovrà distribuire a ciascun allievo e a ciascun docente le credenziali per accedere al wireless campus.

c. Le problematiche da affrontare nella realizzazione di una WLAN scolastica sono legate ai rischi per la sicurezza della rete e alla protezione della navigazione degli studenti e dei docenti.
Tra i principali rischi per la sicurezza ci sono spoofing, accessi non autorizzati e attacchi DoS.
Le tecniche per rafforzare la sicurezza delle reti Wi-Fi si basano sulla crittografia (WEP, TKIP, AES, WPA2) e sull'autenticazione (EAP-RADIUS).
La navigazione degli studenti e dei docenti va protetta mediante dei filtri web (i più diffusi filtrano il DNS) in modo da poter eliminare la visione di siti inadatti ai minori e in generale sconvenienti per il loro contenuto.
In ogni caso va dichiarata e spiegata agli studenti e alle famiglie la Policy della scuola in materia di accesso alla rete e va regolamentato l'uso dei dispositivi mobili personali.
Occorre offrire agli studenti un momento di riflessione sui comportamenti corretti da adottare in rete per farne un uso consapevole e legale.
Le scuole devono inoltre rendere noto alle famiglie e ai ragazzi, attraverso un'adeguata informativa, quali dati raccolgono e come li utilizzano.

A CASA

- Effettua una ricerca in Internet sulle reti locali di tipo wireless; esaminando i diversi casi trovati concentrati su:
  – dispositivi wireless necessari
  – standard utilizzati
  – caratteristiche di sicurezza

- Individua quale caso risulta più affine al contesto illustrato nel tema proposto.
- Leggi l'esempio di svolgimento per verificare se le tue ipotesi si adattano al caso in esame e se la trattazione risulta completa nell'ottica della tua ricerca.
- Raccogli i tuoi risultati in una presentazione in PowerPoint (massimo 5 slide) evidenziando i casi trovati, la relazione con il contesto proposto, eventuali modifiche o aggiunte alla soluzione proposta nell'esempio di svolgimento.

IN CLASSE

- Condividi la presentazione dei tuoi risultati con i compagni.
- Confrontate e discutete i casi che sono stati presentati stabilendo quale rappresenta l'esempio migliore per completezza e realisticità nell'ottica della realizzazione della richiesta del tema.
- Procedi con l'autovalutazione.

AUTOVALUTAZIONE

ATTIVITÀ	LIVELLO			
	INIZIALE	BASE	INTERMEDIO	AVANZATO
Ho compreso senza difficoltà le richieste dell'attività proposta?	Ho compreso solo alcune delle richieste aiutato dal docente. ☐	Con la guida del docente e la collaborazione dei compagni ho compreso quasi tutte le richieste. ☐	Ho compreso le richieste e in parte le ho svolte autonomamente. ☐	Ho identificato le richieste e le ho svolte senza difficoltà. ☐
Ho reperito le informazioni in rete senza difficoltà?	Ho reperito solo alcune delle informazioni aiutato dal docente. ☐	Con la guida del docente ho reperito quasi tutte le informazioni. ☐	Ho reperito le informazioni utili autonomamente e le ho elaborate. ☐	Ho identificato le informazioni utili e le ho elaborate senza difficoltà. ☐
La ricerca in Internet mi ha permesso di definire modifiche e miglioramenti allo svolgimento proposto?	Non sono stato in grado di valutare lo svolgimento proposto. ☐	A partire dalla mia analisi, ho individuato alcuni punti critici nello svolgimento proposto con l'aiuto del docente. ☐	A partire dalla mia analisi, ho individuato i punti critici e le modifiche apportabili nello svolgimento proposto con l'aiuto del docente. ☐	Sono stato in grado di individuare i punti critici e definire le modifiche apportabili in modo dettagliato e completo. ☐

UNITÀ

5 RETI IP E RETI CELLULARI PER UTENTI MOBILI

Guarda la **presentazione** dell'unità

IN QUESTA UNITÀ

DDI+ Didattica Digitale Integrata Plus

conoscenze	abilità	competenze
Architettura di rete IP per la gestione di accessi *mobile*. Protocollo Mobile IP. Tecnologie cellulari usate per l'accesso mobile a Internet. Caratteristiche delle ultime generazioni di reti mobili 4G e 5G.	Saper gestire le modalità di accesso alla rete IP da parte di un utente mobile. Uso della rete cellulare per connettersi alla rete Internet.	Descrivere e comparare il funzionamento di dispositivi e strumenti elettronici e di telecomunicazione.

FLIPPED CLASSROOM

A casa

- Leggi la Lezione 4 di questa Unità;
- leggi il Case study *Reti mobili per la domotica*;
- amplia la trattazione elencando dispositivi e strumenti utili per la sicurezza personale e degli ambienti (sensori antifumo, allarmi, ecc.);
- raccogli i tuoi risultati in una tabella riassuntiva.

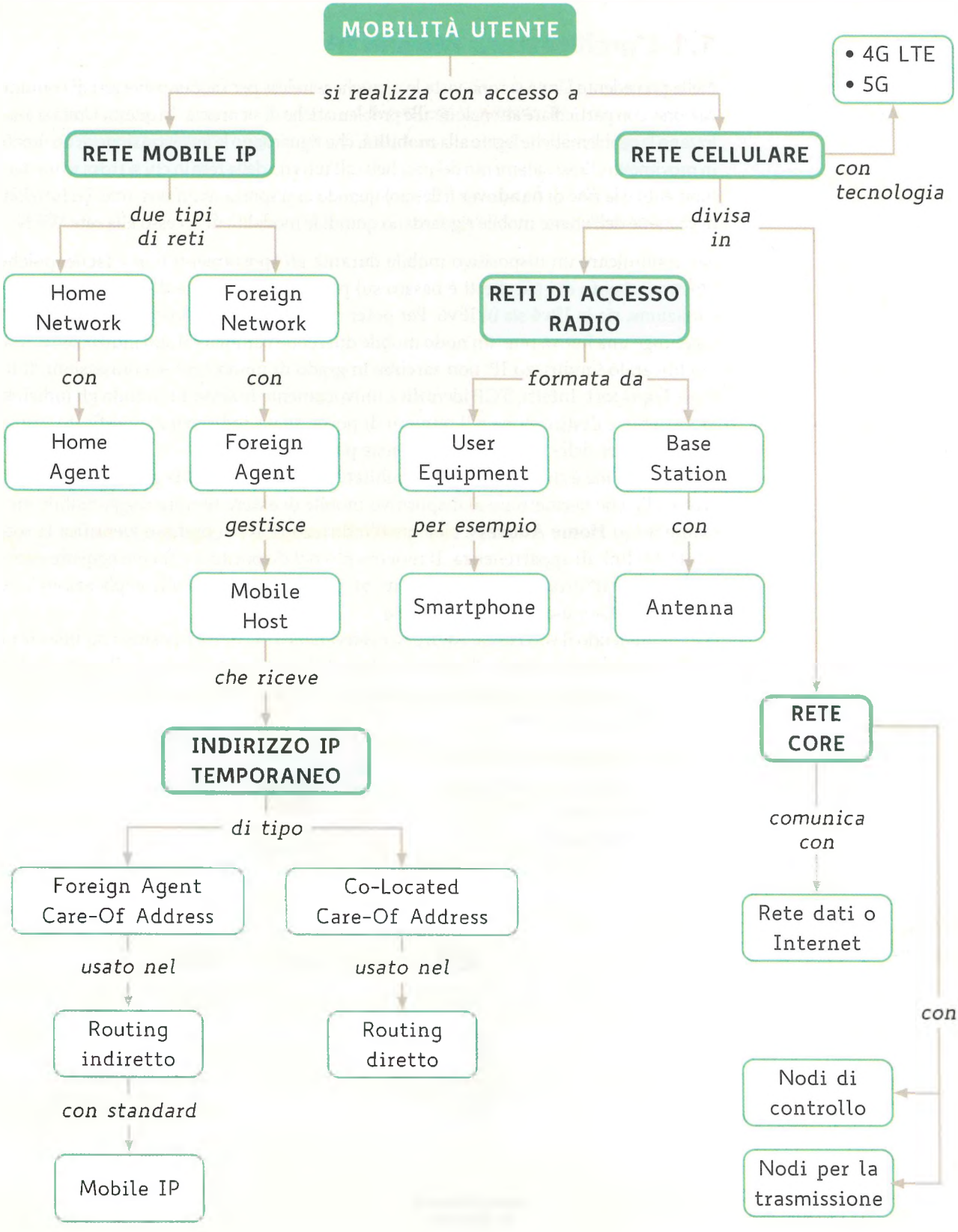
In classe

- Confrontate e discutete le diverse soluzioni proposte;
- valutate con una discussione quali di queste potrebbero essere adottate nelle scuole per la sicurezza di studenti e attrezzature.

MAPPA CONCETTUALE

DIDATTICA INCLUSIVA

Mappa modificabile



1 GESTIRE LA MOBILITÀ IN UNA RETE IP

1.1 L'architettura Mobile IP

Nella precedente Unità si sono viste le tecniche wireless per l'accesso alle reti di comunicazione, con particolare attenzione alle problematiche di sicurezza. In questa Unità si analizzano le problematiche legate alla **mobilità**, che riguardano la localizzazione di un utente in movimento, l'instradamento dei pacchetti all'interno della rete in cui si trova in un dato momento e la fase di **handover** (rilascio) quando ci si sposta in un'altra rete. Le funzioni di gestione dell'utente mobile riguardano quindi le modalità di accesso alla rete WAN.

Far comunicare un dispositivo mobile durante gli spostamenti non è facile, poiché l'instradamento dei pacchetti è basato sul prefisso di sottorete dell'indirizzo di destinazione, sia in IPv4 sia in IPv6. Per poter continuare a comunicare, ogni volta che raggiunge una nuova rete, un nodo mobile dovrebbe cambiare il suo indirizzo IP. Ma, modificando l'indirizzo IP, non sarebbe in grado di mantenere le connessioni di livello Transport. Infatti, TCP identifica univocamente le sessioni usando gli indirizzi IP sorgente e destinazione e il numero di porta; se un indirizzo è modificato prima della chiusura della sessione, questa viene persa.
Per tale ragione è stata costruita un'architettura di gestione della mobilità con nuovi protocolli, che permettono al dispositivo mobile di essere sempre raggiungibile mediante il suo **Home Address**, cioè quell'indirizzo IP il cui prefisso identifica la sottorete e il link di appartenenza. Il movimento del dispositivo e il conseguente cambiamento di IP diventa così trasparente al livello Transport e alle applicazioni, che continueranno a usare l'Home Address.
Pur mantenendo il suo Home Address, nel momento in cui il dispositivo mobile entra in una nuova rete necessita di un secondo indirizzo IP appartenente alla rete ospite; la stessa rete ospite si occuperà di assegnare il nuovo indirizzo e fornire la connessione di accesso alla rete.

Prima di descriverne il funzionamento, definiamo nel dettaglio le componenti fondamentali di un'architettura **Mobile IP** (FIGURA 1).

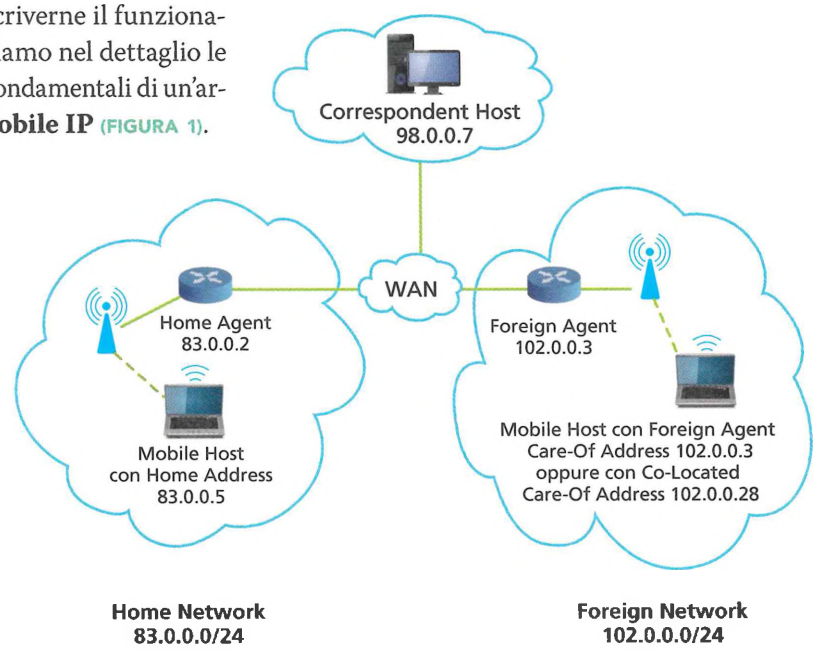


FIGURA 1 Componenti fondamentali di una Mobile IP-architecture WAN

- **Mobile Host**: dispositivo che si sposta dalla Home Network alla rete ospite detta Foreign Network.
- **Home Address (permanent address)**: indirizzo IP del Mobile Host con cui è raggiunto ovunque. In figura è 83.0.0.5.
- **Home Network**: rete a cui il dispositivo è abitualmente connesso. In figura ha indirizzo 83.0.0.0/24.
- **Home Agent**: entità nella Home Network che gestisce la mobilità del Mobile Host e mantiene anche le coordinate relative alla posizione corrente del Mobile Host. L'Home Agent in figura è 83.0.0.2.
- **Correspondent Host**: dispositivo in Internet che sta comunicando con il Mobile Host (in figura è 98.0.0.7).
- **Foreign Network**: rete ospite (in figura è 102.0.0.0/24).
- **Foreign Agent**: entità che gestisce la mobilità nella Foreign Network (in figura è 102.0.0.3).
- **Care-Of Address**: indirizzo IP associato al Mobile Host mentre si trova in una Foreign Network. Si possono avere due tipi di Care-Of Address a seconda del tipo di routing che si utilizza:
  - **Foreign Agent Care-Of Address**: indirizzo del Foreign Agent presso il quale il Mobile Host si registra (in figura 102.0.0.3). È usato nel routing indiretto;
  - **Co-Located Care-Of Address**: indirizzo che il Mobile Host può acquisire quando passa sotto il controllo di una Foreign Network (in figura 102.0.0.28). È usato nel routing diretto.

Il dispositivo mobile che si sposta tra reti diverse può mantenere la comunicazione con il Correspondent Host attraverso due tecniche di routing alternative:

- **routing indiretto**: il Correspondent Host non invia direttamente i pacchetti al Mobile Host, ma passa sempre attraverso lo Home Agent. Inoltre, il Mobile Host utilizza il **Foreign Agent Care-Of Address** cioè lo stesso indirizzo del Foreign Agent;
- **routing diretto**: il Correspondent Host ottiene il Foreign Agent Care-Of Address del Mobile Host e inoltra i messaggi direttamente al Mobile Host. In questo caso il Mobile Host utilizza il **Co-Located Care-Of Address**, quindi un indirizzo assegnatogli solitamente dal DHCP.

Il **routing triangolare** che avviene tra Correspondent Host, Home Agent e Mobile Host consente al dispositivo mobile di essere rintracciato e ricevere i datagram IP che gli invia il dispositivo corrispondente.

#prendinota

Il Foreign Agent Care-Of Address e il Co-Located Care-Of Address funzionano uno in alternativa all'altro. Nel caso di acquisizione del Co-Located Care-Of Address, le funzioni del Foreign Agent possono essere realizzate direttamente dal Mobile Host.

#prendinota

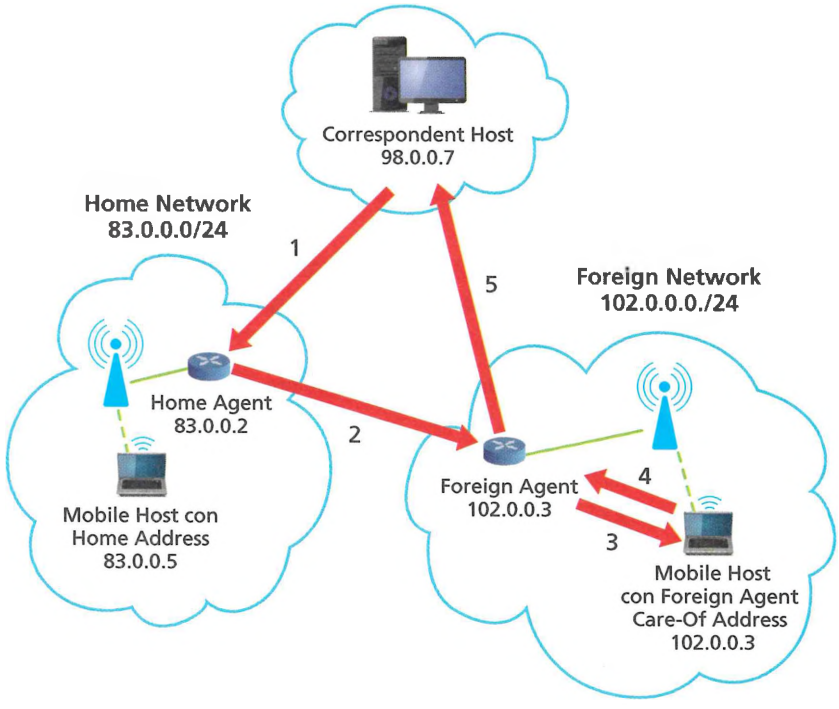
Se il Corrispondent Host si trova all'interno della Home Network, il **routing triangolare** risulterà estremamente inefficiente fino a quando il Mobile Host risulterà anch'esso dentro la propria Home Network.

1.2 Il routing indiretto

Il routing indiretto avviene in 5 passi (FIGURA 2):

1. il Correspondent Host indirizza i pacchetti verso l'Home Agent del Mobile Host;
2. l'Home Agent riceve i pacchetti e li inoltra verso il Foreign Agent;
3. il Foreign Agent riceve i pacchetti e li inoltra verso il Mobile Host;
4. il Mobile Host risponde al Foreign Agent;
5. il Foreign Agent inoltra direttamente al Correspondent Host.

FIGURA 2 Routing indiretto



#prendinota

Il Correspondent Host non deve conoscere l'indirizzo del Foreign Agent ma solo quello dell'Home Agent: si dice che la locazione del Mobile Host è **trasparente** al Correspondent Host.

Nel caso in cui un utente si muova verso un'ulteriore rete, con il routing indiretto si avranno le seguenti azioni:

1. si registra presso un nuovo Foreign Agent;
2. il nuovo Foreign Agent comunica la registrazione all'Home Agent del dispositivo mobile;
3. l'Home Agent aggiorna il Care-Of Address del dispositivo mobile;
4. i pacchetti continuano a essere inoltrati verso il Mobile Host (ma con il nuovo Care-Of Address).

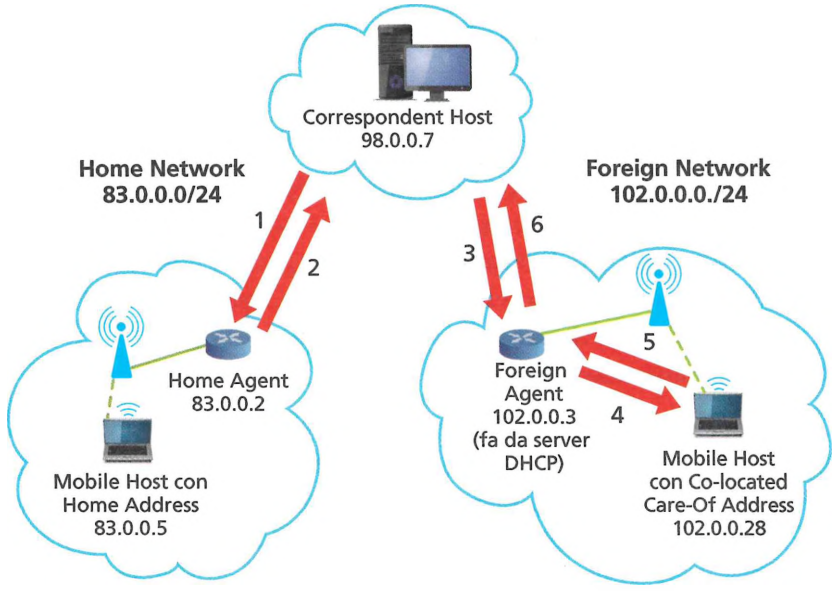
Nel caso in cui tra Mobile Host e Correspondent Host sia instaurata una connessione a livello Transport (per esempio con TCP) lo spostamento del dispositivo mobile in un'altra rete non interrompe la comunicazione. Eventuali datagram persi saranno recuperati grazie ai meccanismi di ritrasmissione che si applicano per le perdite dovute sia alla congestione della rete sia alla mobilità dell'utente.

1.3 Il routing diretto

Il routing diretto avviene in 6 passi (FIGURA 3):

1. il Correspondent Host, prima di inoltrare i pacchetti, chiede il Care-Of Address del Mobile Host all'Home Agent;
2. l'Home Agent risponde inviando l'IP del Foreign Agent DHCP presso cui si trova il Mobile Host;
3. il Correspondent Host può ora inviare i pacchetti al Foreign Agent DHCP;
4. il Foreign Agent DHCP riceve i pacchetti e li inoltra verso il Mobile Host;
5. il Mobile Host risponde al Foreign Agent DHCP;
6. il Foreign Agent DHCP inoltra direttamente al Correspondent Host.

FIGURA 3 Routing diretto



Con l'assegnazione del Co-Located Care-Of Address viene meno la necessità di utilizzare un Foreign Agent. Così, di fatto, esso viene eliminato e il dispositivo mobile gestisce autonomamente (sistema di autoconfigurazione) sia tutta la segnalazione Mobile IP (registrazione, binding update, ecc.) sia il tunneling.
Con il routing diretto emerge la necessità di un protocollo di comunicazione tra Correspondent Host e Home Agent per la localizzazione del Mobile Host (passi 1-2). Inoltre, il Correspondent Host chiede il Care-Of Address all'Home Agent solo una volta, all'inizio, quindi sorge il problema (che non c'era con il routing indiretto) di come ottenere la nuova posizione quando il Mobile Host si sposterà in un'altra rete.

Una soluzione adottata è la seguente:

- il Foreign Agent della prima rete visitata diventa l'**Anchor Foreign Agent**;
- i pacchetti saranno sempre inviati all'Anchor Foreign Agent;
- quando il dispositivo mobile cambia rete, il nuovo Foreign Agent fornisce all'Anchor Foreign Agent il nuovo Care-Of Address del Mobile Host;
- il Correspondent Host continua a inviare i datagram all'Anchor Foreign Agent che li inoltrerà al Mobile Host usando il nuovo Care-Of Address (forwarding a catena).

#prendinota

Il Correspondent Host deve essere informato dell'indirizzo del Foreign Agent: si dice che la locazione del Mobile Host **non è trasparente** al Correspondent Host.

#prendinota

Il routing diretto risolve i problemi di inefficienza del routing triangolare legati all'eventuale presenza del Correspondent Agent nella Home Network.

FISSA LE CONOSCENZE

- Descrivi i due tipi di indirizzi Care-Of Address, spiegandone le differenze.
- Descrivi il funzionamento del routing indiretto.
- Che che cosa succede quando, col routing indiretto, ci si muove da una rete ospite a un'altra?
- Descrivi il funzionamento del routing diretto.
- Che cosa succede quando, con il routing diretto, ci si muove da una rete ospite a un'altra?

2 IL PROTOCOLLO MOBILE IP

IL MOBILE IP SU RETI WIRELESS

In ambito IETF è stato standardizzato un protocollo apposito per il supporto della mobilità degli utenti, che consente a un dispositivo mobile di spostarsi da una rete a un'altra mantenendo sempre lo stesso indirizzo IP. Questo protocollo è denominato **Mobile IP (MIP)** e sono state specificate due versioni distinte per IPv4 e IPv6:

- **RFC 5944 IP Mobility Support for IPv4. Revised**
- **RFC 6275 Mobility Support in IPv6**

#prendinota

Mobile IP non è usato nelle reti cellulari. Questi sistemi implementano meccanismi propri per gestire la mobilità di un dispositivo (fasi di handover e roaming) a livello Data link.

Nelle specifiche RFC 5944 si fa uso del routing indiretto, visto nella Lezione precedente. Mobile IP è implementato principalmente su reti wireless per fornire una continuità di accesso a Internet quando un dispositivo si sposta attraversando più WLAN. Come visto nella Lezione precedente, l'obiettivo è mantenere attiva la connessione TCP instaurata tra il dispositivo mobile e un altro host della rete, seguendo gli spostamenti dell'utente. Il protocollo MIP lavora bene quando il Correspondent Host è un dispositivo fisso; infatti, se anche questo fosse mobile, il sovraccarico sarebbe notevole e il protocollo diventerebbe poco efficiente.

L'architettura definita in Mobile IP contiene molti degli elementi visti nella Lezione precedente. In generale, si possono distinguere 3 parti:

1. **agent discovery**: quando un Mobile Host arriva in una nuova rete deve individuare l'indirizzo del Foreign Agent, così può apprendere di essere passato da una rete a un'altra; ciò avviene tramite l'invio di messaggi Agent Advertisement da parte dell'Home Agent o del Foreign Agent;
2. **registrazione**: una volta che il Mobile Host ha ricevuto un Care-Of Address, questo indirizzo deve essere associato al suo Home Address, registrandolo presso il suo Home Agent;
3. **routing indiretto dei datagram**: Mobile IP definisce le modalità con cui l'Home Agent inoltra i datagram al Mobile Host, specificando varie forme di incapsulamento.

L'Home Agent e il Foreign Agent hanno il compito di inviare degli **Agent Advertisement** attraverso il broadcasting di pacchetti ICMP (Internet Control Message Protocol) estesi. In pratica all'ICMP classico vengono aggiunti dei campi che consentono al Mobile Host di capire che ha cambiato rete.
Il più importante di questi campi aggiuntivi è il **COAs (Care-Of Addresses)**. Questo campo consente all'Agent Advertisement di specificare uno o più indirizzi IP (Care-Of Address) dai quali il Mobile Host isolerà la parte network e la confronterà con la sua parte network: se sono diverse capirà che ha cambiato rete.

> Affinché il Mobile Host sia in grado di **ricevere Agent Advertisement** lungo lo spostamento, occorre che il Mobile Host si sposti lungo un percorso in cui siano presenti reti che implementano l'802.11, altrimenti il Mobile Host non potrebbe ricevere gli advertisement.

Grazie alla ricezione degli Agent Advertisement, il Mobile Host può ricavare il MAC address del Foreign Agent necessario per comunicare con questo ed effettuare così la registrazione.

La **registrazione** è la prima cosa che il dispositivo mobile deve fare presso la rete ospite. Si tratta di un procedimento che consente di associare (**binding**) l'Home Address e il Care-Of Address.

La registrazione avviene nel seguente modo:

- prima, il Mobile Host invia un **Registration Request** al Foreign Agent della Foreign Network in cui si appresta a entrare, al quale fornisce il proprio indirizzo MAC e l'indirizzo IP del suo Home Agent (**binding update**);
- successivamente, il Foreign Agent invia un **Registration Reply** all'Home Agent del Mobile Host, con il quale lo informa del proprio Care-Of Address (**binding acknowledgement**).

Dopo questo scambio, entrambi i router possono aggiornare le proprie tabelle e il Mobile Host risulta rintracciabile nella rete ospite: il Foreign Agent è consapevole della presenza del Mobile Host e l'Home Agent conosce la nuova posizione del Mobile Host.

Infine, per realizzare la triangolazione tramite il Correspondent Host, tipica del **routing indiretto**, si ricorre a un doppio indirizzamento mediante l'aggiunta di due header. Prima il Correspondent Host inserisce un header (FIGURA 4) contenente il proprio indirizzo IP come sorgente e l'Home Address del Mobile Host come destinatario e invia il pacchetto all'Home Agent.

HEADER		
Source IP (Correspondent Host) 98.0.0.7	Destination IP (Home Address) 83.0.0.5	PAYLOAD

FIGURA 4 Header aggiunto dal Correspondent Host

Poi, il pacchetto viene ricevuto dall'Home Agent che lo **incapsula** (imbusta) nel suo payload aggiungendo un secondo header (FIGURA 5) con un'altra coppia di indirizzi IP: il proprio come sorgente e quello del Foreign Agent come destinatario e inoltra il pacchetto al Foreign Agent.

HEADER		PAYLOAD		
Source IP (Home Agent) 83.0.0.2	Destination IP (Foreign Agent) 102.0.0.3	Source IP (Correspondent Host) 98.0.0.7	Destination IP (Home Address) 83.0.0.5	PAYLOAD

FIGURA 5 Header aggiunto dall'Home Agent

La tecnica di incapsulare il datagram IP in un altro datagram è chiamata **tunneling** e viene abilitata settando un flag contenuto nel campo Protocol Type del datagram stesso. Il flag settato permette al Foreign Agent di capire che sta ricevendo un datagram che ha come payload un altro datagram ed effettuare il **detunneling**, cioè recuperare il pacchetto IP incapsulato.

#prendinota

Un Foreign Agent non deve segnalare all'Home Agent che il Mobile Host ha lasciato la sua rete; questa segnalazione avverrà in automatico, quando il Foreign Agent entrerà in una nuova rete e sarà fatta la registrazione del nuovo Care-Of Address.

FISSA LE CONOSCENZE

- Perché Mobile IP è implementato su reti Wi-Fi?
- Qual è il campo più importante del pacchetto ICMP esteso?
- Come avviene la registrazione presso una rete ospite?
- Che cos'è il tunneling?

3 LE RETI CELLULARI E L'ACCESSO A INTERNET

3.1 La telefonia cellulare

Nelle due Lezioni precedenti è stata trattata la gestione della mobilità in reti IP con accesso wireless alla WAN. La limitazione di questa architettura è proprio nella necessità di avere a disposizione un hotspot Wi-Fi al quale l'utente mobile può connettersi. Sulla spinta della richiesta sempre più elevata di utenti che vogliono connettersi a Internet in qualsiasi momento e posto in cui si trovano, i provider di telefonia cellulare hanno esteso le proprie reti così da supportare non solo la telefonia mobile, servizio per il quale sono nate queste reti, ma anche l'accesso mobile a Internet. Un immediato vantaggio di questa soluzione sta proprio nella copertura delle reti cellulari e nella banda più elevata, che consente di avere un numero maggiore di utenti connessi in contemporanea.

Ogni cellulare può essere individuato mediante un codice univoco chiamato **IMEI** (International Mobile Equipment Identity), che permette di conoscere la casa produttrice, il modello e il numero di serie del cellulare. Alcuni IMEI hanno anche la parte **SV** (Software Version), due cifre ulteriori che identificano la versione del firmware dell'apparecchio. Ogni operatore ha la possibilità di bloccare un cellulare a seguito di un furto, sulla base di questo codice. Una volta bloccato, il cellulare non potrà funzionare neanche cambiando scheda SIM.

#prendinota

L'IMEI fa le veci dell'indirizzo MAC. Infatti, ogni ISP (Internet Service Provider) assegna dinamicamente un indirizzo IP al cellulare nel momento in cui il cellulare si connette a Internet e contestualmente lo associa al suo codice IMEI. Dall'IMEI è poi possibile risalire alla SIM e di conseguenza all'utente e al suo contratto.

La telefonia cellulare è una tipologia di accesso a una rete telefonica attraverso una rete cellulare (FIGURA 6).

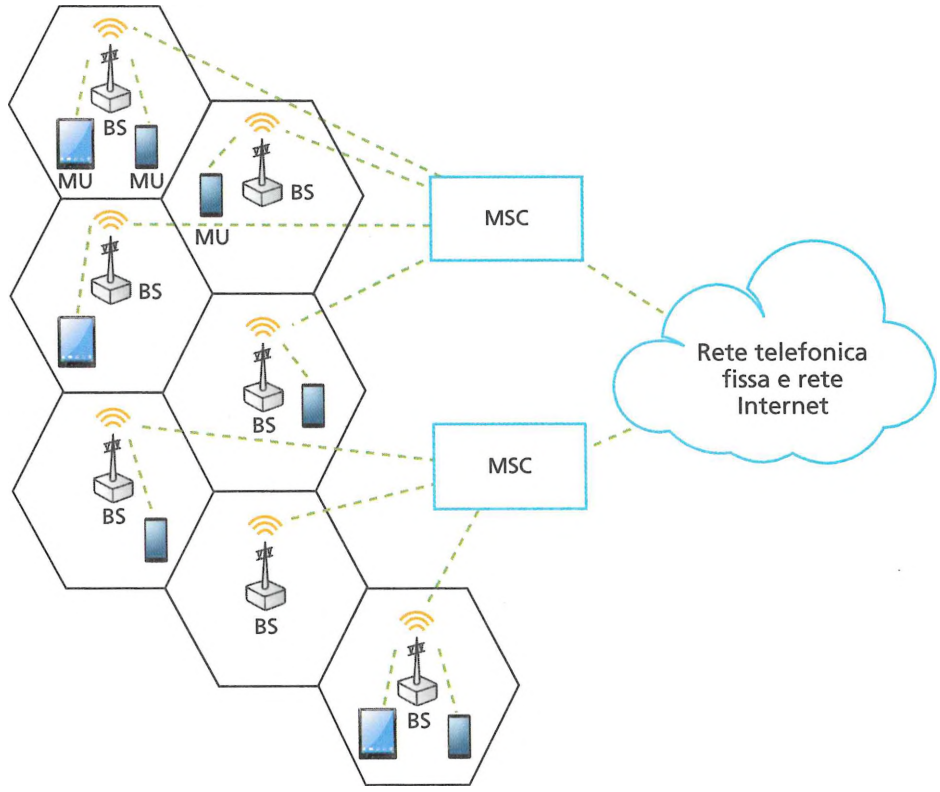


FIGURA 6 Rete cellulare

È realizzata per mezzo di onde radio e ricetrasmettitori terrestri (cioè antenne ubicate sulla superficie terrestre) che danno vita alle **BS** (Base Station), le quali coprono ciascuna una porzione di territorio detta **cella di copertura**. L'antenna riceve i segnali dagli **MU** (Mobile User), cioè dai dispositivi mobili degli utenti, e li trasmette agli **MSC** (Mobile Switching Center) che sono le centraline che, oltre a connettere tra loro le celle, permettono il collegamento alla rete telefonica fissa e alla rete Internet agendo da gateway.

Ogni rete cellulare è costituita da un numero variabile di celle che permettono la copertura radioelettrica e il collegamento tra i terminali mobili e la rete telefonica fissa. Il numero delle celle e la loro grandezza dipende dalla quantità di traffico (e quindi dal numero di terminali mobili) stimata in una data zona. Nelle città il numero delle celle è molto alto e la loro grandezza è molto ridotta.

> Sul territorio sono solitamente presenti più reti cellulari come quella in Figura 6, gestite da operatori diversi (per esempio, Tim, Vodafone, Windtre, ecc.).

Con i sistemi cellulari si ricorre alla tecnica del **riutilizzo delle frequenze**, cioè, una stessa frequenza è utilizzata più volte ma in celle diverse, sufficientemente lontane tra loro in modo da evitare interferenze (FIGURA 7).

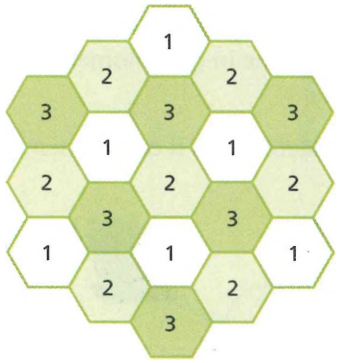


FIGURA 7 Celle adiacenti utilizzano frequenze diverse

3.2 Il cambio di cella e il cambio di operatore

Il problema fondamentale che la telefonia cellulare deve affrontare è la gestione della mobilità, noto come **handoff** (o anche **handover**). In pratica si tratta di evitare le interruzioni nel collegamento a fronte di un cambio di Base Station, cioè di un cambio di cella con relativo cambio di frequenze nell'ambito dello stesso MSC. Va inoltre considerata l'eventualità di un cambio di operatore (**roaming**), cioè un vero e proprio cambio di rete.

L'handoff **sullo stesso MSC** è riassumibile in 9 passi.

1. La vecchia BS informa l'MSC di un imminente handoff e fornisce la lista di una o più nuove BS.
2. MSC instaura l'instradamento (alloca risorse) verso la nuova BS.
3. La nuova BS alloca i canali radio per il dispositivo mobile.
4. La nuova BS segnala all'MSC che è pronta e questo a sua volta lo comunica alla vecchia BS.

5. La vecchia BS attiva il dispositivo mobile per effettuare handoff (il dispositivo mobile non conosce il canale radio di destinazione).
6. Il dispositivo mobile e la nuova BS si scambiano i messaggi per completare l'assegnazione del canale.
7. Il dispositivo mobile comunica alla nuova BS, che a sua volta comunica all'MSC che l'handoff è completato.
8. L'MSC ridireziona le chiamate.
9. La vecchia BS rilascia le risorse.

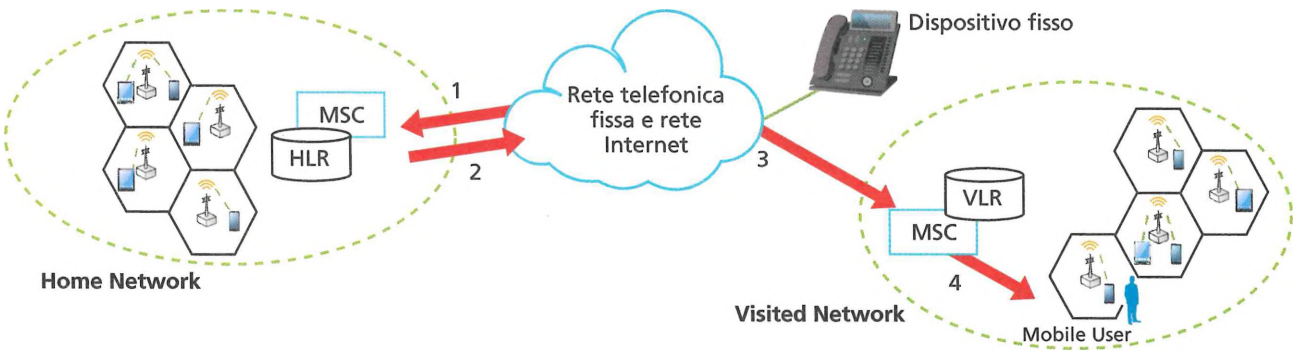
Per comprendere invece come viene gestita la mobilità in caso di **cambio di operatore**, serve specificare due tipi di reti e i loro relativi database:

- **Home Network**: rete del proprio operatore (per esempio Tim, Vodafone, Windtre, ecc.) dotata di **Home Location Register** (**HLR**) cioè del database che contiene informazioni sull'utente, quali il numero di telefono, il tipo di contratto, l'attuale posizione (può essere presso un'altra rete);
- **Visited Network**: rete presso la quale si trova attualmente il dispositivo mobile, dotata di **Visitor Location Register** (**VLR**) cioè del database che contiene informazioni sugli utenti attualmente presenti nella rete, quali il numero di telefono e l'operatore di appartenenza.

Supponiamo per esempio che da un telefono fisso si voglia comunicare con un dispositivo mobile (**Mobile User**) che in quel momento non si trova nella rete del proprio operatore mobile.

Occorreranno 4 passi per rendere attivo il collegamento (FIGURA 8).

FIGURA 8 Reti cellulari per la mobilità



1. La chiamata viene instradata verso la Home Network.
2. L'MSC della Home Network accede al suo HLR, per ottenere il riferimento del dispositivo mobile presso l'altra rete, e imposta la connessione attraverso la rete telefonica fissa (PSTN: Public Switched Telephone Network).
3. Tramite la rete telefonica fissa si raggiunge la Visited Network ove si trova in quel momento il dispositivo mobile.
4. L'MSC della Visited Network, verificata la presenza dell'utente mobile tramite l'accesso al suo VLR, dirama la chiamata radio su tutte le celle della sua rete, l'utente chiamato risponderà dalla cella in cui si trova e verso la quale sarà instradata la chiamata.

3.3 Le tecniche di mobilità con accesso radio a Internet

Per fornire i servizi dati in mobilità, la rete di accesso radio (Radio Access Network) coopera con i nodi a commutazione di pacchetto che, a loro volta, si interfacciano con il database delle utenze (HLR). I nodi fungono da gateway verso Internet o altre reti dati.

Esistono 5 tecniche fondamentali per l'accesso e la condivisione tra più utenti del canale MU-BS (Mobile User-Base Station):

- **FDMA** (Frequency Division Multiple Access): consiste nella suddivisione della banda di frequenza disponibile (canale di trasmissione) in un numero di sottobande (sottocanali) che occupano, in frequenza, una banda più piccola; ognuno di questi sottocanali è assegnato a un diverso utente;
- **TDMA** (Time Division Multiple Access): è realizzata mediante una ripartizione del tempo di accesso al canale da parte degli utenti che potranno utilizzarne l'intera banda ma per un intervallo di tempo limitato (time slot);
- **CDMA** (Code Division Multiple Access): è la tecnica di accesso multiplo a un canale condiviso più diffusa nelle reti wireless. Il suo principio di funzionamento prevede che più stazioni possano trasmettere contemporaneamente utilizzando lo stesso canale fisico: sarà poi la corrispettiva stazione ricevente a decodificare il rumore di fondo così generato, estraendo solo la parte di dati relativa alla propria connessione. Questo è reso possibile grazie all'impiego di particolari schemi di codifica e decodifica (detti *ortogonali*) che permettono di filtrare, con operazioni booleane, il flusso di dati ricevuto, ricostruendo così il canale di trasmissione originario.
  Nell'apparato di ricezione, inoltre, la presenza del cosiddetto **Rake Receiver** (Ricevitore a Rastrello) consente di identificare e catturare non solo i singoli pacchetti relativi alla connessione in corso, ma anche le loro eco, sommando tra loro quelle corrispondenti, così da distinguere meglio il segnale interessante dal rumore di fondo. Le eco si generano quando il segnale subisce riflessioni in più direzioni lungo la tratta;
- **OFDMA** (Orthogonal Frequency Division Multiple Access): con questa tecnica l'accesso multiplo è realizzato assegnando a ciascun utente dei gruppi di sottoportanti, da qualche decina a qualche decina di migliaia, tra loro ortogonali (modulazione *multicarrier*, a multiportante), permettendo così di ottenere un relativamente basso data rate di trasmissione da parte di ogni utente. Il vantaggio primario dell'OFDMA, rispetto agli schemi a singola portante, è l'abilità di comunicare anche in condizione pessime del canale;
- **NOMA** (Non-Orthogonal Multiple Access): permette di allocare la portante a più di un utente nello stesso tempo in una stessa cella. Gli utenti sono differenziati per livelli di potenza (power domain) e nel ricevitore è implementata una tecnica innovativa di cancellazione delle interferenze (SIC, Successive Interference Cancellation). NOMA supporta un maggior numero di connessioni rispetto ai precedenti sistemi; per questa sua caratteristica è stata proposta per le reti di ultima generazione (5G). Per contro i complessi algoritmi che impiega richiedono un'elevata potenza di elaborazione.

#prendinota

Un sistema di telecomunicazioni basato su CDMA offre maggiore protezione sul fronte della sicurezza della comunicazione in quanto solo la conoscenza delle parole di codice permette di poter effettuare la demultiplazione del rispettivo canale all'interno dell'intero flusso multiplato.

#prendinota

Le velocità di trasmissione nella telefonia cellulare non sono paragonabili con quelle raggiungibili con le tecnologie cablate e nemmeno con il Wi-Fi; occorre però considerare che i dispositivi di telefonia cellulare operano con schermi a dimensione ridotta e hanno capacità di memorizzazione e di elaborazione limitata.

La FIGURA 9 illustra le tecniche appena descritte, mostrando l'allocazione dello spettro in modo che i segnali dei diversi dispositivi non si sovrappongano.

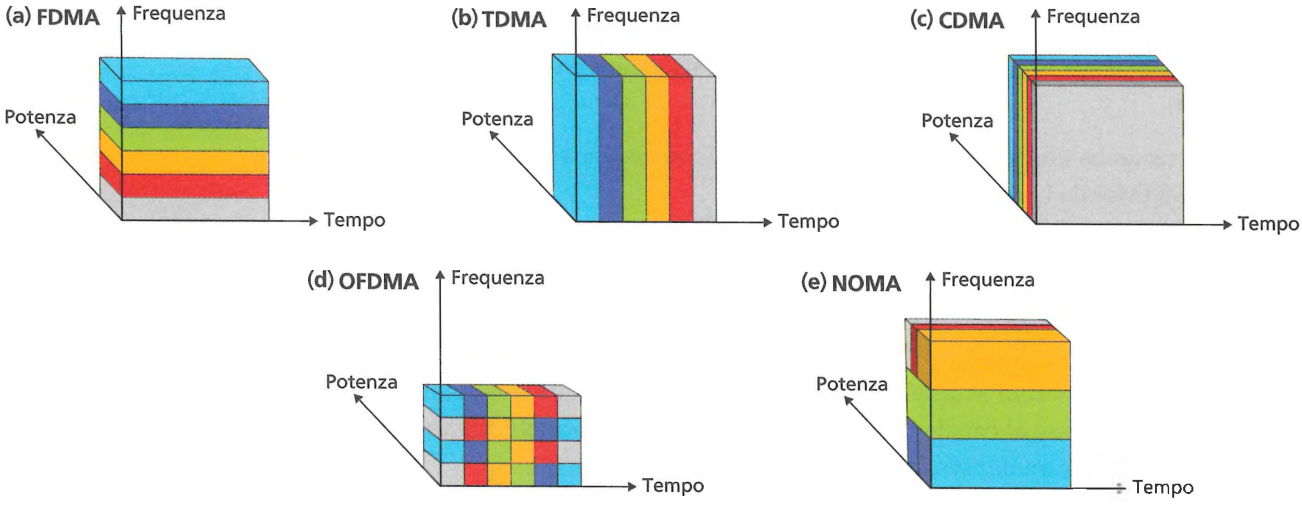


FIGURA 9 Allocazione dei segnali (i diversi dispositivi sono distinti con i colori) con tecnica FDMA (a); TDMA (b); CDMA (c); OFDMA (d); NOMA (e)

La grande comodità di avere Internet sul cellulare (basta che ci sia copertura di rete) rispetto ad averlo sul computer portatile (occorre che ci sia una Wi-Fi Zone) ha portato alla nascita della Internet Key (chiavetta Internet): un modem USB di dimensioni ridotte che consente la connessione a Internet. È sufficiente collegare la **Internet Key** al PC portatile per avere il collegamento a Internet ovunque vi sia campo. Al suo interno la chiavetta Internet ospita, oltre a una piccola quantità di memoria flash, la SIM dell'operatore. I sistemi operativi più recenti hanno già i driver precaricati e quindi riconoscono la Internet Key (che è quindi plug and play).
È anche possibile acquistare computer portatili dotati di modem integrato (o appositi slot per inserirvelo) con tecnologie UMTS, HSPA e similari, in modo da avere il collegamento a Internet tramite la rete cellulare.

FISSA LE CONOSCENZE

- Quali sono le componenti di una rete cellulare?
- Che cosa si intende per handoff (o handover)?
- Come viene gestita la mobilità in caso di cambio di operatore?
- Come funziona una Internet Key?

4 LA MOBILITÀ NELLE RETI 4G LTE

4.1 Le generazioni di telefonia cellulare

La telefonia cellulare è giunta alla quinta generazione attraverso una serie di evoluzioni che possono essere riassunte come segue:

- **0G**: radiomobili analogici di tipo veicolare cioè destinati all'installazione fissa su veicoli. In questa fase l'interoperabilità tra le reti e i dispositivi è quasi inesistente e molti stati sviluppano reti e dispositivi in maniera indipendente;
- **1G** (prima generazione): cellulari analogici con standard **TACS** (Total Access Communication System) e **ETACS** (ExtendedTACS, TACS esteso con l'aggiunta di nuove frequenze);
- **2G** (seconda generazione): primi cellulari digitali con standard **GSM** (Groupe Spécial Mobile, poi diventata Global System for Mobile Communications);
- **2.5G**: cellulari con standard **GPRS** (General Packet Radio Service) in grado di trasmettere dati mediante commutazione di pacchetto (evoluzione del GSM);
- **2.75G**: cellulari con standard **EDGE** (Enhanced Data rates for GSM Evolution). Versione più veloce dello standard GPRS per il trasferimento dati sulla rete cellulare GSM;
- **3G** (terza generazione): videocellulari e cellulari con standard **UMTS** (Universal Mobile Telephone System);
- **3.5G**: cellulari e smartphone con tecnologia **HSPA** (High Speed Packet Access), tecnologia **HSPA Evolution (HPSA+)** e tecnologia **HSDPA** (High Speed Downlink Packet Access). Versioni evolute dello standard UMTS che ne aumentano la velocità;
- **4G** (quarta generazione): cellulari e smartphone con standard **VSF-Spread OFDM** (Variable-Spreading-Factor Spread Orthogonal Frequency Division Multiplexing). Nuova tecnologia **LTE** (Long Term Evolution) e successive **LTE-Advanced**;
- **4.5G**: la versione più evoluta di LTE è detta **LTE-Advanced Pro**, supporta velocità superiori a 500 Mbps arrivando anche a 1 Gbps;
- **5G** (quinta generazione): si pone come obiettivo quello di fornire un'estrema flessibilità in termini di supporto, configurazione, servizi e integrazione di accessi. Come detto, per questa rete è stata proposta la tecnologia NOMA.

4.2 Il 4G LTE (Long Term Evolution)

Le comunicazioni personali, attuate per lo più tramite smartphone e tablet, sono diventate sempre più pervasive e *always-on*: la maggior parte del traffico dati è generato dai video online e dal web browsing. La tecnologia **4G LTE** ha permesso l'offerta di nuovi servizi a cui accedere tramite applicazioni presenti su smartphone e tablet (video HD, gaming, videoconferenza, ecc.).
Rispetto ai sistemi precedenti, la tecnologia di accesso LTE ha portato a innovare sia la rete core di trasporto sia la rete di accesso radio:

1. **EPC (Evolved Packet Core)**: le funzioni di controllo delle comunicazioni sono del tutto separate da quelle di trasporto. Inoltre la rete core è completamente a

#prendinota

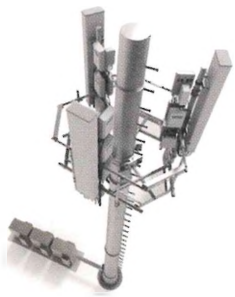
Alcuni operatori telefonici hanno puntato sulle maggiori prestazioni di LTE per offrire ai clienti la sostituzione della linea fissa con quella mobile, offrendo loro un servizio ADSL-like, ma su rete LTE. Questo servizio è particolarmente utile nelle aree non coperte dalla banda larga (*digital divide*).

pacchetto IP; al vantaggio di avere un'unica rete di trasporto delle informazioni, siano esse voce o dati, si associa la necessità di una maggior attenzione alla gestione delle risorse, così da soddisfare i requisiti prestazionali delle applicazioni voce (si ricordi che IP è Best effort);

2. **E-UTRAN** (**Evolved UMTS Terrestral Radio Access Network**): l'accesso radio è costituito da un unico componente **eNodeB** (evolved NodeB), la stazione base radio evoluzione del NodeB del 3G (che a sua volta è l'evoluzione della BS di seconda generazione); eNodeB è responsabile delle procedure radio verso il terminale utente per attivazione, handover e rilascio della sessione.

LTE usa la tecnologia di accesso radio OFDMA che consente di raggiungere velocità più elevate delle precedenti. Inoltre, sono state introdotte antenne più evolute in tecnologia **MIMO**, **Multiple-Input Multiple-Output** (FIGURA 10).

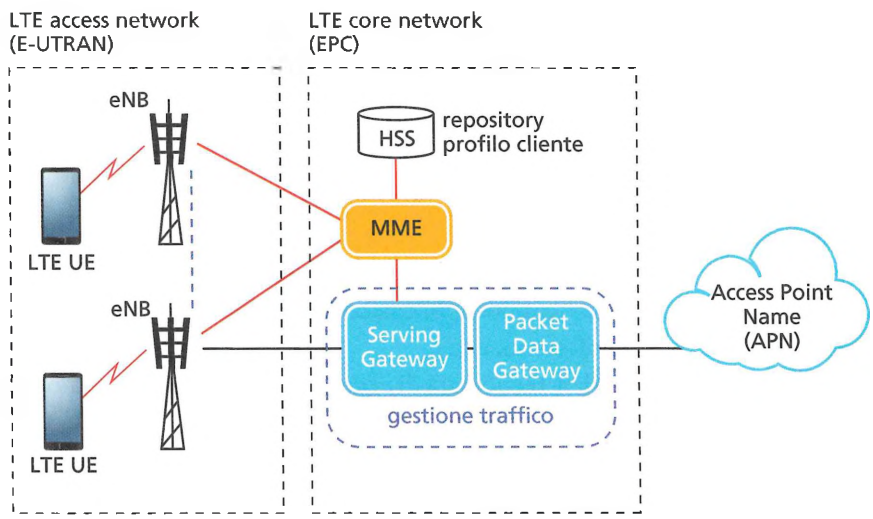
FIGURA 10 Antenna LTE per stazione base



Infatti, nelle aree in cui il traffico è molto intenso e sono presenti numerosi utenti, non è sufficiente l'utilizzo di tutte le frequenze disponibili per aumentare la capacità e soddisfare così le richieste di accesso alla rete. MIMO permette miglioramenti nel throughput e nella distanza di trasmissione senza ricorrere a frequenze addizionali o a maggiore potenza nelle trasmissioni.
Una soluzione è perciò quella di aumentare il numero di antenne sia nella Base Station sia nel dispositivo mobile.
Si consideri il seguente esempio: l'antenna presente in un eNodeB è configurata con 4 porte per la trasmissione e 4 per la ricezione (**4T4R**), gli smartphone che si collegano in downlink a questa Base Station sono dotati di sole 2 antenne per ricevere. L'antenna opera in MIMO 2×2 e non in MIMO 4×4.
Gli smartphone di nuova generazione, denominati **Gigabit LTE**, sono dotati di 4 antenne, quindi se si collegano a un eNodeB con antenna 4T4R potranno ricevere 4 flussi di dati. In quest'ultimo caso si può parlare di MIMO 4×4.

L'architettura LTE è semplificata rispetto alle precedenti, così da migliorarne le prestazioni. Infatti, spostando molte funzioni su eNodeB, si è potuto diminuire la latenza in rete e aumentare il throughput, condizioni indispensabili per i servizi a elevata interattività.
La FIGURA 11 mostra l'architettura di una rete 4G LTE mettendo in evidenza la componente della sicurezza.

FIGURA 11 Architettura di una rete LTE



La parte di **rete di accesso E-UTRAN** è costituita dai seguenti elementi:

- **LTE User Equipment (LTE-UE)**: è il terminale mobile composto da un ricetrasmettitore radio e da una smart card (**USIM**, Universal Subscriber Identity Module), evoluzione della SIM, che contiene i dati identificativi dell'utente, utilizzati per l'accesso al servizio e per l'autenticazione;
- **eNodeB (eNB)**: è la stazione base che si interfaccia alla rete core EPC sul piano di controllo con la componente MME e sul piano utente con la componente SGW, attraverso la quale avviene infatti l'invio dei dati utente. Inoltre, eNodeB svolge funzioni di sicurezza, tipicamente implementate con tecniche di **tunneling** usando la suite **IPsec** (descritta nell'Unità 3), fornendo servizi di autenticazione, integrità e cifratura dei dati.

Gli elementi principali che compongono la rete core EPC sono:

- **Mobility Management Entity (MME)**: è l'elemento fondamentale della EPC che svolge funzioni di controllo, quali, per esempio, l'autenticazione del terminale LTE-UE tramite il database HSS; si occupa della gestione della connessione con il terminale e degli aspetti di mobilità;
- **Home Subscriber Server (HSS)**: è il database della rete che contiene i profili degli utenti (clienti dell'operatore telefonico) e di posizione; HSS include anche l'Authentication Center che si occupa di generare le chiavi per la cifratura dei dati e per la mutua autenticazione dell'utente e della rete;
- **Serving Gateway (SGW) e Packet Data Gateway (PGW)**: sono le entità coinvolte nel trasporto delle informazioni in base al servizio richiesto; il PGW assegna un indirizzo IP al UE che lo manterrà fino a che il terminale non verrà spento;
- **Access Point Name (APN)**: identifica la rete IP a cui può accedere l'utente una volta stabilita la connessione dati. L'APN può puntare a una rete privata (per esempio una intranet aziendale) o pubblica (per esempio Internet). È possibile definire APN distinti per applicazioni diverse, infatti l'APN memorizzato in UE identifica il servizio richiesto dall'utente.

LE RELEASE DA LTE A 5G EMESSE DA 3GPP

3GPP (3rd Generation Partnership Project, *www.3gpp.org*) è un'organizzazione nata nel 1998 per la diffusione di sistemi mobili basati su GSM. Negli anni la sua attività è evoluta nello sviluppo e gestione delle nuove tecnologie mobile.
La tabella che segue elenca alcuni dei documenti, denominati **Release**, emessi da 3GPP negli ultimi anni e quelli previsti per gli anni a venire, tra i quali quelli riguardanti la rete 5G. Si può notare come spesso le Release contengano specifiche relative a più tecnologie.

IN ENGLISH PLEASE

Rel.	Year	Key Features
8	2009	**Long Term Evolution (LTE)**. Dual-carriers **HSDPA**.
9	2010	WiMAX and LTE/UMTS interoperability. Dual-carriers **HSDPA** with **MIMO**.
10	2011	**LTE-Advanced**. Multicarriers **HSDPA**.
11	2013	Advanced IP Interconnection of Services. Coordinated Multi Point **CoMP**.
12	2015	Public safety support. Device-to-device communications. Enhanced Small Cells.

→

13	2016	**LTE-Advanced Pro** features. LTE operation in unlicensed bands. Full-dimension MIMO. LTE-WLAN Aggregation. Narrowband Internet of Things (NB-IoT).
14	2017	LTE-Advanced Pro additional features, such as energy efficient, location services, mission critical data and video over LTE. Study item for **5G New Radio**.
15	2018	Additional LTE-Advanced Pro features, such as ultra-reliable low-latency communications. **Phase 1 of 5G**. Will emphasize enhanced mobile broadband use case and sub-40 GHz operation. Includes Massive MIMO, beamforming, and 4G-5G interworking, including ability for LTE connectivity to a 5G core network.
16	2020	**Phase 2 of 5G**. Full compliance with ITU IMT-2020 requirements. Will add URLLC, spectrum sharing, unlicensed operation and multiple other enhancements.
17	*planned for 2021*	Further LTE and 5G enhancements.

4.3 LTE-Advanced e LTE-Advanced Pro

LTE-ADVANCED (LTE-A)

A partire dalla Release 10 il 3GPP ha lavorato all'evoluzione di LTE (**LTE-Advanced**), introducendo alcune importanti funzionalità. Vediamone alcune.

- **Carrier aggregation**: grazie all'aggregazione di due o più portanti è possibile raggiungere i 100 MHz di ampiezza di banda.
- **Enhanced MIMO**: miglioramento delle tecniche multi-antenna arrivando a configurazioni 8×8 su downlink e 4×4 su uplink (in trasmissione e in ricezione), con conseguente maggiore capacità e copertura.
- **Relaying**: LTE-A prevede l'impiego di ripetitori intelligenti, detti **Relay Node** (**RN**), che, compensando l'attenuazione di propagazione tra UE e eNodeB, consentono di aumentare la capacità e la copertura (FIGURA 12).

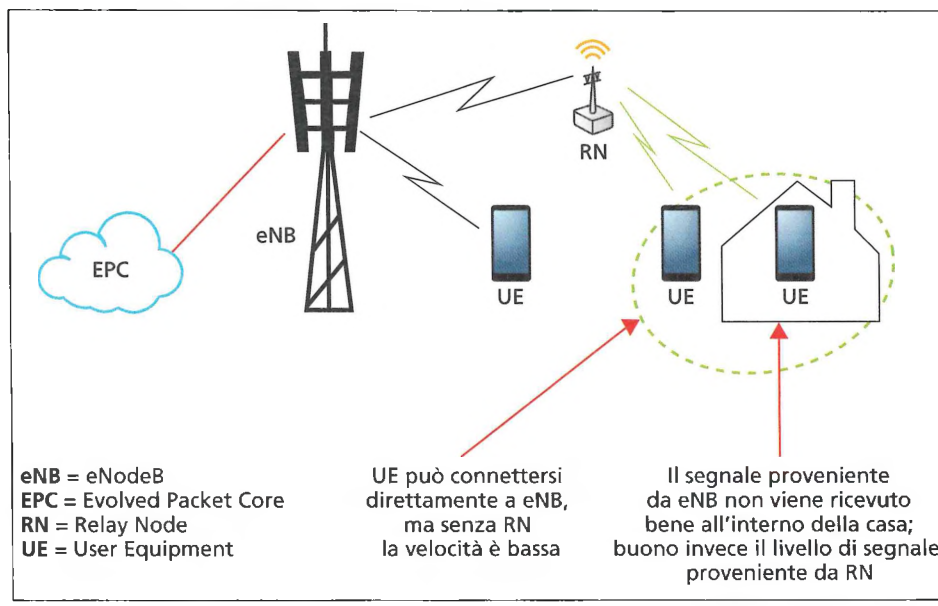


FIGURA 12 Scenario di rete di accesso LTE-A con Relay Node

LTE-ADVANCED PRO (LTE-A PRO)

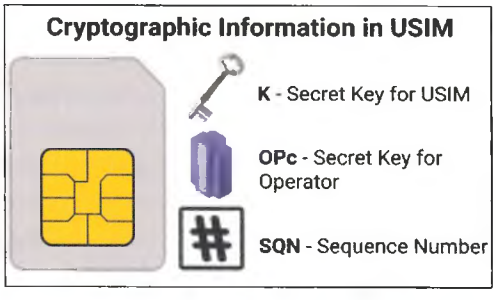
L'ultima versione di LTE, dalla Release 13 in poi, è denominata **LTE-Advanced Pro**, nota anche come **4.5G**, che continuerà a essere aggiornata anche dopo l'introduzione del 5G.

Questa Release introduce numerose funzionalità che migliorano l'efficienza di LTE, ma soprattutto cerca di rispondere alle esigenze di un mercato in continua evoluzione.
Sono state così introdotte:

- migliorie in ambito MTC (Machine-Type Communication), concentrando l'attenzione su categorie di UE poco complesse, come i sensori o gli attuatori usati in ambito IoT, che necessitano di poca banda, ma richiedono di ridurre i consumi energetici per allungare la durata della batteria;
- nuove funzioni per la sicurezza pubblica (per esempio in ambito radiosorveglianza);
- internetworking con le reti Wi-Fi;
- accesso a frequenze non licenziate, condividendo i 5 GHz usati da alcuni dispositivi Wi-Fi;
- aggregazione di un numero maggiore di portanti (carrier);
- impiego di un numero maggiore di antenne per aumentare l'efficienza trasmissiva;
- introduzione di nuovi meccanismi per ridurre ulteriormente la latenza rispetto alle release precedenti.

IN ENGLISH PLEASE

On the **USIM** we've got two values that are entered in when the USIM is provisioned, the K key – Our secret key, and an OPc key (operator key).
These two keys are the basis of all the cryptography that goes on, so should never be divulged.
The only other place to have these two keys in the HSS, which associates each K key and OPc key combination with an IMSI.
The USIM also stores the SQN a sequence number, this is used to prevent replay attacks and is incremented after each authentication challenge, starting at 1 for the first authentication challenge and counting up from there.



FISSA LE CONOSCENZE

- Descrivi le generazioni di reti mobili che si sono succedete negli anni.
- Come sono chiamate le tecnologie LTE del 4G e 4.5G?
- Qual è il ruolo del 3GPP?
- Quali componenti sono presenti nella rete di accesso LTE?

Case study
Reti mobili per la domotica

5 LA RETE 5G

5.1 Release, caratteristiche e servizi 5G

#techwords

Abstract Syntax Notation One (più comunemente conosciuto come ASN.1) è un linguaggio per definire standard senza far riferimento all'implementazione.

La FIGURA 13 mostra l'evoluzione **da LTE-Advanced Pro a 5G**, e i rilasci delle relative specifiche, denominate **Release**, da parte del 3GPP. I 3 stadi previsti sono:

- **Stage 1**: descrizione del servizio dal punto di vista dell'utente che ne usufruirà;
- **Stage 2**: definizione dell'architettura funzionale e dei flussi informativi tra i vari elementi che la compongono;
- **Stage 3**: implementazione concreta delle nuove funzionalità e protocolli sugli elementi fisici che corrispondono agli elementi logici descritti nell'architettura (Stage 2).

FIGURA 13 3GPP Release per l'introduzione del 5G

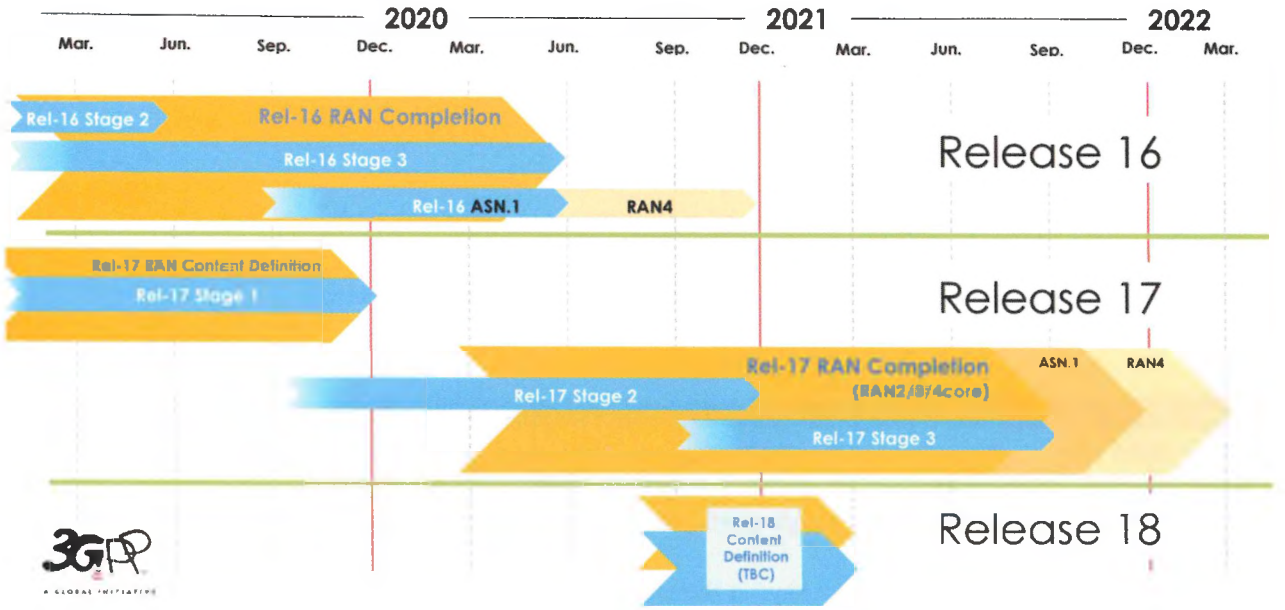
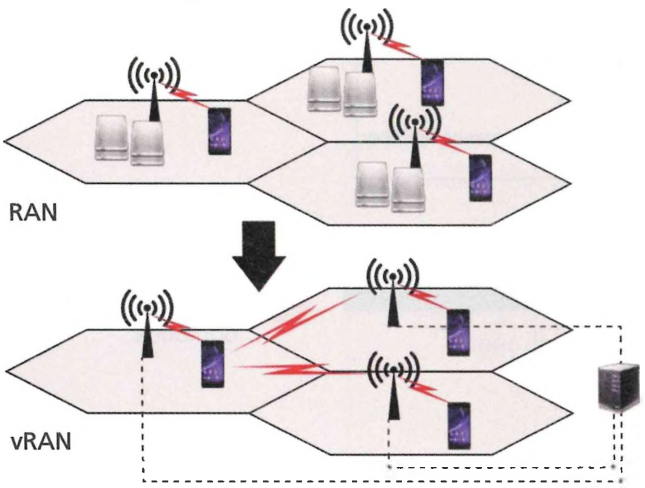


FIGURA 14 Evoluzione verso architetture centralizzate



La continua evoluzione della capacità elaborativa delle tecnologie al silicio, spinge gli operatori telefonici a ripensare l'architettura della rete di accesso radio (**RAN**, Radio Access Network) verso una soluzione virtualizzata (**vRAN**, virtual RAN) dove porzioni sempre maggiori delle funzionalità di elaborazione dei protocolli radio vengono centralizzate e ospitate in data center (FIGURA 14).

La "virtualizzazione" di buona parte dei livelli protocollari e degli algoritmi di elaborazione del segnale, consentirà un'estrema versatilità nelle operazioni di riconfigurazione e di implementazione di nuove funzionalità in modalità flessibile e sostenibile.

Come 2G coesiste ancora con 3G e 4G, anche 5G coesisterà per alcuni anni insieme alle tecnologie LTE.

La rete 5G nasce sulla spinta di alcuni fattori emergenti:

- **crescita esponenziale del traffico dati** per l'aumento del numero di smartphone, con velocità di trasferimento elevata, e dell'incremento della domanda per applicazioni multimediali (il traffico video ora è circa il 50% del traffico dati sulla rete mobile e aumenterà ancora con i video 3D);
- **connessione a Internet di dispositivi prima isolati**: l'**Internet of Things** si occupa di comunicazioni Machine-to-Machine (M2M); questo traffico, in ambito 3GPP, è definito **Machine-Type Communications** (MTC), per distinguerlo dal traffico generato dalle persone (**Human-Type Communications**, HTC); si tratta di trasmissioni sporadiche di piccole quantità di dati da parte di numerosissimi dispositivi a bassa mobilità che, dispiegati sul territorio, devono assicurare anni di funzionamento senza dover sostituire la batteria (per esempio apparecchiature di magazzino, sistemi di localizzazione);
- **trasporto di dati non IP**, per esempio quelli generati dai dispositivi IoT (sensori, attuatori);
- **supporto di accessi non-3GPP e da rete fissa**, per esempio accessi provenienti da reti WLAN;
- l'**introduzione del protocollo IPv6** per poter gestire l'aumento esponenziale di terminali mobili contemporaneamente attivi.

#prendinota

Un esempio di comunicazioni M2M sono quelle dei sensori per rilevare da remoto i consumi energetici di un'apparecchiatura; oppure quelle dei sistemi di allarme in grado di rilevare immagini e contattare le centrali di controllo in caso di necessità.

Elenchiamo alcune delle caratteristiche del 5G, rispondenti ai fattori citati, con l'indicazione dei servizi che potranno essere realizzati grazie a queste:

- elevata quantità di banda a disposizione per lo sviluppo di servizi basati su video e servizi in cloud per il trasferimento dati e l'elaborazione distribuita;
- possibilità di costruire reti con bassissima latenza, fondamentale per trasporti e auto a guida autonoma e per i sistemi di controllo industriale;
- possibilità di gestire un numero molto maggiore di connessioni a costi e consumi energetici contenuti che agevola lo sviluppo dei servizi legati all'IoT (le comunicazioni di sensori e attuatori saranno sempre più numerose);
- flessibilità e rapidità nel riconfigurare le reti.

Le caratteristiche sopra elencate rendono il 5G una tecnologia abilitante per tutta una serie di servizi che possono essere raggruppati in 3 grandi categorie (FIGURA 15).

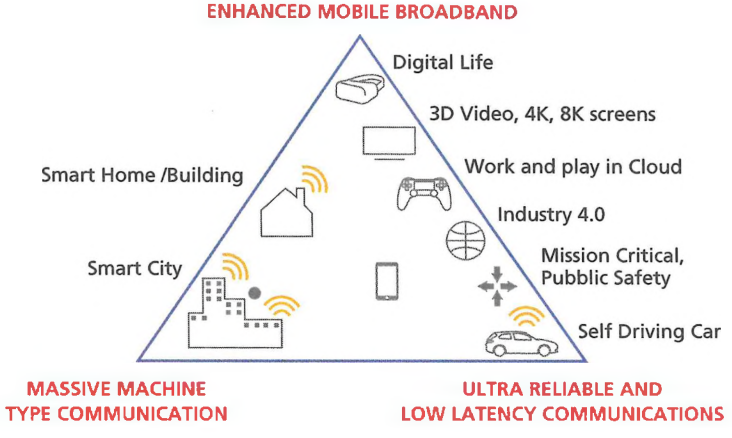
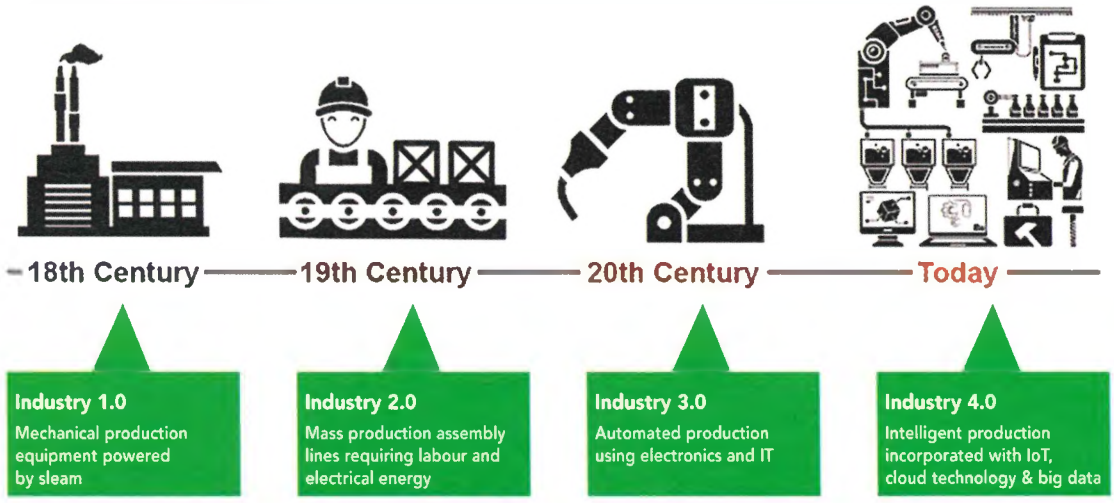


FIGURA 15 La piramide dei servizi 5G

1. **I servizi del mobile ultrabroadband evoluto** (**eMBB**, Enhanced Mobile Broadband): i principali servizi saranno l'accesso a Internet a banda ultralarga e l'impiego del cloud per lavoro o per gaming, le applicazioni di realtà aumentata e realtà virtuale (AR/VR), ma si avranno anche impatti nel settore dell'educazione e formazione.
2. **I servizi dell'IoT massivo** (**mIoT**, massive Internet of Things o **mMTC**, massive Machine-Type Communication): la comunicazione è caratterizzata da un numero elevato di dispositivi collegati in rete, con trasmissione di poche informazioni non particolarmente sensibili al ritardo. Il numero di oggetti, sensori, attuatori da collegare, presenti in un'area ristretta, supererà di molto il numero di esseri umani, l'IoT massivo porterà trasformazioni nell'industria (Industry 4.0) e nell'agricoltura (Smart Agricolture) e in molti altri settori quali Smart City, Smart Building, sistemi di assistenza sanitaria domestica, sicurezza da remoto.
3. **I servizi critici** (**URLLC**, Ultra-Reliable & Low Latency Communication): esistono aree applicative che richiedono altissima affidabilità, latenza ridotta, con elevati requisiti di sicurezza e disponibilità di servizio, per esempio:
   - **veicoli a guida autonoma**, che trasformeranno il settore industriale dell'auto e tutta l'economia dei trasporti e della mobilità; rientrano qui le comunicazioni Vehicle to Vehicle e Vehicle to Infrastructure (V2X) rese già disponibili con LTE, che forniscono al guidatore e al veicolo informazioni (e comandi) per ridurre gli incidenti, ma anche l'inquinamento;
   - **droni autonomi e connessi in rete**, sistemi non semplicemente teleguidati, che avranno innumerevoli applicazioni nel campo del monitoraggio, delle Smart City e della logistica;
   - **Industry 4.0**, in cui l'elevato grado di automazione richiede, per esempio, una comunicazione sicura e in tempo reale tra i robot (FIGURA 16).

FIGURA 16
Evoluzione dell'industria



FISSA LE CONOSCENZE

- Che cos'è una vRAN?
- Quali saranno i principali servizi abilitati dal 5G?
- Descrivi le principali caratteristiche delle reti 5G.

6 PACKET TRACER: L'IoT PER LA SMART HOME

In questa esercitazione di laboratorio realizzeremo con il simulatore Packet Tracer una smart home controllabile da remoto attraverso le tecnologie 3G/4G.

esercizio

File sorgenti
Scarica il file

→ PROBLEMA

Realizzare un servizio IoT per consentire all'utente registrato di comandare, attraverso il proprio smartphone, i dispositivi intelligenti della propria casa.

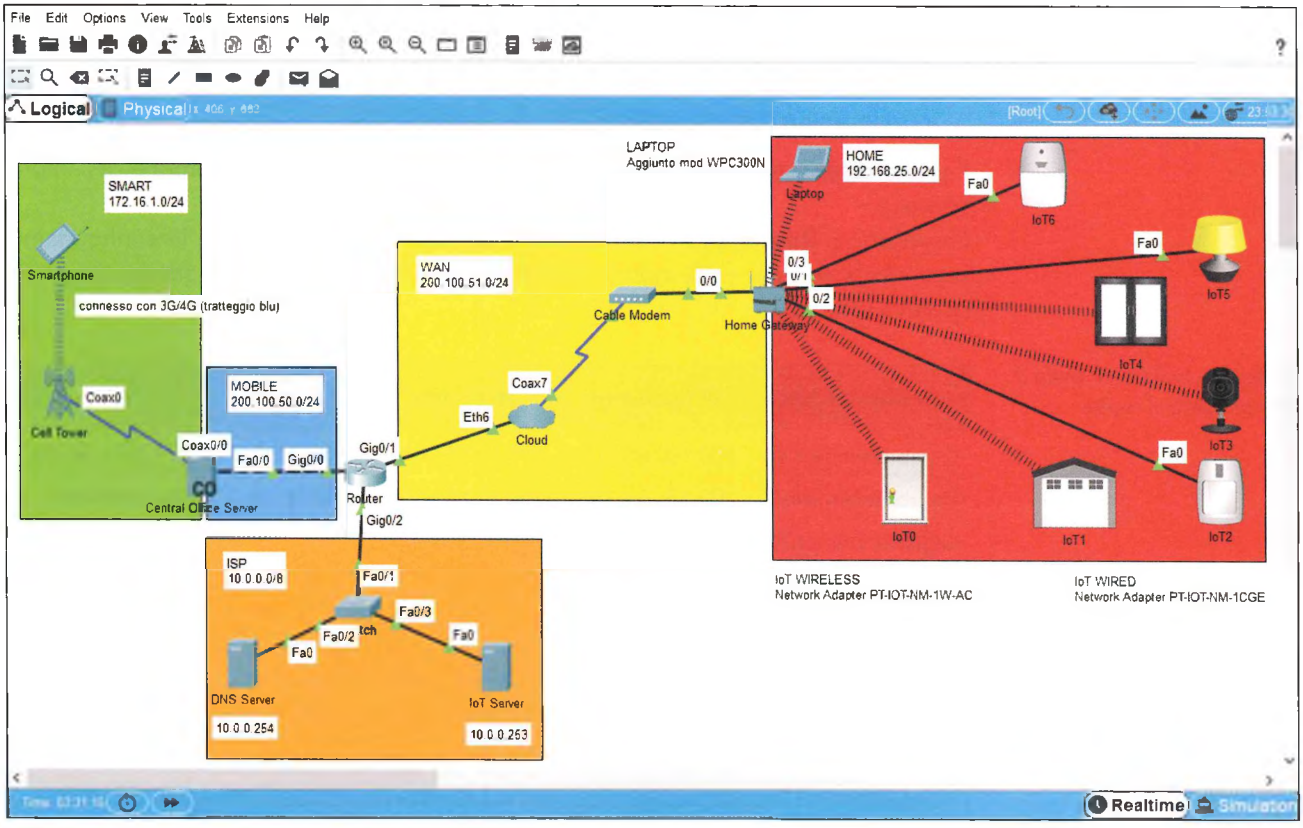
→ ANALISI DEL PROBLEMA

Bisogna innanzitutto realizzare, attraverso un **IoT Server**, la registrazione dell'utente al servizio. Poi rendere il servizio accessibile attraverso il web all'utente registrato. L'utente deve potersi collegare col proprio smartphone alla rete telefonica cellulare **3G/4G**, accedere al servizio con username e password e comandare i dispositivi IoT della casa.

→ SVOLGIMENTO

Si consideri lo scenario mostrato in FIGURA 17.

FIGURA 17 Scenario IoT per la smart home



CONFIGURAZIONE DELLE RETI

Sono presenti 5 reti di cui 3 collegate direttamente al router centrale (ISP, MOBILE e WAN). Queste 3 reti costituiscono l'infrastruttura necessaria a realizzare il servizio e renderlo disponibile su Internet.
Le restanti 2 (HOME e SMART) riguardano l'utente del servizio: la sua rete di casa e quella in cui si trova col suo smartphone.

Queste 2 reti vengono realizzate mediante 2 dispositivi:

- il **Central Office Server** che da un lato gestisce il backbone su cui fluisce il traffico mobile da e verso Internet, dall'altro lato si collega alla **Cell Tower** a cui lo smartphone si aggancia. Il Central Office Server rappresenta quindi l'interfaccia tra l'utente mobile e le dorsali di Internet;
- l'**Home Gateway** che da un lato collega tutti i dispositivi IoT della casa in modalità wired e wireless, dall'altro lato si collega attraverso un modem al **Cloud** sulla rete Internet.

Sia sul Central Office Server che sull'Home Gateway è configurato di default il servizio DHCP per assegnare automaticamente gli indirizzi IP privati ai dispositivi mobili ed eventualmente fissi connessi alla rete.

Vediamo nel dettaglio le 5 reti:

d) ISP (10.0.0.0): rete privata del provider con i server necessari al funzionamento del servizio;

e) MOBILE (200.100.50.0): rete pubblica con Central Office Server per gestire il backbone su cui fluisce il traffico mobile;

f) WAN (200.100.51.0): rete pubblica a cui si collegano i dispositivi IoT della smart home attraverso l'Home Gateway;

g) HOME (192.168.25.0): rete privata con Home Gateway per gestire i dispositivi IoT della casa;

h) SMART (172.16.1.0): rete privata gestita dal Central Office Server con la Cell Tower a cui lo smartphone si collega;

Il primo dispositivo da configurare è il router che funge da nodo centrale dell'intero scenario.
Prendiamo il **Router 2911** fornito di 3 interfacce GigabitEthernet e le configuriamo secondo la TABELLA 1. Gli indirizzi IP delle 3 interfacce faranno da gateway per le rispettive reti.

TABELLA 1 Indirizzi IP delle 3 reti collegate al router

Interfaccia router	IP (gateway)	IP di rete	Nome	Server
GigabitEthernet0/0	200.100.50.1/24	200.100.50.0/24	MOBILE	Central Office Server
GigabitEthernet0/1	200.100.51.1/24	200.100.51.0/24	WAN	Home Gateway
GigabitEthernet0/2	10.0.0.1/8	10.0.0.0/8	ISP	DNS Server: 10.0.0.254 IoT Server: 10.0.0.253

a. Rete ISP

La configurazione verso la rete ISP può essere fatta manualmente assegnando in maniera statica gli indirizzi all'interfaccia del router e ai 2 server (DNS e IoT) come riportato in Tabella 1 e rappresentato in Figura 17.

In seguito configureremo sui 2 server i relativi servizi (DNS e IoT), per ora configuriamo solo i parametri di rete.

b. Rete MOBILE

La configurazione delle altre 2 interfacce può essere fatta manualmente ma è consigliabile impostare un servizio DHCP verso le reti MOBILE e WAN, mettendo a disposizione un pool di indirizzi da assegnare automaticamente. In questo modo è possibile assegnare contemporaneamente anche gli indirizzi di gateway e DNS.

Per quanto riguarda la rete MOBILE la sequenza di comandi da scrivere nella CLI del router diventa quindi:

```
Router(config)#interface GigabitEthernet0/0
Router(config-if)#ip dhcp pool MOBILE                          Assegna un nome al pool di indirizzi per il DHCP.
Router(dhcp-config)#network 200.100.50.0 255.255.255.0         Configura l'indirizzo di rete e la subnet mask.
Router(dhcp-config)#default-router 200.100.50.1                Imposta il gateway della rete.
Router(dhcp-config)#dns-server 10.0.0.254                      Imposta il DNS della rete.
Router(dhcp-config)#exit
Router(config)#
```

L'unico dispositivo collegato alla rete MOBILE è il **Central Office Server** che riceverà dunque un IP appartenente al pool MOBILE (solitamente 200.100.50.2) e tutti i parametri di rete (gateway e DNS).

c. Rete WAN

Per quanto riguarda la rete WAN la sequenza di comandi, del tutto analoga alla precedente, da scrivere nella CLI del router diventa quindi:

```
Router(config)#interface GigabitEthernet0/1
Router(config-if)#ip dhcp pool WAN                             Assegna un nome al pool di indirizzi per il DHCP.
Router(dhcp-config)#network 200.100.51.0 255.255.255.0         Configura l'indirizzo di rete e la subnet mask.
Router(dhcp-config)#default-router 200.100.51.1                Imposta il gateway della rete.
Router(dhcp-config)#dns-server 10.0.0.254                      Imposta il DNS della rete.
Router(dhcp-config)#exit
Router(config)#
```

L'unico dispositivo collegato alla rete WAN è l'**Home Gateway** che riceverà dunque un IP appartenente al pool WAN (solitamente 200.100.51.2) e tutti i parametri di rete (gateway e DNS).

Sia sul Central Office Server che sull'Home Gateway va impostato il DHCP dalla scheda Config selezionando l'opportuna interfaccia:

- INTERFACE **Backbone** per il Central Office Server;
- INTERFACE **Internet** per l'Home Gateway.

> Della rete WAN fanno anche parte un dispositivo **Cloud** che ricevuto il segnale su cavo Ethernet lo inoltra su cavo coassiale e un dispositivo **Cable Modem** che fa l'operazione inversa.

Sul dispositivo Cloud, dalla scheda Config→INTERFACE, occorre configurare l'interfaccia **Ethernet6** con **Provider Network** selezionato su **Cable**. Inoltre, dalla scheda Config→CONNECTIONS, occorre configurare la connessione **Cable** aggiungendo (Add) la entry che crea l'associazione **Coaxial7-Ethernet6**.
Sul dispositivo Cable Modem non è necessario configurare alcunché.

d. Rete HOME

Dobbiamo innanzitutto settare la scheda **Wireless** dell'Home Gateway che farà da Access Point per tutti i dispositivi IoT wireless presenti nella casa. Lasciamo l'**SSID** di default (HomeGateway) e impostiamo l'**Authentication** WPA2-PSK con Pass Phrase **0123456789**.

Il dispositivo che gestisce la rete HOME è, come abbiamo già detto, l'Home Gateway. Questo dispositivo dispone di un servizio DHCP che assegna gli IP automaticamente in classe 192.168.25.0/24 nel seguente modo:

- 192.168.25.1 all'interfaccia **LAN** dell'Home Gateway che fa da Default Gateway per i dispositivi IoT;
- da 192.168.25.100 a 192.168.25.255 per i **dispositivi IoT** che abbiano settato il DHCP nella scheda Config.

La rete HOME è costituita da numerosi dispositivi IoT di vario tipo: porte, garage, rilevatori di movimento, finestre, sirene, luci e webcam. Su ognuno di essi possiamo configurare il **Network Adapter** a seconda che il dispositivo venga cablato (wired) o collegarlo col Wi-Fi (wireless).

Selezionando un qualsiasi dispositivo IoT, aprendo la scheda **Specifications** e cliccando su **Advanced**, si avrà la possibilità di selezionare la nuova scheda **I/O Config** dove impostare il Network Adapter (FIGURA 18). Per esempio:

- PT-IOT-NM-1CFE o PT-IOT-NM-1CGE per cablare il dispositivo su una porta FastEthernet o GigabitEthernet;
- PT-IOT-NM-1W o PT-IOT-NM-1W-AC per collegare wireless il dispositivo col Wi-Fi.

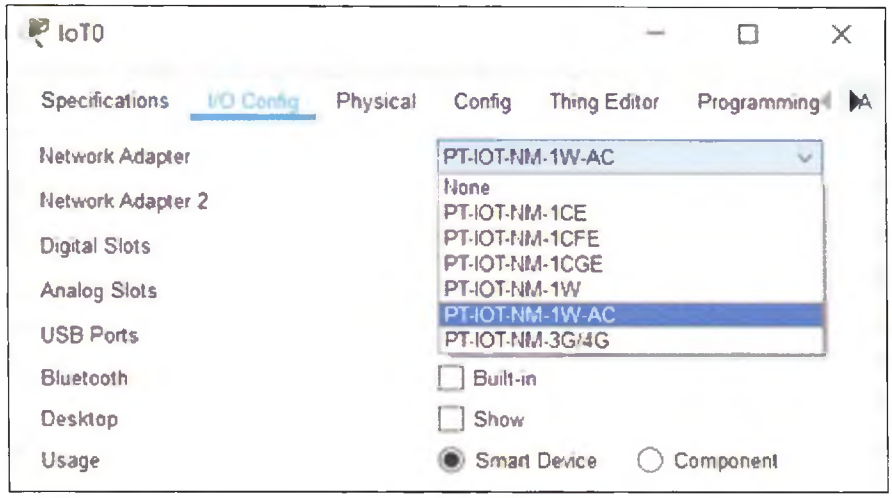


FIGURA 18 Configurazione del Network Adapter

I dispositivi **wired** sono subito pronti, il DHCP dell'Home Gateway gli assegna immediatamente i parametri di rete. Naturalmente su ogni dispositivo IoT wired dovrà essere impostato il DHCP sull'interfaccia Ethernet verso l'Home Gateway.

I dispositivi **wireless** vanno prima configurati per collegarsi in Wi-Fi all'Home Gateway e poi va impostato il DHCP sull'interfaccia wireless verso l'Home Gateway.

Su tutti i dispositivi IoT, wired e wireless, previsti nella rete HOME va impostato il DHCP.

La FIGURA 19 mostra l'avvenuto assegnamento alla sirena, che è cablata, dei seguenti parametri di rete:

- IP e subnet mask: 192.168.25.106/24;
- Gateway: 192.168.25.1 (indirizzo dell'Home Gateway);
- DNS Server: 10.0.0.254 (indirizzo del DNS Server dell'ISP).

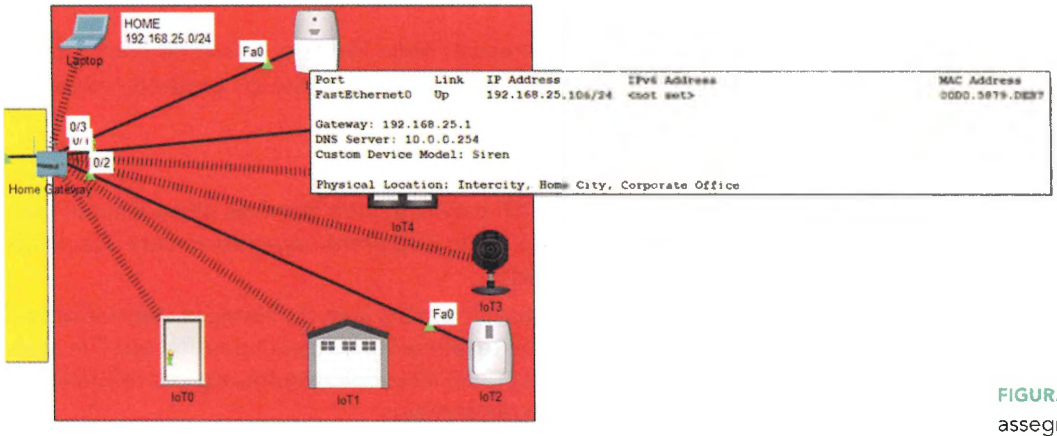


FIGURA 19 Parametri di rete assegnati a un IoT wired

Sui dispositivi IoT wireless dobbiamo impostare l'**SSID** di default (HomeGateway) e l'**Authentication** WPA2-PSK con Pass Phrase **0123456789**, esattamente come è stato fatto per l'Home Gateway. Impostiamo poi il **DHCP**, esattamente come è stato fatto per tutti i dispositivi IoT cablati della casa.
A questo punto, anche ai dispositivi IoT wireless vengono assegnati i parametri di rete.

Per poter gestire e testare tutti i dispositivi IoT da locale, configuriamo un **Laptop** a cui è stato aggiunto un modulo **mod WPC300N** per consentirgli di connettersi al Wi-Fi della rete HOME.
Anche sul Laptop, dopo aver aggiunto il modulo, impostiamo l'**SSID** di default (HomeGateway), l'**Authentication** WPA2-PSK con Pass Phrase **0123456789** e il **DHCP**, esattamente come è stato fatto per tutti i dispositivi IoT della casa.

#prendinota

Sul Laptop è anche possibile configurare l'accesso alla rete wireless (SSID = HomeGateway) selezionando Desktop→PC Wireless→Connect

e. Rete SMART

Il Central Office Server per la rete SMART si comporta esattamente come l'Home Gateway per la rete HOME.

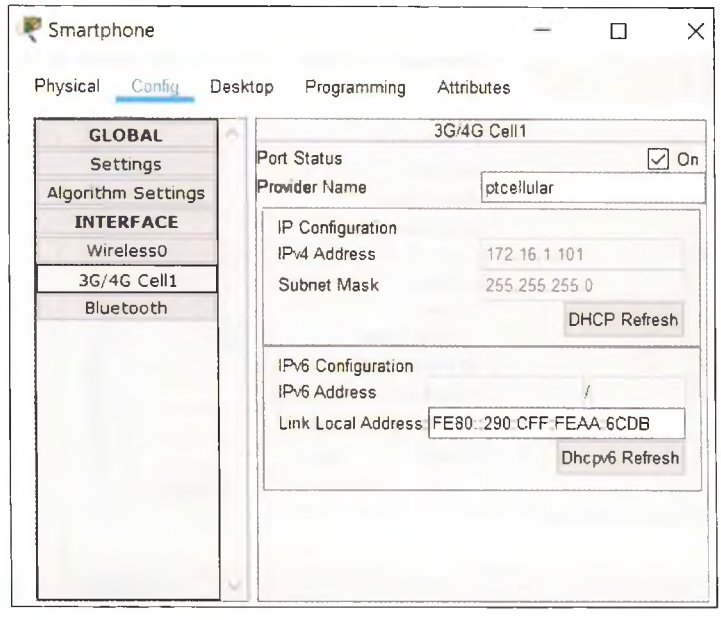
Il dispositivo che gestisce la rete SMART è, come abbiamo già detto, il Central Office Server. Questo dispositivo dispone di un servizio DHCP che assegna gli IP automaticamente in classe 172.16.1.0/24 nel seguente modo:

- 172.16.1.1 all'interfaccia **Cell Tower** del Central Office Server che fa da Default Gateway per gli smartphone;
- da 172.16.1.101 a 172.16.1.255 per gli smartphone che abbiano settato il DHCP nella scheda Config.

La Cell Tower fa da **3G/4G Server** per gli smartphone consentendo loro di collegarsi al Central Office Server mediante un collegamento coassiale.
Dal Central Office Server i pacchetti proseguiranno su Ethernet.

Dopo aver settato il DHCP, lo Smartphone riceverà dal Central Office Server tutti i parametri di configurazione per l'interfaccia **3G/4G Cell1** (FIGURA 20) e l'utente potrà connettersi a Internet attraverso la rete telefonica cellulare.

FIGURA 20 Parametri di rete assegnati allo Smartphone



CONFIGURAZIONE DEL SERVIZIO

Terminata la configurazione delle reti presenti nello scenario, possiamo configurare il servizio per il controllo, da locale e da remoto, dei dispositivi IoT presenti nella smart home.

Cominciamo col configurare i 2 server:

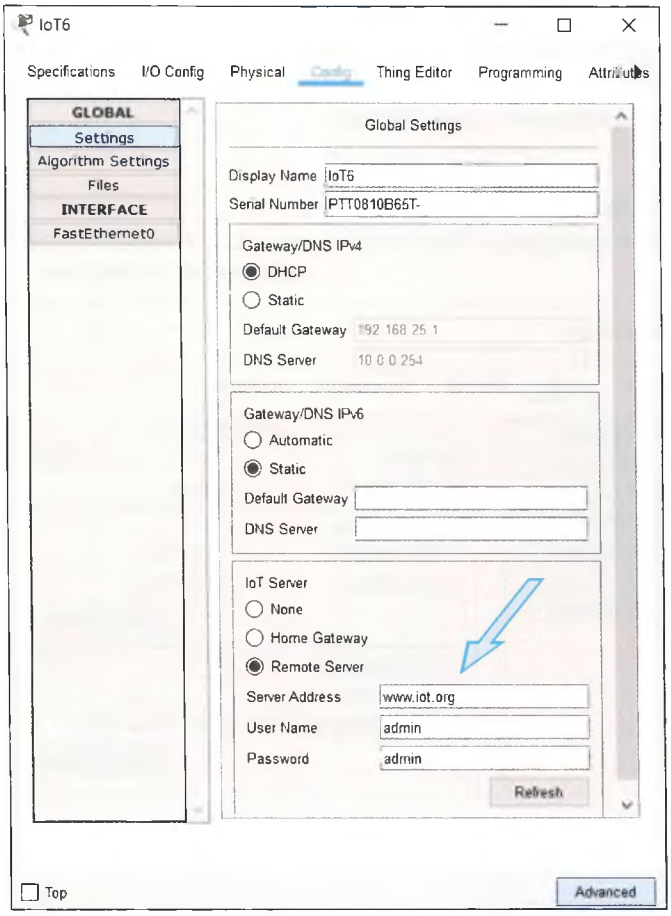
- clicchiamo sull'IoT Server della rete ISP e dalla scheda **Services** selezioniamo il servizio **IoT** e lo mettiamo **On**. In questo modo sarà pronto quando arriverà una richiesta di creazione o di accesso al servizio;
- Clicchiamo sul DNS Server della rete ISP e dalla scheda **Services** selezioniamo il servizio **DNS** e aggiungiamo (Add) un **Resource Records** di tipo ARecord che associ all'indirizzo IP dell'IoT Server (10.0.0.253) il Name **www.iot.org** per renderlo più facilmente raggiungibile dagli utenti del servizio:

www.iot.org – A Record – 10.0.0.253

> Provare con un comando ping (dal Command Prompt o con un Simple PDU dall'interfaccia grafica) tra il Laptop e www.iot.org per verificare il funzionamento della rete.

A questo punto configuriamo il servizio sui dispositivi IoT della casa. Prendiamo un qualunque IoT e dalla scheda Config→GLOBAL selezioniamo Settings e impostiamo IoT Server su **Remote Server** con i valori

- Server Address: www.iot.org
- User Name: admin
- Password: admin



Al termine con il bottone in basso a destra Connect o Refresh, effettuiamo la richiesta di collegamento all'IoT Server della rete ISP.
Il DNS Server inoltrerà all'IP corretto la richiesta inoltrata a www.iot.org.

La FIGURA 21 mostra l'operazione svolta sull'IoT6 (la sirena).

Identica operazione va svolta su tutti gli IoT della casa.

FIGURA 21 IoT Server configurato sll'IoT6

VERIFICA DEL SERVIZIO

Cominciamo a verificare il controllo dei dispositivi IoT da locale, mediante il **Laptop** della rete HOME.

Dalla scheda Desktop selezioniamo IoT Monitor (FIGURA 22). Nella scheda che si apre inseriamo nell'IoT Server Address **www.iot.org** e lasciamo **admin** come User Name e Password (FIGURA 23).

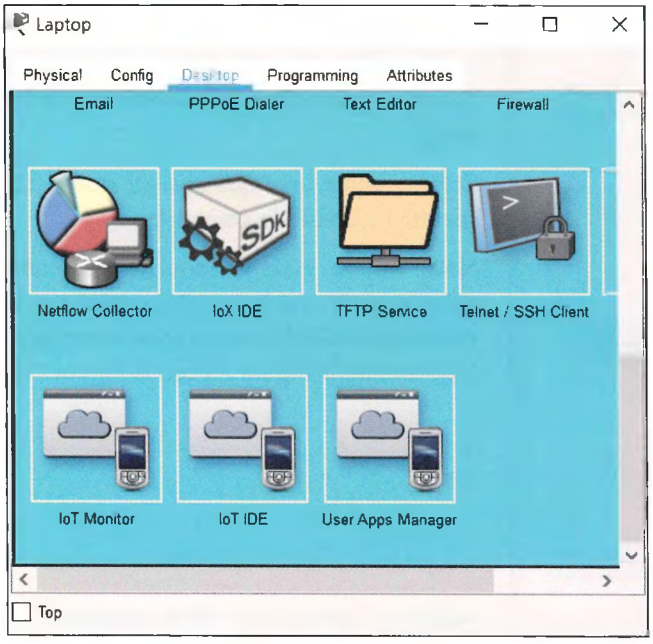


FIGURA 22 IoT Monitor

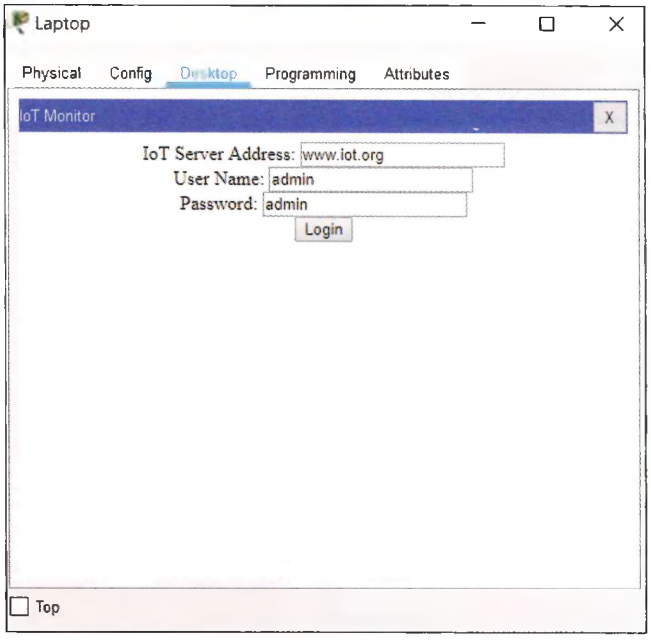


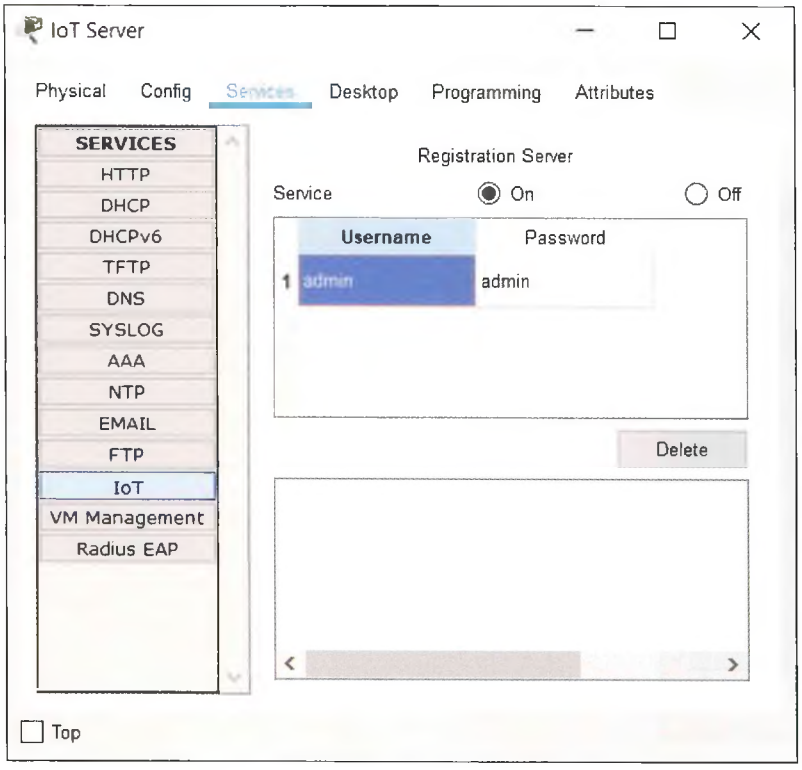
FIGURA 23 IoT Server Address

Al primo accesso da parte del Laptop, l'IoT Server (www.iot.org) richiede la creazione di un account a cui andiamo a mettere **admin** come User Name e come Password. La funzione di Server Registration dell'IoT Server registrerà automaticamente User Name e Password dell'utente e consentirà l'accesso solo agli utenti con le corrette credenziali.

#prendinota

Anche il Laptop, pur essendo nella rete HOME, passa attraverso i server della rete ISP per accedere al servizio e controllare i dispositivi IoT.

Per verificare che l'utente **admin admin** sia stato correttamente registrato, clicchiamo sull'IoT Server e dalla scheda **SERVICES** selezioniamo il servizio **IoT**. La FIGURA 24 mostra l'avvenuta registrazione dell'utente sull'IoT Server dell'ISP.



Dopo questa operazione può essere necessario rifare il Connect o Refresh sui dispositivi IoT illustrato in Figura 21.

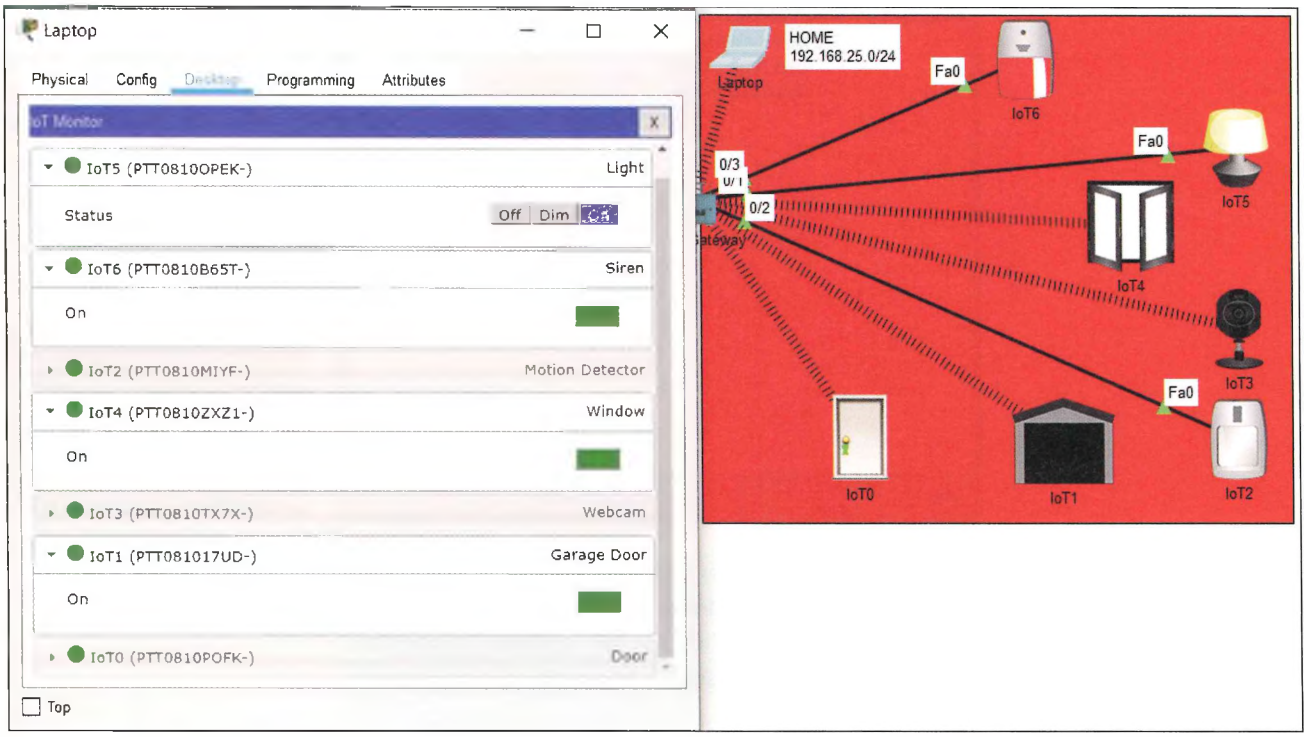
Effettuato il Login con il Laptop apparirà un pannello di controllo con tante righe quanti i dispositivi IoT connessi (pallini verdi).

Selezionando uno qualsiasi di questi dispositivi è possibile comandarli.

Nella FIGURA 25 è mostrato lo scenario dopo aver acceso la lampada, azionato la sirena, aperto la finestra e aperto il garage (confrontare la Figura 25 con la Figura 17).

FIGURA 24 Utente admin admin registrato sull'IoT Server

FIGURA 25 Pannello del Laptop per controllo da locale



Verifichiamo infine il controllo dei dispositivi IoT da remoto, mediante lo **Smartphone** della rete SMART.

Esattamente come fatto per il Laptop e mostrato nelle Figure 6 e 7, dalla scheda Desktop selezioniamo IoT Monitor e nella scheda che si apre inseriamo nell'IoT Server Address **www.iot.org** e lasciamo **admin** come User Name e Password.

Effettuato il Login apparirà un pannello di controllo con tante righe quanti i dispositivi IoT connessi (pallini verdi). Selezionando uno qualsiasi di questi dispositivi è possibile comandarli.

Nella FIGURA 26 è mostrato lo scenario dopo aver chiuso la finestra e il garage (confrontare la Figura 26 con la Figura 25).

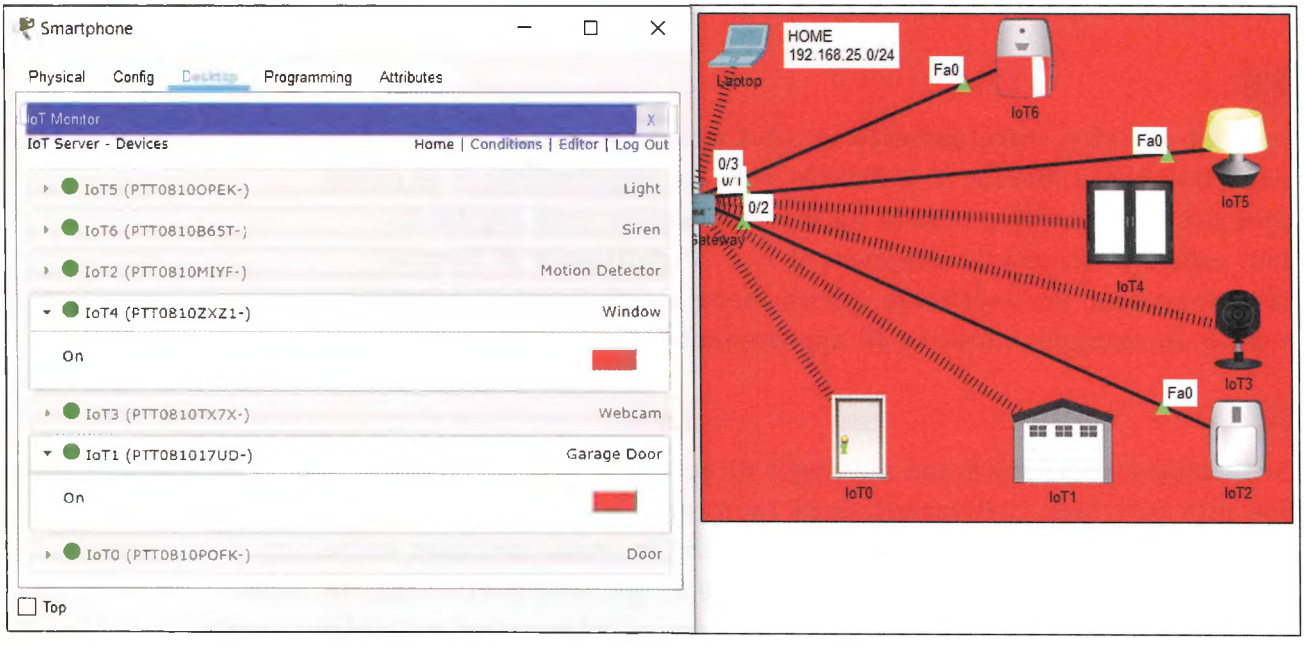


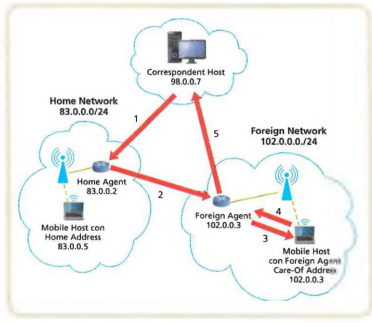
FIGURA 26 Pannello dello Smartphone per controllo da remoto

FISSA LE CONOSCENZE

- Quali sono i compiti del Central Office Server?
- Quali sono i compiti dell'Home Gateway?
- Quali sono i server della rete ISP e come vanno configurati?
- A che cosa serve il Network Adapter sugli IoT della casa?
- A che cosa serve l'IoT Monitor su Laptop e Smartphone?

DIDATTICA INCLUSIVA

1 Gestire la mobilità in una rete IP



Con mobilità si intende la capacità di un dispositivo di comunicare durante gli spostamenti. In IPv4 e in IPv6, l'instradamento dei pacchetti è basato sul prefisso di sottorete dell'indirizzo di destinazione in essi contenuto. Perciò, per poter continuare a comunicare, un nodo mobile dovrebbe cambiare il suo indirizzo IP in ogni nuova rete. Per realizzare la comunicazione mobile è necessario effettuare il routing triangolare, cioè una triangolazione tra router che consente al dispositivo mobile di essere rintracciato nella rete ospite.

2 Il protocollo Mobile IP

In IPv4 e IPv6 è stato definito un protocollo apposito per la mobilità: rispettivamente Mobile IP e Mobile IPv6. La registrazione è la prima cosa che il dispositivo mobile deve fare presso la rete ospite. La rete ospite si occupa di assegnare il nuovo indirizzo e di fornire la connessione. Per realizzare questo viene assegnato al dispositivo mobile un secondo indirizzo IP appartenente alla rete ospite.

3 Le reti cellulari e l'accesso a Internet

La telefonia cellulare è una tipologia di accesso a una rete telefonica attraverso una rete cellulare. Utilizzando onde radio per l'accesso alla rete telefonica, è in grado di servire intere aree geografiche in modo continuo anche con utenti mobili. Il problema fondamentale è la gestione della mobilità, noto come handoff. In pratica si tratta di evitare le interruzioni nel collegamento a fronte di un cambio di cella con relativo cambio di frequenze o a fronte di un cambio di operatore (roaming), cioè un vero e proprio cambio di rete.

4 La mobilità nelle reti 4G LTE

Gli ultimi progressi in ambito radio hanno permesso la diffusione della rete 4G, che si basa sulla tecnologia LTE (Long Term Evolution), la quale fornisce ai terminali utenti (smartphone, tablet, ecc.) una connettività IP completa.

5 La rete 5G

Il 5G nasce sulla spinta di alcuni fattori emergenti come la crescita esponenziale del traffico dati, la connessione a Internet di dispositivi prima isolati (Internet of Things) e il trasporto di dati non IP. La continua evoluzione della capacità elaborativa delle tecnologie al silicio, spinge gli operatori telefonici a ripensare l'architettura della rete di accesso radio verso una soluzione virtualizzata, più flessibile e sostenibile.

VERIFICA DI FINE UNITÀ

Test
Svolgi il **test interattivo**

Quali delle seguenti affermazioni sono vere (V) e quali false (F)?

1. Correspondent Host è il dispositivo con il quale sta comunicando il Mobile Host. V F
2. Il Foreign Address di un Mobile Host corrisponde al Care-Of Address. V F
3. I messaggi Agent Advertisement sono inviati in modalità broadcast. V F
4. Il protocollo Mobile IP è più efficiente se il Correspondent Host è un dispositivo mobile. V F
5. Celle adiacenti utilizzano frequenze diverse per evitare interferenze. V F
6. Ogni cellulare è individuabile mediante un codice univoco chiamato MAC (Media Access Control). V F
7. Nell'architettura LTE i profili degli utenti sono contenuti nel componente HSS. V F
8. I veicoli a guida autonoma sono un tipo di servizio ad alta affidabilità e bassa latenza. V F
9. L'handoff consiste nell'evitare le interruzioni nel collegamento di un dispositivo mobile a fronte di un cambio di cella con relativo cambio di frequenze. V F
10. L'impiego di tunnel IPsec in LTE garantisce la cifratura dei dati ma non la loro integrità. V F

Domande a scelta multipla (una sola è la risposta esatta)

1. **Quale entità controlla il Mobile Host nella rete visitata?**
   A Foreign Agent
   B Home Agent
   C Care-Of Address
   D Permanent Address

2. **L'informazione riguardante in quale rete il Mobile Host si trova in un dato momento è mantenuta:**
   A nei core router della rete WAN
   B nel router della Home Network
   C nell'Access Point della rete Wi-Fi home
   D esclusivamente nel Mobile Host

3. **Il codice identificativo univoco dei cellulari si chiama:**
   A APN
   B KEY
   C IMEI
   D USIM

4. **Quale dei seguenti non è un meccanismo usato in LTE per aumentare la velocità delle trasmissioni?**
   A MIMO
   B User Authentication
   C Carrier Aggregation
   D Banda utilizzata

Ascolta le **risposte**

PREPARATI PER IL COLLOQUIO ORALE

1. LEZIONE 1 **Definisci la Home Network e la Foreign Network.**
2. LEZIONE 1 **Come è stato risolto il problema di mantenere lo stesso indirizzo IP (Home Address) quando il Mobile Host si muove da una rete a un'altra?**
3. LEZIONE 2 **Spiega le caratteristiche del protocollo Mobile IP.**
4. LEZIONE 2 **Come si realizza il routing triangolare nel protocollo Mobile IP?**
5. LEZIONE 3 **Spiega la modalità di accesso a Internet tramite la rete telefonica cellulare.**
6. LEZIONE 3 **In che cosa consiste la tecnica del riutilizzo delle frequenze nelle reti cellulari?**
7. LEZIONE 4 **Descrivi l'architettura di rete mobile LTE.**
8. LEZIONE 5 **Quali sono i fattori che hanno spinto a standardizzare una nuova generazione di rete mobile, la 5G?**
9. LEZIONE 5 **Spiega la rappresentazione a piramide dei servizi abilitati dalla tecnologia 5G.**

IN ENGLISH, PLEASE

CLIL

Ascolta la **pronuncia del testo** e verifica la **traduzione**

ABSTRACT

Mobile and cellular networks

A mobile node is a node that changes its point of attachment into the network over time. Mobility management allows a mobile user to maintain ongoing connection while moving between networks. Mobile Host keeps its address (called home or permanent address) as it moves from one network to another. When a mobile node is resident in a Foreign Network, all traffic addressed to the node's permanent address now needs to be routed to the Foreign Network. Mobile IP is an IETF complex standard for supporting mobility Wi-Fi access. If you cannot access a Wi-Fi hotspot, nowadays you can use cellular networks.
This technology also allows users to maintain their TCP sessions while traveling by car or by train.

LTE has become a global cellular standard and is being deployed quickly; its capabilities continue to improve. Next generation, 5G, is expected for 2020, but many of its capabilities are appearing in advanced forms of LTE (i.e. IoT).

EXERCISES

Use the appropriate number to match words and meanings.

...	Correspondent Host	1	A network element in radio access network responsible for radio transmission and reception
...	Home Agent	2	The ability for a device to function in a serving network different from the home network
...	Permanent Address	3	Code that uniquely identifies a mobile phone
...	Base Station	4	The entity within the Home Network that performs the mobility management functions on behalf of the Mobile Host
...	Mobile IP	5	Mobility management in cellular telephony
...	Roaming	6	The entity that communicates with the Mobile Host
...	Handoff	7	Protocol for the mobility support
...	IMEI	8	The Home Address of the Mobile Host

GLOSSARY

Agent Discovery: it performs task of identifying the passage of the Mobile Host from network to network.
Care-Of Address: the IP address associated with Mobile Hosts visiting a Foreign Network.
Foreign Network: any network other than the mobile node's Home Network.
Machine-to-Machine (M2M): direct communication between devices using a wired or wireless channel.
Mobile Host: a generic terminal that moves from its Home Network to a Foreign Network.
Mobile Switching Center (MSC): the central that, in addition to connecting cells, allows the connection to the fixed telephone network and to the Internet network by acting as a gateway.
Mobility Binding: the association of a Home Address with a Care-Of Address, along with the remaining lifetime of that association.
Uplink: a unidirectional radio link for the transmission of signals from a user terminal to a base station.
Tunneling: a technique to encapsulate the IP datagram in another datagram.

LAVORARE PER COMPETENZE

COMPETENZE IN GIOCO

Competenze disciplinari

- Saper scegliere la tecnologia cellulare adeguata alle richieste di progetto.
- Saper scegliere i sevizi di cloud computing adeguati alle richieste di progetto.
- Saper descrivere e documentare le soluzioni adottate.
- Utilizzare le reti e gli strumenti informatici nelle attività di studio, ricerca e approfondimento disciplinare.

Competenze chiave di cittadinanza

- Interpretare il testo.
- Risolvere problemi.
- Comunicare.
- Competenza digitale.

obiettivi formativi

- Stimolare azioni di ricerca e approfondimento disciplinare.
- Consultare fonti Internet.
- Contestualizzare in un caso reale le nozioni teoriche acquisite studiando.
- Esporre i risultati della ricerca alla classe.

tempi

- Preparazione: 2 ore.
- Presentazione dei risultati e dibattito: 1 ora.
- Autovalutazione: 10 minuti.

strumenti

- Libro di testo.
- Dispositivo connesso a Internet.
- Foglio di carta.
- Software PowerPoint.
- Proiettore collegato al computer in classe o in laboratorio.

TEMA PROPOSTO

Diverse aziende nello svolgimento delle proprie attività si avvalgono di una "flotta aziendale", cioè un insieme di automezzi condotti da autisti alle proprie dipendenze.
La società ACME offre soluzioni SaaS (Software as a Service) e vuole fornire alle aziende sue clienti un servizio di "Fleet Management" (Gestione della flotta) il cui obiettivo è il controllo in tempo reale degli automezzi della flotta mediante dispositivi di rilevamento e comunicazione installati sugli automezzi stessi.
La soluzione SaaS fornita dalla società ACME consiste nella gestione di un servizio centralizzato di monitoraggio degli automezzi e nella fornitura di dispositivi che inviano in tempo reale le principali informazioni riguardo al movimento e allo stato degli stessi (posizione geografica, velocità, eventi anomali, ecc.) ma devono anche poter ricevere informazioni dal servizio centralizzato (informazioni sul percorso, cartografia, messaggi anche vocali, ecc.).
Le aziende clienti, che hanno installato i dispositivi sui loro automezzi, accedono al servizio attraverso un'interfaccia web che permette loro di monitorare il movimento e lo stato degli automezzi e di inviare a questi opportune informazioni.
Il servizio deve essere autenticato e deve operare nel rispetto della riservatezza dei dati all'interno dell'azienda, garantendo adeguati standard di sicurezza.

Dopo aver formulato eventuali ipotesi aggiuntive, sviluppare i seguenti punti:

- analizzare la realtà di riferimento e produrre un modello grafico che descriva il sistema, ne ponga in evidenza le varie componenti e le loro interconnessioni, motivando le scelte effettuate;
- descrivere, anche utilizzando uno schema grafico, le funzionalità tecnologiche che dovranno possedere i dispositivi a bordo degli automezzi.

SVOLGIMENTO

Ipotesi aggiuntive

L'ACME sceglie di avvalersi dei servizi di un'azienda di cloud computing quindi di un data center esterno.

Descrizione

- L'analisi dello scenario proposto porta all'individuazione di 4 componenti interconnesse tra loro.

1. L'ACME: una società il cui core business consiste nel fornire alle aziende sue clienti un servizio di *Fleet Management* centralizzato. Per fare questo offre una soluzione SaaS attraverso due programmi: un'applicazione da installare sui dispositivi mobili a bordo degli automezzi e un'applicazione centralizzata per la gestione della flotta aziendale. L'ACME sceglie di avvalersi dei servizi di un'azienda di cloud computing, quindi di un data center esterno.
2. L'azienda di cloud computing: azienda terza che ha il compito di fornire le risorse per realizzare il SaaS della ACME attraverso un **web service** (protocollo HTTP) ospitato nella server farm del proprio data center. Deve quindi rendere disponibile, all'applicazione installata sui dispositivi mobili, l'accesso a un'applicazione web installata su un proprio server. Deve inoltre rendere disponibile il programma per la gestione di ciascuna flotta aziendale tramite un'altra applicazione web (anch'essa installata su un proprio server, eventualmente virtualizzato) accessibile mediante un browser dalla LAN delle aziende clienti della ACME. Infine, anche l'ACME, dalla propria LAN, dovrà poter accedere da remoto al cloud per gestire i suoi clienti. I web service e l'applicativo di gestione condivideranno un database che l'azienda di cloud metterà a disposizione nel proprio data center (cloud storage).
3. L'azienda cliente della ACME: è un'azienda che ha una flotta di automezzi che vuole controllare e gestire da remoto in tempo reale.
4. La flotta del cliente: è l'insieme di automezzi aziendali dotati di dispositivo mobile.

Lo schema funzionale in FIGURA 1 riassume le componenti individuate e le loro interconnessioni.

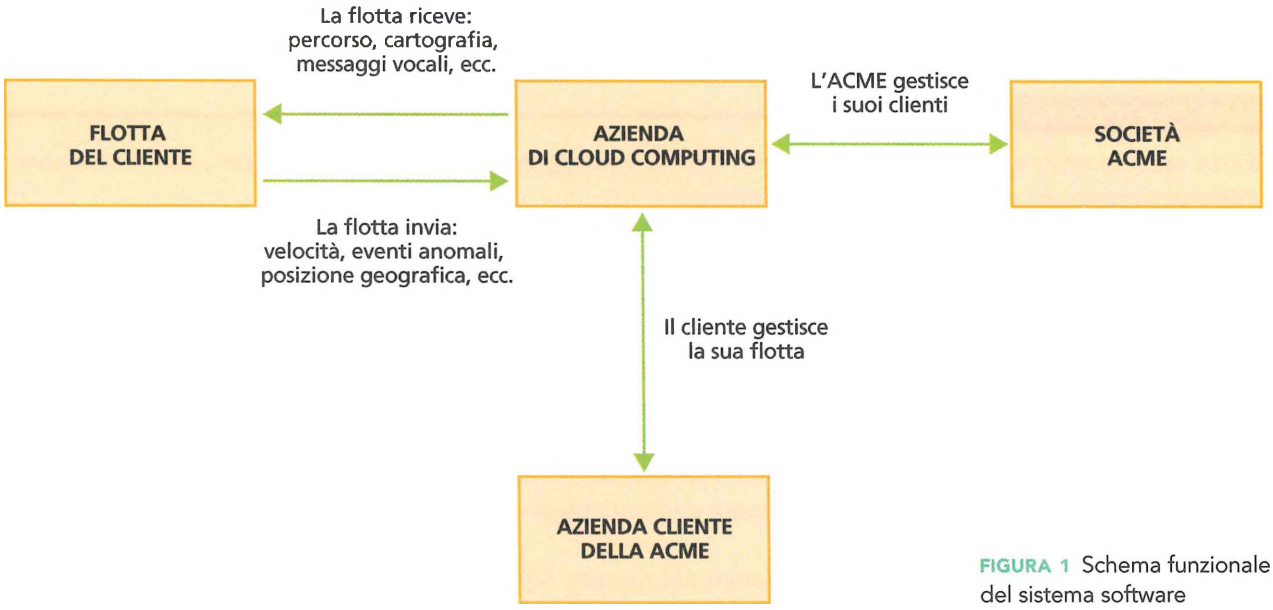


FIGURA 1 Schema funzionale del sistema software

La scelta della ACME di avvalersi di un'azienda di cloud computing specializzata nella distribuzione di servizi attraverso il web consente di superare le difficoltà legate ai costi iniziali e alla complessità del sistema e al contempo permette all'ACME di concentrarsi sul proprio core business.

L'azienda di cloud computing per garantire la funzionalità del servizio dovrà formalizzare un accordo (SLA, Service Level Agreement) col fornitore di servizi Internet (ISP, Internet Service Provider).

- Il punto cruciale del sistema è garantire la comunicazione in tempo reale tra i dispositivi installati sugli automezzi e il web service operante in cloud.
  Poiché gli automezzi sono in movimento, il modo migliore per accedere alla rete Internet è attraverso la telefonia cellulare con tecnologia **4G/LTE-Advanced**.
  Le due componenti fondamentali sono **LTE Access Network** e **LTE Core Network**:
  - LTE Access Network è costituita dai dispositivi mobili a bordo degli automezzi della flotta e dalle stazioni base che si interfacciano alla rete core. Ogni dispositivo mobile deve essere dotato di Universal Subscriber Identity Module (USIM) evoluzione della SIM, che contiene i dati identificativi dell'utente, utilizzati per l'autenticazione e l'accesso al servizio;
  - LTE Core Network è costituita essenzialmente dal Mobility Management Entity (MME) che svolge funzioni di controllo, quali, per esempio, l'autenticazione del dispositivo mobile tramite il database Home Subscriber Server (HSS); si occupa anche della gestione della connessione e degli aspetti di mobilità.

La FIGURA 2 riassume graficamente gli elementi fondamentali della rete LTE-Advanced che consentono l'interazione tra le flotte delle varie aziende (2 in figura) e i rispettivi uffici.

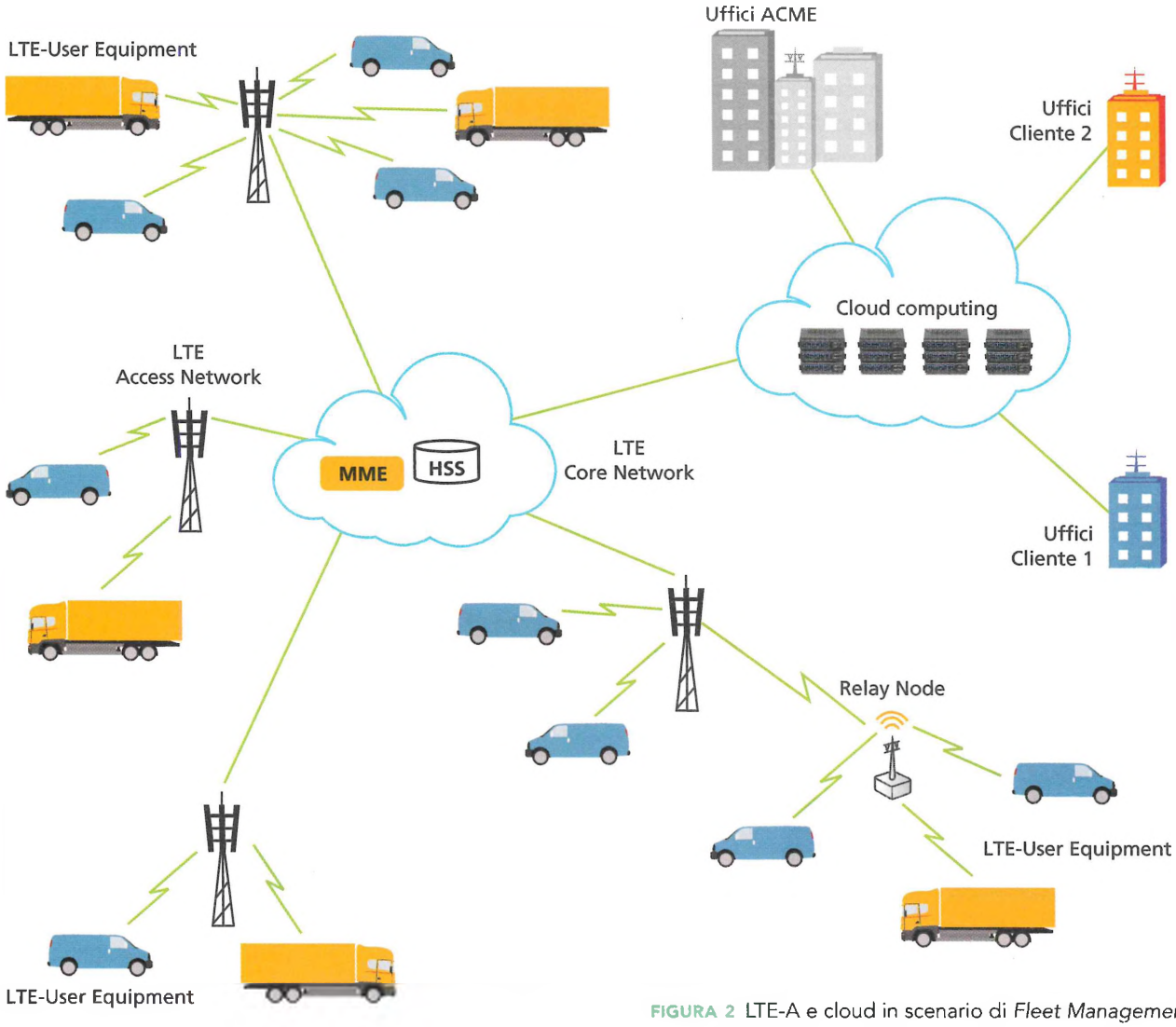


FIGURA 2 LTE-A e cloud in scenario di *Fleet Management*

In LTE Core Network le funzioni di controllo delle comunicazioni sono del tutto separate da quelle di trasporto.

Inoltre la rete core è completamente a pacchetto IP. Cioè, al vantaggio di avere un'unica rete di trasporto delle informazioni, siano esse voce o dati, associa la necessità di una maggior attenzione alla gestione delle risorse, così da soddisfare i requisiti prestazionali delle applicazioni (si ricordi che IP è Best effort).

L'evoluzione di LTE (**LTE-Advanced**) ha introdotto alcune importanti funzionalità.
Tra queste l'impiego di ripetitori intelligenti, detti Relay Node, che, compensando l'attenuazione di propagazione tra dispositivo mobile e stazione base, consentono di aumentare la capacità e la copertura.

La ACME fruirà della piattaforma di cloud computing per fornire alle aziende clienti il servizio di *Fleet Management* richiesto.
I dispositivi installati a bordo degli automezzi di ciascuna flotta aziendale sono verosimilmente dispositivi progettati dalla ACME, esclusivamente dedicati, come richiesto, a inviare le principali informazioni riguardo al movimento e allo stato dell'automezzo su cui sono installati (posizione geografica, velocità, eventi anomali, ecc.) e ricevere informazioni dal servizio centralizzato (informazioni sul percorso, cartografia, messaggi vocali, ecc.).

La soluzione più semplice consiste nell'utilizzare tablet commerciali, per esempio con sistema operativo Android, su cui installare l'applicazione della ACME e dotarli di carica batteria e supporto di fissaggio per auto.
Tali dispositivi, in ogni caso, dovranno avere le seguenti caratteristiche:

- connettività 4G/LTE-A;
- USIM, *Universal* Subscriber Identity Module;
- GPS integrato;
- display 10" touchscreen per l'interazione con l'interfaccia utente dell'applicazione che consente di accedere all'applicazione web della ACME (web service);
- Bluetooth per la connessione al sistema audio di bordo per la riproduzione in viva voce di messaggi e avvisi;
- microfono integrato.

L'utilizzo di un tablet consente anche di avere a disposizione processore, memoria RAM e SSD sicuramente adeguate alle necessità del servizio.

USER EQUIPMENTS


Laptop


Smartphone


Security Camera


Tablet

Data card

A CASA

- Effettua una ricerca in Internet sulle principali tecnologie per la telefonia cellulare; esaminando le diverse tecnologie trovate, concentrati su:
  – 4G/LTE/LTE-Advanced
  – 4.5G/LTE-Advanced Pro
  – 5G
- Individua quale, tra le tecnologie trovate, risulta affine al contesto illustrato nel tema proposto.
- Leggi l'esempio di svolgimento proposto per verificare se le tue ipotesi si adattano al caso preso in esame e se la trattazione proposta risulta completa nell'ottica dei risultati della tua ricerca.
- Raccogli i tuoi risultati in una presentazione in PowerPoint (massimo 5 slide) evidenziando i casi trovati, la relazione con il contesto proposto, eventuali modifiche o aggiunte da effettuare alla soluzione proposta nell'esempio di svolgimento.

IN CLASSE

- Condividi la presentazione dei tuoi risultati con i tuoi compagni.
- Attraverso una discussione stabilite quali sono le migliorie sul piano tecnologico e dei servizi digitali che potrebbero essere apportate all'azienda.
- Preparate un report che sintetizzi la discussione elencando i cambiamenti necessari che sono emersi come proposte. Il report deve contenere i dettagli sui sistemi, i dispositivi e il loro funzionamento.
- Procedi con l'autovalutazione.

AUTOVALUTAZIONE

ATTIVITÀ	LIVELLO			
	INIZIALE	BASE	INTERMEDIO	AVANZATO
Ho compreso senza difficoltà le richieste dell'attività proposta?	Ho compreso solo alcune delle richieste aiutato dal docente. ☐	Con la guida del docente e la collaborazione dei compagni ho compreso quasi tutte le richieste. ☐	Ho compreso le richieste e in parte le ho svolte autonomamente. ☐	Ho identificato le richieste e le ho svolte senza difficoltà. ☐
Ho reperito le informazioni in rete senza difficoltà?	Ho reperito solo alcune delle informazioni utili aiutato dal docente. ☐	Con la guida del docente e la collaborazione dei compagni ho reperito quasi tutte le informazioni. ☐	Ho reperito le informazioni utili autonomamente e le ho elaborate. ☐	Ho identificato le informazioni utili e le ho elaborate senza difficoltà. ☐
La ricerca in Internet mi ha permesso di definire modifiche e miglioramenti allo svolgimento proposto?	A partire dalla mia analisi, non sono stato in grado di individuare nessun punto critico nello svolgimento proposto. ☐	A partire dalla mia analisi, sono stato in grado di individuare alcuni punti critici nello svolgimento proposto con l'aiuto del docente. ☐	A partire dalla mia analisi, sono stato in grado di individuare i punti critici e alcune modifiche apportabili nello svolgimento proposto con l'aiuto del docente. ☐	A partire dalla mia analisi, sono stato in grado di individuare i punti critici e definire le modifiche apportabili in modo dettagliato e completo. ☐

UNITÀ

6 PROGETTARE STRUTTURE DI RETE: DAL CABLAGGIO AL CLOUD

Guarda la **presentazione** dell'unità

IN QUESTA UNITÀ

DDI+ Didattica Digitale Integrata Plus

conoscenze	abilità	competenze
Conoscere le norme del cablaggio strutturato.	Saper scegliere gli opportuni mezzi fisici e gli apparati di rete.	Scegliere dispositivi e strumenti in base alle loro caratteristiche funzionali.
Conoscere i servizi standalone e le possibili alternative.	Saper scegliere l'opportuna tecnologia in base ai diversi scenari d'utilizzo.	Saper progettare una rete in termini di cablaggio e collocazione dei servizi.
Conoscere la virtualizzazione dei sistemi e delle applicazioni.	Comprendere le necessità delle aziende nella progettazione della rete.	Saper proporre soluzioni di virtualizzazione e soluzioni cloud.
Conoscere l'approccio cloud ai servizi.		

FLIPPED CLASSROOM

A casa

- Leggi la Lezione 3 e la Lezione 6 di questa Unità;
- leggi il Case study *Virtualizzazione e cloud*;
- ricerca in Internet informazioni sulle Agende Digitali Locali;
- raccogli i risultati in una presentazione in PowerPoint (massimo 5 slide), riportando almeno due esempi.

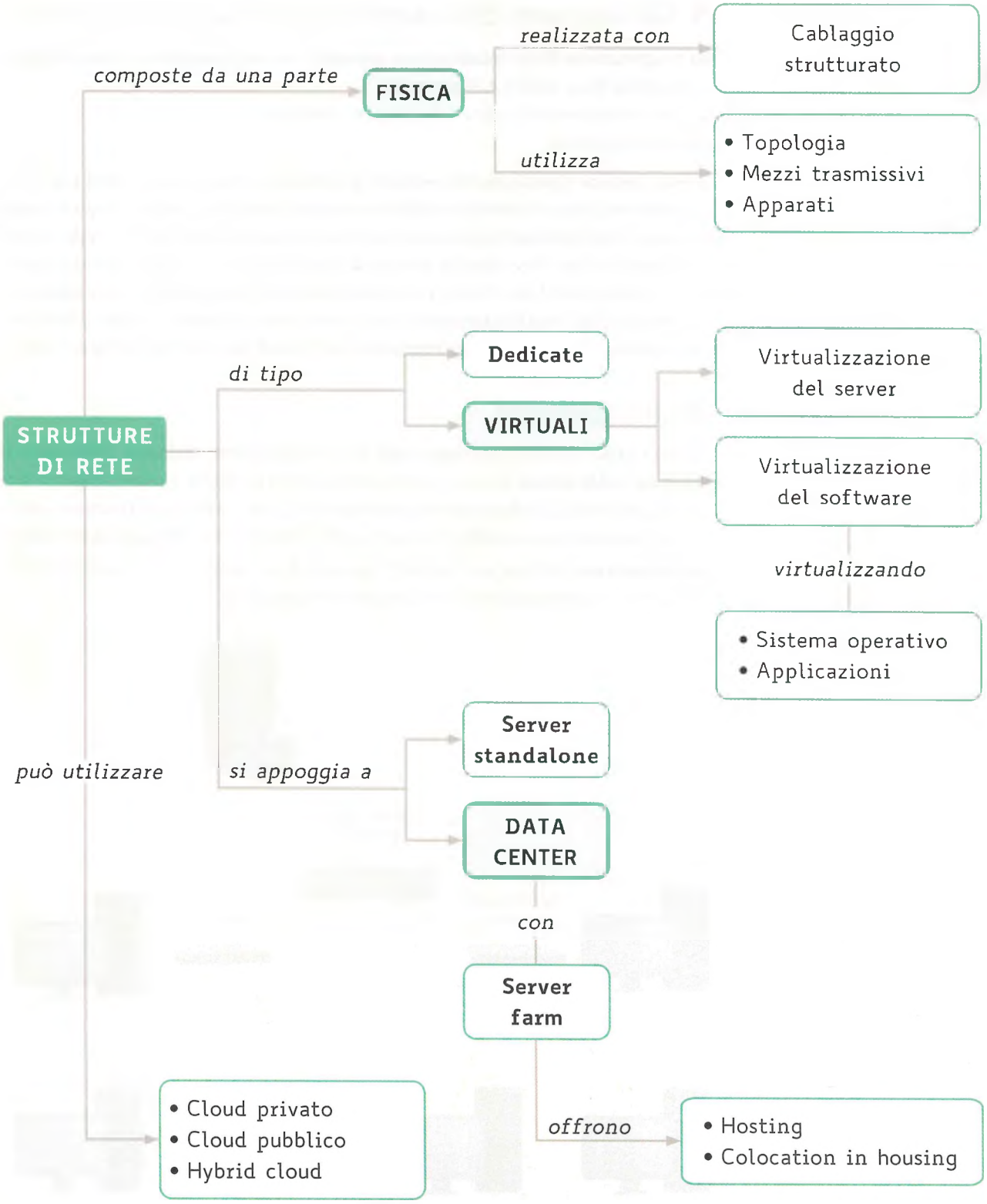
In classe

- Confrontate i risultati trovati;
- valutate se tra questi ve ne sono alcuni che possono ampliare la soluzione proposta nel *Case study*.

MAPPA CONCETTUALE

DIDATTICA INCLUSIVA

Mappa modificabile



1 PROGETTARE LA STRUTTURA FISICA DI UNA RETE AZIENDALE

1.1 Gli elementi che caratterizzano la rete aziendale

LEZIONE ONLINE

PROGETTARE LA STRUTTURA FISICA DELLE LAN

Una LAN aziendale è composta da elementi wireless e wired (cavi, apparati di rete) che devono essere collegati tra loro per realizzare una topologia di rete adeguata alle necessità dell'azienda, nel rispetto degli standard internazionali per il cablaggio degli edifici.

Nella progettazione di una moderna rete aziendale, occorre considerare 3 macrofattori:

1. la struttura fisica della LAN aziendale
2. la virtualizzazione delle risorse hardware e software
3. il cloud computing

In questa Lezione ripassiamo brevemente gli elementi base e gli standard che si applicano nel realizzare la struttura fisica di una rete aziendale. Alcuni di questi argomenti erano stati affrontati nel volume del terzo anno, ora sono ripresi e approfonditi nella Lezione online *Progettare la struttura fisica delle LAN*. Nelle Lezioni seguenti entreremo invece nel Data Center per comprendere le varie possibilità di collocazione dei server, macchine fondamentali per le attività di un'azienda. Infine affronteremo le problematiche della virtualizzazione e del cloud uscendo dall'ambito locale.

1.2 La topologia

La struttura fisica prevalentemente usata nella realizzazione delle reti LAN segue la **topologia a stella estesa** (FIGURA 1), detta anche a stella gerarchica: essa collega tra loro più topologie a stella. Anche se questa topologia porta a un aumento del numero dei cavi rispetto, per esempio, a quella a bus o ad anello, offre notevoli vantaggi in termini di:

- **fault-tolerance** (tolleranza ai guasti): il guasto di un canale o di un'interfaccia della rete non ne compromette il funzionamento generale;

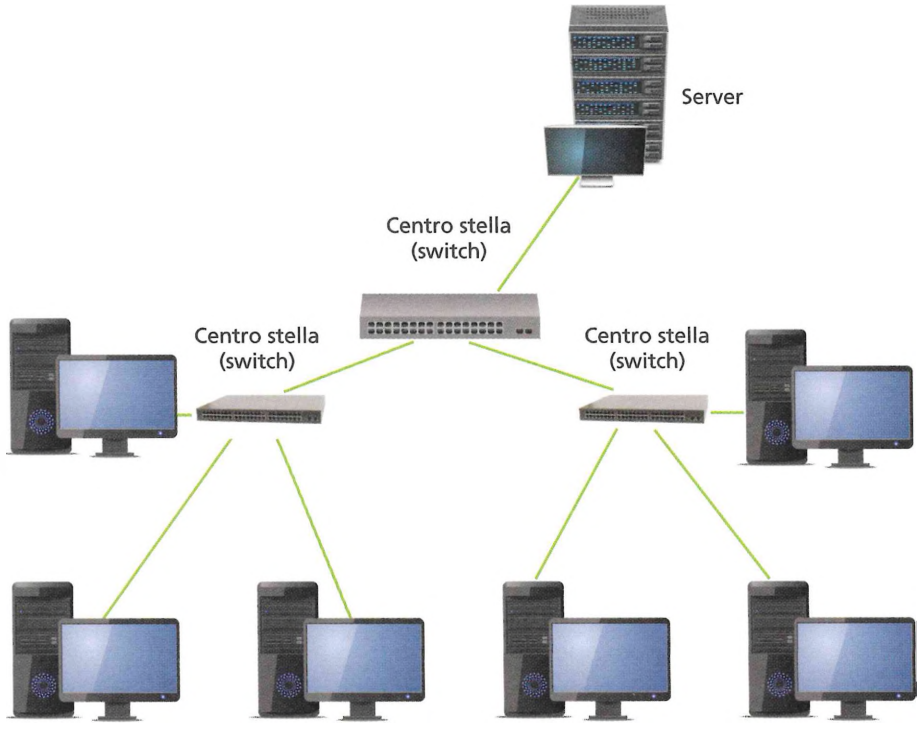


FIGURA 1 Topologia a stella estesa

- **flessibilità ed espandibilità**: lo spostamento di un host da un punto a un altro della rete o l'inserimento di uno nuovo non richiedono il fermo della rete.

Per contro tale topologia è vulnerabile al livello degli apparati che fungono da centro stella, cioè gli switch: infatti se l'apparato che svolge questo ruolo si guasta, la rete, o parte di essa, smette di funzionare.

1.3 Il cablaggio strutturato della LAN

Uno degli aspetti da considerare nello sviluppo di una rete è il collegamento tra gli apparati per la realizzazione delle varie topologie di rete. In pratica si tratta di definire dove collocare i nodi e come collegarli tra loro, indicando dove tirare i cavi o inserire i punti di accesso wireless.
L'insieme delle regole che portano a soddisfare i criteri sopra elencati è detto **cablaggio strutturato**. Tra i vari standard di riferimento, descritti nel volume del terzo anno e nella Lezione online di questa Unità, riprendiamo lo standard ISO/IEC 11801; la sua classificazione delle reti a stella segue, in parte, la dislocazione degli apparati all'interno degli edifici:
1° livello: **centro stella di comprensorio** (**CD** = Campus Distributor);
2° livello: **centro stella di edificio** (**BD** = Building Distributor);
3° livello: **centro stella di piano** (**FD** = Floor Distributor).
I punti terminali sono le **prese utente** (**TO** = Telecommunication Outlet).

Il cablaggio si suddivide in due tipi:
- **verticale** (**VCC** = Vertical Cross-Connect), anche detto cablaggio di dorsale;
- **orizzontale** (**HCC** = Horizontal Cross-Connect).

La FIGURA 2 riepiloga graficamente i concetti sin qui espressi con un esempio di cablaggio su due edifici ed evidenzia le lunghezze massime dei cablaggi.

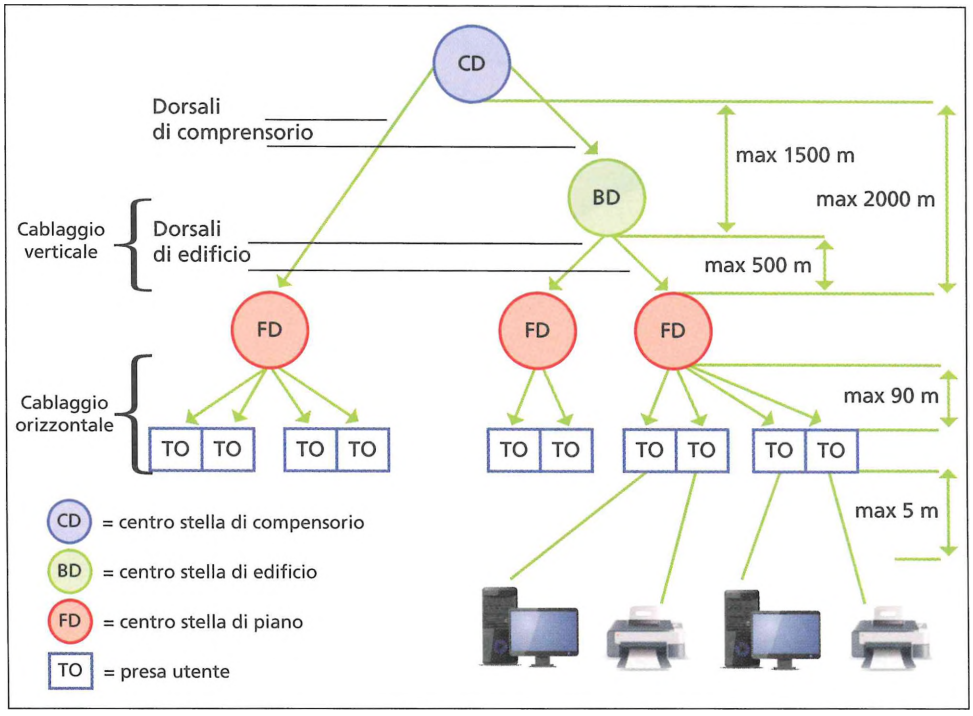


FIGURA 2 Schema logico di una LAN su due edifici (ISO/IEC 11801)

Lo schema logico delineato nella Figura 2 rappresenta il cablaggio di una LAN costituita da un comprensorio di due edifici:

1. un primo edificio (a sinistra) di un solo piano, con un solo centro stella di piano (FD) e in cui è situato il centro stella di comprensorio (CD), che in questo caso svolge anche funzioni di centro stella di edificio (BD);
2. un secondo edificio (a destra) di due piani, con due centro stella di piano (FD) collegati al centro stella di edificio (BD).

Le prese utente (TO) sono distribuite nei punti del piano dove sono collocate le postazioni utente o, per esempio, una stampante di rete.

Il cablaggio orizzontale è solitamente realizzato con cavi UTP o STP, raramente si impiegano le fibre ottiche, per via dei costi maggiori e della complessità nella posa. Nelle dorsali, invece, è preferibile utilizzare le fibre ottiche, anche per distanze ridotte. Nella FIGURA 3 viene mostrata una tipica distribuzione di armadi e prese utente nei piani di un edificio sede di una LAN aziendale.

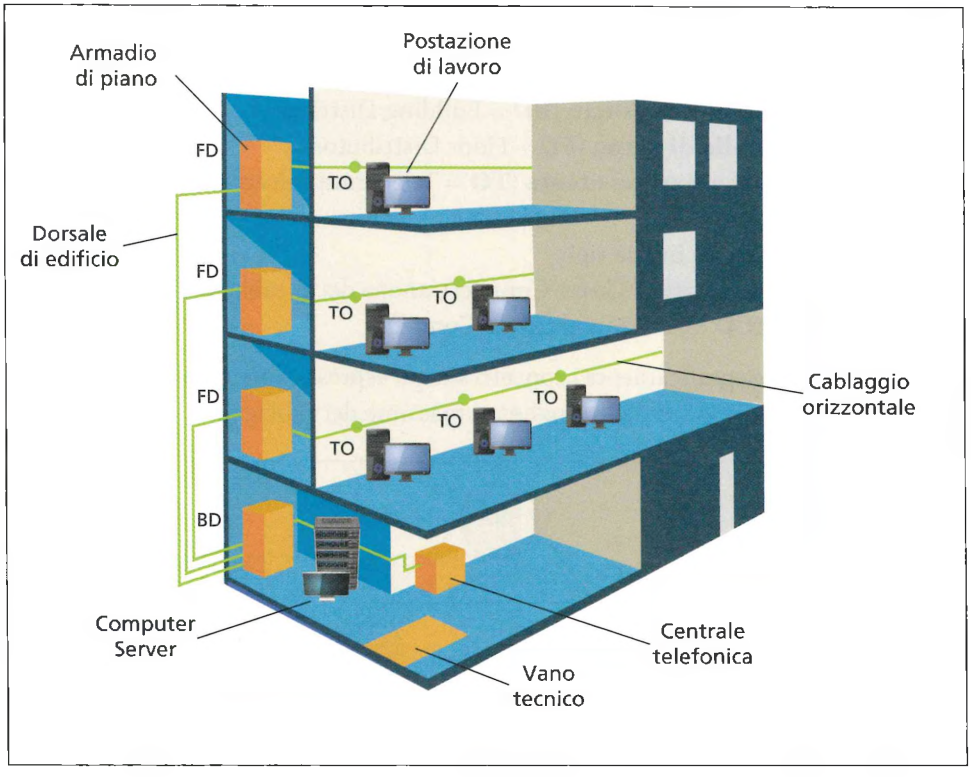


FIGURA 3 Esempio di distribuzione di armadi e prese utente

FISSA LE CONOSCENZE

- Perché nelle reti LAN si usa prevalentemente la topologia a stella estesa?
- Quali sono i 3 livelli di classificazione in cui lo standard ISO/IEC 11801 suddivide la rete?
- Quali sono i due tipi di cablaggio che occorre realizzare?
- Quali tipi di cavi si usano nel cablaggio orizzontale e qual è la massima lunghezza prevista?

2 PROGETTARE LA COLLOCAZIONE DEI SERVER

2.1 La collocazione dei server

Discutiamo di seguito le caratteristiche, il funzionamento e il posizionamento delle macchine server in una rete. Cominciamo analizzando le necessità delle piccole imprese, alle quali è sufficiente servirsi di macchine **standalone**, per poi passare alle aziende di medie o grandi dimensioni che allestiscono **data center** interni o si appoggiano alle **server farm** gestite da data center esterni.
I server vengono identificati in base al servizio che erogano. I principali sono:

- **File Server**: che permettono agli utenti di accedere ai file situati sul server come se fossero sulla propria macchina, agevolando la condivisione di informazioni;
- **Database Server**: che permettono di gestire intere banche dati;
- **FTP Server**: che forniscono alla rete accesso a cartelle pubbliche o con autenticazione;
- **Web Server**: usati per ospitare un sito web (per esempio server HTTP);
- **Application Server**: usati per far funzionare un'applicazione web e condividerne le funzionalità tra gli utenti;
- **Mail Server**: usati per la gestione della posta elettronica;
- **Print Server**: che permettono di mettere in comune una o più stampanti tra gli utenti di una rete con l'eventuale gestione dei diritti di accesso;
- **DHCP Server**: usati per l'assegnazione automatica di indirizzi IP ai computer di tipo host;
- **DNS Server**: che forniscono la risoluzione dei nomi di dominio dei siti (per esempio, *www.google.it*) nei loro indirizzi IP;
- **Active Directory (AD) Server**: usati per realizzare una rete con dominio (Domain Controller);
- **VPN Server**: che forniscono, attraverso un client VPN, l'accesso alla LAN da remoto;
- **Virtual Network Computing (VNC) Server**: che forniscono, attraverso un client VNC, un desktop remoto;
- **Proxy Server**: che forniscono una cache di accesso al web e la possibilità di controlli di autenticazione (ACL) e di filtro;
- **Server di autenticazione**: che permettono di autenticare l'accesso ad altre risorse;
- **Server grafico o Display Server**: dotati di acceleratore grafico;
- **Game Server**: che ospitano risorse per rendere possibili i giochi multiutente in linea;
- **Grid computing**: infrastrutture di calcolo distribuito, utilizzate per l'elaborazione di grandi quantità di dati, mediante l'uso di una vasta quantità di risorse distribuite. Permettono la condivisione coordinata di risorse all'interno di un'organizzazione virtuale.

I principali produttori di server garantiscono macchine per operare con Windows e Linux ed entrambi i sistemi possono essere virtualizzati.

2.2 I server standalone

Come si capisce dal lungo elenco, le macchine server all'interno di un'azienda devono svolgere molte funzioni diverse.

FIGURA 4 Server tower IBM System x3100 M4

FIGURA 5 Server rack Dell PowerEdge R710

FIGURA 6 Server blade HP BladeSystem c7000 (con 16 lame)

Un **server standalone** per piccole e medie aziende è il cosiddetto **server tower** (FIGURA 4). Si tratta di un computer assemblato in un case verticale (simile ai personal computer) per essere utilizzato come server in grado di funzionare in modo autonomo (standalone), sovente dotato di capacità di storage dell'ordine dei terabyte e supporto RAID.
Questi server vengono utilizzati per raccogliere e gestire i dati aziendali anche delle filiali. Caratteristiche indispensabili sono la virtualizzazione, la gestione dei file e del sito web, delle applicazioni e dei dispositivi condivisi.
Server tower multipli possono essere usati contemporaneamente in un'azienda associandoli a processi diversi. Questi server sono affidabili e scalabili e con l'ulteriore vantaggio di essere di facile raffreddamento. Gli svantaggi di utilizzare più server tower sono la voluminosità, il rumore e i cablaggi complessi.
Benché siano stati fatti molti passi avanti in tema di dimensioni e rumore, molte aziende preferiscono affidarsi a server tower progettati con alcune varianti come i **server rack** (FIGURA 5) e i **server blade** (FIGURA 6).
I server rack, costruiti per essere montati su armadi rack, garantiscono compattezza, semplificano i cablaggi e consentono una facile scalabilità.
Quando il problema principale è l'occupazione di spazio, si ricorre ai server blade. Una singola lama (blade in inglese significa appunto lama) costituisce una macchina server (fisica) distinta che, da sola o in concorso con altre lame, può simulare *N* macchine server virtuali.
Infatti, la virtualizzazione rappresenta una soluzione tipica associata ai server blade, unita al consolidamento di diversi sistemi di storage.

2.3 I data center

Il termine data center in Italia è conosciuto come **CED (Centro Elaborazione Dati)** e si riferisce ad aree attrezzate per il trattamento e l'archiviazione di dati.
Spesso il data center è collocato nello stesso locale tecnico che funge da centro stella di comprensorio o di edificio.
Non è difficile immaginare che tutto ciò che noi osserviamo a livello digitale, dalle pagine web, all'archivio delle nostre telefonate, al deposito momentaneo di un SMS in attesa di trovare il cellulare del destinatario acceso, fino alle nostre email e al profilo Facebook, sia depositato da qualche parte nel mondo. Questi posti sono i data center (FIGURA 7).
Molte aziende hanno il proprio data center in cui i tecnici informatici si occupano di tutta la gestione delle informazioni digitali e aggiornano le tecnologie e le infrastrutture informatiche.

FIGURA 7 Un data center con armadi rack per i server

Altre aziende si affidano invece a data center esterni specializzati, a cui delegano la locazione e la gestione dei propri server e dei propri dati.
All'interno del data center viene dunque collocata una serie di server che prende il nome di **#server farm** (o **web farm**).
La collocazione in un unico ambiente consente di centralizzare la gestione, la manutenzione e la sicurezza della server farm. Spesso all'interno delle server farm vengono costituiti dei sistemi cluster per gestire in maniera migliore, attraverso una tipica architettura distribuita, carichi di lavoro pesanti o critici (server email, web, database, rendering, grid computing, ecc.) garantendo al contempo affidabilità e tolleranza ai guasti tramite ridondanza fisica degli apparati.

#techwords

La **server farm** (o **web farm**) è costituita da una serie di server collocati in unico ambiente.

I DATA CENTER INTERNI ALLE AZIENDE

Riassumiamo in TABELLA 1 i vantaggi e gli svantaggi per un'azienda di avere un data center interno al perimetro fisico aziendale.

Vantaggi di un data center interno	Svantaggi di un data center interno
Possibilità di agire fisicamente in tempi rapidi in caso di malfunzionamenti.	Necessità di aree fisiche da destinare a tale uso, con l'aumento dei costi di affitto degli uffici.
Possibilità di avere un rapporto fisico tra l'area amministrativa e operativa di un'azienda e l'area sistemi e sviluppo.	Acquisto dell'hardware e delle risorse per gestire i dati.
Controllo diretto sulla riservatezza dei dati a garanzia della privacy di dipendenti e clienti.	Costi per l'aggiornamento dei server e per la formazione del personale.
Controllo diretto sulla sicurezza dei dati in caso di intrusioni e potenziali minacce software (virus).	Costi per la sicurezza anti intrusione, backup e conservazione dell'integrità dei dati.

TABELLA 1 Vantaggi e svantaggi di un data center interno

I DATA CENTER ESTERNI ALLE AZIENDE

Esternalizzare un data center, che si tratti di un singolo server centralizzato o che si tratti di architetture più complesse, è un'operazione che presenta vantaggi importanti, quali la possibilità di collocare una macchina server in aree appositamente protette e di poter disporre dell'esperienza professionale del fornitore in materia di sicurezza hardware, software e dei dati.
Oltre a liberarsi delle macchine e dei costi vivi di manutenzione e allocazione interni alla propria azienda, questa soluzione permette anche di ridurre le problematiche inerenti la connettività o l'alimentazione.
Questa soluzione, inoltre, risulta utile soprattutto in caso di Web Application e di aperture di servizio all'esterno.
Le applicazioni web-based sono il fondamento di alcuni dei servizi più diffusi in ambito aziendale, come per esempio il sito web con login, la webmail (server di posta), l'e-commerce e l'e-learning (piattaforme di apprendimento).
Affidare a server esterni la gestione dei servizi che prevedono l'accesso di utenti online limita i rischi di intrusione nella LAN aziendale.
I data center e le aziende specializzate (spesso ISP, Internet Service Provider) offrono anche consulenze tecniche per trovare migliori soluzioni, sia in quanto a costi sia in quanto a performance dei sistemi.

2.4 Le server farm

#prendinota

In una server farm, un server riesce a rimanere connesso a Internet anche per 500 giorni consecutivi, senza perdita di connettività neanche per un millesimo di secondo.

Le server farm sono aree fisiche, normalmente ubicate nel sottosuolo, che possono ospitare decine, centinaia e a volte migliaia di macchine server, che offrono le seguenti caratteristiche:

- sicurezza fisica e sistemi anti intrusione;
- alimentazione ridondata (duplicata), con gruppi di continuità;
- impianto di condizionamento per mantenere la temperatura bassa;
- connettività a Internet stabile, garantita e affidabile;
- sicurezza software tramite firewall e protezione logica delle macchine.

Le problematiche che un data center deve affrontare si manifestano particolarmente nel caso di game server, ossia di macchine destinate a ospitare decine di migliaia di giocatori in ambienti multiplayer (ossia in cui molti giocatori giocano in tempo reale interagendo tra loro), e in cui l'instabilità della connessione Internet si traduce in un blocco totale dell'applicazione con la conseguente disconnessione dall'ambiente di gioco e una perdita di credibilità del circuito.
Data center specializzati esterni alle aziende forniscono servizi completi attraverso la loro server farm. Vediamo i principali servizi offerti dalle server farm.

2.5 I servizi offerti dalle server farm

HOSTING

#prendinota

L'hosting si differenzia anche in base alla piattaforma, cioè al sistema operativo installato sul server: Windows o Linux per esempio.

È il tipo di servizio offerto dalle server farm più diffuso ed economico. Nella sua forma più semplice consiste nell'ospitare (dall'inglese *to host*) su un web server della server farm le pagine di un sito web aziendale o privato, rendendolo così accessibile alla rete Internet e ai suoi utenti.
Più in generale consiste nell'installare la propria applicazione web in server di proprietà del provider e gestiti dal provider stesso.

L'hosting può prevedere:

- uno o più domini ospitabili;
- uno o più indirizzi di posta elettronica;
- spazio per dati e database dell'ordine dei terabyte;
- velocità di banda adeguata e garantita;
- utenze FTP attivabili senza limiti;
- mail box illimitate.

Le prestazioni (e i costi) possono variare a seconda che si voglia un server dedicato oppure uno condiviso e in base all'uso che si vuole fare del sito web.
Si va dall'hosting gratuito a quello a pagamento con costi via via a salire in base alle performance richieste.

L'**hosting gratuito** comprende solitamente una (o comunque poche) casella di posta elettronica e un certo quantitativo di spazio web, spesso con l'obbligo di banner pubblicitario.
Forniscono hosting gratuito, e a volte anche il dominio, Altervista (sicuramente il più noto), Hostinger, Netsons, Ilbello (il più vecchio) e tanti altri.

Tra i limiti dell'hosting gratuito, rispetto a quello a pagamento, vi sono:

- l'indirizzo del sito ospitato che coincide, in massima parte, con il nome dell'Internet Provider che lo ospita;
- prestazioni tecniche poco performanti (molto spesso, per esempio, è possibile pubblicare soltanto siti statici scritti in linguaggio HTML);
- mancata garanzia del servizio (con il rischio quindi che i siti ospiti possano non essere attivi per un determinato periodo di tempo);
- una larghezza di banda contesa tra numerosi utenti.

L'**hosting a pagamento** supera tutte le limitazioni descritte, consentendo servizi che vanno dal dominio personalizzato e illimitato agli infiniti indirizzi email a disposizione, dai filtri antispam a quelli antivirus, dalla gestione di un sito dinamico alla banda adeguata al traffico generato dal sito stesso.
In particolare per la gestione di un sito dinamico si possono avere a disposizione sia il supporto per linguaggi di scripting sia il supporto per database online. È possibile anche garantirsi servizi di statistiche e analisi del traffico.

COLOCATION IN HOUSING

Questo servizio permette di localizzare uno o più server (o gli equipaggiamenti di telecomunicazioni) di proprietà dell'azienda nella server farm del data center. L'azienda quindi acquista per proprio conto il server in commercio che più le serve, occupandosi poi personalmente della gestione e risoluzione dei problemi sia hardware sia software, mentre pagherà alla server farm solo il prezzo di locazione (affitto dello spazio fisico, alimentazione, rete, ecc.). Tuttavia, in caso di interventi sulla macchina, è necessario concordare un appuntamento con il fornitore del servizio, cosa che potrebbe comportare un ritardo nell'intervento.
I servizi realizzabili in housing coincidono con quelli in hosting a pagamento, con la differenza che con l'housing l'azienda è proprietaria dei server e li gestisce direttamente pur non avendoli all'interno delle mura perimetrali.
Al data center esterno è demandato il compito di garantire sicurezza e alte prestazioni di banda.
Le aziende ricorrono all'housing per applicazioni di rete critiche per le quali occorrerebbero infrastrutture autonome troppo costose.
Nella stragrande maggioranza dei casi si tratterà di aziende di housing che comprano a loro volta questo servizio dalla server farm, per rivenderlo sotto forma di contratto di hosting, colocation housing e connettività. Questo significa che spesso si è in subaffitto.
La TABELLA 2 riassume i vantaggi e gli svantaggi della colocation in housing.

#prendinota

Il costo dell'housing si ammortizza nei mesi rispetto al noleggio del server, che ha un costo ulteriore mensile rispetto alla semplice colocation di un server di proprietà.

Vantaggi della colocation in housing	Svantaggi della colocation in housing
Proprietà dell'hardware e risparmio del canone del noleggio del server dedicato.	Impossibilità di intervenire con rapidità in caso di danno hardware, procedura a carico della server farm in caso di server noleggiato.
Il sistema operativo e i software sono installati dall'azienda di housing prima di posizionare la macchina in server farm.	Costo iniziale di startup che comprende l'acquisto della macchina e la configurazione di base.
Possibilità di amministrare totalmente la macchina e di fare aggiornamenti software in qualsiasi momento.	Aggiornamenti di sicurezza e dei sistemi a carico del cliente.

TABELLA 2 Vantaggi e svantaggi della colocation in housing

SERVER DEDICATI

I data center possono mettere a disposizione delle aziende clienti alcuni server dedicati a **uso esclusivo**. Con questa formula il cliente noleggia un server pagando le spese di collocazione del server e le spese di noleggio. L'amministrazione software del server è completamente a carico e a disposizione del cliente (con possibilità di intervento da remoto).

Il vantaggio di noleggiare il server in una server farm è che in caso di guasto è il data center provider che deve occuparsi del ripristino del server in tempi brevi.

Il servizio di noleggio dei server dedicati si è diffuso nelle piccole aziende come quelle di web design. Questa soluzione permette di pagare soltanto l'affitto del canone mensile di collocazione nell'armadio della macchina e il costo di connettività, che ovviamente porta con sé anche i costi dell'infrastruttura tecnica di sicurezza, la continuità elettrica e in generale tutte le caratteristiche delle server farm. A differenza della colocation in housing, il noleggio di un server dedicato permette al cliente, pagando il canone di affitto della macchina, di non doversi preoccupare dei costi di upgrade dei sistemi operativi e di eventuali riparazioni delle macchine, a carico della società che offre il servizio. Inoltre, ha un costo minore di startup.

Disporre di un server dedicato è decisamente utile, sia perché si ha a completa disposizione la macchina, escludendo quindi possibili problemi dovuti all'attività di altri clienti su quella macchina, sia perché si dispone di tutta la potenza di calcolo e delle risorse intere dell'hardware.

La TABELLA 3 riassume i vantaggi e gli svantaggi dell'impiego di server dedicati.

TABELLA 3 Vantaggi e svantaggi dei server dedicati

Vantaggi del noleggio di server dedicati	Svantaggi del noleggio di server dedicati
Delega degli aggiornamenti di sicurezza allo staff del supporto sistemistico della server farm o dell'azienda che rivende il servizio.	Delega del funzionamento allo staff della server farm, operazione che richiede fiducia e competenza in caso di applicazioni critiche.
Nessun costo di acquisto iniziale della macchina e di installazione e configurazione iniziale.	Costo di affitto mensile dei server che può risultare alto in caso di applicazioni di rete critiche, in aggiunta al costo di connettività e di affitto dello spazio rack (colocation).
Costo di affitto dei server noto a priori e distribuito in pagamenti mensili.	Impossibilità di ricevere da subito una macchina personalizzata, poiché il noleggio di server dedicati nella maggior parte delle server farm non consente personalizzazioni di default particolari, se non con costi aggiuntivi.

SERVER VIRTUALI

I server virtuali (**VPS**, Virtual Private Server) permettono di superare i limiti imposti dai tradizionali servizi di hosting in termini di configurazione e personalizzazione dei servizi e di usufruire, come nel caso dei server dedicati, di un sistema completo. A differenza dei server dedicati, però, il servizio di VPS non è fornito su un hardware dedicato, ma su una **porzione di hardware** condiviso con altri sistemi virtuali, in piena sicurezza. Il provider, cioè, mette a disposizione una macchina virtuale collocata su un server fisico che conterrà altre macchine virtuali.

Alle aziende poste sullo stesso server virtualizzato sembrerà di possedere a tutti gli effetti una macchina dedicata, con la differenza che non ne sosterranno completamente le spese, ma il costo sarà diviso con gli altri clienti ospitati sulla stessa macchina.

L'azienda cliente gestirà la sua macchina virtuale mentre il provider si occuperà solo della macchina fisica. L'azienda cliente potrà scegliere risorse in termini di capacità di elaborazione, di memoria esterna e velocità/banda di rete.
La TABELLA 4 riassume i vantaggi e gli svantaggi dell'impiego di server virtuali.

TABELLA 4 Vantaggi e svantaggi dei server virtuali

Vantaggi del server virtuale	Svantaggi del server virtuale
Costi bassi.	Mancanza di una macchina fisica a uso esclusivo come server.
Delega di cura tecnica e sicurezza del server fisico alla società che fornisce il servizio.	Possibilità di problemi legati allo scarso setup della virtualizzazione di uno degli utenti presenti sul server virtuale.
Separazione netta tra gli ambienti occupati da diverse aziende che affittano lo stesso server fisico.	La garanzia delle prestazioni dipende dalla capacità di dividere il carico di lavoro tra gli utenti senza personalizzazioni.

A oggi, i software che operano la divisione della macchina (quindi i software di virtualizzazione) consentono anche di dividere il carico di CPU e RAM allocati a ogni cliente, assicurando quindi a ognuno di disporre di un buffer garantito di memoria su cui fare affidamento e un'adeguata capacità di elaborazione.

2.6 La connettività nella server farm

La maggioranza dei server allocati in una web farm contiene applicazioni che necessitano di andare in rete. Una server farm deve essere provvista di allacciamenti ridondanti sulle dorsali di rete per permettere una velocità elevata e una quantità di banda necessaria a soddisfare tutte le esigenze di centinaia di armadi. La rete viene poi distribuita attraverso hub, switch, firewall e gateway solitamente di proprietà del provider con tecnologia in fibra ottica, a esclusione dell'allacciamento al cliente, che può avvenire attraverso un cavo Ethernet.
Solitamente l'acquisto della banda viene fatto in **modalità flat** (connettività garantita) calcolata con un picco massimo prestabilito (che può essere aumentato in caso di necessità). L'ampiezza di banda garantita sarà quella indicata nel contratto scelto.
Per ogni server noleggiato o alloggiato in colocation, vengono fornite una o più interfacce di rete e un IP statico pubblico; eventuali ulteriori interfacce di rete sugli switch o eventuali aggiuntivi indirizzi IP statici pubblici vengono conteggiati separatamente.

FISSA LE CONOSCENZE

- Che cosa caratterizza un server standalone?
- Che cosa troviamo all'interno di un data center?
- Che cosa sono le server farm?
- Quali sono i limiti dell'hosting gratuito rispetto a quello a pagamento?
- Qual è la differenza tra hosting e colocation in housing?
- Che differenza c'è tra l'utilizzo di server virtuali e quello di server dedicati?

3 LA VIRTUALIZZAZIONE DEI SERVER

3.1 Le caratteristiche della virtualizzazione dei server

Oltre all'utilizzazione di macchine server virtuali per i servizi di hosting, come visto nella Lezione precedente, è possibile sfruttare la virtualizzazione del software attraverso la **Server Virtualization**.

La **virtualizzazione dei server** (Server Virtualization) permette di creare su un singolo server più virtual machine, in contemporanea e che condividono le risorse della stessa macchina fisica, su cui vengono eseguiti diversi sistemi operativi e applicativi client.

Con i **sistemi di virtualizzazione** si dà la possibilità di **astrarre alcuni servizi IT** (Information Technology) dalle rispettive dipendenze (hardware, reti, sistemi di storage), abilitando l'esecuzione di più sistemi operativi virtuali su una singola macchina fisica, lasciandoli distinti dal punto di vista logico.
Il sistema operativo ospitante (**host**) crea di fatto una serie di partizioni entro cui poter eseguire più sistemi operativi ospiti (**guest**) senza conflitti (FIGURA 8).

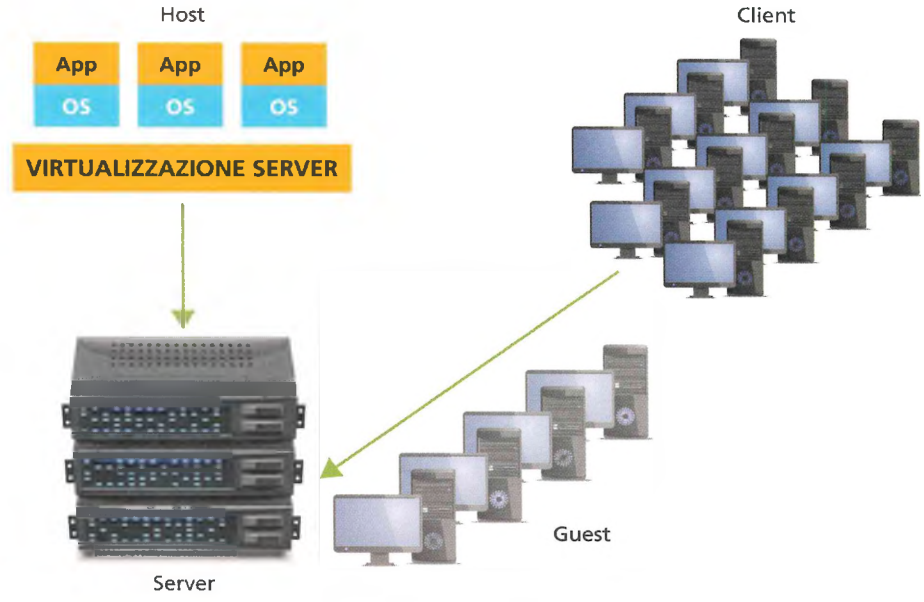


FIGURA 8 Virtualizzazione dei server: host e guest

L'host sarà composto da **due layer**:

1. il **layer inferiore** dello stack software, occupato da una singola istanza di un sistema operativo ordinario che è installato direttamente sul server;
2. il **layer di virtualizzazione** (App) che gestisce il reindirizzamento e l'emulazione delle applicazioni con quel sistema operativo e va a sua volta a comporre il **computer virtuale**.

L'host fornisce le varie caratteristiche del computer fino al livello del BIOS ed è in grado di generare macchine virtuali (e indipendenti) a scelta, basandosi sulle configurazioni definite dall'utente.

Come i server fisici, anche quelli virtuali sono ovviamente inutili fintanto che non vi si installa un sistema operativo, ovvero i *guest*, i quali penseranno di avere tutta la macchina per sé, ignorando l'esistenza degli altri.

I VANTAGGI DELLA VIRTUALIZZAZIONE

Alcuni dei vantaggi di una soluzione di virtualizzazione ben progettata sono:

- riduzione dei costi di implementazione e gestione, consolidando l'hardware;
- riduzione del consumo energetico dell'intero data center;
- allocazione dinamica delle risorse;
- riduzione drastica del tempo necessario alla messa in opera di nuovi sistemi;
- isolamento dell'architettura da problemi di sistema operativo e applicativo;
- semplificazione della gestione delle risorse eterogenee;
- facilitazione di testing e debugging di ambienti controllati.

Un ulteriore e non meno importante vantaggio risiede anche nella grande semplicità con cui la Server Virtualization permette di **gestire l'evoluzione tecnologica**. Se un sistema hardware diventa obsoleto è possibile migrare in maniera abbastanza facile i server su macchine di ultima generazione (tra l'altro guadagnando in performance) senza dover reinstallare tutto, ma solamente reinstallando lo strato emulato e ripristinando i file delle macchine virtuali. Senza contare la possibilità di eseguire **#test fuori linea** in modo molto semplice, per rendere ancora più indolore la migrazione. L'esigenza, quindi, da parte delle aziende di virtualizzare i sistemi potrebbe nascere dall'esigenza di sfruttare al meglio le risorse a loro disposizione (processori, memoria, disco). Inoltre, potrebbe essere la soluzione per quelle aziende che hanno CED di piccole dimensioni, composti da pochi rack (storage e server), senza spazio per altri armadi e sistemi di raffreddamento.

#techwords

Test fuori linea
Test eseguito offline, cioè senza interrompere il normale lavoro dei server.

3.2 Le tecnologie di virtualizzazione di Microsoft

Vediamo come Microsoft approccia la questione della virtualizzazione e quali strumenti mette a disposizione nell'ambito dei suoi sistemi operativi server.
In generale vengono proposte diverse tecnologie (FIGURA 9) a seconda delle diverse esigenze di virtualizzazione. Vediamo le principali.

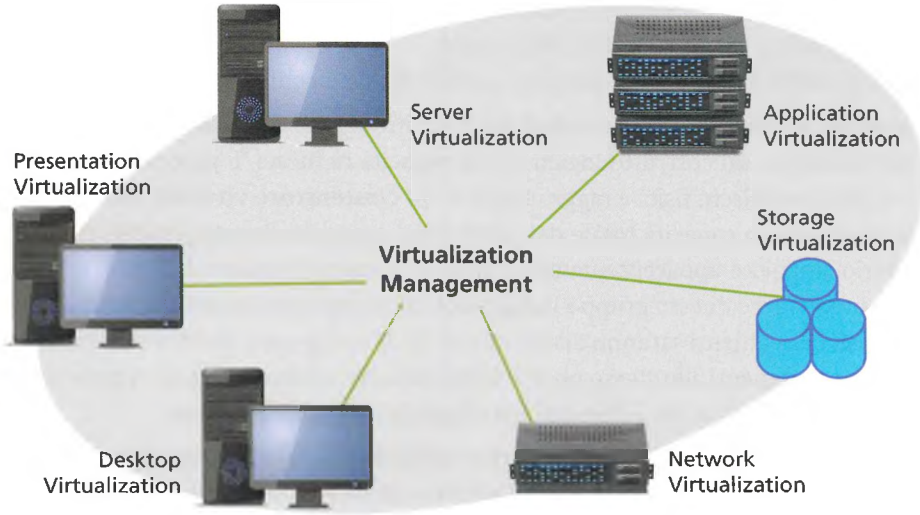


FIGURA 9 Le tecnologie di virtualizzazione di Microsoft

1. **Presentation Virtualization**: è la virtualizzazione del solo livello di presentazione delle applicazioni (cioè la parte di interazione con l'utente). Al client viene mostrata l'interfaccia di interazione dell'applicazione da lui richiesta che è in esecuzione su server remoti. Il principio è dunque quello dell'utente come terminale di I/O. In questo modo si riducono le necessità di distribuzione e manutenzione dei software applicativi garantendo un maggior controllo sul loro utilizzo e riducendo i costi. All'utente diventa difficile capire dove l'applicazione sia realmente eseguita (in remoto o in locale).
2. **Application Virtualization**: può capitare che applicazioni diverse in esecuzione su un computer abbiano problemi di convivenza legati per esempio alla necessità di utilizzare diverse versioni delle stesse librerie dinamiche (DLL). Il problema si risolve agevolmente creando uno strato di isolamento tra l'applicazione, il sistema operativo e le altre applicazioni in esecuzione. Si realizza una *bolla* entro la quale l'applicazione trova quanto necessita per la sua corretta esecuzione, senza entrare in conflitto con l'ambiente software circostante. È anche possibile distribuire le applicazioni come stream di bit quando il client ne ha bisogno trasformando di fatto un'applicazione in una specie di servizio on demand.
3. **Desktop Virtualization**: è una tecnologia per la virtualizzazione delle macchine client. Virtualizzare il client può essere molto utile in situazioni particolari, come per esempio in caso di problemi di compatibilità applicativa. La virtualizzazione del client, a seconda delle necessità, può essere effettuata sostanzialmente in due modi:
   - mettendo il client virtualizzato su un server: in questo caso si utilizzano sostanzialmente le stesse tecnologie utilizzate per la virtualizzazione dei server (Server Virtualization, vedi punto 4);
   - eseguendo una macchina virtuale direttamente sul client. Questo secondo scenario è particolarmente utile in situazioni di laboratorio, studio, sviluppo applicativo o come soluzione temporanea per ovviare a problemi di compatibilità applicativa non altrimenti risolvibili.
4. **Server Virtualization**: è una tecnologia che consente, su un unico hardware, l'esecuzione di più istanze di diversi sistemi operativi. In particolare essa permette:
   - l'esecuzione di differenti sistemi operativi (Microsoft e di terze parti) in macchine virtuali diverse su uno stesso server (host di virtualizzazione);
   - la possibilità di mettere in cluster host di virtualizzazione in modo da garantire l'alta disponibilità;
   - la possibilità di spostare in modo rapido macchine virtuali da un host di virtualizzazione a un altro (Quick Migration);
   - la possibilità di eseguire il backup a caldo delle macchine virtuali in esecuzione.
5. **Storage Virtualization**: è una tecnica di archiviazione virtualizzata che unisce più dischi fisici in un costrutto logico con la capacità richiesta. Il processo consente di scegliere più dischi fisici e raggrupparli in un **contenitore virtuale** (storage pool), in modo che la capacità totale dei dischi fisici associati diventi gestibile come uno spazio singolo e apparentemente continuo. L'amministratore dello storage potrà poi suddividere questo gruppo in segmenti da assegnare a macchine virtuali o server fisici. I segmenti saranno dischi virtuali il cui spazio può spalmarsi su più dischi fisici appartenenti allo stesso pool. L'archiviazione sul disco virtuale si presenta come una lettera di unità o una cartella mappata in **Esplora risorse**.
6. **Network Virtualization**: è una tecnica utilizzata per dotare le macchine virtuali di reti virtuali. Le modalità sono simili a quelle utilizzate per dotare il sistema operativo

di macchine virtuali. La virtualizzazione di rete disaccoppia l'infrastruttura di rete fisica dalle reti virtuali ed elimina dal **#provisioning** delle macchine virtuali i vincoli di VLAN e di assegnazione di indirizzi IP gerarchici. La maggiore flessibilità nella selezione host per la macchina virtuale consente ai proprietari dell'infrastruttura di spostare i carichi di lavoro in qualsiasi punto del data center senza modificare le macchine virtuali o riconfigurare le reti. Per esempio, è possibile la migrazione in tempo reale tra subnet (operazione in precedenza limitata alla stessa subnet, con conseguente limitazione del posizionamento delle macchine virtuali); in questo modo una macchina virtuale può effettuare la migrazione in qualsiasi punto del data center senza alcuna interruzione del servizio. La migrazione in tempo reale tra subnet consente agli amministratori di consolidare i carichi di lavoro in base ai requisiti di risorse dinamiche e di efficienza energetica, oltre a permettere la manutenzione dell'infrastruttura senza interrompere il tempo di attività del carico di lavoro dei clienti.

#techwords

Provisioning
Processo di assegnazione di risorse e privilegi ai client di una rete e a chi la utilizza da remoto. Questo processo può comprendere hardware, software, cablaggio e servizi.

3.3 Microsoft Hyper-V Server 2019

Sin da Windows Server 2008, Microsoft ha posto una particolare attenzione agli ambienti di virtualizzazione grazie all'introduzione del ruolo **Hyper-V** legato alla Server Virtualization. Il server che esegue Hyper-V viene definito host mentre tutte le macchine virtuali sono i guest di tale sistema. Hyper-V consente inoltre, oltre alla Server Virtualization, anche le Desktop e Network Virtualization.

In particolare, Hyper-V offre la virtualizzazione hardware. Ciò significa che ogni macchina virtuale viene eseguita in un hardware virtuale. Hyper-V consente di creare dischi rigidi virtuali, commutatori virtuali e diversi altri dispositivi virtuali che possono essere tutti aggiunti alle macchine virtuali.

La FIGURA 10 mostra l'architettura gerarchica di Hyper-V: un hypervisor, denominato root, ha accesso diretto all'hardware del dispositivo. Questo componente crea degli ambienti isolati, ciascuno con il suo sistema operativo guest (nella figura: Windows 10, Linux e Windows Server 2019) che usufruiscono di un servizio provider (VSP, Virtualization Service Provider) e un servizio consumer (VSC, Virtualization Service Consumer) per comunicare con l'hypervisor root.

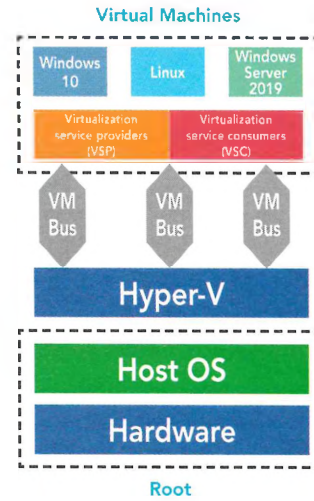


FIGURA 10 L'architettura gerarchica di Hyper-V

La versione **standalone** di Windows Hyper-V Server è gratuita e senza limiti di tempo. La ISO 64-bit è scaricabile qui:

www.microsoft.com/it-it/evalcenter/evaluate-hyper-v-server-2019

Questa versione è scelta soprattutto per gli ambienti in cui si utilizzano macchine virtuali Linux che non richiedono una licenza, a differenza di quelle Windows.

Hyper-V è considerato, all'interno di Windows Server, un ruolo dello stesso server e come tale è configurabile dal Server Manager.

Nella prossima Unità ci occuperemo dei principali ruoli server e di come configurarli attraverso Server Manager o PowerShell.

FISSA LE CONOSCENZE

- Che cosa sono gli host e i guest nella virtualizzazione dei server?
- Descrivi i due layer del sistema operativo ospitante (host).
- Descrivi la Desktop Virtualization.
- Descrivi la Network Virtualization.

4 LA VIRTUALIZZAZIONE DEI SOFTWARE

4.1 La virtualizzazione del sistema operativo

Un programma facile e veloce per virtualizzare un sistema operativo è **Oracle VM VirtualBox** (*www.virtualbox.org*). Si tratta di un programma gratuito, open source e multipiattaforma, disponibile per Windows, Mac OS X e Linux. VirtualBox permette di virtualizzare tutti i principali sistemi operativi in maniera semplice e senza appesantire più del dovuto il computer.
VirtualBox consente di testare diverse combinazioni: Windows e Linux su Mac, Linux su Windows, Windows su Linux, Windows su Windows, e così via.

> VirtualBox ha la caratteristica peculiare di potersi collegare a supporti **iSCSI** (Internet SCSI) e di poterli utilizzare come dischi virtuali.

iSCSI è un protocollo che permette di inviare comandi a dispositivi di memoria SCSI fisicamente collegati a server e/o altri dispositivi remoti. È un protocollo molto utilizzato poiché permette di consolidare l'archiviazione dei dati su dispositivi virtuali, collegati attraverso la rete, dando l'illusione di disporre localmente di un disco fisico che invece si trova in realtà su un dispositivo di storage remoto.
Prima di procedere alla virtualizzazione è necessario procurarsi un'immagine #ISO del CD/DVD d'installazione del sistema operativo. In questo modo il CD/DVD può essere diffuso in rete con maggiore semplicità. Infatti il modo più comune di ottenere un file ISO è quello di scaricarlo (acquistandolo, se si tratta di sistemi operativi proprietari) da un sito web.

#techwords

ISO
Un file ISO è genericamente detto **immagine** a causa del significato del termine ISO, che deriva dal greco *isos* ossia uguale. Un'immagine ISO è quindi un unico file che contiene esattamente gli stessi file e la stessa struttura di un CD/DVD di cui è l'esatta copia.

Un altro programma di virtualizzazione molto diffuso è **VMware** (*www.vmware.com*), disponibile nelle versioni **Workstation** per sistemi Windows e Linux e **Fusion** per sistemi Mac.
Entrambi questi prodotti offrono una versione base denominata **Player** e una avanzata denominata **Pro**. Per le versioni Player è disponibile una licenza gratuita a uso personale.
Gli utenti **Mac** che vogliono virtualizzare Windows o Linux sul proprio computer hanno a disposizione **Parallels Desktop** (*www.parallels.com*) che è probabilmente la migliore soluzione per emulare sistemi operativi sui computer della Apple; offre infatti un'elevata integrazione con OS X e un'estrema facilità di utilizzo. È a pagamento, ma è disponibile in una versione di prova gratuita.

#prendinota

Le macchine virtuali risultano comode per installare su macchine Mac quegli applicativi esistenti in commercio solo per Windows o Linux.

4.2 La virtualizzazione delle applicazioni

Se anziché creare e gestire intere macchine virtuali si desidera virtualizzare solo delle applicazioni (e non l'intero sistema operativo), allora occorre un approccio diverso. Lo spostamento dei database e delle applicazioni business-critical e mission-critical in un ambiente virtualizzato è la soluzione preferita dalla gran parte delle aziende.
Per virtualizzare le applicazioni si può utilizzare, per esempio, **SVS** (**Software Virtualization Solution**). Si tratta di un software sviluppato inizialmente da Altiris (acquisita nel 2007 da Symantec) allo scopo appunto di virtualizzare le sole applicazioni (in ambiente Windows).

Più precisamente, SVS si interpone tra il sistema operativo e il processo di installazione delle applicazioni tenendo traccia dei file inseriti e delle modifiche al registro di sistema, in modo che tali applicazioni non modifichino la configurazione del sistema stesso e non generino conflitti con altri programmi.

La guida in linea di SVS definisce **layer** gli ambienti di virtualizzazione dedicati a ciascuna applicazione. I layer che contengono le varie applicazioni possono essere attivati o disattivati in qualunque momento (anche al momento dell'avvio di Windows), e l'utente di fatto non è in grado di distinguere le applicazioni installate nativamente nel sistema operativo da quelle all'interno del programma di virtualizzazione. Analogamente, disattivandone il layer corrispondente, è possibile rendere del tutto invisibile un'applicazione, le modifiche del registro, i file del programma e le icone sul desktop e nel menu avvio, in modo che tutte le modifiche alla configurazione del sistema vengano nascoste.
Naturalmente, se un programma che potrebbe rendere instabile il sistema viene installato in un layer di SVS, l'installazione non potrà danneggiare in modo permanente il sistema.
Per riportare il sistema allo stato originario sarà sufficiente disattivare il layer corrispondente a tali applicazioni o addirittura eliminarlo.

Altri software per virtualizzare le applicazioni sono prodotti da **VMware**, **Citrix (Virtual Apps and Desktops)** e **Microsoft (Application Virtualization, App-V,** per Windows 10) ed essenzialmente si basano sul concetto di incapsulare un'applicazione in un singolo file eseguibile. Quando è avviato dall'utente, l'eseguibile fa girare l'applicazione in esso inglobata all'interno di un ambiente (bolla) che virtualizza il sistema operativo, il registro di Windows e il file-system.

Riassumendo, le caratteristiche principali e i benefici della virtualizzazione delle applicazioni sono:

- gestione centralizzata delle applicazioni;
- protezione delle applicazioni e dei dati in un data center;
- riduzione immediata del **TCO (#Total Cost of Ownership)** di gestione del parco informatico installato;
- semplicità di accesso e pubblicazione delle applicazioni;
- semplicità di aggiornamento e manutenzione;
- isolamento di applicazioni potenzialmente pericolose o conflittuali;
- controllo completo dell'accesso all'applicazione;
- controllo completo delle attività dell'utente.

Sistemi operativi virtuali e applicazioni virtuali necessitano di un'adeguata infrastruttura sottostante, che spesso è conveniente sia anch'essa virtuale. Questo ha portato allo sviluppo delle soluzioni cloud di cui ci occupiamo nella Lezione 6.

#prendinota

Uno dei vantaggi di Software Virtualization Solution è la possibilità di installare anche molteplici versioni della stessa applicazione sullo stesso sistema senza conflitti di librerie o impostazioni.

#techwords

Total Cost of Ownership
TCO, in italiano costo totale di proprietà o costo totale di possesso, è un approccio sviluppato nel 1987, utilizzato per calcolare tutti i costi del ciclo di vita di un'apparecchiatura informatica IT, per l'acquisto, l'installazione, la gestione, la manutenzione e il suo smantellamento.

FISSA LE CONOSCENZE

- Che cosa è necessario aver preparato prima di procedere alla virtualizzazione del sistema operativo?
- Qual è uno dei principali vantaggi della virtualizzazione delle applicazioni?

5 CREARE UNA MACCHINA VIRTUALE CON VIRTUALBOX

Nella Lezione precedente abbiamo elencato alcuni software per la virtualizzazione dei sistemi operativi. Tra questi uno dei più diffusi è **Oracle VM VirtualBox**.
L'installazione di questa applicazione è molto semplice e completamente guidata: dalla pagina web *www.virtualbox.org/wiki/Downloads* è possibile scaricare il file di installazione relativo al sistema operativo in uso sul computer ospitante (**Host OS**).
Sono disponibili due tipi di package:

- **VirtualBox platform packages**: è il pacchetto base che contiene le componenti necessarie per l'installazione del software sul computer;
- **VirtualBox extension pack**: è un pacchetto per estendere le funzionalità di base di VirtualBox. Tra queste troviamo il supporto per:
  - USB: la macchina virtuale può accedere direttamente ai dispositivi USB;
  - VRDP (VirtualBox Remote Desktop Protocol): la macchina virtuale in esecuzione su un computer può essere visualizzata su un secondo computer;
  - Host webcam passthrough: permette l'utilizzo della webcam del computer anche sulla macchina virtuale.

Si deve effettuare prima l'installazione di VirtualBox platform packages e poi quella di VirtualBox extension pack. Una volta completata l'installazione di VirtualBox, si può creare la macchina virtuale (**VM, Virtual Machine**) in cui installare il sistema operativo desiderato (**Guest OS**). Prima, però, è opportuno procurarsi l'immagine **ISO** di tale sistema, come indicato nella Lezione precedente.

esercizio

→ PROBLEMA

Prendiamo in considerazione un computer con sistema operativo Windows 10 (Host OS), sul quale abbiamo già installato l'applicazione Oracle VM VirtualBox. Procedere ora con la creazione di una macchina virtuale per il sistema Linux Ubuntu 20.04 LTS, che sarà quindi il Guest OS di quel computer.

→ SVOLGIMENTO

Dopo aver avviato l'applicativo VirtualBox precedentemente scaricato e installato, si può procedere seguendo pochi semplici passaggi.

1) Fare Clic sul pulsante **Nuova** nella parte superiore della finestra di **Oracle VM VirtualBox Gestore** (FIGURA 11). Si aprirà una procedura guidata per la creazione di una nuova VM.

FIGURA 11 Menu di gestione di VirtualBox

2) La prima finestra richiede la scelta del nome della VM e del tipo di SO da installare. Se selezioniamo il pulsante in basso **Modalità esperta** visualizziamo in un'unica videata le 3 finestre successive che avremmo visualizzato anche in modalità guidata.

Quindi clicchiamo su Modalità esperta e procediamo con le nostre scelte (FIGURA 12):

- **nome e sistema operativo**: scriviamo il nome della VM (nel nostro esempio: Ubuntu) e selezioniamo il tipo di SO: Linux versione Ubuntu_64. Questa scelta richiede di aver abilitato la virtualizzazione nel BIOS (Virtualization technology, **VTX**); in caso contrario, al termine della creazione della VM, quando si seleziona Impostazioni, è segnalato un avviso nella parte inferiore della finestra;
- **dimensione della memoria** (RAM): benché per Linux il minimo sia 2 GB, se si ha a disposizione una memoria di almeno 8 GB e non si devono far eseguire più macchine virtuali in contemporanea, è consigliabile dedicare 4 GB per la VM, quindi selezioniamo 4096 MB;
- **disco fisso**: selezioniamo l'opzione **Crea subito un nuovo disco fisso virtuale** e clicchiamo sul pulsante **Crea**.

#prendinota

La memoria che si assegna alla VM non sarà disponibile per l'Host OS mentre la VM è in esecuzione, quindi è necessario allocare quanta memoria il Guest OS e le applicazioni richiedono per funzionare correttamente e non di più.

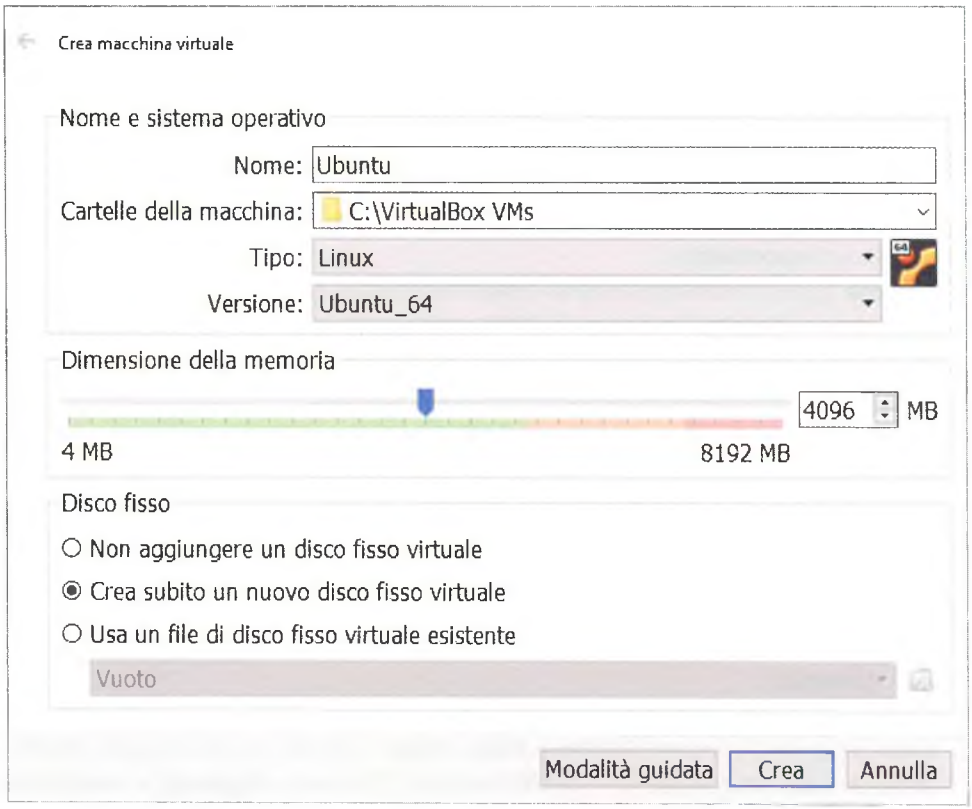


FIGURA 12 Creazione della VM Linux Ubuntu

3) Nella finestra successiva scegliamo il tipo di disco fisso, **VDI (VirtualBox Disk Image)** e la sua dimensione. È preferibile scegliere il tipo di disco virtuale VDI usato di default da VirtualBox quando si crea una nuova VM con un nuovo disco fisso. Creiamo un disco virtuale di 30 GB, allocato **dinamicamente**, per avere una gestione più flessibile della memoria sul disco (la creazione è più veloce rispetto alla scelta di dimensione fissa).
   All'inizio le operazioni di scrittura sul disco dinamico saranno più lente perché il sistema aumenta la dimensione in base allo spazio richiesto, fino alla dimensione massima richiesta. Da notare che anche se cancelliamo dei dati, la dimensione raggiunta non diminuirà.
4) Al termine cliccare sul pulsante **Crea**: viene visualizzata la finestra iniziale di VirtualBox con a sinistra la VM appena creata e a destra i dettagli della sua configurazione (FIGURA 13).

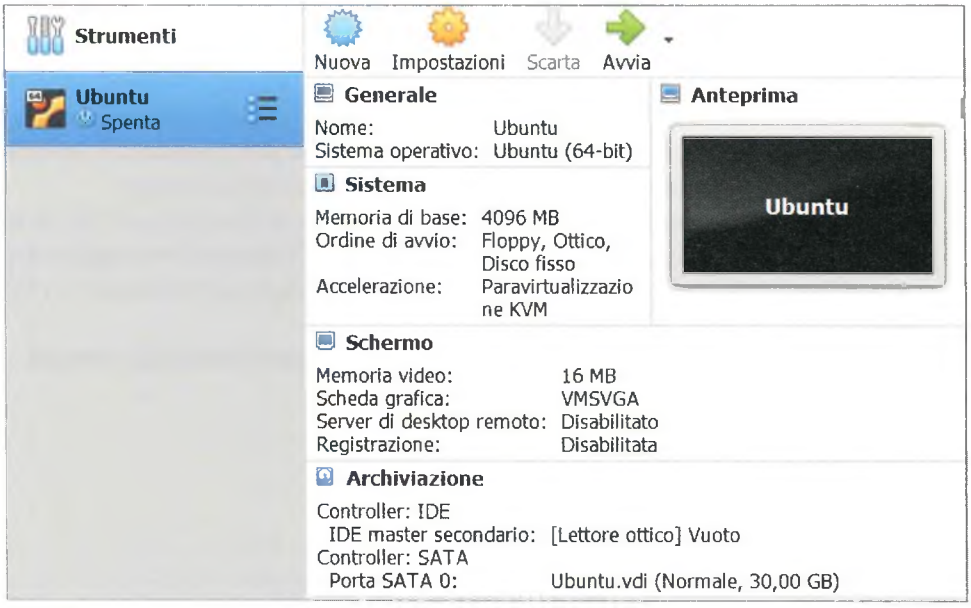


FIGURA 13 Le informazioni sulla VM creata

A questo punto è possibile modificare alcune impostazioni della VM, prima di avviarla, cliccando su **Impostazioni**:

- **Sistema**: si può modificare l'ordine di **boot** e scegliere il numero di processori logici da dedicare alla VM. Come per la RAM, anche qui è presente una barra di scorrimento che consiglia fin dove spingersi nella scelta dei processori al fine di garantire un buon funzionamento della macchina reale (Host OS);
- **Schermo**: è opportuno aumentare la **memoria video** al massimo indicato e abilitare l'accelerazione 3D.

Portato a termine il processo di creazione della VM, occorre avviare l'installazione del sistema operativo Linux. La distribuzione scelta è **Ubuntu 20.04 LTS** (la Long Term Support è supportata per 5 anni) e la ISO si scarica qui: *https://ubuntu.com/download/desktop*. Procedere quindi secondo i passi seguenti:

1) nella pagina iniziale di VirtualBox, dove abbiamo la nostra VM appena creata, cliccare su **Avvia**;
2) compare la finestra **Selezione disco di avvio**, cliccare sull'icona a lato della casella di testo per aprire la finestra **Selettore disco ottico**. Il file ISO di Ubuntu sarà trattato come un disco ottico (cioè un CD/DVD) virtuale. Cliccare su **Aggiungi** e selezionare dal disco l'immagine ISO precedentemente caricata, quindi cliccare su **Scegli**. Tornati nella finestra precedente, risulterà selezionato il file **.iso** scelto, cliccare quindi su **Avvia**;
3) a questo punto è avviata la procedura di **installazione** di Ubuntu sulla VM, in cui si procede esattamente come se lo si stesse installando su un computer reale. Quando viene richiesto di rimuovere il disco ottico, si procede a spegnere la VM: cliccare sulla **X** in alto a destra e scegliere **Spegni la macchina**. Quindi avviarla nuovamente: sarà visualizzata la schermata iniziale di Ubuntu.

FISSA LE CONOSCENZE

- Spiega la differenza tra Host OS e Guest OS.
- Come viene gestito lo spazio sul disco virtuale in VirtualBox?
- Come si installa il sistema operativo sulla VM?

6 LE SOLUZIONI CLOUD

6.1 Il cloud computing

Virtualizzazione e **cloud computing** sono due aspetti dello stesso concetto.
La virtualizzazione permette di ottimizzare le risorse hardware e software aziendali e permette di far fronte a esigenze specifiche secondo il più classico paradigma dell'on demand.
Diverso è il discorso per il cloud.

> Il **cloud computing** è un insieme di tecnologie informatiche che permettono l'utilizzo di risorse hardware e software, virtualizzate e distribuite in remoto in una tipica architettura Client/Server. Ma, ancora di più, il cloud computing è la possibilità di **distribuire e utilizzare servizi IT** attraverso il web.

L'esigenza di questo tipo di ambienti IT in cui gestire uniformemente, in un'unica **nuvola** (**cloud**), le componenti digitali è sempre più sentita, a causa della crescita esponenziale delle apparecchiature connesse in rete e dei processi di streaming di dati in tempo reale e anche per la diffusione di architetture e applicazioni web orientate al servizio, ai progetti di collaborazione e di ricerca.

Con il cloud computing, i sistemi e le applicazioni informatiche che consentono alle aziende di funzionare sono concentrati in pochi grandi data center messi a disposizione degli utenti, in maniera dinamica, elastica e, a richiesta, sotto forma di servizio in abbonamento o a consumo.
In questo modo si abbattono i costi degli investimenti nei centri informatici (CED) delle aziende e degli enti pubblici e al contempo le organizzazioni, grandi e piccole, possono accedere rapidamente a enormi risorse di qualsiasi tipo (calcolo, memorizzazione, ecc.) in maniera del tutto virtuale, abbattendo quindi completamente tutti i costi delle infrastrutture fisse (acquisto, mantenimento, potenziamento, ecc.).
L'utente finale, infatti, pagherà l'uso delle risorse virtuali solo in base al loro effettivo utilizzo.
In questo modo, sono superate le tradizionali barriere alla realizzazione dei sistemi informativi, quali i **costi** e la **complessità**, mentre gli utilizzatori dei sistemi informatici, possono concentrarsi sulla propria missione più strategica (core business).

Le **piccole** e **medie imprese** possono accedere all'innovazione tecnologica, automatizzando i processi aziendali e realizzando rapidamente le funzioni avanzate del business (commercio elettronico, marketing digitale, partnership con altre aziende). Sono opportunità che ora sono accessibili con investimenti limitati. Ciò vale a maggior ragione per le startup e l'imprenditoria giovanile. Per tutti sarà più facile trasformare le nuove idee in prodotti e servizi, affrontare la sfida del mercato e competere.
Naturalmente, qualsiasi azienda che vuole migrare verso il cloud computing deve considerare l'investimento iniziale in termini di **costi operativi e costruzione delle competenze**.

#prendinota

Le **piccole e medie imprese** o PMI sono aziende di dimensioni limitate in termini di dipendenti e di bilancio.
Per **startup** si intende l'avvio di un'attività innovativa sia per il modello di business (ripetibile e scalabile) sia per i suoi prodotti o servizi.
Stati e Regioni di solito mettono in atto politiche di sostegno specifiche verso le PMI e le startup.

I principali tipi di cloud computing sono:

- **Private cloud**: ambiente informatico solitamente interno all'azienda, realizzato virtualizzando le risorse, i servizi e standardizzandone la gestione; il cloud privato può anche essere affidato a provider esterni a condizione di mantenere in mano all'azienda il pieno controllo su aspetti quali l'infrastruttura fisica e i criteri di sicurezza;
- **Public cloud**: fornitura di servizi informatici (sistema operativo, infrastruttura, applicazioni) in forma standard attraverso un provider di servizi esterno all'azienda che ne garantisce efficienza e sicurezza;
- **Community cloud**: i servizi sono condivisi tra più organizzazioni con un interesse comune, ma non sono disponibili pubblicamente. Un esempio è il database medico condiviso tra tutti gli ospedali di una regione o di una nazione;
- **Hybrid cloud**: soluzione che unisce i vantaggi del private, public e community cloud poiché consente da un lato di sfruttare le risorse e i servizi già eventualmente operanti all'interno dell'azienda o che si desidera comunque gestire direttamente, dall'altro di estendere il proprio data center fino al cloud pubblico per utilizzarne dinamicamente le grandi potenzialità a fronte di investimenti contenuti.
  Di Hybrid cloud si parlerà nella prossima Lezione.

È possibile realizzare anche un **Multi-cloud computing** costituito da due o più cloud distinti, siano essi pubblici o privati o di entrambi i tipi.

6.2 L'architettura cloud

L'architettura informatica di un sistema di cloud computing prevede uno o più server reali, generalmente in architettura ad alta affidabilità e fisicamente collocati presso il data center del fornitore del servizio, a cui si collegano via web i client, utenti di quel cloud.
Il sistema cloud comporta componenti multiple che comunicano le une con le altre su interfacce di programmazione, di solito mediante web service.

In una rete cloud possiamo definire le seguenti componenti (FIGURA 14):

- **Cloud client**: composto da hardware (dispositivi di qualsiasi tipo connessi a Internet, server aziendali compresi) e software (un qualsiasi browser come Google Chrome, Firefox, ecc.) di cui il sistema cloud necessita per funzionare correttamente dal lato client;
- **Cloud application**: architetture software che eliminano il bisogno di installare e gestire le applicazioni client sul computer dell'utente, alleviando così il carico di manutenzione del software e delle operazioni in corso;
- **Cloud platform**: servizio che consegna una piattaforma di elaborazione e memorizzazione con stack di soluzioni approntate in base alle esigenze dell'utente senza che quest'ultimo debba avere una conoscenza profonda degli strati del software;
- **Cloud storage**: comporta la capacità di memorizzazione dei dati come un servizio offerto dalla rete (calcolati per gigabyte o terabyte per mese);
- **Cloud infrastructure**: è il servizio che mette a disposizione reti di computer virtuali.

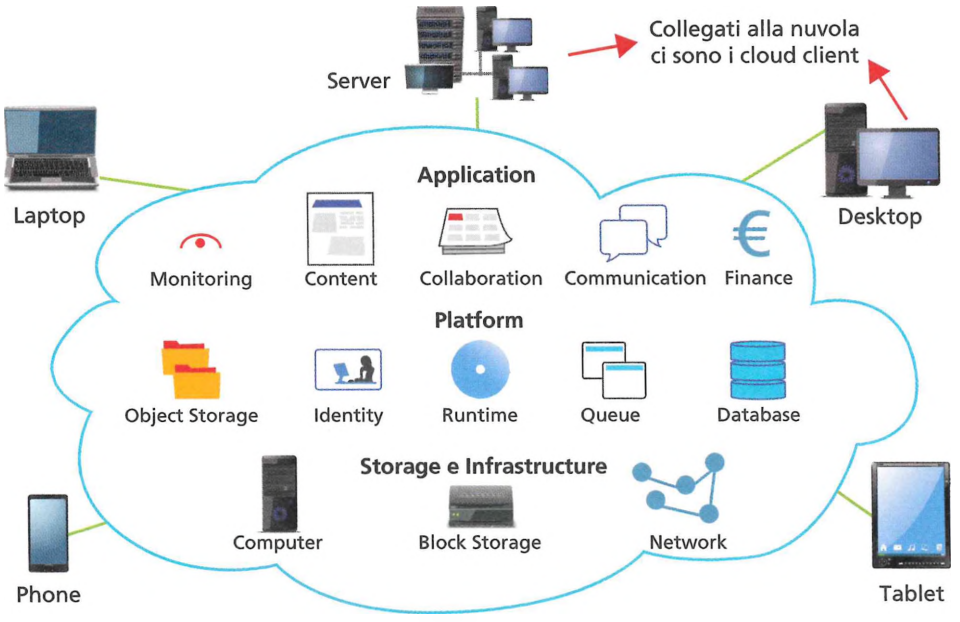


FIGURA 14 Componenti del cloud computing

I MODELLI DI SERVIZI CLOUD

In base alle varie componenti presenti, si possono realizzare diverse tipologie di servizi (o funzionalità) di cloud computing:

- **SaaS** (Software as a Service): consiste nell'utilizzo di programmi installati su un server remoto, cioè fuori dalla LAN aziendale, spesso attraverso un web browser. Servizi come Gmail o Office 365 sono un esempio di SaaS;
- **DaaS** (Data as a Service): con questo servizio vengono messi a disposizione via web solamente i dati, ai quali gli utenti possono accedere tramite qualsiasi applicazione come se fossero residenti su un disco locale;
- **HaaS** (Hardware as a Service): con questo servizio l'utente invia i dati in remoto affinché vengano elaborati da computer messi a disposizione e infine restituiti all'utente in forma di risultato dell'elaborazione effettuata;
- **PaaS** (Platform as a Service): invece che uno o più programmi singoli, viene eseguita in remoto una piattaforma software che può essere costituita da diversi servizi, programmi, librerie e così via. Un esempio di PaaS è Jelastic Cloud di Aruba;
- **IaaS** (Infrastructure as a Service): utilizzo di risorse hardware in remoto. Questo tipo di cloud è quasi un sinonimo di **grid computing**, ma con la caratteristica imprescindibile che le risorse vengono utilizzate on demand nel momento in cui una piattaforma ne ha bisogno, e non vengono assegnate a prescindere dal loro utilizzo effettivo.

#prendinota

Fornitori leader di servizi IaaS e PaaS sono:
Amazon Web Services (*aws.amazon.com*);
Windows Azure (*azure.microsoft.com*);
Google Cloud (*cloud.google.com*).

I RUOLI NEL CLOUD COMPUTING

Le 3 **figure** (o **ruoli**) fondamentali presenti nell'ambiente dell'architettura di cloud computing sono mostrate nella FIGURA 15.

1. **Cloud provider**: la figura che possiede e gestisce le risorse (data center, server farm) delle reti cloud assegnando sia le risorse di elaborazione sia i servizi per ogni utente.

Inoltre, possiede e implementa sistemi di elaborazione di cloud *live* per distribuire servizi a terze parti. Di solito questo richiede risorse significative ed esperienza nella costruzione di centri di elaborazione. Nonostante tutto, alcune grosse organizzazioni hanno notato che possedere un cloud provider porta all'azienda che ne fa un uso esclusivo (private cloud) numerosi benefici in termini di efficienza, soprattutto nella gestione dei casi di picchi di carico. Questi benefici sono controbilanciati da una notevole complessità, sia di tipo economico sia prettamente architetturale.

2. **Cloud user**: il fruitore (cliente finale) della nuvola. Un problema rilevante per questa figura è la privacy che potrebbe essere violata.
3. **Cloud vendor**: è la figura (cliente amministratore) che vende prodotti e servizi che facilitano l'adozione e l'uso del cloud computing.

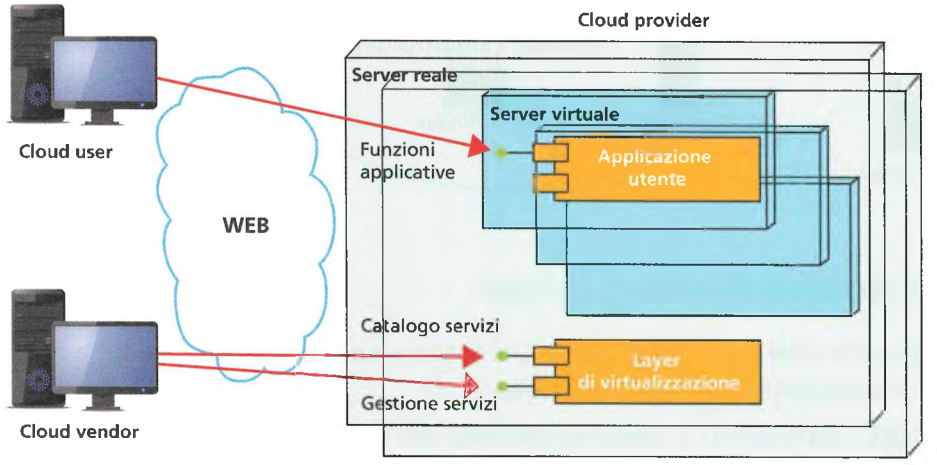


FIGURA 15 Ruoli nell'architettura cloud computing

6.3 Il cloud nella Pubblica Amministrazione

Nel corso degli ultimi anni, l'Information Technology si sta confermando una vera e propria forza motrice per le Pubbliche Amministrazioni (PA).
La possibilità offerta dal cloud computing di utilizzare le tecnologie informatiche con un **modello a consumo** o **ad abbonamento** (si parla anche di modello **a servizio**), liberano l'amministrazione da tutto ciò che riguarda la manutenzione, l'aggiornamento e la distribuzione dei sistemi informativi, rapportando il pagamento all'erogazione di un servizio.
Alcune aziende pubbliche realizzano dei private cloud che prevedono la creazione di data center gestiti dalle amministrazioni stesse, in grado di erogare servizi con tecnologia cloud.
Altre aziende pubbliche realizzano dei public cloud, affidando in toto i loro servizi a cloud provider esterni dotati di propri data center. Attraverso l'ambiente cloud i governi sono in grado di offrire servizi pubblici più efficienti e di soddisfare così esigenze sociali fondamentali in vari settori, dalla salute (**eHealth**) ai servizi amministrativi (**eGovernment**), alla giustizia (**eJustice**).

Nella TABELLA 5 sono elencati i principali vantaggi del cloud computing per le PA e anche per le PMI confrontati con le medesime soluzioni attuate con l'IT tradizionale.

L'efficienza sul piano dei costi emerge come l'elemento chiave che spinge l'investimento sul cloud nell'ambito della Pubblica Amministrazione dei Paesi dell'Unione Europea.

	Soluzioni cloud	IT tradizionale
Investimento iniziale	Costo contenuto incidente su spese operative, per modalità a servizio, a consumo o ad abbonamento.	Forte impatto sulle spese per capitale delle PA
Disponibilità	Capacità di adattamento in casi di: alternanza (on-off), forte crescita, picchi prevedibili (stagionalità, scadenze) o inaspettati.	Difficoltà a seguire andamenti dell'attività come alternanza (on-off), forte crescita, picchi prevedibili o inaspettati.
Scalabilità	Accesso a risorse sofisticate e scalabili in maniera arbitraria, senza costi iniziali e senza la complessità dell'infrastruttura di un data center.	Manutenzione del software e dell'hardware.
Collaborazione	Facilitate le aggregazioni di enti pubblici e uffici decentrati.	Eccessiva settorizzazione e mancanza di comunicazione tra gli enti pubblici.
Sicurezza	Conformità alle politiche di privacy e sicurezza della PA, formalizzate in SLA (Service Level Agreement, Accordi sul livello del servizio).	Necessità di adeguare ciascun sistema alle politiche di privacy e sicurezza della PA

TABELLA 5 Principali vantaggi del cloud computing per le PA

In Italia la PA non costruisce nuovi data center (si limita a procedere agli adeguamenti dei data center esistenti esclusivamente per evitare l'interruzione del servizio) cercando così di anticipare la dismissione per passare ai servizi cloud. Tra questi citiamo i servizi digitali dedicati a cittadini e imprese:

- **CIE**, Carta di Identità Elettronica;
- **SPID**, Sistema Pubblico di Identità Digitale;
- **PagoPa**, piattaforma pagamenti elettronici alla PA;
- **Fatturazione elettronica**;
- **ANPR**, Anagrafe Nazionale della Popolazione Residente;
- **NoiPA**, piattaforma per la gestione del personale della PA.

La PA prevede anche l'Open Data, cioè la possibilità di mettere a disposizione della società civile i dati in suo possesso non sottoposti a vincoli di privacy. L'informazione pubblica può essere diffusa attraverso canali tradizionali (per esempio la notifica a domicilio delle multe, la pubblicazione sulla Gazzetta Ufficiale, l'affissione pubblica) oppure via web.

Man mano che il mercato maturerà e proseguirà la costruzione del sistema europeo, i Governi dovranno impegnarsi nel migliore sfruttamento del potenziale offerto dalla tecnologia cloud. Cloud pubblici e ibridi emergeranno sugli attuali progetti di cloud privato.

FISSA LE CONOSCENZE

- Quali sono i 3 tipi principali di cloud computing?
- Quali sono le diverse tipologie di servizi (o funzionalità) di cloud computing?
- Quali sono le 3 figure (o ruoli) fondamentali nell'architettura di cloud computing?
- Perché il cloud computing è utile per le aziende pubbliche?

Case study
Virtualizzazione e cloud

7 LE SOLUZIONI IBRIDE: HYBRID CLOUD

7.1 L'architettura Hybrid cloud

Perché scegliere tra il data center locale (con server dedicati o virtuali) e il cloud remoto (con server dedicati o virtuali), oppure tra il cloud privato (con data center interno) e il cloud pubblico (con data center esterno)?

Una soluzione **Hybrid cloud** consente di sfruttare il meglio di ogni opzione.

Le aziende ormai affrontano il mondo dell'IT in termini di pool di risorse fruibili attraverso infrastrutture pubbliche, private, dedicate e virtuali, allo scopo di ottenere il giusto mix di prestazioni per il proprio business.
Costruire applicazioni ibride efficienti richiede di essere in grado di far comunicare tutte le risorse che si hanno a disposizione.

Nella FIGURA 16 vediamo come un cloud privato e uno pubblico si combinano attraverso un collegamento VPN (Virtual Private Network, studiata nell'Unità 3). L'architettura comprende sia la struttura di proprietà dell'azienda (**On-Premise**) sia quella di proprietà del provider esterno (**Off-Premise**).
I software per la gestione delle soluzioni ibride consentono di trasformare le varie piattaforme in un'unica entità che può essere gestita come un unico sistema.

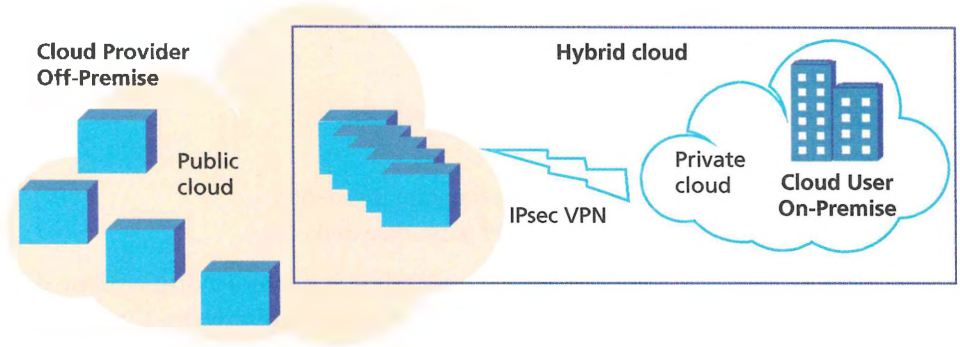


FIGURA 16 Architettura Hybrid cloud

Questo permette di bilanciare le richieste (**load balancer**) di tutte le differenti aree dell'azienda, spostando le risorse laddove sono di maggiore utilità e applicando la scalabilità al sistema in base alle specifiche esigenze dell'azienda.
Per esempio è possibile:

- spostare con facilità carichi di lavoro dal data center aziendale al data center di un provider di servizi hosting, mantenendo una visione completa dell'infrastruttura;
- creare applicazioni ibride rendendole disponibili su server (**App Server**) che sfruttino sia le risorse locali sia quelle nel cloud;
- utilizzare opzioni di archiviazione, backup e ripristino (Warm Disaster Recovery) più efficienti a un costo più conveniente.

Nella FIGURA 17 viene mostrata una soluzione ibrida bilanciata (o equilibrata) per la gestione dei dati e delle applicazioni.

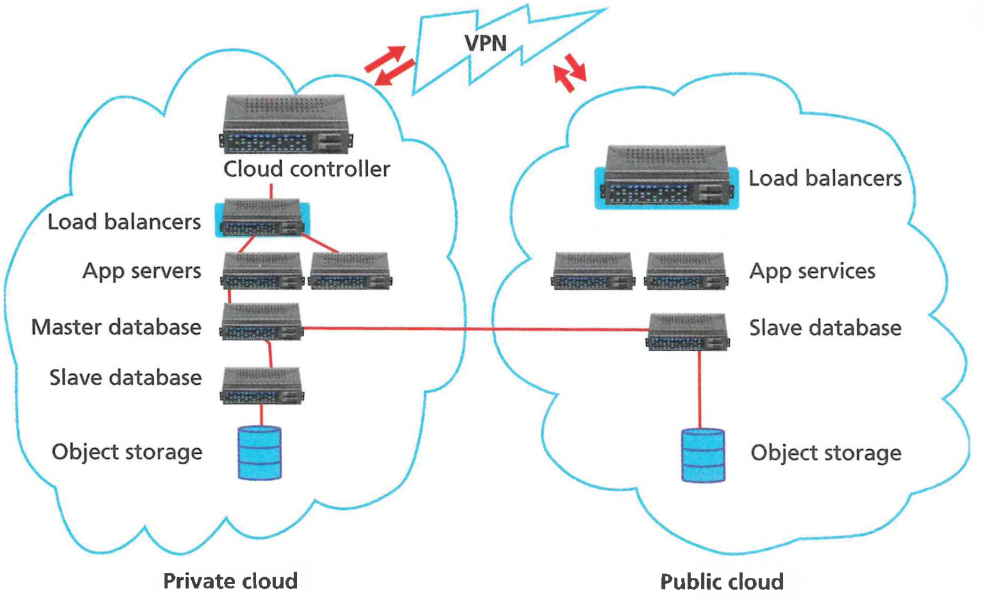


FIGURA 17 Hybrid cloud bilanciato in scenario di Warm Disaster Recovery

7.2 L'adozione del Hybrid cloud

I piani di adozione dell'Hybrid cloud sono in crescita, così come l'interesse verso le possibili strategie per mettere in sicurezza gli ambienti che integrano le risorse aziendali interne e i servizi IT in private cloud con quelli disponibili sui public cloud.

Secondo studi di Gartner Group, entro il 2021 il 90% delle aziende avrà implementato un modello di cloud ibrido.
Il cloud ibrido offre alle aziende la possibilità di spostare rapidamente il carico di lavoro dal private cloud al public cloud o di utilizzare il cloud come luogo di backup per il disaster recovery.
Sui server nel public cloud sono condivisi i dati di più aziende, quindi la sicurezza è una delle priorità richieste da un'azienda: non tutte le piattaforme di crittografia, per esempio, supportano sia i public cloud sia i private cloud.
Inoltre, poiché l'uso dell'Hybrid cloud è più complesso rispetto a quello del semplice public cloud o private cloud, le aziende devono pianificare attentamente in che modo l'Hybrid cloud scalerà in caso di aumento o diminuzione della richiesta di risorse.

FISSA LE CONOSCENZE

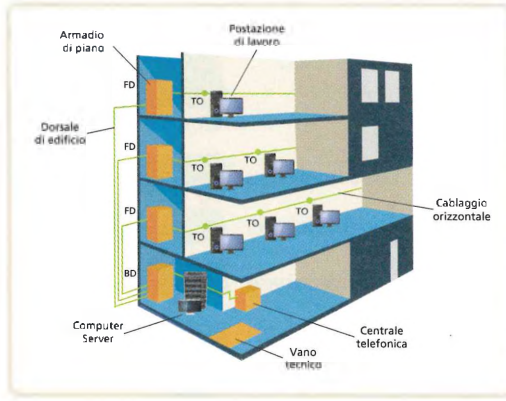
- Da che cosa è composto un cloud ibrido?
- Quali sono i vantaggi di una soluzione ibrida?
- Descrivi la soluzione ibrida bilanciata.

RIPASSIAMO INSIEME

DIDATTICA INCLUSIVA

1 La struttura fisica della rete

La struttura di una rete è ciò che consente a due end system (siano essi host, dispositivi o applicazioni) di essere collegati. Per progettarla occorre stabilire topologia, mezzi trasmissivi e dispositivi, e seguire le norme del cablaggio strutturato, cioè scelta di cavi e dispositivi di rete necessari alla realizzazione fisica della LAN. Uno standard internazionale per il cablaggio per le telecomunicazioni è l'ISO/IEC 11801.



2 La collocazione dei server dedicati e virtuali

In base alle necessità dell'azienda, si stabilisce quali macchine server utilizzare e dove collocarle, scegliendo tra servizi di housing e colocation in hosting e tra server dedicati e server virtuali. Alle piccole imprese sono sufficienti macchine standalone; alle aziende di medie o grandi dimensioni servono data center interni o server farm gestite da data center esterni.

3 La virtualizzazione dei server

Oltre ai servizi di hosting, è possibile sfruttare la virtualizzazione dei server attraverso la Server Virtualization, che consiste nell'esecuzione di diversi sistemi operativi e applicativi client, in tante macchine virtuali (virtual machine) diverse su uno stesso server.

4 La virtualizzazione dei software

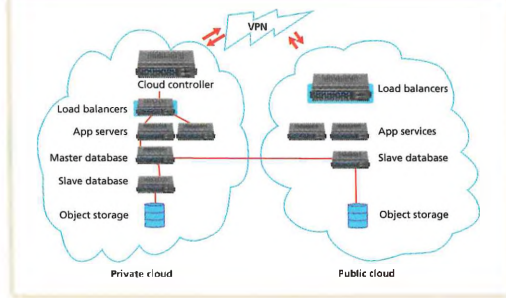
I programmi di virtualizzazione consentono di creare dei PC virtuali sul PC reale, in questo modo è possibile provare sistemi operativi e programmi di ogni genere senza intaccare il sistema originale e senza rischi relativi a virus o crash.

6 Le soluzioni cloud

Il cloud computing è l'insieme di tecnologie informatiche che permette l'utilizzo di risorse hardware e software, virtualizzate e distribuite in remoto in una tipica architettura Client/Server. Ma esso è anche la possibilità di distribuire e usare servizi IT attraverso il web.

7 Le soluzioni ibride: Hybrid cloud

Le aziende ormai affrontano il mondo dell'IT in termini di pool di risorse fruibili attraverso infrastrutture pubbliche, private, dedicate e virtuali, per ottenere le prestazioni necessarie. Occorre quindi scegliere e assemblare tali risorse per costruire la rete aziendale sia in termini di struttura sia di infrastruttura.



VERIFICA DI FINE UNITÀ

Test
Svolgi il test interattivo

Quali delle seguenti affermazioni sono vere (V) e quali false (F)?

1. La topologia fisica utilizzata nelle LAN aziendali è ad anello. V F
2. Lo standard ISO/IEC 11801 prevede 3 livelli di centro stella. V F
3. I data center per sicurezza sono sempre interni alla LAN aziendale. V F
4. In VirtualBox l'immagine ISO del sistema operativo è utilizzata come un disco ottico virtuale. V F
5. La parte di memoria RAM allocata alla macchina virtuale viene tolta per sempre alla macchina reale. V F
6. Il cloud computing facilita le piccole e medie imprese. V F
7. Il cloud computing è svantaggioso per la Pubblica Amministrazione. V F
8. Il cloud computing facilita le startup. V F
9. Una soluzione Hybrid cloud bilanciata è indicata per il backup e ripristino dei sistemi. V F

Domande a scelta multipla (una sola è la risposta esatta)

1. **Quale tra i seguenti non è un centro stella a norma ISO/IEC 11801?**
   - A CD (Campus Distributor)
   - B BD (Building Distributor)
   - C FD (Floor Distributor)
   - D OD (Office Distributor)

2. **Quale tra le seguenti forme di virtualizzazione permette l'esecuzione di SO diversi sullo stesso hardware?**
   - A Desktop Virtualization
   - B Server Virtualization
   - C Application Virtualization
   - D Presentation Virtualization

3. **Quale tra i seguenti non è una componente di una rete cloud?**
   - A Cloud client
   - B Cloud application
   - C Cloud server
   - D Cloud storage

4. **Quale tra le seguenti non è una figura (ruolo) tipica dell'architettura di cloud computing?**
   - A Cloud client
   - B Cloud provider
   - C Cloud user
   - D Cloud vendor

Ascolta le risposte

PREPARATI PER IL COLLOQUIO ORALE

1. LEZIONE 1 **Quali sono i vantaggi della topologia a stella estesa?**
2. LEZIONE 1 **Quali sono le due dorsali di cablaggio e quali centri stella collegano?**
3. LEZIONE 2 **Elenca i server indispensabili in una rete.**
4. LEZIONE 2 **Spiega le differenze tra l'avere il data center interno oppure esterno all'azienda.**
5. LEZIONE 2 **Quali sono i principali servizi che offrono le server farm?**
6. LEZIONE 3 **Elenca i vantaggi della virtualizzazione.**
7. LEZIONE 3 **Descr ivi l'architettura di Microsoft Hyper-V.**
8. LEZIONE 4 **Che cosa sono le virtual machine nel contesto dei software virtuali?**
9. LEZIONE 4 **Riassumi le caratteristiche principali e i benefici della virtualizzazione delle applicazioni.**
10. LEZIONE 6 **Quali sono le componenti di una rete cloud?**
11. LEZIONE 6 **Che cosa si intende per modello cloud a servizio?**
12. LEZIONE 6 **Quali sono i principali vantaggi del cloud computing per le PA (Pubbliche Amministrazioni) e per le PMI (Piccole e Medie Imprese)?**
13. LEZIONE 7 A che cosa serve una VPN (Virtual Private Network) nell'ambito di un Hybrid cloud?

IN ENGLISH, PLEASE

CLIL

Ascolta la **pronuncia del testo** e verifica la **traduzione**

ABSTRACT

Network architecture: from cabling to cloud

The network architecture is what allows the two ends of a network to connect. Its design requires knowledge of topology, transmission media and devices, and the rules of structured cabling. Structured cabling allows the network to be designed according to the international standards in order to create networks using devices from different manufacturers. According to the network type and the needs of the owner (business, company) it must be decided how many servers are required and the way they will be connected to each other and with the public networks on the basis of efficiency, flexibility and security. Server Virtualization allows multiple different operating systems to operate on the same physical machine; it is used to run applications that require different operating systems to work. Virtualization also allows programs and operating systems to run on one physical machine without interfering with its normal operation. Cloud computing is a set of computing technologies that allows the use of virtual hardware and software resources deployed remotely in a typical Client/Server architecture. Moreover, cloud computing makes it possible to deploy and use Information Technology (IT) services over the web.

EXERCISES

Use the appropriate number to match words and meanings.

...	Server farm	1	A service provided by a company to make your website accessible.
...	Server Virtualization	2	Composition of two or more clouds (private, community or public).
...	Housing	3	Virtualized storage service.
...	NIC	4	Different operating systems on the same machine.
...	Hybrid cloud	5	The environment in which a guest OS runs.
...	Cloud storage	6	A collection of computer servers typically mounted on racks in a data center.
...	Hosting	7	Network board.
...	Virtual machine	8	Data server outside the company.

GLOSSARY

Cloud architecture: the structure consisting of several servers to provide network services (storage, application) to users.
Cloud computing: set of computing technologies that allows the use of virtual hardware and software resources deployed remotely in a typical Client/Server architecture over the web.
Data center: a physical place where housing servers, storage systems and associated telecommunication components are located.
Disaster Recovery: a set of policies, tools and procedures to enable critical infrastructure and systems to keep on working after a disruptive event.
Guest OS: the OS that is running inside the virtual machine.
Host OS: the OS of the physical computer on which virtual machine is installed.
ISP (Internet Service Provider): it provides network services over a server farm.
Load Balancer: it distributes the external requests to the hosts based on the hosts current load.
Standalone server: an independent server (it is not part of a group) that provides local authentication and access control to all resources available on it.
Startup: a temporary organization designed to seek, develop and validate a new business model that is repeatable and scalable.

LAVORARE PER COMPETENZE

COMPETENZE IN GIOCO

Competenze disciplinari

- Saper proporre soluzioni interne ed esterne all'azienda.
- Saper proporre soluzioni di virtualizzazione.
- Saper proporre soluzioni cloud.
- Saper descrivere e documentare le soluzioni adottate.
- Utilizzare le reti e gli strumenti informatici nelle attività di studio, ricerca e approfondimento disciplinare.

Competenze chiave di cittadinanza

- Interpretare il testo.
- Risolvere problemi.
- Comunicare.
- Competenza digitale.

obiettivi formativi

- Stimolare l'approfondimento e la ricerca disciplinare.
- Consultare fonti Internet.
- Contestualizzare in un caso reale le nozioni teoriche acquisite studiando.
- Esporre i risultati della ricerca.

tempi

- Preparazione: 2 ore.
- Presentazione dei risultati e dibattito: 1 ora.
- Autovalutazione: 10 minuti.

strumenti

- Libro di testo.
- Dispositivo connesso a Internet.
- Software PowerPoint.
- Proiettore collegato al computer in classe o in laboratorio.

TEMA PROPOSTO

*Proponiamo di seguito una parte del Tema d'Esame di **SISTEMI E RETI** suggerito nel 2015/16 per l'indirizzo INFORMATICA E TELECOMUNICAZIONI articolazione INFORMATICA. In base a quanto appreso in questa Unità, abbiamo gli strumenti per risolvere il quarto quesito della seconda parte del tema.*

«Un giornale locale negli anni Novanta realizzò una propria banca dati telematica per la distribuzione elettronica di un notiziario settimanale. Gli utenti, previo abbonamento, si collegavano via modem e linea telefonica per la lettura degli articoli e l'invio di posta elettronica. Da uno studio preliminare risultava che:

1. a ogni articolo erano associati un titolo, un'immagine ed eventualmente un filmato;

2. un numero settimanale si componeva di circa 100 articoli.

Il nuovo direttore del giornale desidera effettuare l'ammodernamento del sistema, realizzando una nuova rete locale per il collegamento dei computer e di altri dispositivi, la cui collocazione è la seguente:

- un computer e una stampante nell'ufficio del direttore;
- 30 computer distribuiti a due a due negli uffici dei giornalisti;
- 2 computer e 1 stampante professionale nell'ufficio dei redattori;
- altre apparecchiature mobili (smartphone, pc portatili, ecc.), che vengono usate all'occorrenza dai giornalisti o da collaboratori occasionali.

Inoltre, in un locale protetto, vi è un sistema su cui risiedono la banca dati e il web server.
Il giornale ha un sito web contenente informazioni e una sintesi degli articoli pubblicati accessibili a tutti senza autenticazione; contiene inoltre una sezione riservata agli abbonati, i quali possono accedere agli articoli completi. Gli abbonati sono ora circa 5.000.

Il candidato, formulate le opportune ipotesi aggiuntive, sviluppi i seguenti punti: [...]

4. discuta vantaggi e svantaggi dell'offrire il servizio mediante l'attuale soluzione gestita internamente, oppure utilizzando un servizio esterno (hosting o housing), esponendo le motivazioni che inducono alla scelta.»

SVOLGIMENTO

Ipotesi aggiuntive

Ipotizziamo che il direttore del giornale locale voglia fare un investimento per migliorare il servizio offerto agli abbonati, allo scopo di ottenere un aumento sia degli abbonati sia dei visitatori del sito web del giornale.

Descrizione

La nuova rete progettata per il giornale prevede un locale protetto, dedicato ai server per la gestione del sito web e degli abbonati. Questa scelta di collocare il data center aziendale internamente alla sede presenta un grosso svantaggio in termini di costi.

Abbattere i costi, soprattutto quelli iniziali, e potersi concentrare sul proprio business (pubblicare articoli, vendere abbonamenti al giornale, ecc.) e non sugli aspetti tecnologici e di sicurezza legati al funzionamento della rete informatizzata rende preferibile l'esternalizzazione dei servizi.

Il giornale non dovrà quindi assumere dei tecnici sistemisti in pianta stabile ma si potrà avvalere della consulenza informatica delle aziende specializzate in servizi cloud, demandando a loro gli aspetti tecnici.

Anche eventuali picchi di accesso ai server del giornale da parte degli abbonati possono essere previsti e gestiti meglio da potenti server, dedicati o virtualizzati, presenti nelle server farm di chi offre il servizio. Una volta deciso di appoggiarsi a un data center esterno, si ha la possibilità di scegliere tra servizi di hosting o di colocation in housing.

L'hosting potrebbe essere la soluzione ideale per il giornale in quanto consentirebbe di far ospitare il sito web del giornale e l'applicazione per la gestione degli abbonati nella server farm esterna, senza dover né comprare l'hardware (computer server e storage station) né gestire il sistema e avendo a disposizione spazio per i dati dell'ordine dei terabyte. Infatti, non avendo il giornale bisogno di server con prestazioni specifiche, può utilizzare un server di proprietà dell'azienda che fornisce il servizio di hosting.

L'hardware è composto da server di fascia enterprise (i marchi più noti sono DELL, HP e IBM) in formato rack per l'ottimizzazione dello spazio nel data center. Le funzionalità sono simili a quelle dei computer che utilizziamo tutti i giorni per svago o per lavoro ma con caratteristiche tecniche decisamente più performanti.

Il costo per il giornale sarà rappresentato da un canone mensile (quindi una spesa distribuita nel tempo) che potrà essere variabile, legato all'effettivo utilizzo dei server in hosting.

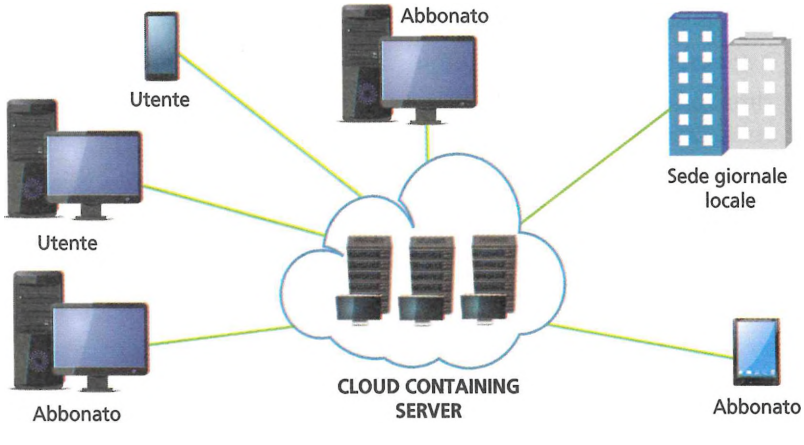
La colocation in housing risulta invece adatta nel caso in cui l'azienda sia proprietaria dei server e non voglia migrare sui server in cloud. In questo caso ne delega solo la gestione, collocandoli (affidandoli) in housing nella server farm specializzata.

Nel caso in cui siano previsti flussi di accessi molto grandi, il direttore potrebbe optare per server dedicati, cioè macchine fisiche all'interno della server farm, esclusivamente dedicate ai servizi offerti online dal giornale.

Viceversa, in caso di flussi medi, potrebbe optare per un server virtualizzato, cioè una macchina fisica che condivide i servizi del giornale con quelli di altre aziende, risparmiando sull'affitto mensile.

Considerando il numero di abbonati di partenza del giornale locale (5.000), un server virtualizzato risulta la soluzione più adatta.

In conclusione, la scelta ottimale che il direttore dovrebbe fare è di abbandonare la soluzione interna e affidare il servizio esternamente in hosting su server virtualizzato (vedi figra a lato). Dovrà quindi rivolgersi a un'azienda di Public cloud computing, cioè un'azienda esperta nella fornitura di servizi informatici (sistema operativo, infrastruttura, server, applicazioni) in forma standard che fornisce i servizi attraverso un provider esterno. Questa gestirà così sia l'efficienza sia la sicurezza.



A CASA

- Effettua una ricerca in Internet sui data center e sui servizi di hosting e colocation in housing; esaminando i diversi servizi trovati concentrati su:
  – vantaggi e svantaggi dei data center interni ed esterni;
  – tipi di hosting proposti.
- Individua quali, tra i casi trovati, risulta affine al contesto illustrato nel tema proposto.
- Leggi l'esempio di svolgimento proposto per verificare se le tue ipotesi si adattano al caso preso in esame e se la trattazione proposta risulta completa nell'ottica dei risultati della tua ricerca.
- Raccogli i tuoi risultati in una presentazione in PowerPoint (massimo 5 slide) evidenziando i casi trovati, la relazione con il contesto proposto, eventuali modifiche o aggiunte da effettuare alla soluzione proposta nell'esempio di svolgimento.

IN CLASSE

- Condividi la presentazione dei tuoi risultati con i compagni.
- Confronta e discuti con i compagni i casi che sono stati presentati.
- Stabilite quale caso rappresenta l'esempio migliore per completezza e realisticità nell'ottica della realizzazione delle misure necessarie richieste nel tema d'esame.
- procedi con l'autovalutazione.

AUTOVALUTAZIONE

ATTIVITÀ	LIVELLO			
	INIZIALE	BASE	INTERMEDIO	AVANZATO
Ho compreso senza difficoltà le richieste dell'attività proposta?	Ho compreso solo alcune delle richieste aiutato dal docente. ☐	Con la guida del docente e la collaborazione dei compagni ho compreso quasi tutte le richieste. ☐	Ho compreso le richieste e in parte le ho svolte autonomamente. ☐	Ho identificato le richieste e le ho svolte senza difficoltà. ☐
Ho reperito le informazioni in rete senza difficoltà?	Ho reperito solo alcune delle informazioni utili aiutato dal docente. ☐	Con la guida del docente e la collaborazione dei compagni ho reperito quasi tutte le informazioni. ☐	Ho reperito le informazioni utili autonomamente e le ho elaborate. ☐	Ho identificato le informazioni utili e le ho elaborate senza difficoltà. ☐
L'analisi dello scenario mi ha permesso di definire modifiche e miglioramenti allo svolgimento proposto?	A partire dalla mia analisi, non sono stato in grado di individuare nessun punto critico nello svolgimento proposto. ☐	A partire dalla mia analisi, sono stato in grado di individuare alcuni punti critici nello svolgimento proposto con l'aiuto del docente. ☐	A partire dalla mia analisi, sono stato in grado di individuare i punti critici e alcune modifiche apportabili nello svolgimento proposto con l'aiuto del docente. ☐	A partire dalla mia analisi, sono stato in grado di individuare i punti critici e definire le modifiche apportabili in modo dettagliato e completo. ☐

UNITÀ

7 ARCHITETTURE WEB: SERVIZI, APPLICAZIONI, AMMINISTRAZIONE

Guarda la **presentazione** dell'unità

IN QUESTA UNITÀ

conoscenze	abilità	competenze
Conoscere l'approccio di Windows Server alle soluzioni server.	Saper installare un Domain Controller.	Saper progettare un'infrastruttura di rete basata su server.
Conoscere i servizi indispensabili da configurare in ogni rete.	Saper configurare utenti, computer, gruppi.	Saper proporre soluzioni per il web aziendale.
Conoscere gli scenari web per le applicazioni e i servizi.	Saper installare un DHCP Server.	Saper amministrare una rete aziendale.
	Saper installare un DNS Server.	
	Comprendere le necessità delle aziende nella progettazione dei servizi.	

DDI+ Didattica Digitale Integrata Plus

FLIPPED CLASSROOM

A casa

- Leggi la Lezione 4 di questa Unità;
- leggi il Case study *Creazione di una rete e gestione degli accessi*;
- in questo scenario definisci la possibile Group Policy dell'azienda (limitazioni accessi, permessi per eseguibili, accesso a database, ecc.);
- illustra la Group Policy elaborata in una presentazione in PowerPoint (massimo 5 slide).

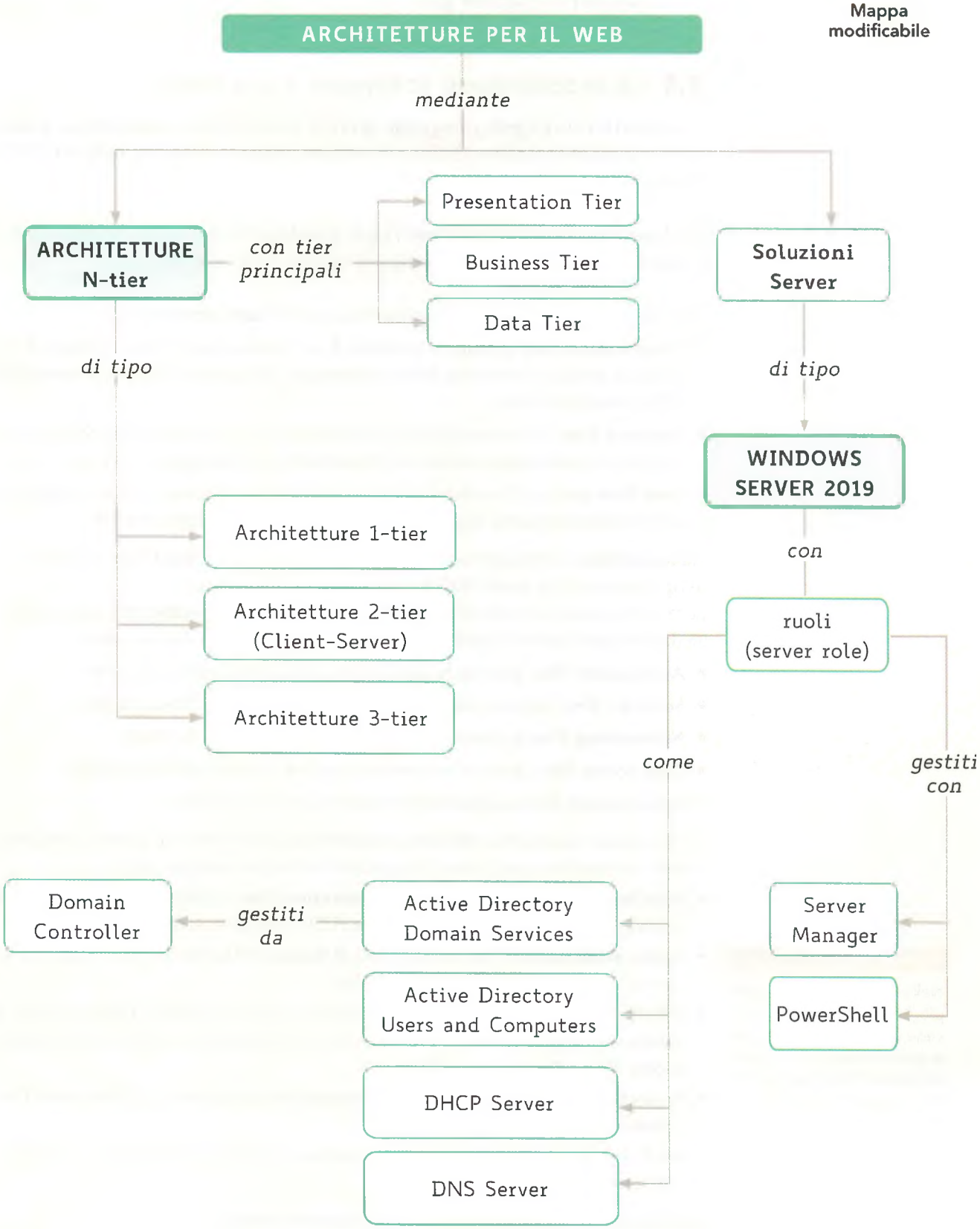
In classe

- Confrontate e discutete l'efficacia delle soluzioni proposte;
- individuate, descrivete e raccogliete in uno schema riassuntivo le soluzioni aggiuntive approntabili per la protezione dell'azienda.

MAPPA CONCETTUALE

DIDATTICA INCLUSIVA

Mappa modificabile



1 LE ARCHITETTURE N-TIER BASATE SU CLIENT-SERVER

1.1 Le architetture software a più livelli

Le architetture per il web, come molti altri tipi di architetture informatiche, si basano su una modellizzazione a livelli: per esempio, abbiamo visto il modello ISO/OSI e l'architettura TCP/IP che ne deriva.

> Nel contesto dei sistemi per il web i livelli prendono il nome di **tier** (**strati**) e le architetture si chiamano **N-tier** in base al numero N di strati progettati.

I tier principali presenti in una architettura web sul **lato server** sono 3.

1. **Presentation Tier**: gestisce la modalità di comunicazione coi client a livello di interfaccia grafica e rendering delle informazioni. Rappresenta quindi il **front-end** dell'applicazione web.
2. **Business Tier**: elabora le richieste dei client e produce i risultati da inoltrare come risposta. In questo strato risiedono le funzionalità che l'applicazione web deve fornire.
3. **Data Tier**: gestisce l'accesso ai dati necessari alle applicazioni web per rispondere alle richieste dei client. Rappresenta il **back-end** dell'applicazione web.

Sul **lato client** è sufficiente un unico tier, il Presentation o **Client Tier**, rappresentato tipicamente da richieste HTTP fatte attraverso il browser.
Le attuali architetture aziendali sono progettate in **N-tier** (**multi-tier**), ossia costituite da altri strati oltre i 3 fondamentali sopra elencati. I più sviluppati sono:

- **Application Tier**: gestisce le applicazioni web in esecuzione sui server;
- **Security Tier**: esegue il monitoraggio e amministra gli accessi alla rete;
- **Networking Tier**: garantisce la connettività e la privacy del client;
- **Data access Tier**: gestisce le autorizzazioni per l'accesso ai dati sensibili;
- **Data storage Tier**: esegue le operazioni richieste sul database.

I tier vengono fisicamente realizzati mediante macchine server in grado di svolgere i compiti richiesti da ogni strato. Le macchine server più utilizzate sono:

- **Web Server**: realizza funzioni di **Presentation Tier** offrendo servizi esterni, cioè riceve, gestisce e risponde alle richieste HTTP provenienti dalla rete;
- **Application Server**: realizza funzioni di **Business Tier** offrendo servizi interni, cioè ricerca informazioni ed elabora dati;
- **DBMS Server** (o Database Server) realizza funzioni di **Data Tier**, gestendo il database; l'architettura può prevedere uno sdoppiamento dello strato in **Data access Tier** e **Data storage Tier**;
- **Proxy Server** realizza funzioni di **Presentation Tier** oltre che di **Security Tier** o **Networking Tier**;
- **AAA Server** (Authentication, Authorization and Accounting Server): realizza funzioni di **Security Tier**.

#prendinota

Nell'e-commerce, per esempio, l'Application Server prevede un Application Tier per la gestione del carrello della spesa e dell'elaborazione dei dati della carta di credito.

Vediamo alcuni scenari che riassumono i concetti espressi.

1.2 Le architetture 1-tier

Nell'architettura 1-tier tutte le componenti, Presentation, Business e Data, fanno parte di un unico tier (FIGURA 1).

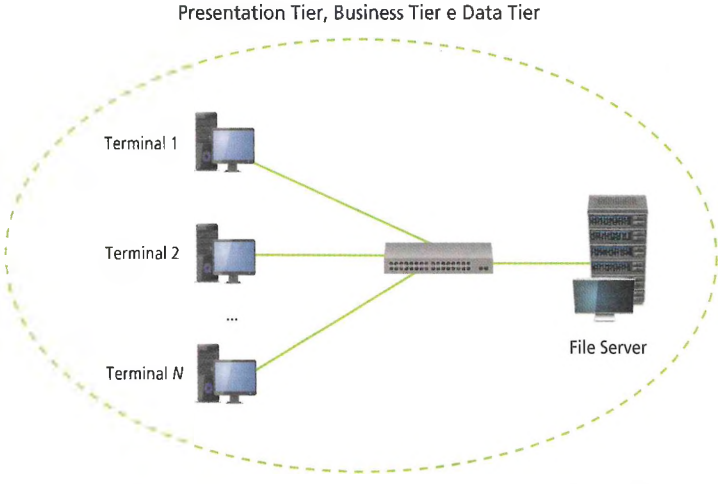


FIGURA 1 Architettura 1-tier

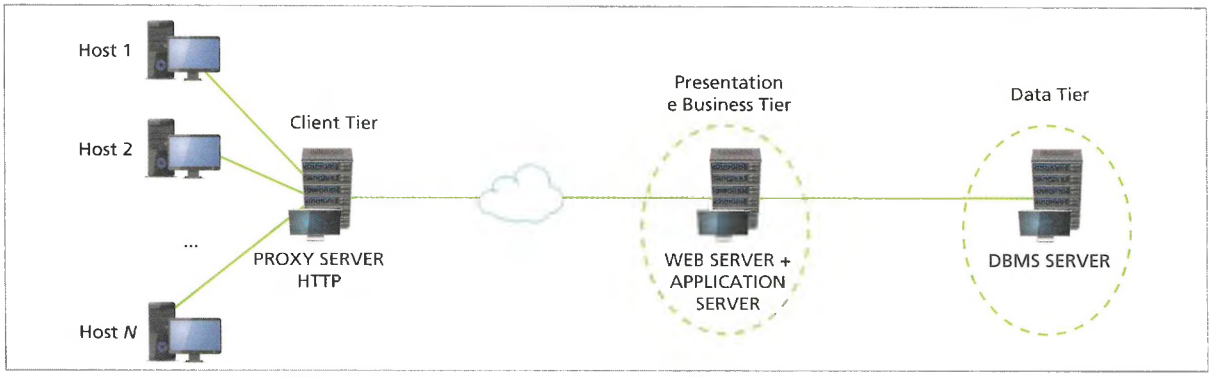
È uno scenario tipico dell'**informatica centralizzata**, dove i client sono terminali di I/O che attraverso sistemi **mainframe** elaborano le applicazioni utente.
Questa architettura fa parte delle tecniche di progettazione utilizzate fino agli anni Novanta del secolo scorso e prevede una stretta relazione tra le 3 componenti principali raggrupate in un unico tier. Questo comporta problemi di:

- **scalabilità**: difficoltà a modificare il quantitativo o il tipo di dati trattati;
- **portabilità**: difficoltà a spostare il sistema in un altro ambiente;
- **aggiornamento**: difficoltà a migrare verso release aggiornate;
- **flessibilità**: difficoltà a modificare una singola componente; le modifiche si ripercuotono sulle altre componenti.

1.3 Le architetture 2-tier

L'architettura 2-tier è il modello **Client-Server** (FIGURA 2) sviluppatosi a partire dagli anni Novanta del secolo scorso diventando il paradigma di Internet.

FIGURA 2 Architettura web 2-tier, lato server



Questo è uno scenario tipico dell'**informatica distribuita**, dove le applicazioni e i dati possono risiedere in remoto ed essere collocate su più macchine, situate anche in luoghi diversi (CED aziendali o data center con server farm).

#prendinota

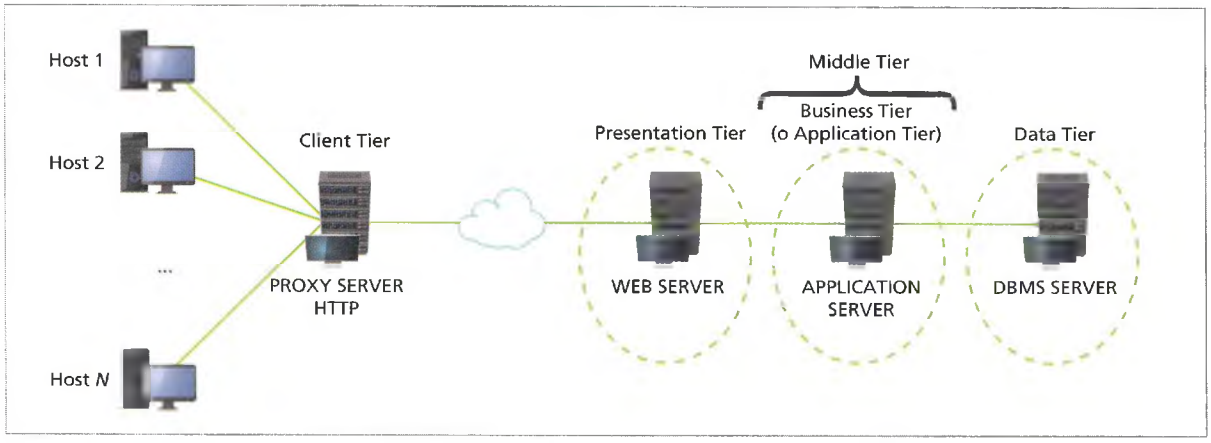
Su una macchina server funzionano sia programmi server sia programmi client, che comportano la creazione di processi server o processi client, tra loro concorrenti.

Questa architettura rende indipendente lo strato Data dagli strati Presentation e Business.
Il client non è più un terminale ma un host in grado di elaborare autonomamente i dati e richiedere servizi in rete, quando ne ha necessità. I server in ascolto elaborano eventuali richieste e forniscono i risultati ai client.
Questa architettura non realizza la completa indipendenza dei tier principali e quindi restano ancora pressoché invariate le problematiche viste per la 1-tier.

1.4 Le architetture 3-tier

Progettando un tier intermedio (**Middle Tier**) sempre sul modello Client-Server, si ottiene un'architettura 3-tier (FIGURA 3) che rende indipendenti i 3 strati.

FIGURA 3 Architettura web 3-tier, lato server

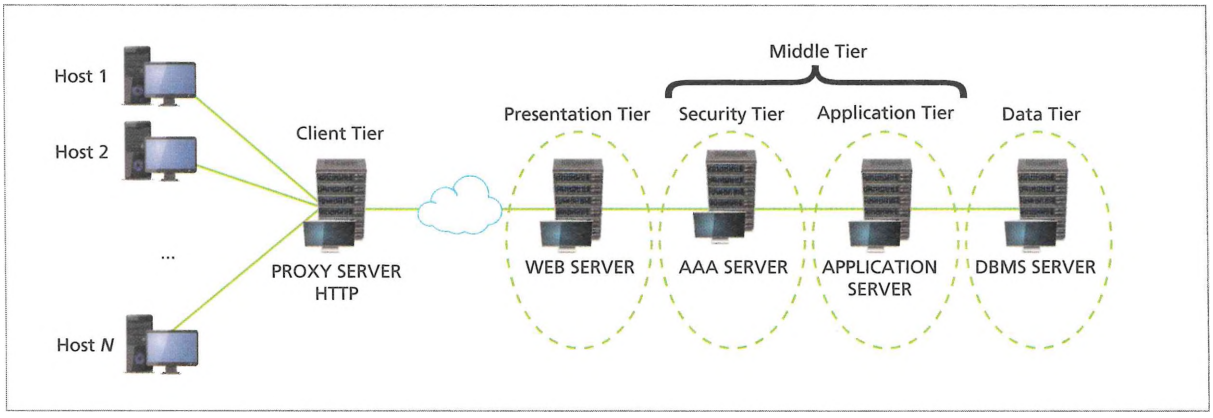


Il tier intermedio, per esempio il Business Tier, agirà da server nei confronti del Presentation Tier e da client nei confronti del Data Tier.
In questa architettura, tipica degli anni Duemila, ogni strato è realizzato su macchine server differenti superando così le problematiche presenti nei due scenari precedenti.

1.5 Le architetture N-tier

Sono le architetture più attuali e prevedono diversi strati intermedi, uno per ogni funzione sviluppata. Vengono anche chiamate **Multi-Tier Architecture**.
La FIGURA 4 presenta un'architettura 4-tier pensata appositamente per migliorare lo sviluppo delle applicazioni per il web in un contesto di sicurezza.

FIGURA 4 Architettura web N-tier, lato server



Anche in questo scenario, ogni tier intermedio agisce sia da client sia da server a seconda della direzione della comunicazione.

LE ARCHITETTURE N-TIER DI MICROSOFT

Microsoft ha scelto di inserire le proprie applicazioni Middle Tier e i servizi di infrastruttura (Active Directory Domain Services, DHCP Server, DNS Server, Remote-access, ecc.) nel sistema operativo Windows Server (che sarà descritto nella Lezione successiva), mentre il ruolo di Application Server è delegato alle tecnologie del .NET Framework.
L'architettura web che Microsoft propone è **Azure**, presente in varie configurazioni N-tier.

1.6 La scalabilità orizzontale e verticale delle applicazioni

La **scalabilità di un'applicazione** è la capacità di aumentarne il throughput in proporzione all'hardware che deve essere impiegato per ospitare l'applicazione. Si distingue in scalabilità orizzontale e scalabilità verticale.

La **scalabilità orizzontale** (**scale-out**) si ottiene aumentando il numero di nodi che ospitano l'applicazione, nodi che sono del tutto simili in termini di CPU e memoria. In questo modo è possibile gestire in parallelo il carico di lavoro.
Un tipico esempio di architettura informatizzata scale-out è il sito web statico: raddoppiando il numero di server che lo ospitano, otteniamo il raddoppio dei potenziali utenti serviti.
Il principale vantaggio è la maggior fault-tolerance: l'errore in un nodo non pregiudica totalmente il funzionamento del servizio.
Gli svantaggi risiedono nei maggiori sforzi in fase di progettazione perché il servizio deve innanzitutto supportare questo modello di scalabilità.

La **scalabilità verticale** (**scale-up**) si ottiene aumentando le risorse di un singolo nodo, per esempio utilizzando una CPU con frequenza maggiore o incrementando i buffer di memoria, al fine di aumentare le prestazioni dell'intero sistema.
Lo scale-up presenta costi maggiori rispetto allo scale-out perché acquistare macchine server più performanti è più costoso che acquistare macchine server equivalenti a quelle che già si hanno. Naturalmente i servizi possono essere proposti in ambito CED locale o in cloud appoggiati ai data center.
La scalabilità verticale è, per esempio, richiesta nel tier del database.

FISSA LE CONOSCENZE

- Quali sono i principali tier presenti in un'architettura web?
- Quali sono le macchine server più utilizzate?
- Che cosa introduce di nuovo l'architettura 2-tier rispetto alla 1-tier?
- Che cosa introduce di nuovo l'architettura 3-tier rispetto alla 2-tier?

2 LE SOLUZIONI DI WINDOWS SERVER 2019

2.1 Le soluzioni server

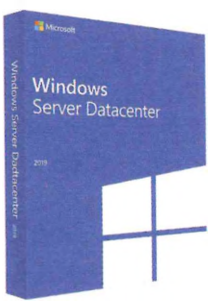
Una buona progettazione dell'infrastruttura di rete necessita dell'analisi dei seguenti punti:

- la **situazione attuale**: esiste già una rete o va costruita da zero? Quali sono i processi operativi da mettere in atto?
- le **esigenze primarie** dell'azienda: avere obiettivi chiari e ben definiti è necessario nel caso dell'organizzazione di una nuova rete o di una ristrutturazione architetturale. Occorre definire i servizi indispensabili dell'infrastruttura, che devono essere forniti da terzi o che devono essere offerti;
- le **esigenze collaterali** dell'azienda: sono legate all'attività svolta, ma spesso tralasciate per fornire soluzioni più economiche, che non sempre si adattano alle esigenze specifiche;
- gli **sviluppi** a breve e medio termine: l'infrastruttura deve essere flessibile, si può usare, per esempio, il Domain Controller, descritto nella Lezione 3, che consente di basare la rete su un dominio, usufruendo in questo modo di diverse funzionalità.

Benché la tendenza sia quella di migrare sempre più verso soluzioni cloud, sono ancora molti i servizi e le applicazioni realizzate per soluzioni server interne all'azienda.
Inoltre, in termini di efficienza, efficacia e sicurezza, è spesso consigliabile mantenere alcune risorse all'interno dell'infrastruttura di rete aziendale; per esempio, i servizi di accesso alla rete in termini di **autorizzazione** e **autenticazione**, ma anche il **DNS Server** e il **DHCP Server**, perché sono strettamente legati alla struttura con cui è stata realizzata la rete aziendale.
Anche la classica condivisione di una stampante o di un hard disk di rete, per esempio, deve essere progettata internamente all'azienda.

Bisogna dunque conoscere la lista dei **server role,** cioè del ruolo (quindi del compito) che ogni server deve svolgere.

2.2 Windows Server 2019



Windows Server 2019 è un sistema operativo, predisposto per il cloud, che supporta i carichi e le modalità di lavoro attuali, in particolare la virtualizzazione, e contemporaneamente introduce nuove tecnologie che facilitano la transizione verso il cloud computing in qualsiasi momento.
Windows Server 2019 si basa sulla precedente versione 2016, che è stata la prima versione predisposta per il cloud computing, tecnologia che nella versione 2019 è stata ulteriormente ampliata.
Per gli amministratori è stata migliorata l'applicazione **Windows Admin Center** che consente, tramite un browser, il controllo da remoto dei server.

Le novità più interessanti introdotte in Windows Server 2019 riguardano:

- **cloud ibrido**: esiste una connessione sempre più stretta tra l'ambiente Windows Server locale e il cloud Azure, sono state infatti aggiunte funzionalità di backup, recovery e aggiornamento;
- **sicurezza**: il sistema accede ai servizi del cloud per la protezione da malware e blocca processi classificati come pericolosi (applicazioni Windows Defender e Advanced Threat Protection); inoltre è possibile eseguire le attività sensibili su una macchina virtuale sicura (strumento **Shielded VM**, macchina virtuale schermata) e crittografare i dati trasferiti tra macchine virtuali;
- **storage**: è semplificato il passaggio alla nuova versione del sistema operativo, ma anche al cloud, grazie alla funzionalità Storage Migration Service;
- **container**: gli sviluppatori di applicazioni si affidano sempre più ai #container per rendere le applicazioni efficienti, veloci e portabili, infatti permettono di creare applicazioni in grado di scalare in orizzontale e in verticale nei datacenter e nel cloud; nella versione 2019 è migliorata la versione Windows Subsystem for Linux (WSL) che permette agli sviluppatori di eseguire un ambiente Linux direttamente in Windows, senza la necessità di ricorrere a una macchina virtuale;
- **System Insight**: è un nuovo strumento di analisi del sistema che si basa su un modello di apprendimento automatico (machine learning) e permette di fornire previsioni su possibili condizioni problematiche che potrebbero verificarsi legate alla capacità della CPU, all'utilizzo del networking e al consumo di storage. Inoltre, è possibile configurare degli script per intraprendere in automatico determinate azioni correttive.

#techwords

I **container** comprimono insieme il codice software, il runtime e le dipendenze in una virtualizzazione a livello di sistema operativo per fornire ambienti veloci e completamente isolati in un singolo sistema.
Come la virtual machine virtualizza l'hardware, così il container virtualizza il sistema operativo.

Windows Server 2019 è disponibile in 3 edizioni:

- **Datacenter**: è indicata per data center con un'elevata percentuale di sistemi virtualizzati e per ambienti cloud;
- **Standard**: è tipicamente utilizzata su server fisici e in ambienti enterprise con un numero limitato di sistemi virtualizzati;
- **Essentials**: utile per piccole imprese con un massimo di 25 utenti e 50 dispositivi (è un server ideale per il cloud).

#prendinota

Per un confronto tra le due edizioni Datacenter e Standard, e per tutto quanto concerne Windows Server, si può far riferimento alla documentazione presente sul sito web Microsoft:
https://docs.microsoft.com/it-it/windows-server

Le edizioni Datacenter e Standard offrono 3 opzioni di installazione:

1. **Server Core**: è la modalità di installazione proposta di default ed è caratterizzata dall'assenza dell'interfaccia grafica (Desktop Experience). Tale modalità, oltre a rendere il sistema più veloce ed efficiente, lo rende anche più sicuro dato che non carica codice extra (che potrebbe contenere vulnerabilità) e non consuma risorse nel visualizzare la GUI. L'amministrazione del sistema può avvenire sia tramite riga di comando con PowerShell sia da remoto tramite Windows Admin Center.
2. **Server con Desktop Experience**: in tale modalità viene installata l'usuale interfaccia grafica di Windows. Rispetto alla modalità Server Core questo tipo di installazione prevede alcuni svantaggi come la richiesta di maggiore spazio su disco, minore efficienza del sistema, tempi di realizzazione superiori ed è più soggetta a vulnerabilità.
3. **Nano Server**: è simile a Server Core, ma molto più piccolo, non ha alcuna funzionalità di accesso locale e supporta solo applicazioni a 64 bit. Richiede molto meno spazio su disco, si configura velocemente e richiede molti meno aggiornamenti e riavvii rispetto alle altre opzioni. Queste sue caratteristiche lo rendono perfetto per

essere installato come sistema operativo all'interno di un container, salvo, però, che l'applicazione che sarà eseguita nel container non necessiti di più funzionalità, in tal caso sarà necessario optare per l'installazione di Server Core.

2.3 PowerShell

PowerShell è una shell sviluppata da Microsoft, resa open source dalla versione 6.0 del 2016. Oltre che per Windows, è disponibile anche per Linux e MacOS. PowerShell offre una shell a linea di comando (CLI) e un linguaggio di script completo, espressamente progettato per l'amministrazione del sistema operativo Windows. Basato su .NET Framework, PowerShell consente a professionisti IT e a utenti esperti di controllare e automatizzare l'amministrazione di Windows e delle applicazioni in esso eseguite. Le principali caratteristiche di PowerShell sono:

#techwords

I comandi di PowerShell sono chiamati **cmdlets** (*command lets*, serie di comandi). Essi permettono di gestire i computer da riga di comando. Le cmdlets sono delle classi .NET, scritte in linguaggio C#.

- comandi specializzati, denominati **#cmdlets**, per l'esecuzione di comuni attività di amministrazione di sistema, per esempio, per la gestione del Registro di sistema, dei servizi e dei registri eventi, nonché per l'utilizzo di WMI (Windows Management Instrumentation), il framework Microsoft per la gestione e configurazione da remoto di server e workstation Windows;
- linguaggio di scripting simile a C#;
- progettazione coerente: poiché i cmdlets e gli archivi dati del sistema utilizzano una sintassi e convenzioni di denominazione comuni, i dati possono essere condivisi facilmente e l'output di un cmdlet può essere utilizzato come input per un altro cmdlet senza necessità di riformattazione o manipolazione;
- esplorazione del sistema operativo semplificata e basata su comandi, così da consentire agli utenti di esplorare il Registro di sistema e gli altri archivi dati con le stesse tecniche utilizzate per l'esplorazione del file system;
- possibilità di manipolazione degli oggetti: in modo diretto o inviandoli ad altri strumenti o database;
- interfaccia estensibile: i produttori di software e gli sviluppatori aziendali possono creare tool e utility personalizzate per amministrare il software.

esercizio

➜ PROBLEMA

Verificare la versione di PowerShell installata su un computer.

➜ SVOLGIMENTO

È possibile verificare la versione di PowerShell installata su un computer mediante tasto destro sul menu **Start** e poi **Windows PowerShell**.
In alternativa, dal Prompt dei comandi, nella console di Windows PowerShell, basterà digitare la cmdlet:

```
Get-Host | Select-Object Version
```

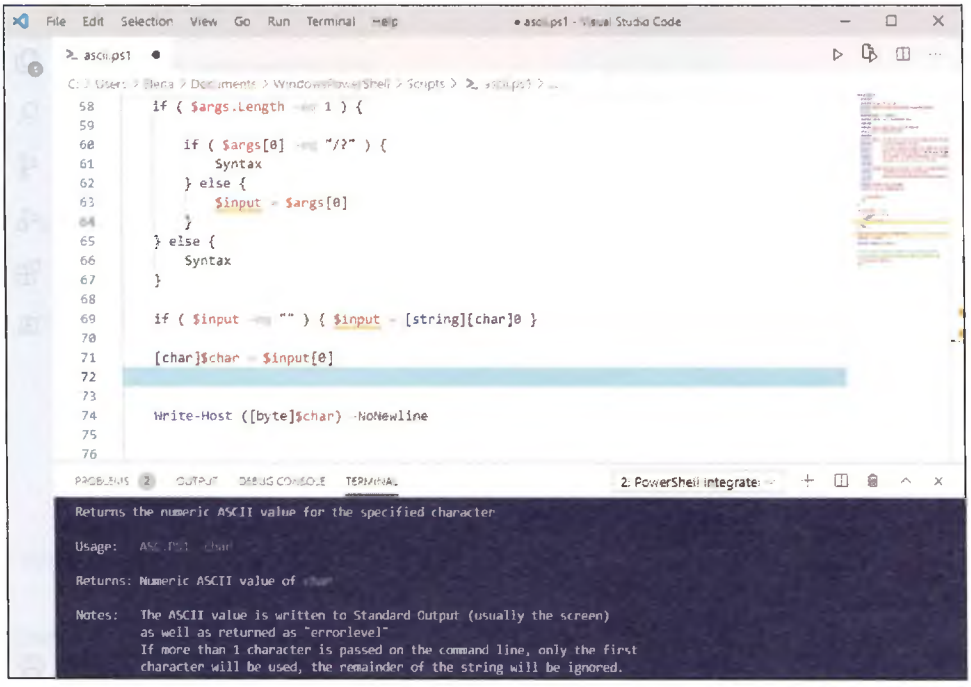
per ottenere la versione di PowerShell installata.
Eseguendo la cmdlet:

```
Show-command
```

comparirà una finestra in cui è mostrata la sintassi di ogni comando che è possibile eseguire.

Per gli sviluppatori è in genere comunque consigliabile utilizzare **Visual Studio Code** con l'estensione PowerShell (da non confondere con Visual Studio). Si tratta di un ambiente per scrivere (FIGURA 5), eseguire e testare script PowerShell con l'aiuto di strumenti tipici della programmazione.

FIGURA 5 Visual Studio Code



2.4 Windows Admin Center

Con Windows Server 2019, Microsoft ha fornito una nuova applicazione agli amministratori: **WAC (Windows Admin Center)**. Questo software non è incluso in Windows Server, ma si scarica a parte, gratuitamente, dal sito web Microsoft.

Le nuove funzionalità presenti in Windows Server 2019 sono gestibili solo attraverso WAC: Storage Migration Services, System Insights, Software-Defined Networking e altre ancora.
Da Windows Admin Center è possibile utilizzare le console web di PowerShell e Remote Desktop.
Gli strumenti di amministrazione da remoto del server, **RSAT (Remote Server Administration Tools)**, non sono, però, stati sostituiti da Windows Admin Center. Infatti i ruoli del server come Active Directory, DHCP, DNS, che vedremo nelle prossime Lezioni, non hanno ancora funzionalità di gestione equivalenti in WAC. Windows Admin Center si occupa della gestione di singoli server, non di sistemi su larga scala, per questi si continuano a utilizzare gli strumenti di **System Center**, l'applicazione Microsoft di gestione e monitoraggio per i data center.
La FIGURA 6 mostra la presentazione di Microsoft degli strumenti disponibili per la gestione di un server, evidenziando nel triangolo i 3 ambienti in cui si può installare un server: piccole-medie aziende, grandi aziende e provider e l'ambiente cloud/hybrid.
Per ognuno di questi 3 ambienti si evidenzia lo strumento di gestione da utilizzare per le operazioni di configurazione, manutenzione e troubleshooting.

#prendinota

Windows Admin Center è ottimizzato per Windows Server 2019, ma gestisce bene anche le versioni precedenti 2016 e 2012. In modo molto limitato può gestire Windows Server 2008 R2.

IN ENGLISH PLEASE

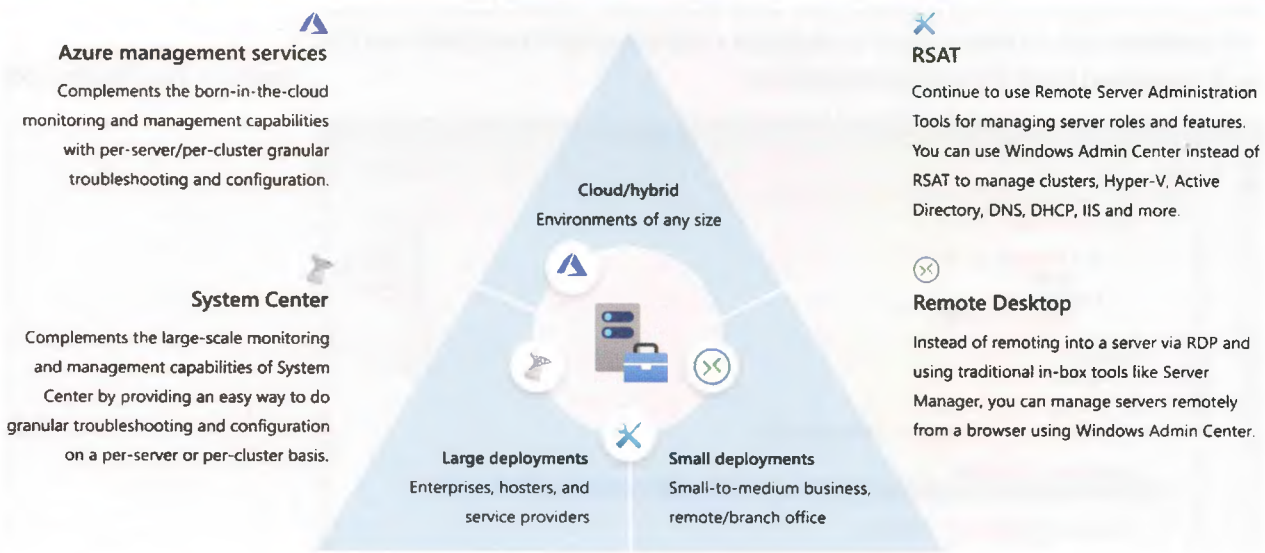


FIGURA 6 Gli strumenti per la gestione di Windows Server

#techwords

Gli **snap-in** sono componenti software che estendono o aggiungono funzionalità a un'applicazione. I servizi tipici offerti dagli snap-in sono quelli relativi all'amministrazione di rete. I programmi di gestione (da shell o da console) permettono di scegliere i moduli amministrativi (detti appunto snap-in) da aggiungere.

Remote Server Administration Tools per Windows 10 include (oltre ad altri strumenti da usare da linea di comando):

- **Server Manager:** è la console di gestione dei sistemi operativi server di Microsoft a partire da Windows Server 2008;
- **Microsoft Management Console (MMC) #snap-in**, quali Device Manager, Internet Information Services, Disk Management, Event Viewer, Local Users e Groups e altre applicazioni di gestione;
- **Windows PowerShell cmdlets.**

SERVER MANAGER

Server Manager è stato riprogettato in Windows Server 2012 per supportare la **gestione remota multi-server** e **aumentare il numero di server** che un amministratore può gestire.

Dal Server Manager possiamo quindi eseguire operazioni quali:

- configurazione del server locale;
- aggiunta di ruoli e funzionalità;
- gestione remota dei server;
- gestione di più server a gruppi.

Nelle prossime Lezioni vedremo come utilizzare questi strumenti per configurare i principali 4 servizi (server role):

- Active Directory Domain Services per i servizi di dominio e il Domain Controller;
- Active Directory Users and Computers per la creazione di utenti e gruppi;
- il DHCP Server;
- il DNS Server.

Informazioni più dettagliate sui servizi si trovano nella documentazione ufficiale su *docs.microsoft.com*.

esercizio

→ PROBLEMA

Installare la console di gestione Server Manager su un PC Windows 10.

→ SVOLGIMENTO

Sui sistemi client Windows 10 Professional o Enterprise si possono installare gli strumenti per la gestione da remoto dei ruoli e delle funzionalità di Windows Server.
La funzionalità Strumenti di amministrazione remota del server (RSAT) è già inclusa tra le **funzionalità su richiesta** in Windows 10. Per utilizzare Server Manager è però necessario attivarlo:

Impostazioni → App → Funzionalità facoltative → Aggiungi una funzionalità

La FIGURA 7 mostra la finestra che viene visualizzata: se nella casella di ricerca si scrive Strumenti di amministrazione, comparirà l'elenco degli strumenti RSAT. Il primo della lista è **Server Manager**: selezioniamo la relativa casella e clicchiamo sul pulsante **Installa**. Terminata l'installazione, l'amministratore potrà utilizzare questo strumento per la gestione remota di Windows Server.

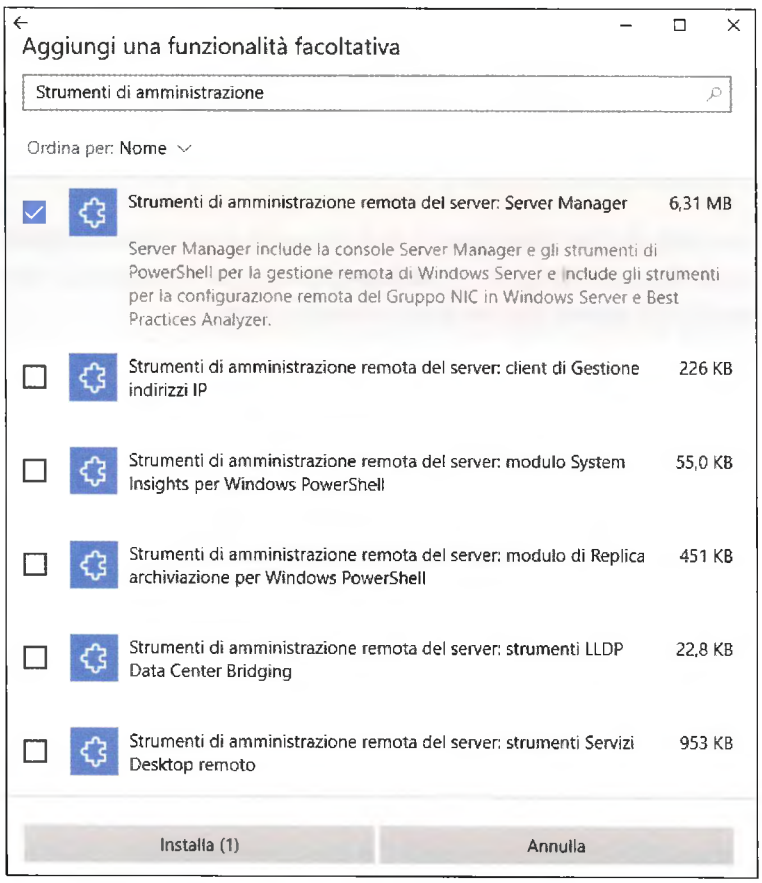


FIGURA 7 Installazione di Server Manager su un PC Windows 10

FISSA LE CONOSCENZE

- Windows Server 2019 è disponibile in 3 edizioni. Quali?
- Che cosa sono le cmdlets?
- Quali strumenti sono disponibili per la gestione dei server Windows?

3 IL DOMAIN CONTROLLER

3.1 I servizi di dominio

Tra tutti i server role, i **servizi di dominio** (Domain Services) rivestono un ruolo molto importante. Essi consentono di memorizzare e gestire informazioni relative a utenti e dispositivi della rete.

Un **controller di dominio** (Domain Controller) permette di definire la gestione dell'informazione all'interno della rete in sicurezza, come il processo di autenticazione degli utenti, la gestione delle condivisioni o le Group Policy.
Il Domain Controller è il vero cuore della rete e i suoi servizi sono necessari al funzionamento di innumerevoli applicazioni.
La prima cosa da considerare è quindi l'installazione di un Domain Controller e in particolar modo di un servizio che prende il nome di **Active Directory Domain Services**.

3.2 Active Directory Domain Services

> Active Directory Domain Services è un **raggruppamento logico** di utenti e computer in un dominio gestito centralmente dai server **Domain Controller**.

Una struttura **AD** (**Active Directory**) è un framework gerarchico di **oggetti**. Gli oggetti cadono in 3 ampie categorie: le **risorse** (per esempio stampanti), i **servizi** (per esempio email) e gli **utenti** (per esempio account e gruppi).
AD fornisce informazioni sugli oggetti, li organizza, controlla l'accesso e ne imposta la sicurezza. Ciascun oggetto rappresenta una **singola entità** – come un utente, un computer, una stampante oppure un gruppo – e i suoi attributi. Alcuni oggetti possono anche essere contenitori di altri oggetti.

> Un **oggetto** è identificato univocamente dal suo nome e ha un insieme di **attributi** che l'oggetto può contenere - le **caratteristiche** e l'**informazione** - definiti da uno schema, il quale determina anche il tipo di oggetti che possono essere immagazzinati in Active Directory.

Per poter ottimizzare la gestione degli oggetti, è necessario organizzarli in modo coerente su due livelli fondamentali: **logico** e **fisico**.

A livello logico troviamo le seguenti categorie di oggetti.

- **Organizational Unit**: una serie di oggetti del dominio raggruppati tra loro per affinità di interesse (per esempio, stampanti, reparti, ecc.). Utilizzando queste strutture è possibile formare una gerarchia all'interno del dominio, facilitandone l'amministrazione, per esempio applicando politiche di gestione dei gruppi (Group Policy Objects, GPOs).
- **Dominio**: gruppo di oggetti che condividono un database (detto directory database). I #domini sono identificati in base alla struttura del loro namespace (nome DNS).
- **Albero di dominio**: si tratta di uno o più domini che condividono un namespace contiguo.

#techwords

Un **dominio** Windows Server è un gruppo logico di computer che eseguono versioni del sistema operativo Microsoft Windows e che condividono un directory database contenente gli account utente e le informazioni di protezione per le risorse presenti nel dominio. Ogni persona che utilizza i computer all'interno di un dominio riceve un account univoco o un nome utente. A tale account può essere assegnato il grado di accesso alle risorse disponibili.

- **Foresta di dominio**: insieme di uno o più alberi presenti nel directory database. Questi alberi condividono tra loro un catalogo globale, uno schema di directory, una struttura logica e una configurazione. La foresta rappresenta perciò l'area in cui utenti, computer, gruppi e altri oggetti sono accessibili.

A livello fisico troviamo le seguenti categorie di oggetti.

- **Sito**: un oggetto #sito in Active Directory rappresenta una locazione geografica fisica che ospita reti. I siti possono essere usati per assegnare Group Policy Objects, semplificare l'individuazione delle risorse, gestire la replicazione della active directory e gestire il traffico di collegamento alla rete. I siti possono essere collegati ad altri siti. Agli oggetti di un sito collegato possono essere assegnati costi che rappresentano velocità, affidabilità, disponibilità o altre proprietà reali di una risorsa fisica. I siti contengono oggetti detti Subnet.
- **Subnet**: uno specifico indirizzamento IP con una specifica subnet mask.

Una componente importante di Active Directory è il **Global Catalog**: un database nel quale sono presenti tutti gli oggetti dei diversi domini presenti all'interno della nostra foresta, elencati attraverso una rappresentazione sintetica (non vengono catalogati tutti gli attributi di ogni singolo oggetto), offrendo una visione globale di **ogni oggetto** presente in **ogni dominio** di **ogni foresta**. Il Global Catalog riveste molta importanza in una rete aziendale in cui siano presenti due domini all'interno della stessa foresta.

#techwords

Siti

Una o più subnet che coesistono tra loro.
Nel caso di reti aziendali con sedi sparse in diverse città, le specifiche Sito e Subnet diventano fondamentali per la comunicazione in rete.

3.3 Prima installazione di un Domain Controller

esercizio

→ PROBLEMA

Installare un Domain Controller su un server Windows, configurando il servizio Active Directory Domain Services. Svolgere l'attività utilizzando l'applicazione Server Manager.

→ SVOLGIMENTO

Avviamo l'esecuzione di Server Manager e iniziamo la configurazione del nostro server impostando anzitutto un nome server, per esempio **dc1**, per *domain controller 1*. A questo punto, dal menu **Manager** selezioniamo **Add Roles and Features Wizard** e scegliamo il tipo di installazione (**Installation Type**) voluta, come mostrato nella FIGURA 8.

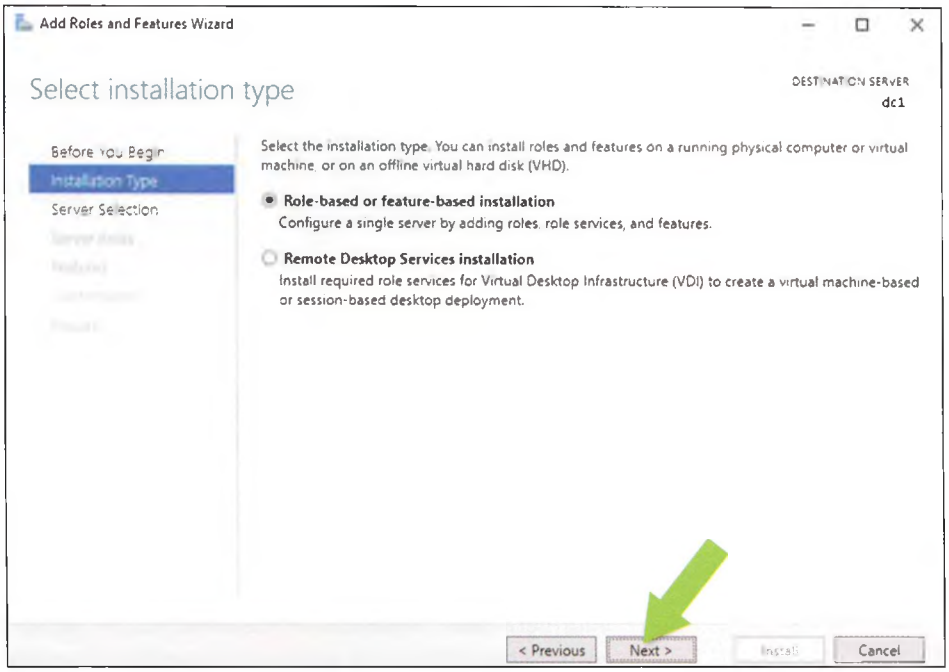
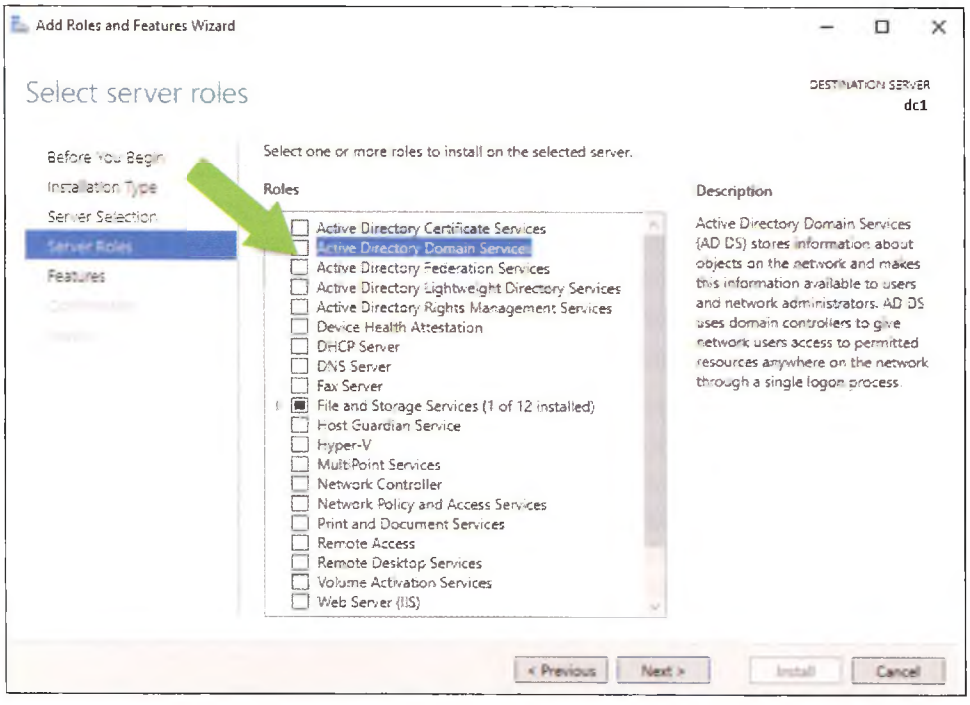


FIGURA 8 Installazione basata su ruoli o basata su funzionalità

Nella stessa finestra selezioniamo i ruoli server (**Server Roles**) e spuntiamo la voce relativa al servizio che intendiamo installare. Nel nostro caso **Active Directory Domain Services** (FIGURA 9).

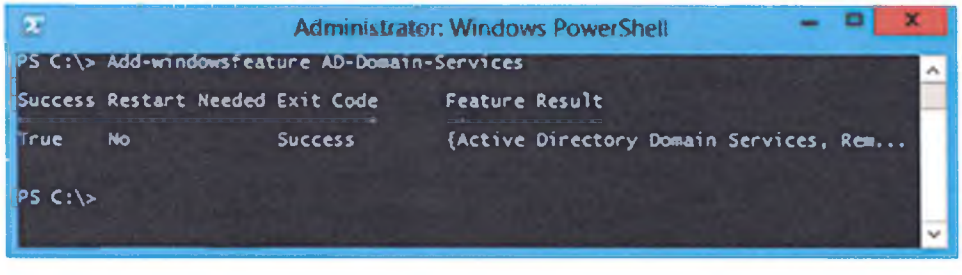
FIGURA 9 Scelta dei servizi da assegnare al server



Alcuni dei servizi elencati in Figura 9 (DHCP Server e DNS Server) saranno affrontati nelle prossime Lezioni.

L'installazione di Active Directory Domain Services, come per tutti gli altri ruoli e funzionalità del server, può essere fatta non solo utilizzando Server Manager ma anche Windows PowerShell (FIGURA 10).

FIGURA 10 Server Manager per Windows PowerShell



L'utilizzo del wizard grafico in Server Manager o del modulo Server Manager per Windows PowerShell consente installazioni locali e remote. Con l'esecuzione di più istanze di wizard o cmdlet e il targeting su diversi server, è possibile distribuire domini Active Directory per più controller di dominio contemporaneamente, il tutto da una singola console.

Selezioniamo dunque il nostro server dalla lista di server disponibili e procediamo con la scelta dei ruoli.
In automatico, al momento della scelta Active Directory Domain Services, il wizard ci informerà della necessità di installare alcune funzionalità aggiuntive necessarie alla corretta esecuzione del ruolo e ci consentirà di scegliere eventuali altre funzionalità.

Ora può partire il processo di installazione. Nella finestra **Installation progress**, che si apre automaticamente all'avvio del processo, è possibile vedere riassunte in **Results** tutte le funzionalità aggiuntive installate (FIGURA 11).

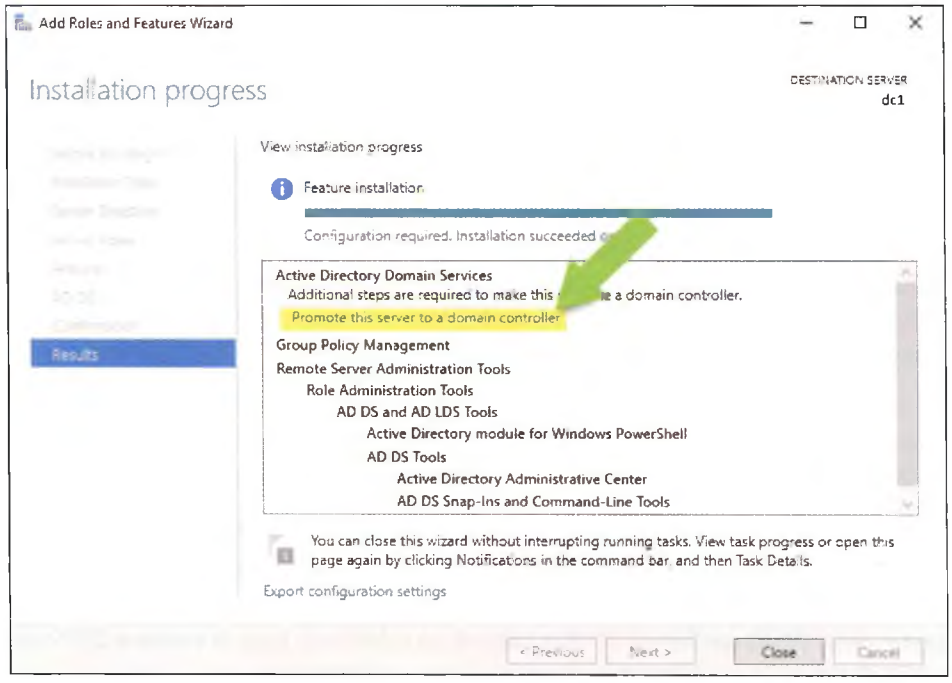


FIGURA 11 Installazione dell'Active Directory Domain Services completata

A questo punto, non resta che promuovere il nostro server a controller di dominio. Nella stessa schermata di installazione facciamo clic su **Promote this server to a domain controller** (freccia in Figura 11). La **promozione** di un server a Domain Controller inizia aprendo la finestra di **Deployment Configuration** (FIGURA 12). In questa occorre scegliere dove andare a installare il nuovo Domain Controller.

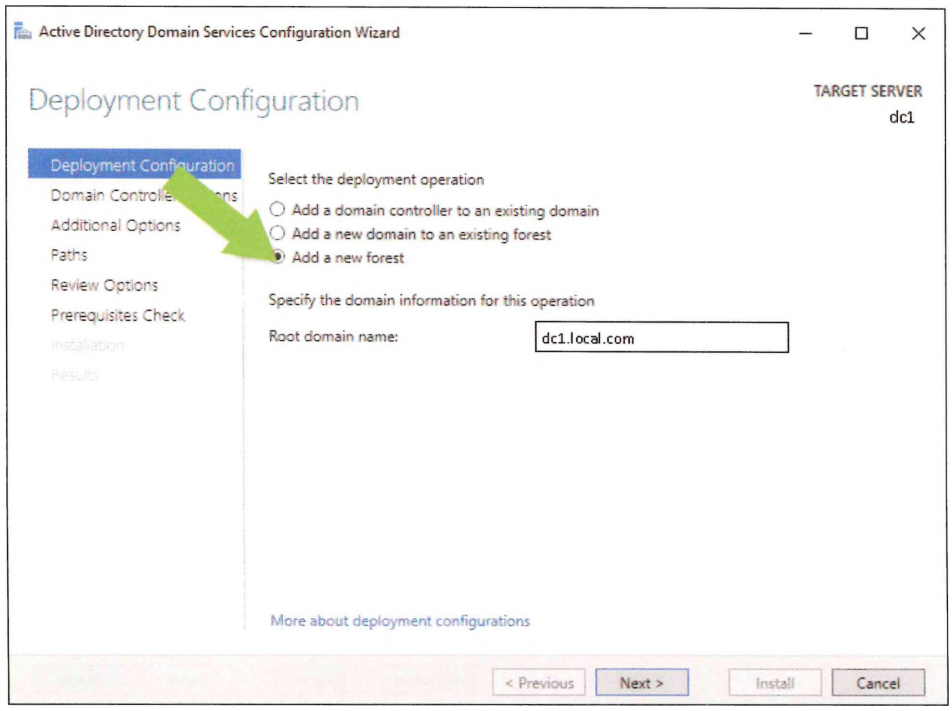


FIGURA 12 Creazione di una foresta

Ci sono 3 possibilità:
1) aggiungere un Domain Controller a un dominio esistente;
2) aggiungere un nuovo dominio a una foresta esistente;
3) creare una nuova foresta.

Selezioniamo **Add a new forest**. A questo punto è necessario:

- fornire un nome di **Root domain** valido: non può essere single-labeled, per esempio, va bene *local.com* o *dc1.local.com* ma non *local* o *dc1*;
- **non** creare nuove foreste di Active Directory con lo stesso nome di un DNS esterno, per evitare problemi di compatibilità future. Per esempio, se l'URL DNS Internet è *http://dc1.com*, bisogna scegliere un nome diverso per la foresta interna;
- scegliere un nome unico e improbabile per il traffico web: per esempio, *dc1.local.com* (Figura 12), dove la presenza del suffisso *.local* consente di distinguerlo dal dominio Internet.

Una nuova foresta non ha bisogno di nuove credenziali per l'account di amministratore del dominio. Il processo di promozione del controller di dominio utilizza le credenziali dell'account **Administrator** salvate in fase di creazione della radice della foresta.

#prendinota

Non c'è modo (per impostazione predefinita) di disattivare o bloccare l'account Administrator salvato e inoltre questo è l'unico punto di ingresso in una foresta se gli altri account di dominio amministrativo sono inutilizzabili. È fondamentale quindi conoscere la password prima di distribuire una nuova foresta.

Nella finestra **Domain Controller Options** (FIGURA 13), alla richiesta sul livello di configurazione della foresta (cioè il livello di compatibilità delle funzionalità con le versioni precedenti di Windows Server presenti sulla rete), basterà scegliere il livello preconfigurato, ossia Windows Server 2016 in caso di un solo livello (con la versione 2019 non è stato definito un nuovo livello, quindi la scelta resta 2016). In caso contrario occorre conoscere il livello di configurazione degli altri server presenti sulla rete e adeguarsi. Nella stessa finestra occorre introdurre una password per **Directory Services Restore Mode** (DSRM) necessaria quando si richiede l'accesso al server in modalità DSRM, comunemente nota come **modalità di ripristino**.

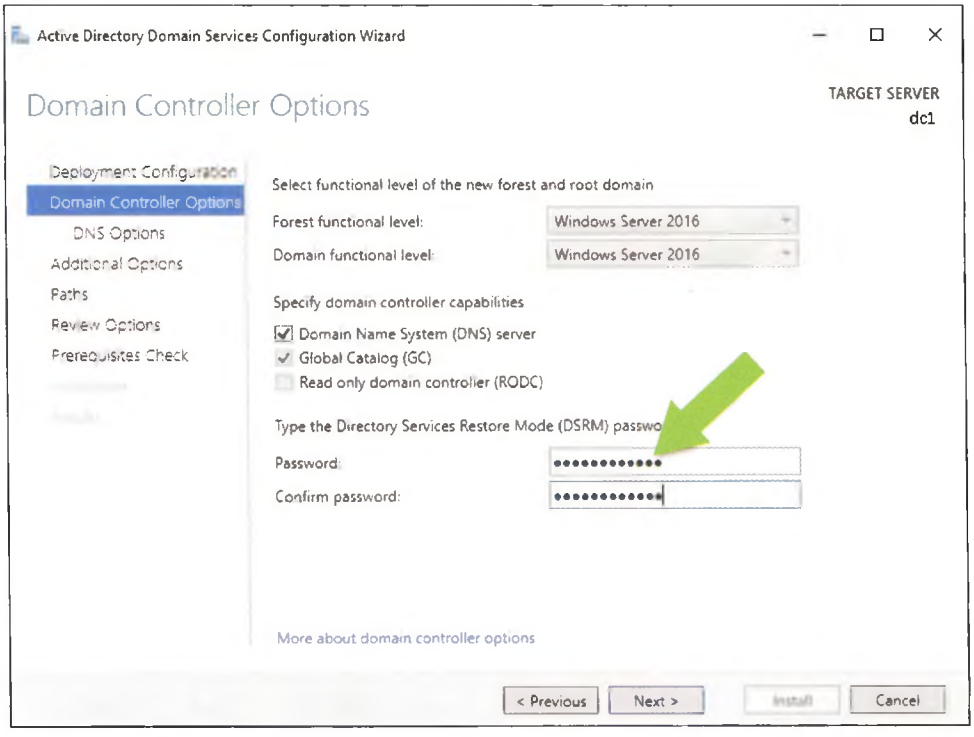


FIGURA 13 Livello di configurazione della foresta e scelta della password DSRM

Nella schermata successiva, **DNS Options**, è probabile che compaia un avviso che informa che non è possibile configurare queste opzioni essendo stato selezionato il DNS Server nella pagina Domain Controller Options (Figura 13). Possiamo però comunque procedere oltre perché nei passaggi successivi lo stesso wizard si occuperà di installare ciò che manca al dominio.
Scegliamo **Next**, indichiamo un nome di dominio **NetBios** (nel nostro caso **DC1**) e verifichiamo la configurazione scelta nella **Review Options** (FIGURA 14).

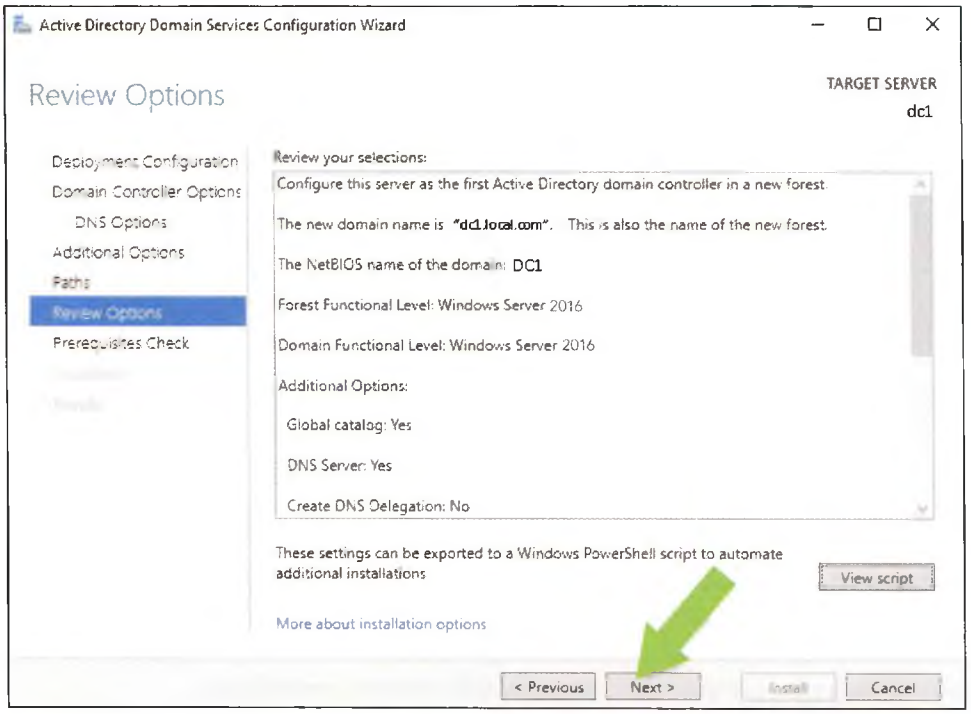


FIGURA 14 DNS Options

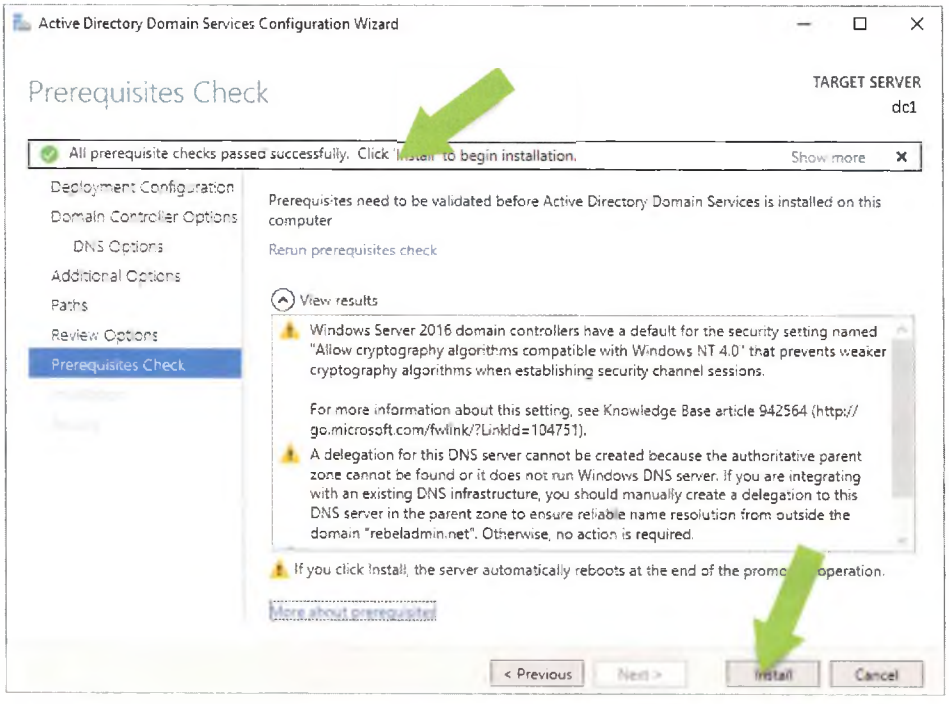
Tutti i wizard di Windows Server permettono di esportare le operazioni scelte in uno script PowerShell. Ciò è molto utile soprattutto per coloro che ancora non hanno dimestichezza con tale ambiente. Nel nostro caso, la promozione del nostro server a controller di dominio si trasformerebbe come qui a fianco indicato.

```
#
# Windows PowerShell Script for AD DS Deployment
#
Import-Module ADDSDeployment
Install-ADDSForest `
-CreateDNSDelegation `
-DatabasePath "C:\Windows\NTDS" `
-DomainMode "Win2016" `
-DomainName "id1.local.com" `
-DomainNetBIOSName "DC1" `
-ForestMode "Win2016" `
-InstallDNS:$true `
-LogPath "C:\Windows\NTDS" `
-NoRebootOnCompletion:$false `
-SYSVOLPath "C:\Windows\SYSVOL"
-Force:$true
```

L'ultimo step prima dell'installazione e del riavvio effettua un check e ci informa sugli eventuali errori da risolvere mediante la finestra **Prerequisites Check** come illustra la FIGURA 15 a pagina seguente.
Come già indicato in precedenza, possiamo ignorare ciò che riguarda la delega DNS: il ruolo DNS Server verrà installato automaticamente durante il processo successivo, come possiamo notare alla voce **DNS Server**: **Yes** di Figura 14. Cliccando su **Install** terminiamo la configurazione.

Una volta riavviato il server troveremo nel menu Tools del Server Manager i nuovi **snap-in** relativi ad Active Directory e al ruolo DNS. Attraverso la finestra di **Local Server**, ora che il nostro dominio di rete è stato configurato, è buona prassi configurare i servizi di **gestione remota** e **desktop remoto** in modo da poter gestire e controllare da remoto il nostro server.

FIGURA 15 Prerequisites Check



3.4 Installazione di ulteriori Domain Controller

Nell'esercizio precedente abbiamo installato un unico Domain Controller (dc1). In una configurazione ad alta affidabilità, è consuetudine installare un secondo Domain Controller come replica del primo. Lo scopo è quello di avere migliori garanzie in termini di sicurezza per quei nodi che sono difficilmente controllabili.
Con questa configurazione, il database di Active Directory Domain Services contenuto in **NTDS.DIT** (comprensivo degli user account) e una copia della cartella System Volume, **SYSVOL** saranno sempre replicate nel nuovo nodo.
Ci sono due modi per farlo:

- installare un Domain Controller **Replica**;
- installare un Domain Controller come **Read Only Domain Controller** (**RODC**) per porre in sola lettura sia NTDS.DIT che SYSVOL.

esercizio

→ PROBLEMA

Installare su un nuovo server Windows un secondo Domain Controller come replica del Domain Controller primario già installato. Svolgere l'attività utilizzando l'applicazione Server Manager.

→ SVOLGIMENTO

Utilizzando l'interfaccia del Server Manager sul nuovo server che vogliamo promuovere come replica, andiamo a installare il ruolo di Domain Controller.
I primi passi sono identici a quelli descritti per la prima installazione fino alla promozione del server.
A questo punto nella finestra di **Deployment Configuration** (Figura 12), scegliamo

Add a domain controller to an existing domain per installare il nuovo server all'interno di un dominio esistente.
Nella finestra di **Domain Controller Options** (Figura 13) si devono invece spuntare sia il **GC** (**Global Catalog**) sia il **RODC** (**Read Only Domain Controller**) anziché il DNS Server.
Dopo aver inserito una password per il **DSRM** (**Directory Services Restore Mode**) si può procedere con l'installazione delle Additional Options.
Nella finestra di **Additional Options** vengono richieste informazioni relative alla replica e al server di partenza da replicare. Occorre anche specificare se è necessario usare supporti diversi all'installazione (**IFM**, **Install From Media**).
Il wizard prosegue l'installazione con la finestra **Paths** (FIGURA 16), in cui si devono scegliere le cartelle dove memorizzare database, **SYSVOL** e **log**.

Gli ultimi passaggi ripetono quelli della prima installazione con:

- il riepilogo dei dati immessi (finestra Review Options di Figura 14);
- la verifica dei prerequisiti (finestra Prerequisites Check di Figura 15).

Al termine del processo di installazione viene richiesto di riavviare il server. Al termine del riavvio il dominio RODC configurato sarà disponibile.

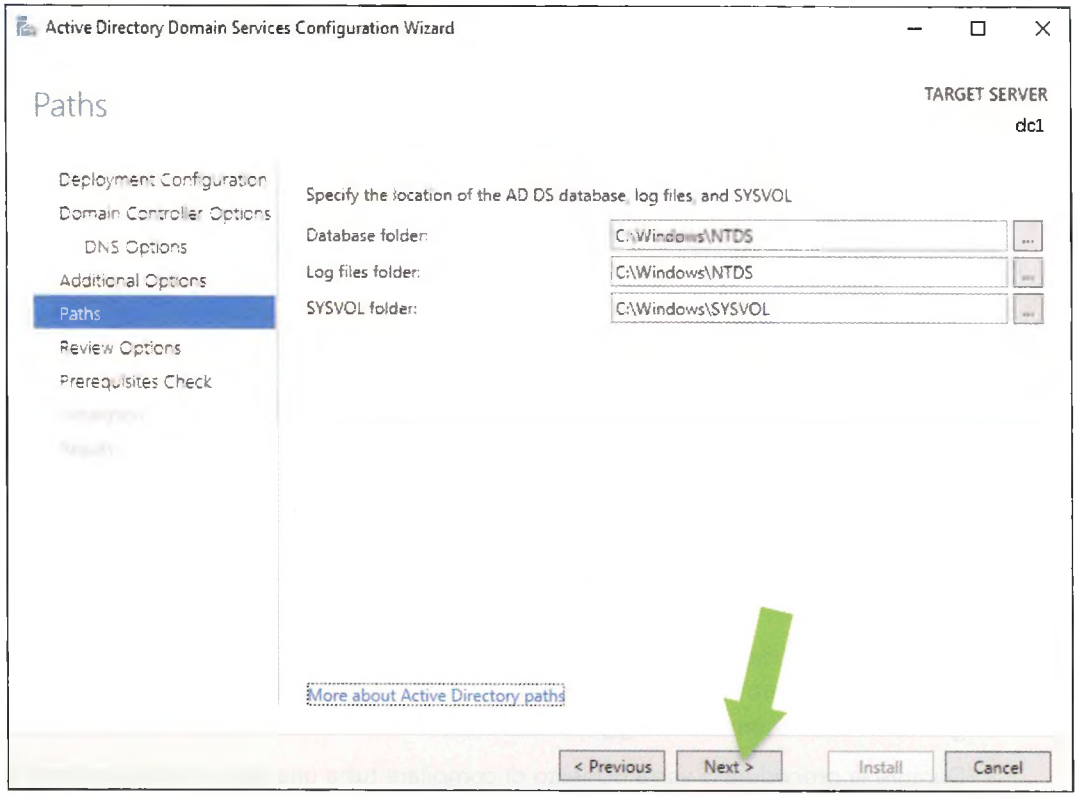


FIGURA 16 Paths

FISSA LE CONOSCENZE

- Che cos'è Active Directory Domain Services?
- Che cos'è il Global Catalog?
- Come suddividiamo, a livello logico, gli oggetti della rete con l'approccio Active Directory?
- E invece a livello fisico?

4 LA CONFIGURAZIONE DI UTENTI E COMPUTER

4.1 La gestione degli utenti, dei gruppi e dei computer con Active Directory

Uno dei motivi fondamentali per cui si sceglie un'architettura server basata su Active Directory è la necessità di **autenticare utenti verso le risorse della rete**.
Tramite il solito Server Manager possiamo individuare i vari snap-in associati ad Active Directory:

- **Active Directory Users and Computers**: permette di gestire utenti, computer, gruppi e organizational unit;
- **Active Directory Sites and Services**: è lo snap-in usato per la gestione della replica, il networking dell'intera rete e i servizi a esso relativi;
- **Active Directory Domains and Trust**: gestisce le possibili relazioni tra alberi di foreste;
- **Active Directory Administrative Center**: è un'interfaccia basata su PowerShell per la gestione di tutto il mondo Active Directory.

esercizio

→ PROBLEMA

Creare un nuovo utente con Active Directory.
Svolgere l'attività utilizzando l'applicazione Server Manager.

→ SVOLGIMENTO

Per iniziare la configurazione degli utenti, dal menu **Tools** del Server Manager scegliamo **Active Directory Users and Computers**.
Per quanto concerne la creazione di utenti bisogna sottolineare che, in una rete basata su Windows Server, possiamo avere sostanzialmente due tipi di utenze:

- **utenti locali**: definiti sul singolo computer, possono operare, limitatamente ai permessi accordati, solo su quella macchina;
- **utenti di dominio**: definiti nel pannello di Active Directory e generalmente, a meno di policy applicate, possono operare su qualsiasi risorsa del dominio.

Per creare un nuovo utente, dal pannello **Active Directory Users and Computers**, esploriamo l'albero del nostro dominio *dc1.local*, selezioniamo la voce **Users** e scegliamo di **Creare un nuovo oggetto utente**.

Durante la procedura ci verrà richiesto di compilare tutta una serie di dati personali e di scegliere un nome utente con il quale verrà eseguito l'accesso.

Tale nome deve essere univoco all'interno di tutta la rete.
Scegliamo nella schermata successiva una password da consegnare all'utente per il primo login e lasciamo spuntata l'opzione sul cambiamento obbligatorio di password all'accesso successivo, in maniera da consentire agli utenti piena autonomia e confidenzialità nella scelta della propria.
Una finestra ci informerà poi di tutti i dati scelti, e cliccando su **Fine** avremo terminato la creazione del nostro primo utente.

Un doppio clic sull'utente che abbiamo appena creato consente di configurare gli **attributi** (**Properties**) dell'utente stesso attraverso una serie di schede (FIGURA 17).

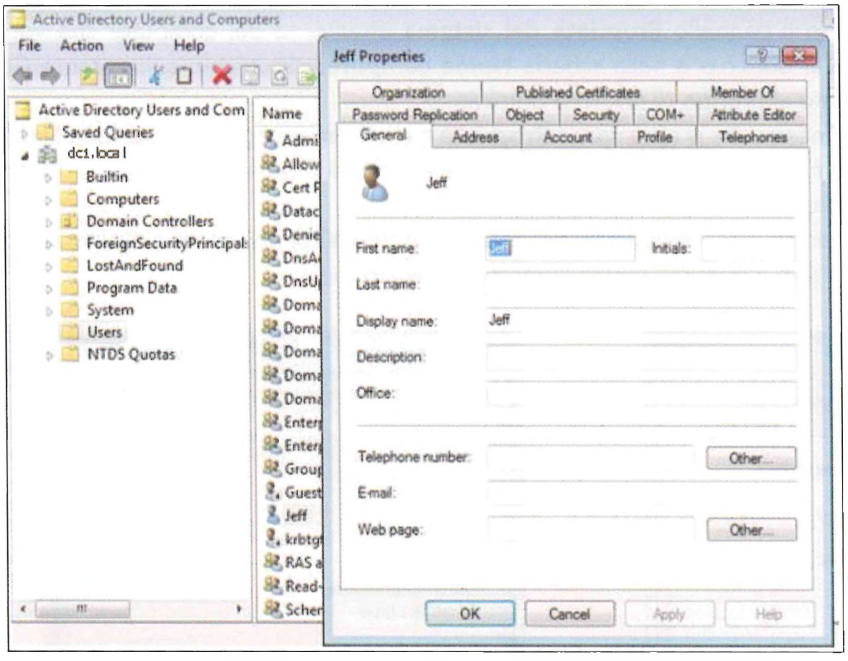


FIGURA 17 Scheda relativa al profilo dell'utente Jeff

Nella scheda relativa al **profilo** (profile: forse la scheda più importante) si possono configurare 3 proprietà.

1) **Profile path**: percorso per il salvataggio delle proprietà desktop dell'utente. Generalmente possono essere salvate localmente nel PC in uso oppure salvate in un percorso di rete. Quest'ultimo caso porta a lavorare con i cosiddetti Roaming Profile.
2) **Logon script**: script di accesso che permette di indicare il percorso del file da eseguire all'avvio.
3) **Local path**: percorso da indicare perché una risorsa funzioni come storage personale dell'utente.

Un modo molto comune per lavorare su questi attributi, al fine di indicare i giusti percorsi, è quello di usare la variabile %username%. In questa maniera ogni utente avrà una sua sottocartella partendo da una risorsa condivisa comune.

Potremmo per esempio considerare una configurazione del tipo:

- **Profile Path**: \\DC1-DC\Profile\%username%;
- **Home Folder** configurata come Connect con "Z:" per l'unità specificata e \\DC1-DC\Home\%username% per il percorso.

4.2 La configurazione del computer dell'utente

esercizio

→ PROBLEMA

Configurare il computer dell'utente ed eseguire il login utente.
Svolgere l'attività utilizzando l'applicazione Server Manager.

→ SVOLGIMENTO

Per prima cosa occorre abbinare al dominio (join a dominio) il computer dell'utente precedentemente creato.

Apriamo il pannello **Proprietà del sistema** (FIGURA 18) del computer che vogliamo legare al dominio e nella scheda **Nome computer** clicchiamo sul pulsante **Cambia** associato al gruppo di lavoro o dominio.

Nella finestra che si apre con le **Proprietà del sistema** scegliamo l'opzione **Dominio** e inseriamo il nostro nome di dominio precedentemente configurato (*dc1.local*), come mostrato in FIGURA 19.

Ci verranno successivamente richieste le credenziali di un utente abilitato alle operazioni di join a dominio (come l'utente Administrator).

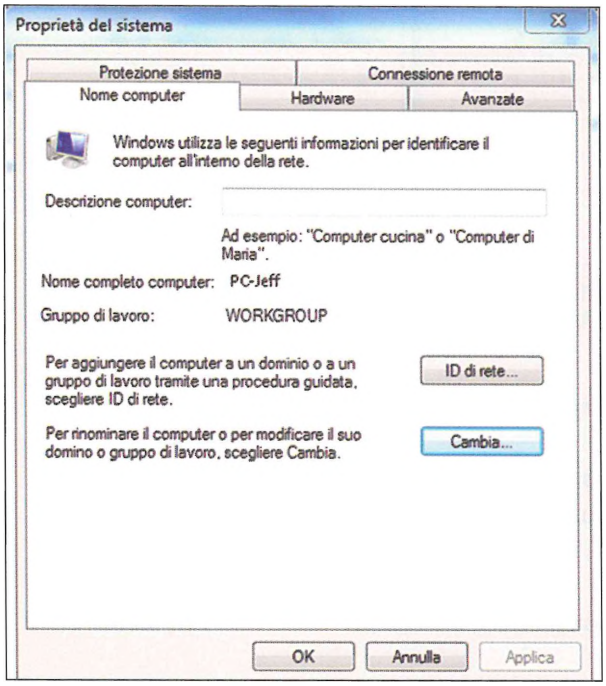


FIGURA 18 Proprietà del sistema

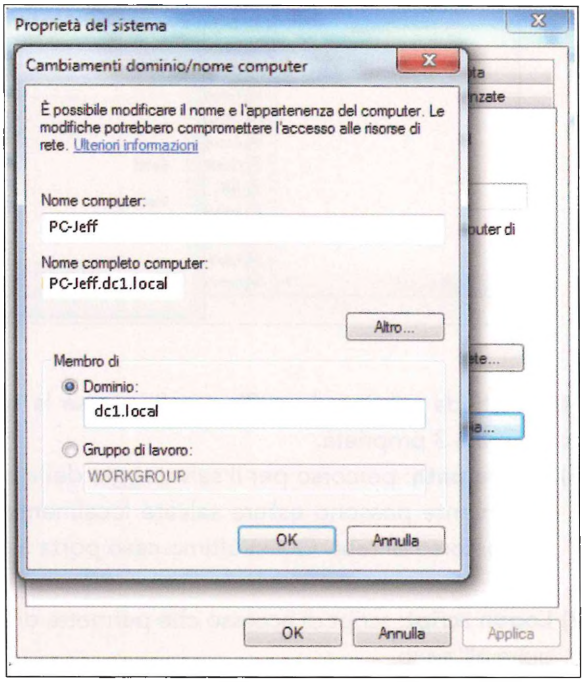


FIGURA 19 Cambiamenti dominio/nome computer

A questo punto il join a dominio è effettuato con successo e un riavvio della macchina ci consentirà di effettuare il login usando delle credenziali valide di un utente appartenente al dominio.

Dopo aver riavviato la macchina, il computer farà parte del dominio.

Nella fase di join a dominio, l'utente Administrator del dominio viene automaticamente aggiunto come membro del **gruppo administrators locale**.

Facendo quindi login come utente Administrator si potranno installare tutti i programmi che si desiderano.

Se invece si vogliono dare privilegi particolari a un utente del dominio (come per esempio il diritto di installare i programmi) lo si dovrà importare/aggiungere localmente accedendo al **Pannello di controllo**, **Account utente**, **Gestisci account utente**, **Aggiungi** (FIGURA 20); con il pulsante destro del mouse possiamo gestire un utente attraverso il menu associato.

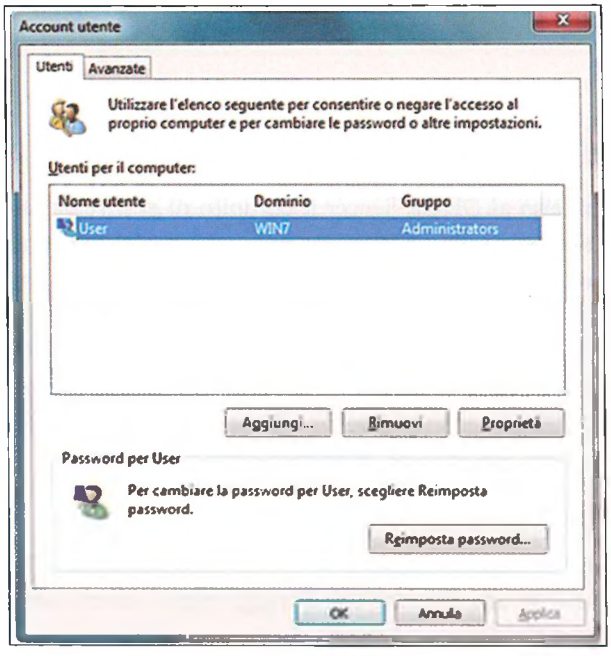


FIGURA 20 Gestione account utente

4.3 La configurazione dei gruppi

In scenari medio-piccoli la gestione degli utenti può essere effettuata anche a mano ma, pensando alla scalabilità, la soluzione più versatile ed efficace è quella di organizzare gli utenti in gruppi, usando i **Group Account**.

In Windows Server esistono sostanzialmente due tipi di gruppi:
- **sicurezza**: usato principalmente per l'applicazione di policy;
- **distribuzione**: usato per applicazioni di tipo mail, come invio di messaggi broadcast.

Oltre alla tipologia, un gruppo ha anche un suo **Ambito** (o **scope**):
- **locale al dominio**: applicabile a tutti gli oggetti del dominio;
- **globale**: applicabile a tutti gli oggetti del dominio e dei domini *trusted*;
- **universale**: applicabile a tutti gli oggetti della foresta.

Per creare un nuovo gruppo possiamo usare lo stesso meccanismo applicato alla creazione di un nuovo utente e scegliere l'opzione Gruppo. Attribuiamo al gruppo un nome, scegliamo un ambito e un tipo a seconda della nostra esigenza e confermiamo la creazione.
Possiamo ora aggiungere nuovi membri al gruppo creato. Per fare ciò possiamo selezionare gli utenti che vogliamo legare al gruppo con il tasto destro e scegliere l'opzione **Aggiungi** a un gruppo oppure aprire ogni singolo oggetto e, dal pannello **Membro di**, possiamo aggiungere un nuovo gruppo indicandone il nome.

FISSA LE CONOSCENZE

- In una rete basata su Windows Server possiamo avere due tipi di utenze. Quali?
- In una rete basata su Windows Server possiamo avere due tipi di gruppi. Quali?
- Un gruppo può avere più ambiti (scope). Quali?

Case study
Creazione di una rete e gestione degli accessi

5 I SERVIZI DHCP E DNS

5.1 La configurazione di un DHCP Server

Gli amministratori di rete demandano al DHCP Server il compito di gestire l'assegnazione degli indirizzi IP agli host della rete. La gestione manuale, anche in reti di medie o piccole dimensioni, è gravosa e spesso inefficiente. Inoltre, la tecnologia che è alla base del DHCP permette di distribuire sulla rete non solo indirizzi IP, ma anche altre informazioni di configurazione.
Su una rete in cui vi siano, per esempio, dei telefoni VoIP (Voice over IP) è possibile indicare dov'è il file del *provisioning* del telefono stesso attraverso delle semplici regole DHCP.
Le modalità di configurazione del DHCP Server di Windows Server sono due.

POLICY BASED ASSIGNMENT

Con questa modalità il DHCP Server valuta le richieste DHCP in base alle policy che si definiscono. In pratica consente a un amministratore di raggruppare in uno scope (ambito) i client per attributi specifici in base ai campi contenuti nel pacchetto di richiesta del DHCP Client.

I campi del pacchetto di richiesta del DHCP Client disponibili per la definizione delle politiche sono:

- Vendor Class;
- User Class;
- MAC address;
- Client Identifier;
- Relay Agent Information.

Quindi la Policy based assignment è una funzionalità che consente un'amministrazione mirata e un maggiore controllo dei parametri di configurazione.
Una singola richiesta del client può associarsi a molteplici policy e una policy può essere associata a più intervalli di indirizzi (dunque a più scope di client).

Questo consente flessibilità per alcuni scenari comuni. Vediamone alcuni.

- **Multiple device types**: una rete che comprende molti dispositivi DHCP Client diversi, per esempio stampanti, telefoni IP e desktop. Gli amministratori devono saper classificare questi dispositivi utilizzando diversi intervalli di indirizzi IP (scope diversi).
- **Multiple roles**: una rete che comprende diversi tipi di computer (portatili, desktop e server) nella stessa subnet. A seconda del tipo di client, l'amministratore potrebbe voler fornire diverse impostazioni di durata del **#lease**. Per esempio, a tutti i client wireless che si connettono tramite un **relay agent** specifico può essere assegnata una durata di locazione di 4 ore. Il DNS può essere disattivato per i client corrispondenti a questi criteri.
- **Virtualization**: una rete di data center che utilizza la virtualizzazione delle applicazioni. Le macchine virtuali vengono aggiunte e rimosse dinamicamente a seconda delle esigenze di carico in un dato momento. Un amministratore che desideri instradare diversamente il traffico sulla rete per le macchine virtuali è in grado di creare una policy basata sul **MAC address prefix** per assegnare una breve durata del lease, un intervallo specifico di indirizzi IP e un diverso gateway predefinito.

#techwords

Lease, affitto in inglese. Indica il tempo in cui i dati di configurazione restano assegnati al cliente. Scaduto il lease la richiesta deve essere rinnovata.

DHCP FAILOVER

Questa modalità permette di avere **due DHCP Server** abilitati entrambi ad assegnare gli indirizzi IP e le opzioni di configurazione nell'ambito della stessa net o subnet, fornendo la disponibilità continua del servizio DHCP ai client.
I due DHCP Server replicano le **informazioni di leasing** tra le parti, consentendo così, a uno qualsiasi dei due server, di assumersi la responsabilità per la manutenzione dei client per l'intera subnet, quando l'altro server non è disponibile.
La configurazione di failover del DHCP Server che è pronto a subentrare è detta **hot standby.**
Inoltre, è possibile configurare il failover in una modalità a **carico bilanciato** (**load balance**), dove le richieste dei client sono distribuite tra i due server in un rapporto di failover. Si tratta dunque di una tecnica per assicurare la disponibilità continua del servizio DHCP ai client.
Attraverso la DHCP console possiamo configurare il server nella modalità **hot standby** o **load balance**.

Riassumendo, i vantaggi del DHCP Failover includono:

- **Semplicità**: esiste una procedura guidata per creare relazioni di failover tra DHCP Server. La procedura guidata replica automaticamente gli scope e le impostazioni dal server primario al partner di failover;
- **Flessibilità**: DHCP Failover può essere configurato per fornire ridondanza o, in modalità di bilanciamento del carico, per distribuire le richieste dei client tra due DHCP Server;
- **Seamless** (senza soluzione di continuità): i DHCP Server condividono le informazioni di leasing, permettendo a un server di assumersi la responsabilità dei servizi offerti ai client se l'altro server non è disponibile. Quando un lease si rinnova, i DHCP Client possono mantenere lo stesso indirizzo IP anche se il lease è rilasciato da un altro DHCP Server;
- **Multi-site**: DHCP Failover supporta un'architettura di distribuzione che include più siti. I server partner di DHCP Failover non hanno bisogno di essere situati nello stesso luogo fisico.

esercizio

→ PROBLEMA

Configurare il ruolo di DHCP Server in uno scenario con Active Directory.
Svolgere l'attività utilizzando l'applicazione Server Manager.

→ SVOLGIMENTO

Una volta stabilita la modalità (policy based o failover) si può procedere a configurare il ruolo di DHCP Server con le funzionalità necessarie.
Bisogna ricordare che un DHCP Server in uno scenario con Active Directory deve essere autorizzato **nello stesso dominio**. Ciò è reso possibile già nel processo di installazione del ruolo DHCP.
Dalla solita interfaccia del Server Manager, avviare il processo di installazione cliccando su **Add Roles and features**, scegliendo poi su quale server andare a installare il nuovo ruolo.

Una delle prime cose che ci troviamo a dover gestire sono i **DHCP scope**.

Il DHCP Failover può essere configurato su un unico DHCP scope. È possibile configurare più scope contemporaneamente se tutti utilizzano la stessa *failover relationship* (relazione di failover tra due DHCP Server).
Per configurare più scope utilizzando la console DHCP, bisognerà scegliere questi ambiti tra quelli disponibili nella procedura guidata di configurazione di failover.
Gli scope per essere disponibili devono essere presenti sul DHCP Server locale e non già abilitati per DHCP Failover.
Per configurare un nuovo scope nella console DHCP facciamo clic con il pulsante destro del mouse su **IPv4** e selezioniamo **New Scope**.

Al fine di configurare uno scope dobbiamo fornire alla console DHCP alcune importanti informazioni:

- nome e descrizione dello scope;
- range degli indirizzi IP che vogliamo assegnare;
- subnet mask di appartenenza;
- una lista di singoli indirizzi IP che vogliamo escludere dal lease (per esempio i server allocati staticamente);
- il tempo massimo (delay) prima che il server offra un indirizzo IP (DHCP OFFER);
- il tempo massimo (lease duration) prima che scada l'indirizzo IP assegnato al client;
- le option che servono per ulteriori informazioni aggiuntive come, per esempio, 003 – Default Gateway e 006 – DNS Server.

Possiamo anche configurare uno scope per indirizzi IPv6 al fine di permettere tale indirizzamento nella rete.
In alcuni scenari, abbiamo la necessità di riservare alcuni indirizzi IP per macchine specifiche. Per fare ciò prendiamo nota del MAC address della macchina che vogliamo configurare e torniamo sulla console DHCP per configurare la reservation (prenotazione). Inserendo il MAC address e associandolo al desiderato indirizzo IP, ogni volta che la macchina con scheda di rete che ha quell'indirizzo MAC effettuerà una DHCP REQUEST le verrà assegnato l'indirizzo IP specificato.

5.2 La configurazione di un DNS Server

La risoluzione dei nomi di dominio è uno dei principi alla base del buon funzionamento di una rete. Sulla rete vengono inoltrate continuamente richieste per la risoluzione di servizi Internet o per la risoluzione di indirizzi a cui sono associate risorse interne. Per questo, i servizi Active Directory sono in strettissima collaborazione con tutto ciò che concerne i DNS (Domain Name System).

> Il **DNS**, dal nostro punto di vista, è un servizio che utilizza un **database distributional** al fine di risolvere le richieste (o query) FQDN (Fully Qualified Domain Name) e altre richieste da hostname a indirizzo IP.

Per quanto concerne l'installazione del DNS Server, ricordiamo che, durante il processo di promozione del Domain Controller esaminato nelle Lezioni precedenti, abbiamo considerato l'opzione di installazione del ruolo DNS Server direttamente sul controller di dominio.
Per cui, sullo stesso controller possiamo, dal Server Manager, lanciare il tool di gestione del DNS Server. In alternativa, possiamo decidere di installare un nuovo DNS Server all'interno della nostra rete, così da avere un secondo nodo che svolga questa funzione.

esercizio

→ PROBLEMA

Installare un DNS Server sul server con il role Domain Controller.
Svolgere l'attività utilizzando l'applicazione Server Manager.

→ SVOLGIMENTO

Avviamo Server Manager, dal menu **Manager** selezioniamo **Add Roles and Features Wizard** e scegliamo un server per il ruolo di DNS Server. Al termine del processo di installazione, sotto la voce **Tools** del Server Manager troviamo il collegamento al tool di gestione **DNS** (FIGURA 21).
Col DNS Manager è necessario creare una nuova **DNS Zone**: una porzione dell'intero namespace DNS nella quale vengono registrati i diversi **hostname** sotto forma di **record**.

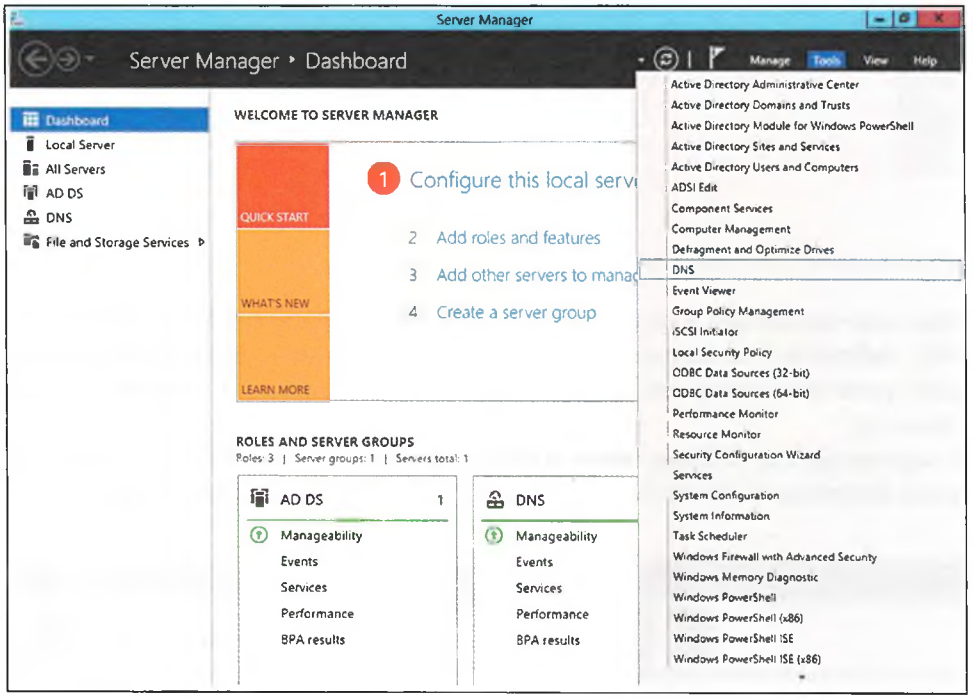


FIGURA 21 Dal Server Manager viene avviato il DNS Manager

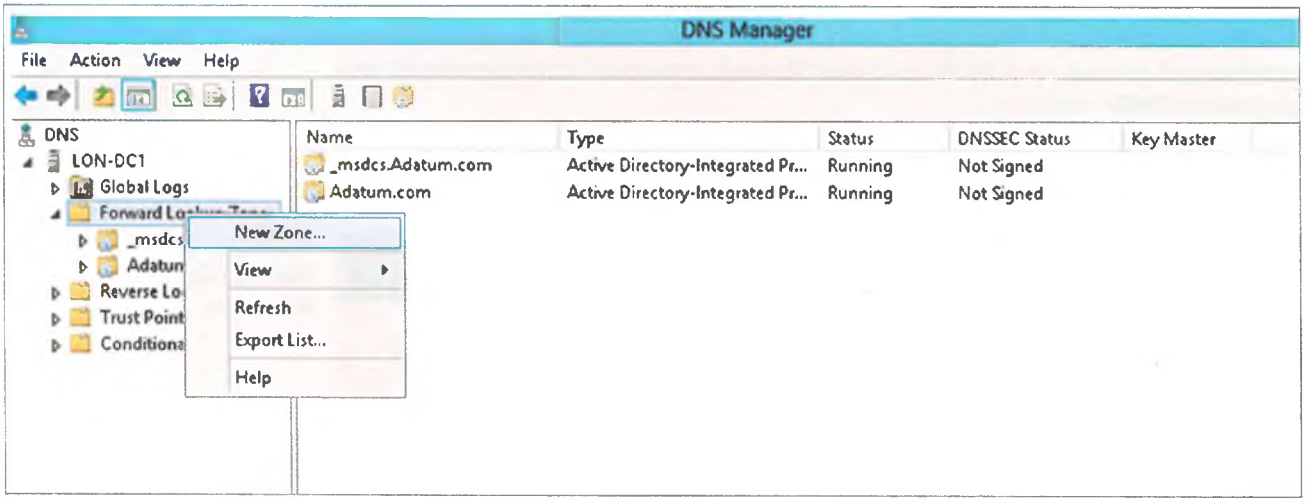
Gli hostname (detti **DNSname**) possono essere: nomi di host (record **A**), alias (record **CNAME**), servizi (record **SRV**), mail exchange (record **MX**), start of autority (record **SOA**) e name server (record **NS**). Solo dopo la creazione della DNS Zone, i client possono unirsi (join) al nuovo nome di dominio.
Possiamo notare come vengono differenziate le zone a seconda del tipo di query da gestire:

- **Forward Lookup Zone**: risolve gli hostname in indirizzi IP;
- **Reverse Lookup Zone**: all'opposto, risolve gli indirizzi IP in nomi di dominio.

Ogni record del database distribuito conterrà dunque la mappatura degli hostname e i corrispondenti indirizzi IP.
Occorre dunque decidere il tipo di zona da configurare. L'attività indispensabile all'interno di una rete è quella che necessita di Forward Lookup Zone: i client conoscono i nomi (degli altri client, dei siti, dei servizi, dei server, ecc.) e necessitano degli IP.
Lavorare direttamente sugli IP sarebbe come avere una rubrica telefonica organizzata per numeri di telefono crescenti, anziché per nomi in ordine alfabetico.

Scegliamo dunque la prima opzione (**Forward Lookup Zone**, **New Zone** come mostrato in FIGURA 22) col vantaggio che tutte le query DNS che non possono essere risolte internamente saranno reindirizzate verso un altro DNS Server presente al di fuori della rete locale (generalmente quello del nostro provider di connettività).
La scelta fatta porta all'avvio del wizard per la creazione della New Zone.
Volendo creare una nuova zona scegliamo la prima opzione, **Primary zone**.

FIGURA 22 Dal DNS Manager creiamo la New Zone



Dopo aver selezionato il server (o i server) che dovranno gestire la zona del nostro DNS, definiamo la porzione dello spazio dei nomi associati a questo server, ossia su quale parte del namespace DNS questo server ha il permesso di risolvere le query (FIGURA 23).
È ragionevole che lo **Zone Name** scelto rappresenti un sottodominio (*nomezona.nomedominio.com*) del dominio principale (*nomedominio.com*) dell'azienda.

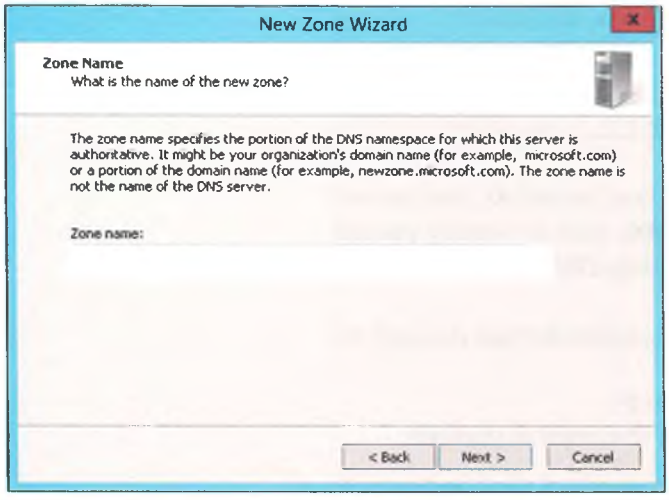


FIGURA 23 Scelta dello Zone Name

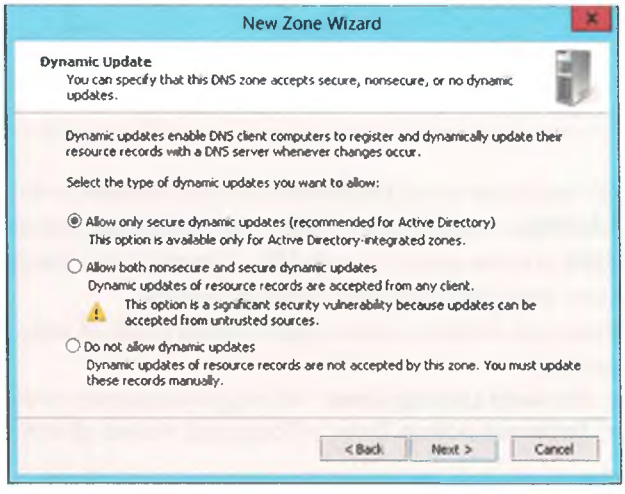


FIGURA 24 Scelta del tipo di aggiornamento

Confermiamo la creazione del database dei nomi (**Zone File**) e scegliamo la tipologia di aggiornamenti permessi su questo server in termini di nuovi record all'interno dello spazio dei nomi (FIGURA 24).

In alcuni casi l'amministratore può preferire l'aggiornamento manuale dei record.
A questo punto verrà richiesto di inserire il server d'inoltro (DNS forward query) cioè l'indirizzo IP del DNS Server cui inoltrare le richieste non risolvibili in locale.
Al termine di quest'ultima operazione, la nuova zona risulterà configurata (FIGURA 25).

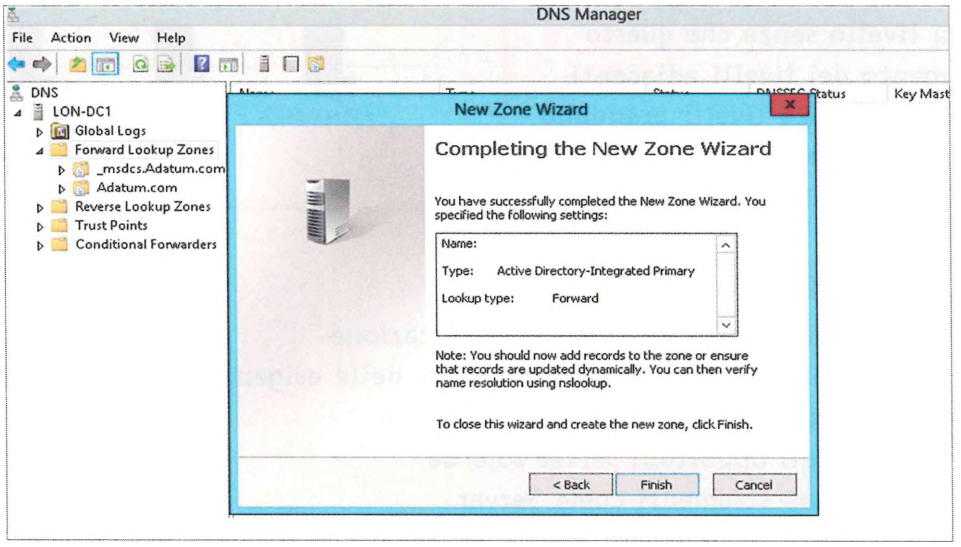


FIGURA 25 Completamento della configurazione della New Zone

5.3 Altri ruoli server

Di solito sono configurati molti altri ruoli server in una rete.
Tra questi i più frequenti sono:

- File and Storage Services: consente di gestire i file, le cartelle e altri spazi di storage (anche in cloud), facilitandone la condivisione;
- Hyper-V: l'applicazione Microsoft per la virtualizzazione dei server;
- Web Server (IIS): basato su Internet Information Services, fornisce una piattaforma per l'hosting di siti servizi e applicazioni web;
- Network Controller: consente di gestire, configurare e monitorare l'infrastruttura di rete virtuale e fisica di un data center; Microsoft segnala di installare questo ruolo su una macchina virtuale (Hyper-V virtual machine) e non fisica;
- Print and Documentation Services: permette di centralizzare le attività tipiche del print server (per esempio il controllo delle code di stampa) e delle stampanti di rete.

Per il wizard su tali servizi consigliamo la documentazione ufficiale reperibile su *docs.microsoft.com*.

FISSA LE CONOSCENZE

- Quali sono le due modalità di configurazione del DHCP Server di Windows Server?
- Che cos'è un DHCP scope?
- Descrivi la modalità per riservare determinati indirizzi IP a macchine specifiche usando il servizio DHCP.
- Descrivi la modalità hot standby.
- Come si differenziano le zone DNS a seconda del tipo di query da gestire?
- Gli hostname (detti DNSname) possono generare diversi tipi di record. Quali?
- Quali altri ruoli server si possono configurare su Windows Server, oltre a DHCP Server e DNS Server?

LABORATORIO ONLINE

LA CONFIGURAZIONE DI SAMBA SU LINUX

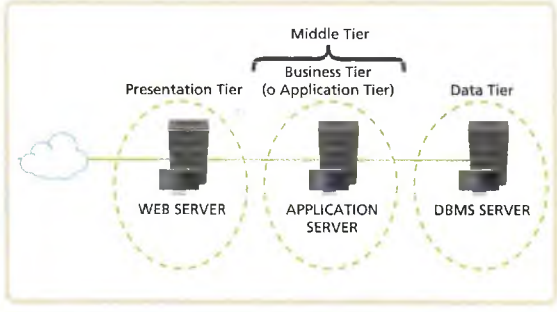
Samba è una suite di strumenti software che si installa su Linux (server e client) per la gestione di reti formate da computer con sistemi operativi diversi (per esempio Windows e Linux).

RIPASSIAMO INSIEME

DIDATTICA INCLUSIVA

1 Architetture N-tier basate su Client-Server

Le architetture per il web si basano su una modellizzazione a livelli, che offre il vantaggio di poter intervenire su un livello senza che questo comprometta il funzionamento dei livelli adiacenti. Nel contesto dei sistemi per il web i livelli prendono il nome di tier (strati) e le architetture si chiamano N-tier in base al numero N di strati progettati.



2 Le soluzioni di Windows Server 2019

Nella Lezione si affrontano le varie fasi di una buona progettazione dell'infrastruttura di rete: conoscenza della situazione attuale, delle esigenze dell'azienda, sia primarie sia collaterali, previsione degli sviluppi. Questa analisi porterà a scegliere gli opportuni server role da configurare e a imparare a utilizzare strumenti come Server Manager o PowerShell per l'amministrazione del sistema operativo Windows Server e delle applicazioni in esso eseguite.

3 Il Domain Controller

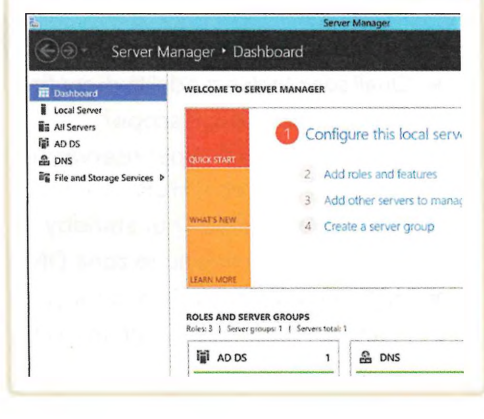
Il Domain Controller (DC), controllore di dominio, rende possibile l'esecuzione di svariate applicazioni cloud della rete. Il primo passo è l'installazione di un DC e del servizio Active Directory Domain Services, raggruppamento logico di utenti e computer in un dominio gestito appunto dal DC.

4 La configurazione di utenti e computer

Uno dei compiti di Active Directory è l'organizzazione degli utenti. Attraverso Active Directory è possibile creare un nuovo utente, locale o di dominio, configurare il computer ed effettuare il login utente e per configurare i gruppi.

5 I servizi DHCP e DNS

Alcuni dei servizi (server role) configurabili in una rete sono fondamentali e spesso indispensabili. Tra questi sicuramente ci sono i servizi DHCP e DNS. Il primo assegna indirizzi IP e i parametri di configurazione in modo dinamico agli host di una rete. Il secondo risolve i nomi di dominio delle risorse esterne e interne alla rete aziendale. Anche un DHCP Server e un DNS Server possono essere configurati con lo strumento Server Manager.



VERIFICA DI FINE UNITÀ

Test
Svolgi il **test interattivo**

Quali delle seguenti affermazioni sono vere (V) e quali false (F)?

1. Le architetture a strati favoriscono l'indipendenza delle componenti. V F
2. I tier vengono fisicamente realizzati mediante macchine server in grado di svolgere i compiti richiesti da ogni strato. V F
3. L'architettura 2-tier (corrispondente al Client-Server) è da considerarsi un'architettura ottimizzata. V F
4. Windows Server 2019 è disponibile in 3 edizioni. V F
5. Dal Server Manager non possiamo eseguire operazioni di configurazione del server locale. V F
6. Una struttura Active Directory è un framework gerarchico di oggetti: risorse, servizi e utenti. V F
7. Ogni oggetto è caratterizzato da un attributo. V F
8. In Windows Server si hanno sostanzialmente due tipi di utenze: locali e di dominio. V F

Domande a scelta multipla (una sola è la risposta esatta)

1. **Quali sono i 3 tier principali presenti in una architettura web?**
   - A Presentation, Data access, Data storage
   - B Presentation, Client, Data
   - C Presentation, Business, Data
   - D Presentation, Security, Data

2. **Quali sono i tier che lavorano sia come client sia come server?**
   - A I Middle Tier
   - B Il Presentation Tier
   - C Il Data Tier
   - D Tutti i tier lavorano sia come client che come server

3. **Active Directory consente di organizzare la rete a livello fisico attraverso:**
   - A organizational unit e dominio
   - B albero di dominio e foresta di dominio
   - C sito e subnet
   - D domino e subnet

4. **Lo scope (ambito) di un gruppo configurato in Windows Server può essere:**
   - A locale al dominio, globale e universale
   - B locale alla foresta, globale e universale
   - C solo locale al dominio
   - D solo locale alla foresta

PREPARATI PER IL COLLOQUIO ORALE

Ascolta le **risposte**

1. LEZIONE 1 **Quali sono i problemi dell'architetuta 1-tier e a che cosa sono dovuti?**
2. LEZIONE 1 **Descrivi l'architettura per il web di tipo 2-tier e spiega perché coincide col modello Client-Server.**
3. LEZIONE 1 **Descrivi l'architettura per il web di tipo N-tier spiegando come funzionano i Middle Tier.**
4. LEZIONE 2 **Che cos'è indispensabile capire per una buona progettazione dell'infrastruttura di rete?**
5. LEZIONE 3 **A che cosa serve il Domain Controller?**
6. LEZIONE 4 **Quali sono i passi principali da seguire per creare un nuovo utente?**
7. LEZIONE 4 **Nella scheda relativa al profilo utente si possono configurare 3 proprietà. Quali?**
8. LEZIONE 4 **Quali operazioni sono disponibili per gestire un account utente?**
9. LEZIONE 5 **Quali sono le caratteristiche principali della modalità DHCP Failover?**
10. LEZIONE 5 **Che cos'è una DNS Zone?**

IN ENGLISH, PLEASE

CLIL

Ascolta la **pronuncia del testo** e verifica la **traduzione**

ABSTRACT

Web architecture: services, applications and administrative tasks

A N-tier architecture is a Client-Server architecture providing a model where the presentation, business and data management functions are logically and physically separated. These functions are running on a separate server (or clusters) to provide services.
It is important to understand how to install and configure servers to run these services, as well as configure clients. Windows Server 2019 allows the creation of a network in which some services remain within the company (i.e. DHCP and DNS services), while others can be virtualized externally through the Server Manager and PowerShell. The Domain Controller permits the creation of cloud applications and manages the Active Directory Domain Services, to logically group users and computers.
In the Windows networks there are two types of user accounts: local users and domain users. Users and computers can be put together in a group. Groups are useful to assign rights and permissions to the entire group rather than to each user/computer individually. In order to integrate Linux/Unix Servers and Desktops into Active Directory environments, we can use the tool Samba. It provides secure and fast file and print services for all clients using the SMB protocol.

EXERCISES

Use the appropriate number to match words and meanings.

...	Presentation Tier	1	At this level the information is stored and retrieved from a database.
...	Business Tier	2	User interface.
...	Data Tier	3	An Active Directory object.
...	Scale-up	4	A logical group of Windows objects defined in a directory database.
...	Scale-out	5	A set of systems located at different nodes but appearing to the user as a single system
...	Distributed network	6	Vertical scalability.
...	Domain	7	It coordinates the applications, processes commands and makes decisions.
...	Site	8	Horizontal scalability.

GLOSSARY

Active Directory Domain Services: a logical grouping of users and computers in a domain managed by Domain Controllers.
Application Server: provides a complete solution for hosting and managing distributed business applications.
cmdlets (command-lets): specialized .NET classes implementing a particular operation. They are used in PowerShell to perform administrative tasks.
Domain Controller: a server that responds to security authentication requests within a Windows domain.
N-tier architecture: a Client-Server architecture in which several functions such as application processing, data management, security and so on, are physically separated.
Network Services: services provided by a network server (i.e. DHCP and DNS services).
Platform: a system on which application programs can run and execute a specific task.
PowerShell: a Microsoft framework consisting of a command-line shell and associated scripting language.
Server Role: a primary duty that a server performs (i.e. Application Server, Web Server, Database Server and so on).
Roaming User Profile: a user profile stored on a Windows Server. The profile is automatically available when the user logs on to any computer on the network.

LAVORARE PER COMPETENZE

COMPETENZE IN GIOCO

Competenze disciplinari

- Saper amministrare una rete aziendale.
- Scegliere i servizi da configurare in base alle esigenze.
- Saper descrivere e documentare le soluzioni adottate.
- Utilizzare le reti e gli strumenti informatici nelle attività di studio, ricerca e approfondimento disciplinare.

Competenze chiave di cittadinanza

- Interpretare il testo.
- Risolvere problemi.
- Comunicare.
- Competenza digitale.

obiettivi formativi

- Stimolare l'approfondimento e la ricerca disciplinare.
- Consultare fonti Internet.
- Contestualizzare in un caso reale le nozioni teoriche acquisite studiando.
- Esporre i risultati della ricerca alla classe.

tempi

- Preparazione: 2 ore.
- Presentazione dei risultati e dibattito: 1 ora.
- Autovalutazione: 10 minuti.

strumenti

- Libro di testo.
- Dispositivo connesso a Internet.
- Software PowerPoint.
- Proiettore collegato al computer in classe o in laboratorio.

TEMA PROPOSTO

La rete di una scuola è organizzata in due reti separate: una rete utilizzata dal personale amministrativo e una rete utilizzata per la didattica.
L'attuale separazione fisica delle due reti garantisce che le informazioni trattate all'interno della rete amministrativa non siano accessibili dalla rete didattica.

Progettare la realizzazione di alcuni servizi da implementare sulla rete della scuola, descrivendone la configurazione.

SVOLGIMENTO

Viste le caratteristiche della rete scolastica, con parte dedicata alla didattica e parte riservata all'amministrazione, decidiamo di gestire le risorse condivise organizzando gruppi di utenze in base al ruolo: docente, studente, assistente tecnico, segretario, dirigente o altro.
Alcuni dei servizi configurabili in una rete sono fondamentali e spesso indispensabili. Tra questi sicuramente ci sono:

- l'Active Directory Domain Service per installare un Domain Controller Server che effettui i processi di identificazione degli utenti e di accounting relativi al grado di accesso alle risorse disponibili all'interno del dominio;
- il DHCP (Dynamic Host Configuration Protocol) a cui gli amministratori di rete demandano la configurazione della rete: in pratica ha il compito di gestire l'assegnamento degli indirizzi IP agli host della rete;
- il DNS (Domain Name System) per la risoluzione dei nomi di dominio per i servizi Internet e per la risoluzione degli indirizzi delle risorse interne alla rete;
- l'FTP (File Transfer Protocol) per fornire l'accesso a cartelle pubbliche o con autenticazione;
- il servizio WWW (World Wide Web), per l'accesso al sito web della scuola installato su un server web;
- il servizio di posta elettronica, reso disponibile su un mail server;
- il servizio di stampa gestito da un Print Server che permette di mettere in comune una o più stampanti tra gli utenti di una rete con l'eventuale gestione dei diritti di accesso.

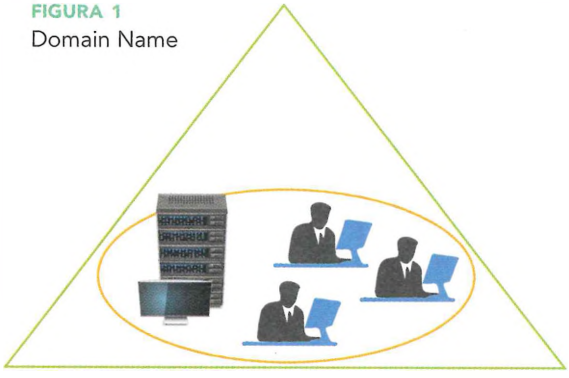
Il principale è sicuramente l'Active Directory Domain Service e quindi scegliamo di descriverlo.

Active Directory Domain Service

L'Active Directory consente di suddividere gli elementi costitutivi della rete (chiamati oggetti), in 3 categorie:

1. le risorse (per esempio una stampante di rete presente in ciascuno dei laboratori didattici);
2. i servizi (per esempio una piattaforma di e-learning per la didattica);
3. gli utenti (per esempio gli account docenti o i gruppi amministrativi).

FIGURA 1
Domain Name



Gli oggetti delle 3 categorie possono essere logicamente raggruppati in un dominio (Domain Name, FIGURA 1) e installando un Domain Controller è possibile definirne la gestione.
Installare un Domain Controller vuol dire gestire un dominio. In pratica vuol dire, per esempio, autenticare gli utenti (come docenti oppure come studenti, ecc.) e in base al loro account consentire l'accesso a certe risorse e ad altre no. Oppure stabilire delle Group Policy in base alle quali applicare vincoli di sicurezza come limitare l'accesso a determinate cartelle, disabilitare il download di file eseguibili, disabilitare l'uso di unità esterne (penne USB, dischi ottici) e così via.
Il Domain Controller è il vero cuore della rete e le sue funzioni sono indispensabili per il funzionamento di molti servizi.

La FIGURA 2 è un esempio di rete basata su Active Directory per la gestione dell'interfaccia utente per l'accesso alle risorse interne della rete (sito, database), il servizio e-mail e l'accesso al web.

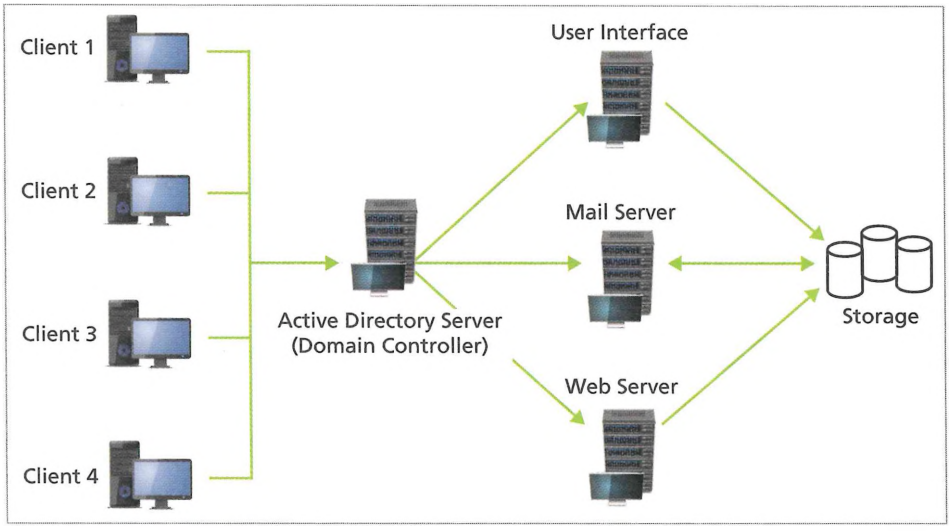


FIGURA 2 Rete con Active Directory Server

In una configurazione ad alta affidabilità, è consuetudine installare un secondo Domain Controller (FIGURA 3) come replica del primo.
Lo scopo è quello di avere maggiori garanzie in termini di sicurezza per quei componenti della rete che sono difficilmente controllabili o indispensabili al funzionamento della rete e dei suoi servizi.

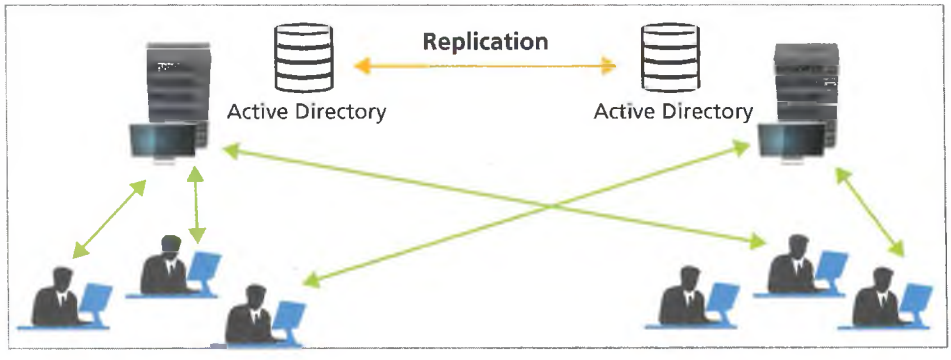


FIGURA 3 Rete con due Active Directory Server

A CASA

- Effettua una ricerca in Internet sui principali servizi (server role) di rete; esaminando i diversi servizi trovati concentrati su:
  - servizio di identificazione e accounting degli utenti;
  - servizio di assegnazione degli indirizzi di rete agli host;
  - servizio di risoluzione dei nomi di dominio.
- Individua quali, tra i casi trovati, risulta affine al contesto illustrato nel tema proposto.
- Leggi l'esempio di svolgimento proposto per verificare se le tue ipotesi si adattano al caso preso in esame e se la trattazione proposta risulta completa nell'ottica dei risultati della tua ricerca.
- Raccogli i tuoi risultati in una presentazione in PowerPoint (massimo 5 slide) evidenziando i casi trovati, la relazione con il contesto proposto, eventuali modifiche o aggiunte da effettuare alla soluzione proposta nell'esempio di svolgimento.

IN CLASSE

- Condividi la presentazione dei tuoi risultati con i compagni.
- Confronta e discuti con i compagni i casi che sono stati presentati.
- Stabilite quale caso rappresenta l'esempio migliore per completezza e realisticità nell'ottica della realizzazione delle misure necessarie richieste nel tema d'esame.
- Procedi con l'autovalutazione.

AUTOVALUTAZIONE

ATTIVITÀ	LIVELLO			
	INIZIALE	BASE	INTERMEDIO	AVANZATO
Ho compreso senza difficoltà le richieste dell'attività proposta?	Ho compreso solo alcune delle richieste aiutato dal docente. ☐	Con la guida del docente e la collaborazione dei compagni ho compreso quasi tutte le richieste. ☐	Ho compreso le richieste e in parte le ho svolte autonomamente. ☐	Ho identificato le richieste e le ho svolte senza difficoltà. ☐
Ho reperito le informazioni in rete senza difficoltà?	Ho reperito solo alcune delle informazioni utili aiutato dal docente. ☐	Con la guida del docente e la collaborazione dei compagni ho reperito quasi tutte le informazioni. ☐	Ho reperito le informazioni utili autonomamente e le ho elaborate. ☐	Ho identificato le informazioni utili e le ho elaborate senza difficoltà. ☐
L'analisi dello scenario mi ha permesso di definire modifiche e miglioramenti allo svolgimento proposto?	A partire dalla mia analisi, non sono stato in grado di individuare nessun punto critico nello svolgimento proposto. ☐	A partire dalla mia analisi, sono stato in grado di individuare alcuni punti critici nello svolgimento proposto con l'aiuto del docente. ☐	A partire dalla mia analisi, sono stato in grado di individuare i punti critici e alcune modifiche apportabili nello svolgimento proposto con l'aiuto del docente. ☐	A partire dalla mia analisi, sono stato in grado di individuare i punti critici e definire le modifiche apportabili in modo dettagliato e completo. ☐

UNITÀ 8

LA GESTIONE DELLA RETE E DEI SISTEMI

Guarda la presentazione dell'unità

IN QUESTA UNITÀ

conoscenze	abilità	competenze
Conoscere le caratteristiche del protocollo SNMP.	Saper gestire una rete utilizzando protocolli standard.	Scegliere gli strumenti più adeguati per mantenere sotto controllo la rete.
Conoscere come è strutturata una MIB.	Saper individuare le MIB standard e proprietarie di un apparato.	Mettere in atto procedure per rendere la rete affidabile.
Conoscere strumenti e procedure impiegati per la gestione delle reti e dei sistemi e per il troubleshooting.	Saper utilizzare tecniche di troubleshooting per l'individuazione di anomalie sulle reti e nei sistemi.	Configurare, installare e gestire sistemi di elaborazione dati e reti.

DDI+ Didattica Digitale Integrata Plus

FLIPPED CLASSROOM

A casa

- Leggi la Lezione 1 di questa Unità;
- leggi l'Esercizio commentato *Monitoraggio della rete*;
- ricerca in Internet due file che riportino la documentazione di rete (per esempio la «Documentazione di fine lavori rete in fibra ottica di Lepida spa»).

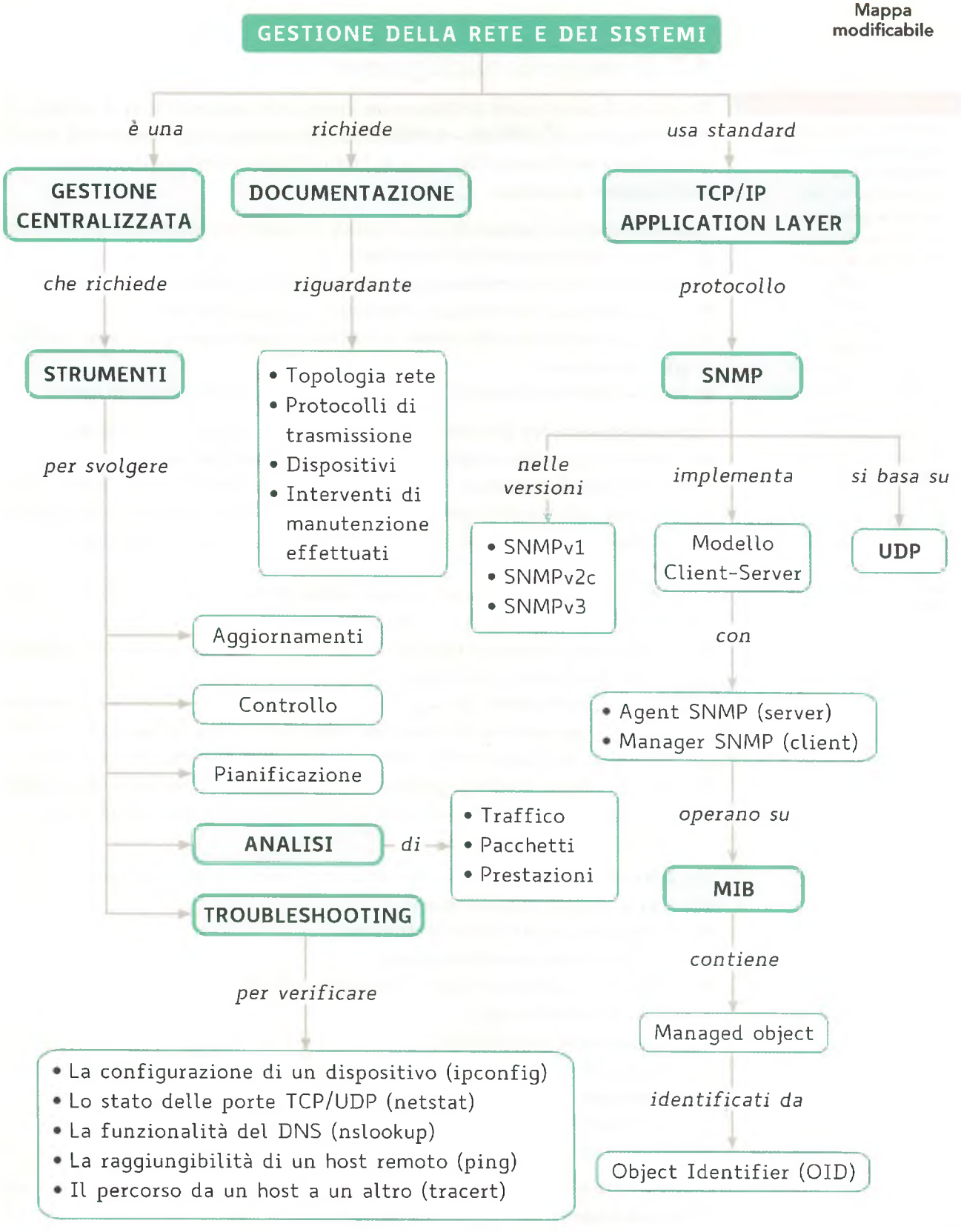
In classe

- Confrontate i risultati trovati;
- scegliete dei criteri di valutazione per la documentazione (come completezza, chiarezza, reperibilità, ecc.);
- stilate una classifica delle documentazioni trovate.

MAPPA CONCETTUALE

DIDATTICA INCLUSIVA

Mappa modificabile



1 LA GESTIONE DELLE RETI

1.1 Il network management

IN ENGLISH PLEASE

«Network management includes the deployment, integration and coordination of the hardware, software, and human elements to monitor, test, poll, configure, analyze, evaluate, and control the network and element resources to meet the real-time, operational performance and Quality of Service requirements at a reasonable cost.»
T. Saydam and T. Magedanz, "From Networks and Network Management into Service and Service Management" Journal of Networks and System Management, Dec. 1996.

Da quanto finora studiato è chiaramente emerso che una rete è fatta di molte parti complesse, pezzi di hardware e software che interagiscono: dai collegamenti, switch, router, host e altri apparati fisici ai molti protocolli che controllano e coordinano l'attività di questi dispositivi.

Quando si mettono insieme decine, centinaia di queste componenti per formare una rete non c'è da sorprendersi del fatto che:
- ogni tanto qualche componente non funzioni correttamente;
- alcuni apparati o host non siano configurati in modo adeguato;
- ci siano risorse di rete sottoposte a un utilizzo troppo intenso con conseguenti degradi prestazionali;
- qualche elemento di rete subisca guasti (per esempio la rottura di un cavo).

L'**amministratore** che deve mantenere in funzione la rete (up and running) deve essere in grado di gestire, o meglio ancora prevenire, questi problemi.
Se la rete è fatta di migliaia di componenti sparse a livello geografico (WAN), l'amministratore necessita di strumenti che lo aiutino nel suo compito (network management tools). Anche le reti di modeste dimensioni sono entità complesse che cambiano continuamente.
La sfida per l'amministratore o, più in generale, per il gruppo che si occupa dell'Information Technology di un'azienda è avere tutti gli strumenti necessari per identificare situazioni critiche e decidere se intervenire prima che si generi un malfunzionamento o un guasto.
Per esempio, supponiamo che uno strumento rilevi che un server sta lavorando al limite della sua potenza. Se questo accade solo la mattina, quando tutti i suoi utenti effettuano il login, è lecito pensare di non intraprendere alcuna azione immediata. Se, invece, il server è sovraccarico per la maggior parte del tempo, allora la situazione deve essere esaminata con attenzione in quanto il suo funzionamento è a rischio.

Con **network management** si individua un insieme di attività da svolgere per la gestione di una rete di comunicazione:
- pianificazione di rete (network planning);
- allocazione delle risorse (allocating);
- trattamento privilegiato di alcune applicazioni (QoS);
- realizzazione (deploying);
- coordinamento (coordinating);
- gestione della banda (bandwidth management);
- monitoraggio delle risorse di rete (monitoring);
- aggiornamento del firmware o del software (upgrading);
- distribuzione delle chiavi di crittografia (cryptographic key distribution).

Le tecniche di network management variano a seconda della dimensione della rete o della sua importanza.

Su reti di grandi dimensioni, per esempio, gli amministratori usano applicazioni che effettuano un controllo continuo dei dispositivi e delle connessioni per verificarne il corretto funzionamento. Se un device non risponde oppure la risposta arriva con troppo ritardo, l'applicazione automaticamente segnala l'anomalia, solitamente con un cambiamento di colore sull'interfaccia grafica e un messaggio testuale.
Su reti piccole, invece, l'impiego di simili applicazioni e un'attività di analisi così approfondita non sono economicamente sostenibili, quindi tipicamente si utilizzano applicazioni open source che periodicamente testano i dispositivi e le connessioni per stabilire se sono funzionanti o meno, senza pretese di controllo delle prestazioni.
Dall'elenco riportato in precedenza, si evince che con network management non si identificano solo le attività legate alla rilevazione e alla risoluzione di anomalie (troubleshooting), ma anche quelle legate all'operatività della rete. Per esempio, se analizzando le statistiche di utilizzo della rete si rileva che un router è particolarmente lento e corre il rischio di essere congestionato dal traffico, l'amministratore può intervenire su CPU e RAM oppure può sostituirlo con un router di maggiore capacità, il tutto prima che gli utenti della rete sperimentino dei rallentamenti o perdite di pacchetti.

Una buona pianificazione e gestione della rete consente di ridurre i costi aziendali; una rete non funzionante per un certo periodo di tempo (network downtime) per gli utenti si traduce spesso nell'impossibilità di svolgere il proprio lavoro, con ripercussioni sul business aziendale.
Comunque, prima di intervenire sulla rete o anche solo di effettuare delle previsioni sul suo stato, è importante che l'amministratore conosca bene la sua struttura fisica e logica e come funziona in condizioni normali. Da qui l'importanza della documentazione.

IN ENGLISH PLEASE

Standard organizations have identified five functional areas for network management (**FCAPS**):
F: Fault management
C: Configuration management
A: Accounting management
P: Performance management
S: Security management

1.2 La documentazione di rete

Un'operazione molto utile è disegnare schemi della rete per rappresentare graficamente i dispositivi e le connessioni esistenti tra loro. La FIGURA 1 è un esempio di diagramma di una complessa rete aziendale, con una sede centrale e succursali remote (branch). Non si ha qui la pretesa di descrivere nei dettagli tutte le componenti; lo scopo è mostrare come documentare ad alto livello un'architettura complessa, sapendo che ogni parte dovrà poi essere dettagliata indicando la tipologia di device (produttore, modello, ecc.) e la sua configurazione.

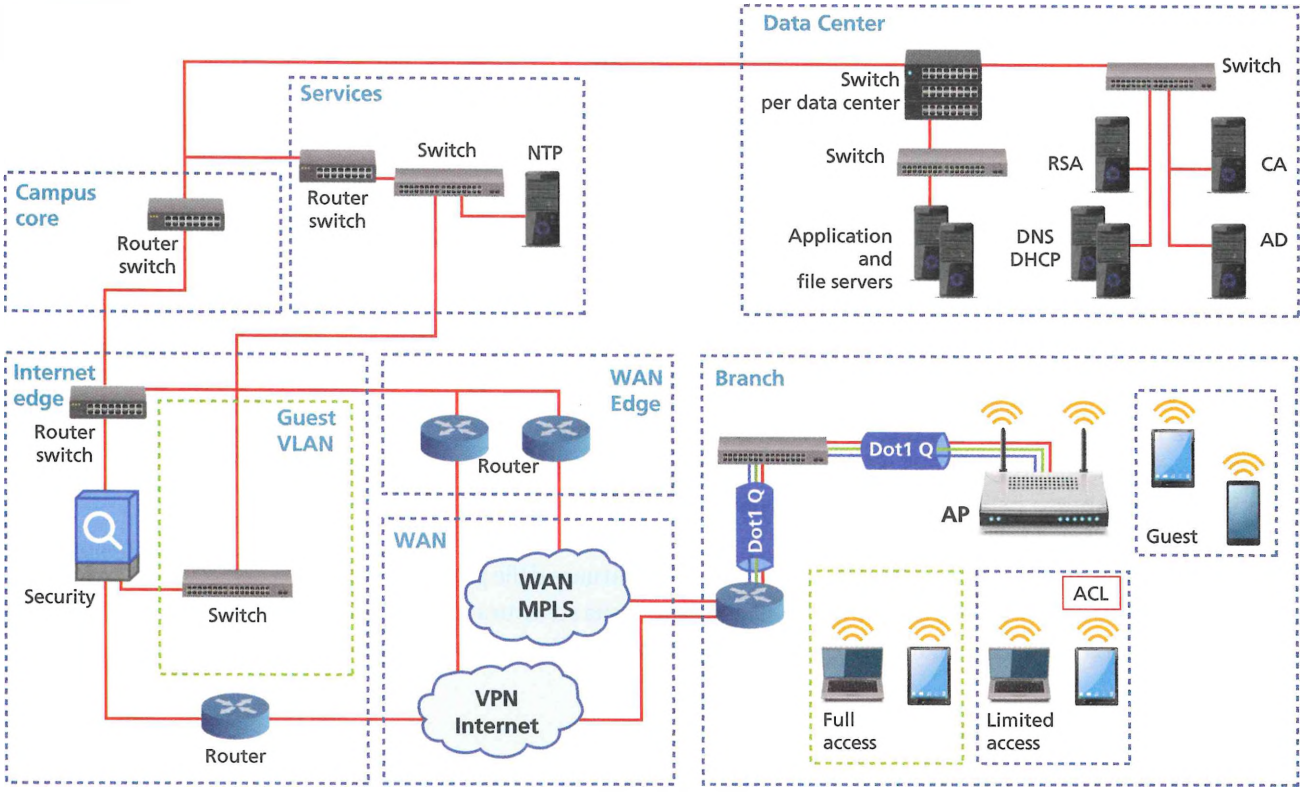
Un'adeguata gestione della rete richiede che un amministratore conosca e mantenga aggiornate alcune importanti informazioni su di essa, quali:

- **topologia fisica**: quali topologie sono usate nella rete (a bus, a stella, a stella gerarchica, ecc.)? Quali mezzi trasmissivi sono usati? Come è stato effettuato il cablaggio?
- **metodo d'accesso al mezzo trasmissivo**: quale standard è utilizzato per la gestione dell'accesso (802.3, 802.5. 802.11, ecc.)? Quale velocità di trasmissione fornisce?
- **protocolli**: quali protocolli sono usati dai server, dai router, ecc.?
- **dispositivi**: quali tipi di dispositivi sono presenti in rete e in quale numero? Dove sono collocati fisicamente? Qual è il produttore, il modello e il numero di serie?
- **sistemi operativi**: quali sistemi operativi sono installati sui computer? Quali sugli apparati di rete? Qual è la versione di firmware che ciascun dispositivo utilizza?
- **applicazioni**: quali applicazioni sono usate dai client e dai server? Dove sono memorizzate (sulla macchina o in modo centralizzato)? Qual è la loro versione (release)?

Con quale frequenza il produttore del software rilascia nuove release, patch, aggiornamenti e alert sulla sicurezza?

- **configurazioni**: come sono configurati i sistemi operativi e le applicazioni sui server, desktop e apparati di rete? Qual è la configurazione hardware di queste macchine?

FIGURA 1 Esempio di diagramma di rete aziendale



- **Router:** apparati che forniscono la connettività alla rete WAN
- **Switch:** apparati che forniscono l'accesso cablato (wired) alla rete locale
- **Router switch:** apparati con funzioni di instradamento a livello Data Link e Network
- **NTP server:** Network Time Protocol server, sincronizza gli orologi dei computer all'interno della rete
- **RSA server:** agisce come server di autenticazione dei client che si connettono alla rete
- **CA server:** Certification Authority server, gestisce i certificati
- **AD server:** Microsoft Active Directory server
- **Security:** su questo apparato sono implementate funzionalità di sicurezza (firewall, intrusion prevention, ecc.)
- **AP:** Access Point, fornisce la connettività Wi-Fi, gestisce le richieste di autenticazione, e può convogliare su tunnel il traffico verso la rete aziendale (campus) o effettuare lo switching del traffico locale nella sede remota (branch)

Certamente recuperare tutte queste informazioni richiede tempo, però è assolutamente indispensabile; per questo, la documentazione andrebbe aggiornata man mano che si inseriscono i dispositivi in rete.
Una volta che le informazioni sono state raccolte è necessario organizzarle in modo che possano essere facilmente recuperate e aggiornate; tipicamente si usano strumenti come i database, ai quali accede tutto il personale che amministra la rete.

1.3 Gli strumenti per la gestione della rete

Al fine di agevolare lo svolgimento delle numerose e complesse attività di network management, negli anni sono stati sviluppati dei **network management tools**, strumenti che permettono di eseguire funzioni di gestione, quali:

- il monitoring dei livelli di traffico nella rete;

- l'individuazione di punti di congestione (bottleneck);
- il controllo sull'utilizzo del software.

Questi tool permettono una supervisione di tutta la rete, dai router ai desktop. Solitamente forniscono una rappresentazione grafica della rete, con varie icone e colori per indicare lo stato di ciascun device.
Si tratta di applicazioni software altamente configurabili, che si adattano a qualunque ambiente di rete. Per contro sono solitamente molto costosi e richiedono una procedura di personalizzazione (customizing) non semplice.

Gli strumenti per la gestione di reti e sistemi sono moltissimi e possono essere grossolanamente suddivisi in due gruppi:

1. strumenti sviluppati dai **produttori di apparati** di rete per la gestione dei propri dispositivi;
2. strumenti sviluppati allo scopo di gestire reti formate da **apparati eterogenei** (non di un singolo produttore).

Gli strumenti del primo gruppo vengono anche detti **element manager** in quanto permettono di svolgere operazioni di gestione sui dispositivi di un certo produttore, per esempio:

- Cisco Prime Infrastructure
- Avaya Unified Communication Management

Esempi di prodotti appartenenti al secondo gruppo sono:

- HPE Intelligent Management Center
- CA Unified Infrastructure Management
- Solarwinds NPM

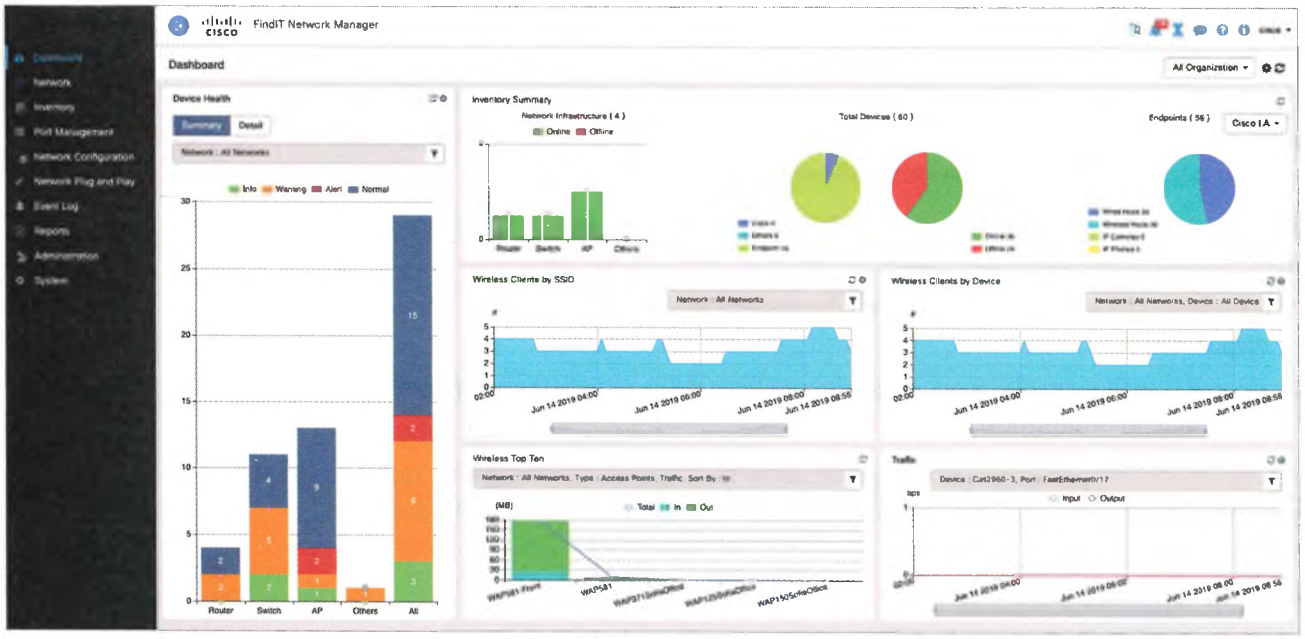
L'impiego di tool per la gestione degli apparati di uno specifico produttore consente di gestire molto bene i device e la rete di cui fanno parte. Se, però, si prevede di acquisire in futuro anche apparati di altri costruttori, difficilmente si riuscirà ad avere una visione unitaria della rete. Alcuni strumenti offrono la possibilità di gestire anche apparati dei loro concorrenti, ma in modo poco approfondito, spesso limitato a una supervisione del funzionamento degli apparati senza funzionalità più specifiche, quali, per esempio, la configurazione.
Spesso gli strumenti di gestione di tipo proprietario si compongono di due parti: una postazione centrale che offre un'interfaccia grafica all'amministratore con la visione di tutta la rete e un'applicazione che viene installata sui dispositivi da gestire. Quest'ultima dialoga con la postazione centrale per attività di monitoring e configurazione del dispositivo su cui è installata. Un esempio di strumento di questo tipo è **Cisco FindIT Network Manager**, rivolto alle piccole e medie imprese per la gestione di switch, router e access point wireless.

Si presenta con due applicazioni:

- **Probe**: si installa in ogni LAN di cui si compone la rete aziendale e svolge il compito di individuare in automatico i dispositivi presenti nella rete locale e di prenderli in gestione;
- **Manager**: raccoglie i dati e gli allarmi provenienti dalle varie Probe, li elabora e li visualizza sull'interfaccia grafica.

La FIGURA 2 mostra la tipica dashboard dell'applicazione Manager, che presenta graficamente informazioni sui vari dispositivi, segnalando con colori diversi gli eventi ricevuti dalle Probe, e sul traffico generato su un singolo dispositivo.

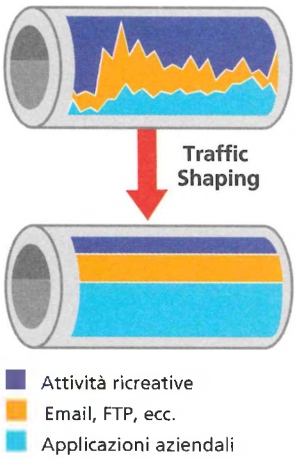
FIGURA 2 La dashboard di Cisco FindIT Network Manager



IL TRAFFIC SHAPING

Il termine **traffic shaping** identifica una tecnica di gestione delle prestazioni delle reti che gestiscono volumi elevati di traffico. Essa consiste nel manipolare certe caratteristiche dei pacchetti, flussi di dati o connessioni, al fine di gestire la quantità di traffico che attraversa l'intera rete o anche una sola interfaccia.
Il traffic shaping è utile quando si vuole gestire la QoS in rete, garantendo la consegna puntuale del traffico più importante e, nel contempo, offrendo le migliori prestazioni possibili ai restanti utenti (Best effort). Le tecniche implementate possono infatti riguardare il rallentamento del traffico meno critico, l'aumento della priorità del traffico più importante e la limitazione della quantità di traffico che attraversa un'interfaccia in uno specifico intervallo di tempo.

FIGURA 3 Effetto dell'applicazione di tecniche di traffic shaping



La FIGURA 3 delinea gli effetti dell'applicazione delle tecniche di traffic shaping alla connessione Internet di un'azienda: limitando il traffico legato ad attività ricreative, si dà maggior banda al traffico generato dalle applicazioni legate al business aziendale. Tipicamente l'amministratore di rete definisce un'ampiezza di banda minima, una massima e una garantita, da allocare a ciascun tipo di traffico, poi stabilisce le policy: per esempio al traffico voce viene allocata sempre la banda garantita, così da non perdere in qualità durante una chiamata vocale.

FISSA LE CONOSCENZE

- Qual è il ruolo dell'amministratore nella gestione della rete?
- Descrivi quali informazioni sono utili al lavoro dell'amministratore di rete.
- Quali sono le tipologie di strumenti per il network management?
- Che cosa si intende con traffic shaping?

Esercizio commentato Monitoraggio della rete

2 LA GESTIONE DI RETI TCP/IP

2.1 La gestione a livello Application

All'inizio della diffusione delle reti a commutazione di pacchetto, la gestione avveniva a livello Data Link e consentiva il controllo dei dispositivi di commutazione presenti nella rete.
Gli strumenti di gestione usati erano quindi parte dei protocolli di basso livello e consentivano di controllare un nodo di commutazione anche quando non funzionavano più i protocolli dei livelli alti, per esempio quelli del livello Application.
Una rete geografica TCP/IP (una **Internetwork**), essendo composta da più reti fisiche interconnesse dai router IP, non ha un singolo protocollo Data Link. Gli apparati da gestire in queste reti, infatti, sono di vario tipo e utilizzano differenti protocolli di comunicazione. Inoltre, il computer su cui risiede il software di gestione potrebbe non far parte della stessa rete fisica a cui appartengono gli apparati da controllare. Quindi, lo strumento di gestione deve necessariamente comunicare con i dispositivi tramite protocolli che forniscano una connettività end-to-end attraverso Internet.

> Il protocollo per la gestione di una Internetwork TCP/IP è definito a **livello Application** e comunica usando i protocolli del livello Transport, così da essere svincolato dal tipo di rete fisica usata e dai protocolli di routing utilizzati.

Progettare software di gestione a livello Application presenta diversi **vantaggi**:

- i protocolli possono essere definiti senza tenere conto di come il computer si connette fisicamente alla rete, quindi si può usare lo stesso insieme di protocolli per tutti i tipi di rete;
- l'uniformità di gestione consente all'amministratore di lavorare sui router della rete con lo stesso insieme di comandi;
- l'amministratore può controllare i dispositivi senza avere collegamenti diretti a ognuno di essi, come avveniva con la gestione implementata al livello Data Link. Infatti il software di gestione usa il protocollo IP per la comunicazione con gli apparati, ovunque essi si trovino su Internet.

Il software di gestione a livello Application comporta anche alcuni **svantaggi**:

- l'amministratore potrebbe non riuscire a collegarsi a un router su cui deve intervenire se qualcosa nel software applicativo o di trasporto non funziona correttamente (problema che non esisteva quando il protocollo di gestione era definito a livello Data Link);
- se il sistema operativo di un router ha un malfunzionamento, l'apparato non potrà più essere gestito in quanto l'applicazione di gestione non sarà più funzionante, anche se il router potrebbe ancora instradare i pacchetti.

2.2 Il modello architetturale

Il modello utilizzato per realizzare la gestione della rete è del tipo **Client-Server**, come per molte altre applicazioni TCP/IP. I ruoli, però, qui sono invertiti, perché il

software del client si trova sulla stazione dell'amministratore della rete, mentre ogni host gestito (router, switch, server, workstation, ecc.) esegue un programma server.

> Il software del server è detto **Management Agent (MA)**, o **agent**, mentre il software dell'amministratore è detto **Management Client (MC)**, o **manager**.

In FIGURA 4 si mostra un esempio di gestione di una rete in cui la stazione manager esegue il software di MC, il quale comunica con il software di MA che si trova sui dispositivi gestiti (**managed device**) della rete. I dispositivi che non hanno installato l'agent non potranno essere gestiti (**unmanaged device**).

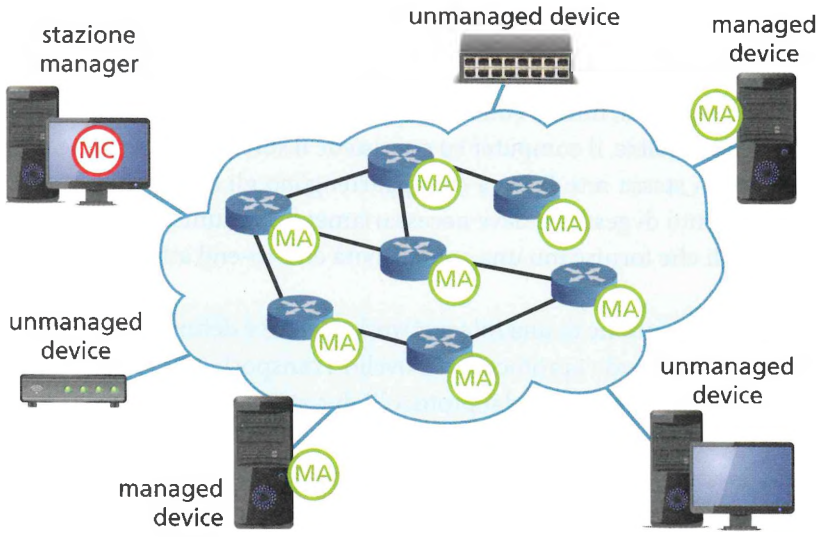


FIGURA 4 Esempio di gestione di rete con MC e MA

Il gestore attiva l'MC sul suo computer e specifica l'agent con cui vuole comunicare. Una volta instaurata la connessione, il manager invia all'agent richieste di informazioni oppure comandi per effettuare modifiche sul dispositivo.

Il software di gestione della Internetwork usa un meccanismo di autenticazione per garantire l'accesso o il controllo del dispositivo solo ai gestori autorizzati.
Esistono vari livelli di privilegi, così da permettere, per esempio, a molti gestori di ottenere informazioni su un certo router, ma a uno solo di controllarlo intervenendo anche in modifica.

Per capire le problematiche della gestione della rete e come queste vengano affrontate, può essere utile fare un parallelo con quanto avviene in un'azienda con filiali sparse su un territorio più o meno vasto. L'amministratore dell'azienda, dalla sede centrale, deve controllare che tutte le filiali operino correttamente, quindi periodicamente chiederà al responsabile di ciascuna di esse un report sull'attività svolta, con indicazioni sulla produttività, sul budget, ecc.
Da parte sua, il responsabile di una filiale avviserà in modo spontaneo l'amministratore quando sorge un problema che richiede la sua attenzione. Questa conversazione all'inizio si basa sulla raccolta di informazioni utili a chiarire la situazione, e si può tradurre poi in azioni da eseguire nella filiale.
La TABELLA 1 mostra il parallelo tra questa realtà umana e quella delle reti di comunicazione, indicando gli strumenti che sono stati definiti per la gestione delle reti TCP/IP.

Gestione di un'azienda reale	Gestione di reti di comunicazione	Standard
Amministratore centrale che controlla tutta l'azienda.	Network Management Station (applicazione centrale tramite la quale il gestore controlla la rete).	Management Client (manager).
Sedi remote dell'azienda (filiali).	Managed devices (apparati di rete, computer, stampanti, ecc.).	Management Server (agent).
Comunicazione di report periodici tramite richiesta.	Protocollo di comunicazione da manager a managed device (manager invia richieste al device).	Protocollo SNMP: messaggi Get e Set.
Segnalazioni di problemi inviate dalle filiali.	Segnalazione di un evento inaspettato da parte del managed device al manager (non è la risposta a una richiesta del manager).	Protocollo SNMP: messaggio Trap.
Dati quantitativi da acquisire/inviare (limiti di budget, misure sulla produttività, ecc.).	I dati quantitativi da acquisire/inviare (stato on/off del device, traffico in/out su ciascuna interfaccia di un router, percentuale di errori, ecc.).	Management Information Base (MIB).

TABELLA 1 Analogia tra la gestione di un'azienda e la gestione di una rete

2.3 Gli standard

L'organismo preposto alla definizione degli standard per Internet è IETF, che ha definito un #framework per la gestione delle reti TCP/IP il quale si compone di 3 parti:

1. il **protocollo SNMP** (**Simple Network Management Protocol**): usato per la comunicazione tra manager e agent;
2. gli **oggetti della MIB** (**Management Information Base**): informazioni di gestione rappresentate come una collezione di managed object che insieme formano un database virtuale a cui è stato dato il nome di MIB.
   Un managed object può essere:
   – un contatore, per esempio il numero di pacchetti IP scartati su un'interfaccia di un router;
   – un testo descrittivo, per esempio il sistema operativo installato su un host;
   – un'informazione di stato, per esempio se un'interfaccia del router è abilitata o meno (stato on/off);
3. un linguaggio per la definizione dei dati, detto **SMI** (**Structure of Management Information**), che definisce i **tipi di dati** e le **regole** per scrivere le informazioni di gestione; gli oggetti della MIB sono specificati usando questo linguaggio.

Il framework così definito ha il pregio di essere modulare: il protocollo SNMP è indipendente dalla definizione di MIB; MIB e SMI sono indipendenti da SNMP.
Mantenere la definizione di MIB indipendente dal protocollo per la gestione di rete presenta alcuni vantaggi sia per i produttori di apparati sia per i gestori di rete:

- un produttore può includere il software SNMP Agent nei suoi dispositivi, sapendo che continuerà a rispettare lo standard anche dopo che saranno definiti nuovi elementi nella MIB;
- un gestore può utilizzare lo stesso software client di gestione di rete, SNMP Manager, per gestire dispositivi che usano versioni diverse di MIB.

#techwords

Framework
È una struttura, letteralmente intelaiatura, che offre un insieme di software e librerie a supporto per lo sviluppo di un'applicazione.

FISSA LE CONOSCENZE

- Perché è stato scelto di definire i protocolli per la gestione della rete a livello Application?
- Descrivi le entità Management Agent e Management Client.
- Quali parti compongono il framework per la gestione delle reti TCP/IP?
- Spiega i vantaggi della struttura modulare definita per la gestione delle reti TCP/IP.

3 L'ORGANIZZAZIONE DEI DATI DA GESTIRE

3.1 Come scrivere i dati

I dati che l'agent deve fornire al manager, per la gestione dell'host in cui è installato, devono essere definiti in modo rigoroso e non ambiguo, sia sintatticamente sia semanticamente.
Pertanto IETF ha specificato un linguaggio di definizione da usare per la scrittura di MIB, denominato **SMI** (Structure of Management Information).
Esistono due standard: **SMIv1** (RFC 1155) usato con SNMPv1 e **SMIv2** (RFC 2578) usato con SNMPv2 e SNMPv3.

Per vedere alcune delle numerose **MIB** definite, si può visitare il sito *www.mibdepot.com.*

SMI si basa su un altro linguaggio di definizione specificato in ambito ISO: l'**ASN.1** (**Abstract Syntax Notation One**), rispetto al quale, però, sono stati introdotti dei tipi di dati specifici per SNMP.
Tra questi troviamo, per esempio, il tipo IPaddress (32-bit per IPv4) e i contatori Counters32 (da 0 a $2^{32} - 1$) e Counters64 (da 0 a $2^{64} - 1$).

esempio

Definizione dell'oggetto sysDescr con il linguaggio SMI
L'oggetto sysDescr è relativo alla descrizione del sistema in uso sul dispositivo che si vuol gestire e in SMI è definito con la seguente sintassi:

```
mib-2(1).system(1).sysDescr(1) :
– sysDescr OBJECT-TYPE
SYNTAX DisplayString (SIZE (0..255))
ACCESS read-only
STATUS mandatory
DESCRIPTION "A textual description of the entity. This value should include the full
name and version identification of the systems' hardware type ...".
::= { system 1 }
```

- La prima riga si riferisce all'OBJECT IDENTIFIER = 1.3.6.1.2.1.1.1 di sysDescr ottenuto percorrendo l'albero dei nomi (Object Identifier Namespace, descritto nel prossimo paragrafo); si indicano solo le etichette del sotto-albero MIB-2 (1.1.1).
- Il costrutto OBJECT-TYPE è usato per definire il tipo di dato, lo stato e la semantica dell'oggetto (managed object) che sarà contenuto nella MIB.
- SYNTAX specifica il tipo di dato associato all'oggetto e in questo caso indica che il valore assegnato a un'istanza dell'oggetto sysDescr sarà una stringa con dimensione massima di 255 byte.
- ACCESS identifica la modalità con cui si può accedere all'informazione contenuta nell'oggetto: in sola lettura, in scrittura, se può essere creato e se il dato può essere inviato in un messaggio. Quasi sempre gli oggetti sono definiti con accesso in sola lettura e su pochi è consentita anche la modifica.
- STATUS indica se la definizione dell'oggetto è valida (mandatory) o non più aggiornata (obsolete), quindi da non implementare, o non aggiornata ma implementabile (deprecated) per ragioni di interoperabilità con vecchie implementazioni.
- DESCRIPTION contiene la definizione dell'oggetto in forma testuale e fornisce le informazioni semantiche necessarie alla sua implementazione.

3.2 Il namespace

I nomi degli oggetti MIB sono presi dallo spazio degli identificatori di oggetti denominato **Object Identifier Namespace** (OID namespace), gestito da ISO e ITU.
Infatti, IETF ha deciso di non creare un nuovo namespace per identificare gli oggetti MIB, ma di adottare il framework già standardizzato da ISO.

> OID è un namespace **assoluto** (i nomi sono strutturati in modo da essere univoci) e **gerarchico** (l'autorità è suddivisa a ogni livello e singoli gruppi possono ottenerla per assegnare dei nomi senza dover consultare un'autorità centrale).

In FIGURA 5 si mostra la parte del namespace usata per assegnare un nome alle variabili MIB. Ogni elemento dell'albero ha un nome e un numero, così da essere identificabile in modo sintetico dalla sequenza di numeri partendo dalla radice.

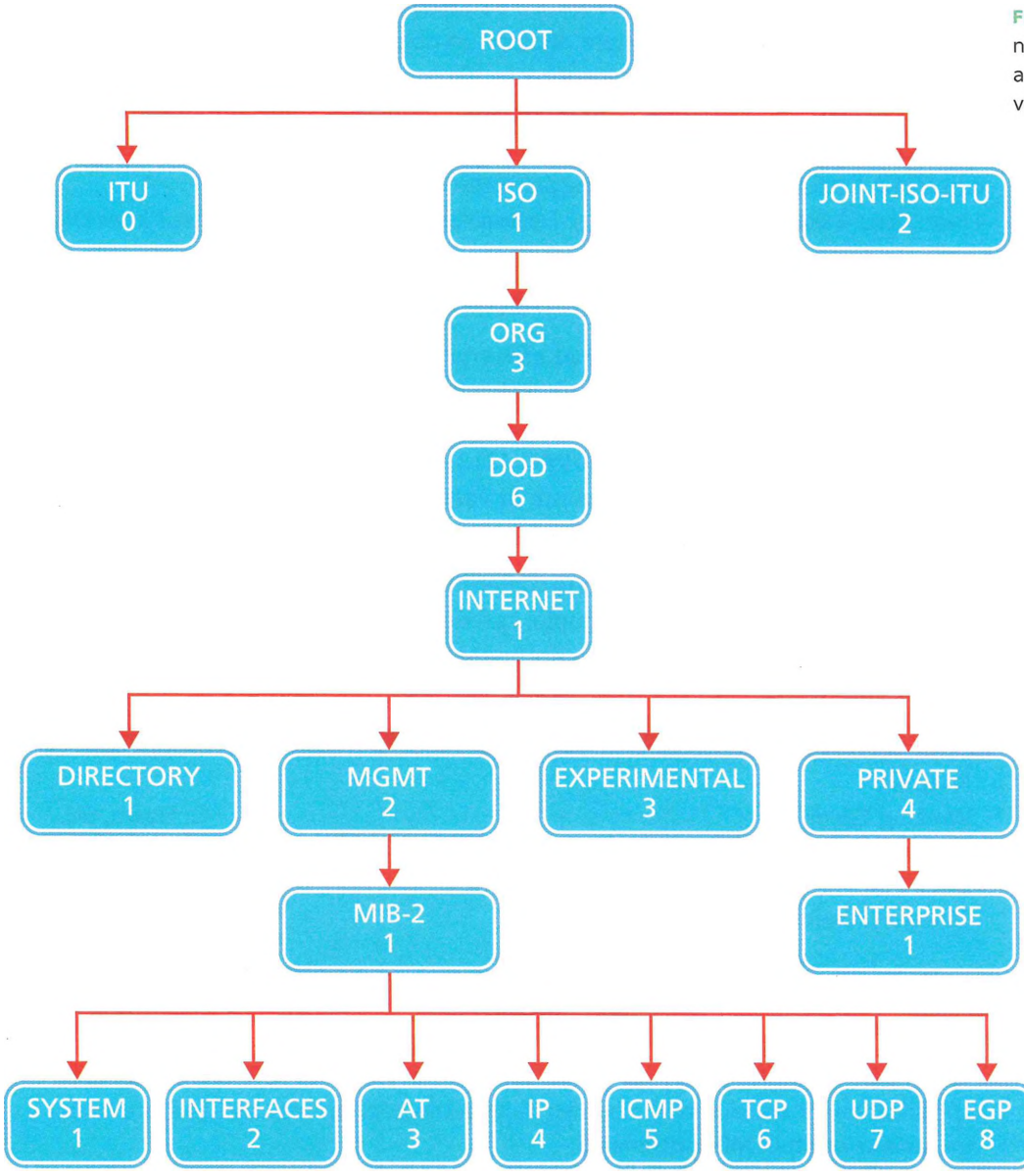


FIGURA 5 Parte del namespace usata per assegnare i nomi alle variabili MIB

L'object identifier **dod (1.3.6)** identifica il Dipartimento della Difesa degli Stati Uniti (US Department of Defense), presente nel namespace in quanto genitore di Internet. Infatti è stato definito un unico sottoalbero con radice dod che è, appunto, Internet (object identifier: 1.3.6.1).

esempio

Vediamo con qualche esempio come si compongono i nomi degli oggetti MIB:

- il sottoalbero di Internet specifico per il network management è identificato con l'etichetta **mgmt**, il suo OID si compone di tutti i numeri corrispondenti ai nodi dell'albero attraversati: partendo da ISO risulta OID = **1.3.6.1.2**. All'identificatore numerico corrisponde un identificatore testuale: **iso.org.dod.internet.mgmt**;
- l'oggetto **ip** si identifica con
  OID = **1.3.6.1.2.1.4** e **iso.org.dod.internet.mgmt.mib-2.ip**

Per consentire ai produttori di apparati o di software di definire MIB per la gestione dei loro prodotti, nell'albero della Figura 5 è stato specificato un apposito namespace **private** sotto Internet in cui è stato definito un object identifier **enterprise** sotto il quale sono inserite tutte le MIB vendor-specific.
Per esempio al vendor Cisco è stato assegnato il numero 9, viene quindi identificato con l'OID 1.3.6.1.4.1.9. La MIB relativa ai router Cisco della serie 4000 è identificata con l'OID 1.3.6.1.4.1.9.1.7, il cui nome per esteso è:
1 (iso). 3 (org). 6 (dod). 1 (internet). 4 (private). 1 (enterprises). 9 (cisco). 1 (ciscoProducts). 7 (cisco4000)

3.3 Management Information Base

Quando in ambito IETF si iniziò ad affrontare il problema della gestione della rete e dei suoi apparati, fu definito un unico documento (RFC 1066 del 1988) che specificava una singola MIB, molto estesa. Dopo la pubblicazione della seconda generazione, denominata **MIB-II** (RFC 1213 del 1991), IETF adottò un approccio diverso consentendo la definizione di varie MIB, una per ciascuna tipologia di dispositivo.

RFC 4181 è il documento di riferimento contenente le linee guida per scrivere una MIB. A questo fanno riferimento, per esempio, i produttori di apparati e sistemi, per la definizione di MIB specifiche per i loro prodotti hardware e software.

IN ENGLISH PLEASE

Network
Working Group — C. Heard, Ed.
Request for Comments: 4181 — September 2005
BCP: 111
Category: Best Current Practice

Guidelines for Authors and Reviewers of MIB Documents

Abstract

This memo provides guidelines for authors and reviewers of IETF standards-track specifications containing MIB modules. Applicable portions may be used as a basis for reviews of other MIB documents.

Nella TABELLA 2 sono elencati alcuni oggetti MIB associati ai protocolli TCP/IP. Alla maggior parte di essi viene assegnato un singolo valore numerico, però, possono essere presenti anche strutture più complesse; per esempio, la IpRoutingTable si riferisce a un'intera tabella di instradamento.

Oggetto MIB	Categoria	Descrizione
sysContact	system	Riferimenti della persona da contattare per quel dispositivo.
sysUpTime	system	Periodo di tempo trascorso dall'ultimo restart.
ifNumber	interfaces	Numero di interfacce di rete presenti sul dispositivo.
ipInReceives	ip	Numero di IP datagram ricevuti.
tcpMaxConn	tcp	Connessioni massime di TCP consentite.
tcpInSegs	tcp	Numero di segmenti TCP ricevuti.

TABELLA 2 Esempi di oggetti MIB di TCP/IP

È importante sottolineare che la MIB non è la base di dati vera e propria, le definizioni degli oggetti contenute nella MIB sono usate dalla stazione manager per recuperare le informazioni dall'agent.

I dati ricevuti dal manager sono coppie OID-valore e vengono memorizzati dal manager in un database reale denominato **MDB, Management DataBase** (FIGURA 6).

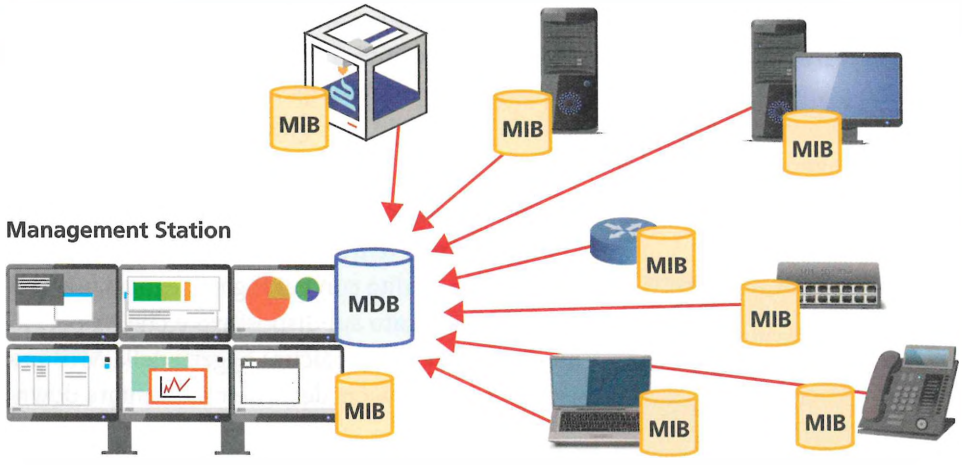


FIGURA 6 MIB e MDB della stazione di gestione

FISSA LE CONOSCENZE

- Spiega il ruolo di SMI nella gestione delle reti TCP/IP.
- Descrivi le caratteristiche e la struttura dell'Object Identifier Namespace.
- Quale oggetto della MIB identifica il numero 1.3.6.1.2.1.6?
- Scrivi per esteso il nome corrispondente all'identificatore numerico 1.3.6.1.2.1.4.

4 IL PROTOCOLLO SNMP

4.1 Le caratteristiche di SNMP

SNMP (Simple Network Management Protocol) è il protocollo usato per la comunicazione tra manager e agent per la gestione delle reti TCP/IP. La prima versione di questo protocollo è stata standardizzata da IETF nel 1990, successivamente sono state specificate altre due versioni SNMPv2c e SNMPv3 (TABELLA 3).

TABELLA 3 Le versioni del protocollo SNMP

Nome	RFC	Caratteristiche
SNMPv1	1157	È la prima versione dello standard, introduce il modello manager-agent e specifica i messaggi base: request, response e trap. La sicurezza è affidata a una password di accesso (community string), non crittografata.
SNMPv2c	1901	È la versione community-string-based di SNMPv2, che usa ancora lo stesso meccanismo di sicurezza di SNMPv1 e alcune evoluzioni specificate in SNMPv2, quali il nuovo messaggio get-bulk-request. È lo standard ancora oggi più diffuso, nonostante la nuova versione SNMPv3.
SNMPv3	3512 (informativo) e altri specifici	Il framework è stato completamente rivisto, introducendo il concetto di SNMP-entity al posto dei precedenti manager e agent. Sono stati introdotti meccanismi di sicurezza quali: autenticazione, criptazione e integrità del messaggio. Non sono state apportate modifiche alle operazioni che possono essere effettuate.

Il protocollo SNMP è usato per la comunicazione tra manager e agent, al fine di trasportare le informazioni MIB presenti sui dispositivi controllati dagli agent.
L'uso più comune di SNMP è nella modalità richiesta-risposta: il manager invia una richiesta all'agent (**get** o **set**), la quale si traduce in una query sulla MIB; l'agent risponde inviando i dati richiesti.

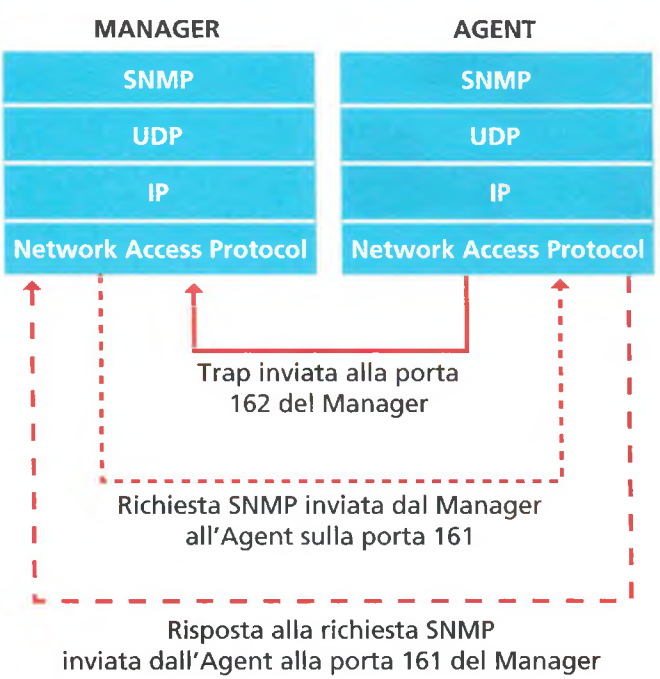


FIGURA 7 I protocolli dello stack TCP/IP usati per SNMP

Un secondo utilizzo è per inviare un messaggio in modo spontaneo dall'agent verso il manager (**trap**). Questa è la modalità con cui l'agent segnala un evento che si è verificato sul dispositivo e che ha portato a modificare i valori di alcuni oggetti della MIB (per esempio, un'interfaccia del router è diventata down).

La FIGURA 7 mostra il modello di comunicazione usato tra manager e agent.

SNMP si basa su **UDP** come protocollo di trasporto e utilizza le porte:

- 161 per inviare/ricevere i messaggi SNMP;
- 162 per inviare/ricevere le trap.

La scelta di UDP come protocollo di trasporto è dovuta alla sua natura connectionless che rende più veloce la comunicazione tra manager e agent. Dal momento che UDP non è un protocollo affidabile, è la stessa applicazione SNMP a verificare che non siano stati persi alcuni datagram.
Quando il manager invia una richiesta all'agent imposta un timer per l'attesa della risposta, allo scadere del quale la richiesta è ritrasmessa.

4.2 Il formato dei messaggi SNMP

Nella TABELLA 4 sono elencati i 7 tipi di messaggi previsti nello standard SNMPv2c.

Messaggio	Descrizione
get-request	Estrae il valore dall'istanza dell'oggetto MIB presente sul device.
get-next-request	Estrae il valore dell'istanza successiva dell'oggetto MIB. Usata per leggere liste o tabelle.
get-bulk-request	Estrae una grande quantità di dati (per esempio una tabella).
set-request	Memorizza un valore in una o più istanze di un oggetto MIB presente sul device.
inform-request	Viene usato tra manager e manager per trasferire le informazioni su device gestiti non direttamente (un manager assume il ruolo di proxy).
response	È la risposta inviata dall'agent a una qualsiasi delle richieste precedenti.
snmp-trap	È il messaggio inviato in modo spontaneo dall'agent a seguito del verificarsi di un evento locale e non a seguito della ricezione di una richiesta.
report	Non è definito.

TABELLA 4 I messaggi di SNMPv2c

Nel messaggio di richiesta, il manager specifica l'OID degli oggetti MIB dei quali vuole ricevere il valore. Come descritto nella Lezione 3, la MIB contiene la definizione degli oggetti, scritta secondo le regole SMI; nel momento in cui si deve assegnare un valore all'oggetto, è necessario crearne un'istanza e a questa sarà assegnato il valore (nei documenti spesso le istanze degli oggetti MIB sono dette variabili MIB).
La gestione delle reti con SNMP è quindi realizzata secondo i principi della **progettazione e programmazione object oriented**.

4.3 La sicurezza in SNMP

SNMPv1 e SNMPv2c usano la nozione di community per stabilire una **connessione** fidata tra manager e agent. La community è usata in modo simile a una normale password di accesso.
Un agent è configurato con 3 **community name**:

- **read-only**
- **read-write**
- **trap**

Ognuna di queste controlla diversi tipi di attività: per esempio la community *read-only* permette al manager di sapere il numero di pacchetti che è stato trasferito attraverso le interfacce di un router, ma non consente di azzerare questi contatori. Infatti quest'operazione può essere svolta solo usando la community *read-write*. La community *trap* permette al manager di ricevere trap dall'agent.
La maggior parte dei produttori di apparati configura delle **community string** di default; tipicamente si usano: public per read-only e private per read-write.

#prendinota

Per minimizzare il rischio di attacco ai sistemi della rete tramite SNMP si può configurare il firewall in modo da consentire il transito di datagram UDP solo da un elenco di host conosciuti. Per esempio si permette traffico UDP sulla porta 161 solo se proviene da uno dei sistemi manager della rete. Analogamente, si permette traffico UDP sulla porta 162 solo se è generato da uno degli host della rete che si sta gestendo.

È quindi importante cambiare questi valori di default nel momento in cui si connette l'apparato alla rete. Nel Laboratorio online si descrive come farlo su apparati Cisco.

LABORATORIO ONLINE

CONFIGURARE SNMP SUI DEVICE

In questo Laboratorio si mostra come installare e configurare un SNMP Agent e un SNMP Manager su:
apparati di rete Cisco
computer Windows 10
computer Linux Ubuntu

Se un host ha un **accesso read-write** ai device della rete, può avere il controllo su di essi usando SNMP (per esempio può disattivare l'interfaccia di rete o modificare le routing table).

Un modo per proteggere le community string è usare una VPN (Virtual Private Network) e criptare tutto il traffico di rete. Un altro modo, valido per qualunque stringa usata come password, è cambiare frequentemente la community string (usando uno script se la rete è estesa).

Con **SNMPv3** sono stati introdotti meccanismi di sicurezza che hanno colmato le lacune delle precedenti versioni, migliorando anche la parte di amministrazione.

Non sono state apportate modifiche né al protocollo, né alle operazioni che possono essere effettuate, che restano quelle elencate nella Tabella 4.

In SNMPv3 è stata modificata la nomenclatura: pur identificando lo stesso software, infatti, sono stati abbandonati i termini manager e agent in favore di un unico nome: **SNMP entity**. Questa entità può assumere un ruolo di manager o di agent a seconda delle funzioni che svolge. Come mostrato in FIGURA 8, ogni entità contiene un SNMP engine e una o più applicazioni.

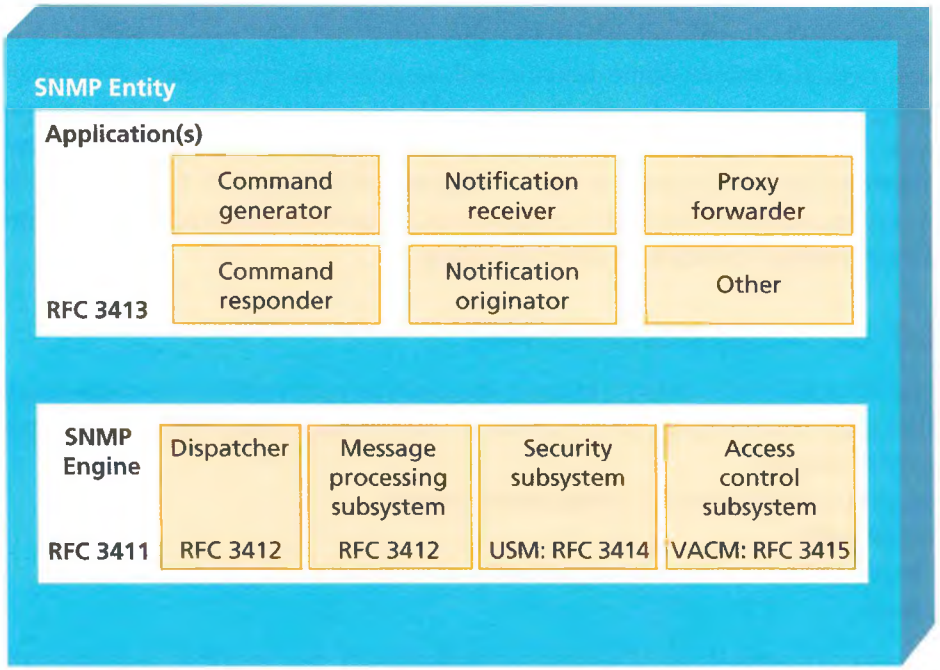


FIGURA 8 SNMP entity e relativi documenti di specifica (RFC)

La nuova architettura definita in SNMPv3 aiuta a separare in modo chiaro le diverse parti del sistema SNMP così da rendere possibile una sua implementazione applicando tecniche di sicurezza. Infatti SNMPv3 supporta:

- l'**autenticazione dei messaggi** (security subsystem): per assicurare che le istruzioni da impartire al device (agent) abbiano origine da un gestore (manager) autorizzato;

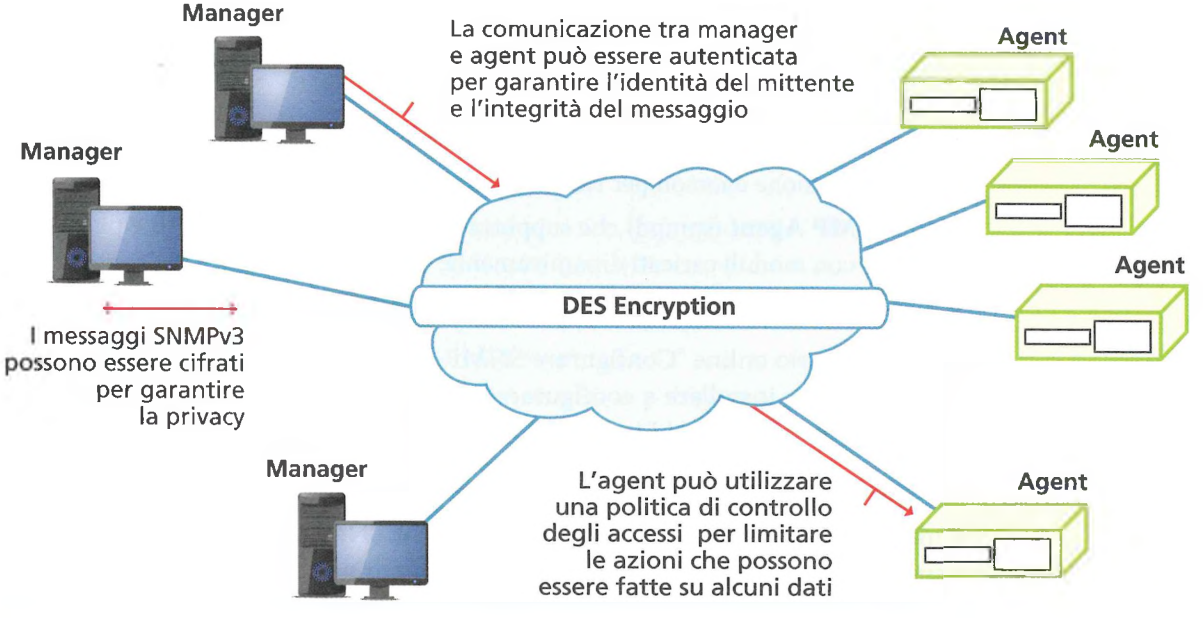
- la **crittografia** (security subsystem): affinché nessuno possa leggere i messaggi mentre sono in transito tra l'host del manager e il dispositivo gestito;
- l'**integrità del messaggio** (security subsystem): per garantire che il contenuto di un pacchetto non sia stato modificato o danneggiato durante la trasmissione;
- il **controllo degli accessi** (access control subsystem): basato sul concetto di *view* (vista) per garantire che solo i manager autorizzati abbiano accesso a determinati oggetti delle MIB dell'agent.

Lo standard SNMPv3 definisce un modello per ciascuno dei due sistemi di sicurezza (security subsystem e access control subsystem), lasciando aperta la possibilità di implementarne altri.

I modelli definiti in SNMPv3 per la sicurezza sono:
- **USM** (User-based Security Model): è usato per autenticare una SNMP entity e fornisce servizi di crittografia (encryption) per rendere sicure le comunicazioni tra manager e agent;
- **VACM** (View-based Access Control Model): è usato per configurare i diritti di accesso a un gruppo di entity (manager) tramite la definizione di viste che permettono di filtrare l'accesso agli oggetti delle MIB.

La FIGURA 9 evidenzia le caratteristiche di SNMPv3 relative alla sicurezza.

FIGURA 9 La sicurezza in SNMPv3



FISSA LE CONOSCENZE

- Quali sono le versioni standardizzate di SNMP?
- Come viene usata l'operazione trap?
- Descrivi il formato dei messaggi SNMP.
- Quali meccanismi di sicurezza offrono i subsystem security e access control di SNMPv3?

5 APPLICAZIONI PER IL MONITORING CON SNMP

Nella prima Lezione si è accennato alla necessità, per un amministratore di rete, di mantenere la rete e i sistemi **up and running**, utilizzando applicazioni per monitoraggio, analisi, configurazione, testing e controllo dell'operatività della rete e delle sue performance. Oltre alle applicazioni proprietarie, sviluppate dai produttori per meglio gestire i propri dispositivi, esistono software per il monitoraggio di ambienti eterogenei, utili per un controllo quanto più completo di tutta l'infrastruttura.
Vediamo alcuni esempi.

NET-SNMP

Si tratta di una suite di applicazioni open source, disponibile per Unix, Linux e Windows, scaricabile dal sito *sourceforge.net/projects/net-snmp*. Sul sito *www.net-snmp.org* si trovano anche informazioni sullo sviluppo del progetto.
La suite Net-SNMP comprende:

- **applicazioni** con un'interfaccia testuale che consentono di:
  - ottenere dati dal managed device utilizzando richieste semplici (snmpget, snmpgetnext) o multiple (snmpwalk, snmptable, snmpdelta);
  - manipolare dati di configurazione sul managed device (snmpset);
  - ottenere un insieme di dati dal managed device (snmpdf, snmpnetstat, snmpstatus);
  - convertire gli identificatori della MIB (MIB OID) dalla forma numerica a quella testuale e viceversa, visualizzando la struttura e il contenuto della MIB (snmptranslate);
- un **MIB browser** grafico che usa Tk/Perl (tkmib);
- un'applicazione daemon per ricevere le notifiche SNMP (snmptrapd);
- un **SNMP Agent** (snmpd) che supporta un elevato numero di MIB e può essere esteso con moduli caricati dinamicamente;
- una **libreria** per sviluppare nuove applicazioni SNMP che fornisce API in C e Perl.

Nel Laboratorio online "Configurare SNMP sui device" si è fatto uso delle librerie Net-SNMP per installare e configurare la parte client (SNMP Manager) e server (SNMP Agent) su sistemi Linux.

SNMP MIB BROWSER

È un'applicazione utile per monitorare dispositivi SNMP. È sviluppata in Java (contiene in bundle *Java Runtime Environment*, quindi non richiede di installare Java sulla macchina manager). Può essere installata sia su Windows sia su Linux. Non è open source, ma il tool è scaricabile gratuitamente dal sito *www.manageengine.com*.

Nagios®

NAGIOS

Nagios è un'applicazione open source per il monitoraggio di host, servizi e rete (c'è anche una versione a pagamento). Molto usata nei sistemi Linux, caratterizzata da un framework su cui si innestano moduli aggiuntivi (plugin ed extension) che consentono di realizzare soluzioni molto flessibili. Questa applicazione comporta però un carico di rete superiore a quello di altri prodotti e una modalità di gestione dei task che appesantisce il lavoro del server utilizzato per il monitoraggio.

ZABBIX

ZABBIX

È una soluzione open source per il monitoraggio delle reti. Si tratta di un software che monitora numerosi parametri di una rete e lo stato e l'integrità dei server. Le versioni più recenti supportano anche il monitoring di servizi in cloud, delle macchine virtuali e di varie applicazioni software.
Tutte le statistiche e i rapporti prodotti con Zabbix, così come i parametri di configurazione, sono accessibili tramite un front-end web-based.
Gli oggetti analizzati possono essere utilizzati per realizzare grafici real time dei dati ricevuti.

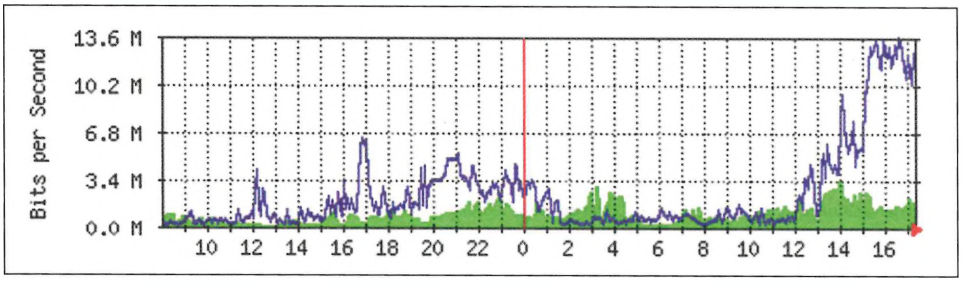
MRTG (MULTI ROUTER TRAFFIC GRAPHER)

MRTG
MULTI ROUTER TRAFFIC GRAPHER

Si tratta di un'applicazione open source utile per il monitoring della rete; infatti consente di controllare il traffico generato sia all'interno della LAN sia verso Internet. Inizialmente sviluppata per il monitoring dei router e la misurazione del carico dei link, è stata poi estesa per lavorare con qualsiasi tipo di host di rete.

Vediamo le sue principali caratteristiche:

- è un software scritto in Perl (alcune funzioni particolarmente critiche sono, però, scritte in C);
- funziona con molti sistemi operativi: Windows, Linux, Mac OS;
- usa SNMP come protocollo di comunicazione e in particolare SNMPv2c; l'host oggetto del monitoraggio deve avere installata una MIB in cui sono memorizzati due OID (Object IDentifier) che contengono i dati da inviare a MRTG tramite SNMP;
- crea un file di log costruito come documento HTML, con i grafici che riportano le informazioni sul traffico per gli host oggetto del monitoraggio.



Sul sito web di MRTG (*oss.oetiker.ch/mrtg*) si trovano numerosi script che possono essere usati per creare statistiche, access list di firewall, ecc.

FISSA LE CONOSCENZE

- Quali tipologie di applicazione possiamo usare per il monitoring della rete con SNMP?
- Spiega brevemente il progetto Net-SNMP.
- Quali sono le caratteristiche di MRTG?
- Quali software è necessario installare sulla macchina che ospiterà MRTG?

6 PROBLEM SOLVING E TROUBLESHOOTING

6.1 Il problem solving nelle reti

«Il computer non si connette alla rete Internet»: questa è la tipica frase che sentiamo quando un utente non riesce ad accedere ad alcun sito web. Le cause sono molteplici, da guasti alla rete fisica (scheda di rete, connettore, cavo) a problemi di indirizzamento e routing, fino ad arrivare alle applicazioni.
L'analisi della rete e dei sistemi che ne fanno parte, eseguita per ricercare l'origine di un malfunzionamento, ha tutte le caratteristiche di un processo di **problem solving**, svolto con l'obiettivo di arrivare all'identificazione delle cause prime di un guasto.
L'attività di monitoring della rete, però, non consiste solo nell'intervenire a fronte di un guasto, ma anche nell'individuare eventuali anomalie che a lungo andare potrebbero causare un malfunzionamento.

Quindi si deve agire secondo due diverse modalità operative:

- **gestione reattiva**, consiste nell'intervenire tempestivamente quando si verifica un guasto, in modo da contenere il più possibile le conseguenze del malfunzionamento;
- **gestione proattiva**, consiste nel prevenire i problemi evitando che si trasformino in un guasto; fondamentale per questa gestione è l'analisi delle prestazioni della rete e dei sistemi, per individuare le cause che potrebbero comportare anomalie e guasti.

La gestione reattiva si focalizza sul guasto, quella proattiva sui fattori che potrebbero causarlo.

#prendinota

Self-adaptive system
Un sistema automatico adattativo è in grado di adattarsi dinamicamente ai cambiamenti che possono insorgere anche a seguito di un guasto, senza l'intervento umano. Questa capacità di adattamento può essere reattiva o proattiva.

6.2 La metodologia Root Cause Analysis

La metodologia **RCA (Root Cause Analysis)** è un metodo del problem solving impiegato per identificare la causa prima di un problema.
Si applica non solo in ambito ICT (Information and Communication Technologies), ma anche in altri contesti quali, per esempio, i processi industriali e la diagnosi medica.

La **Root Cause Analysis** è una metodologia utilizzata nella gestione proattiva per individuare la **causa prima** che porta al verificarsi di un'anomalia al fine di rimuoverla. Si potrebbero rilevare altri fattori causali che, pur rimossi, non garantirebbero che il problema non si possa ripresentare.

In generale, la RCA si svolge in 4 passi:

1. **identificazione e descrizione**: è necessario non solo individuare il problema, ma anche descriverlo correttamente nel dettaglio;
2. **cronologia**: l'analisi deve stabilire la sequenza di eventi anche in termini di tempo, per capire le relazione tra il problema, eventuali concause e la causa prima;

3. **differenziazione**: grazie all'attività svolta nei due punti precedenti, si può arrivare a distinguere gli elementi tra quelli che possono concorrere a causare un guasto e la causa prima (anche questa può, in certi casi, essere composta da più fattori); in questa fase è di aiuto poter attingere alla documentazione di problemi già analizzati in passato;
4. **creazione del grafico causale**: al termine dell'analisi, si procede a realizzare un grafico (FIGURA 10) in cui inserire gli eventi chiave analizzati e indicare la causa prima che ha originato il problema.

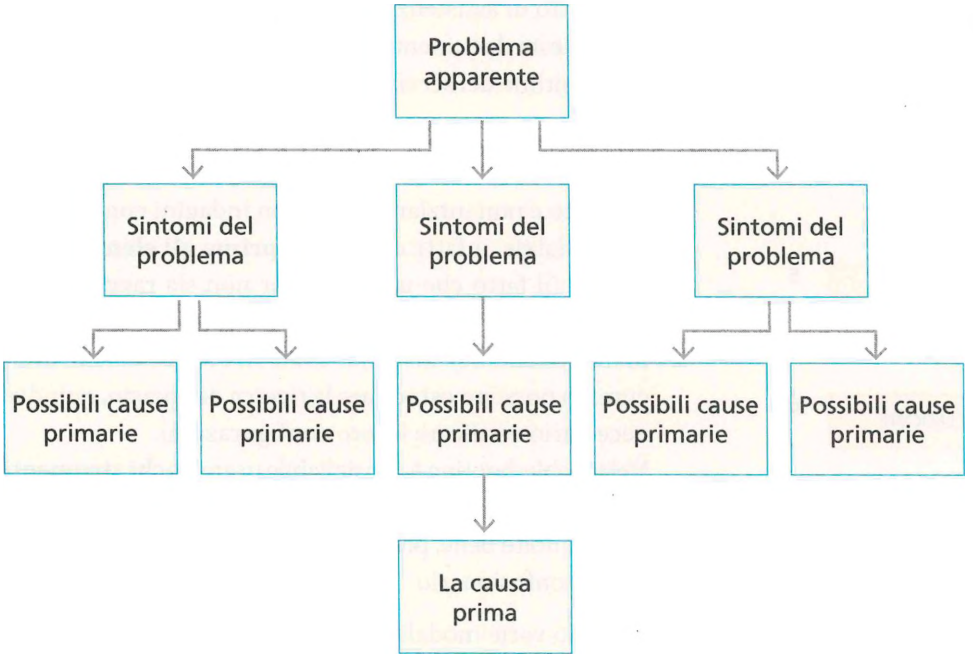


FIGURA 10 Esempio di grafico RCA

Da notare che la correzione del problema, rimuovendone la causa prima, non fa parte dell'attività RCA, quello è il passo finale dell'attività di problem solving, di cui RCA è una parte.

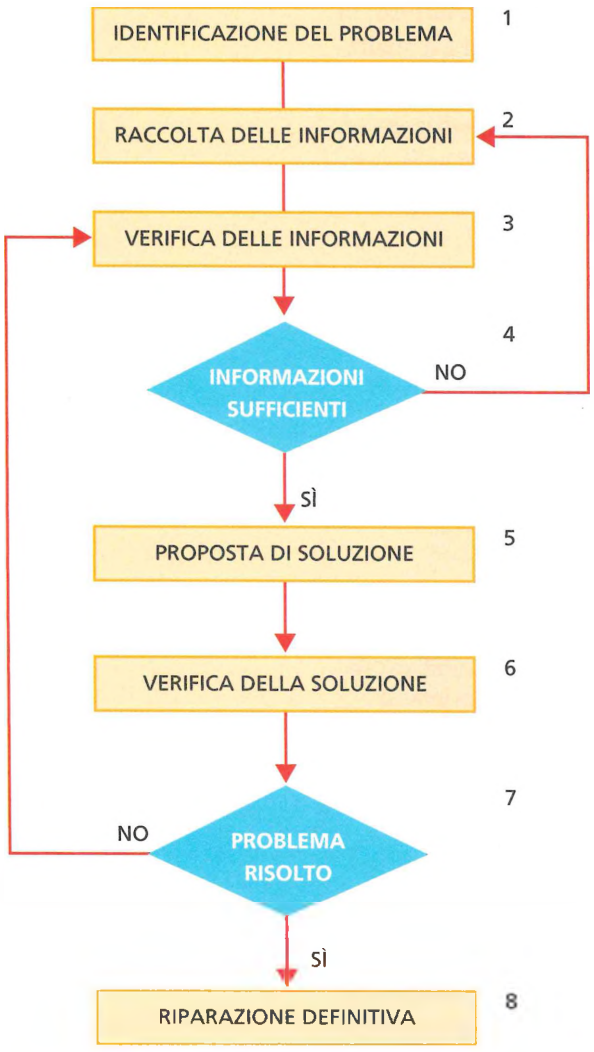
6.3 Il troubleshooting

Il processo di ricerca delle anomalie (troubleshooting) è **sistematico**, ossia si basa sull'applicazione di un metodo per risolvere manualmente un problema. Esso richiede esperienza, competenza e un'ottima conoscenza dell'ambiente di rete in cui si opera.

La FIGURA 11 mostra un esempio di procedura di ricerca e risoluzione di un malfunzionamento, valida in generale sia per le reti sia per i device, che si svolge in 8 fasi. Esistono svariati sistemi che utilizzano schemi logici analoghi a quello mostrato in figura, finalizzati a guidare e semplificare la ricerca dei guasti.

Quando si inizia l'attività di ricerca e riparazione di un guasto si deve porre attenzione a procedere effettuando **una sola modifica alla volta** e verificando subito se il problema è risolto.

FIGURA 11 Procedura di analisi e risoluzione del problema in 8 fasi



In questo modo è possibile capire qual è l'esatta azione da compiere per risolvere il problema, così da poterla replicare velocemente quando il problema si presenterà di nuovo.
Per questo la **documentazione** è fondamentale: se si documentano i sintomi e le azioni compiute per risolvere il guasto, inclusi gli strumenti utilizzati, altri tecnici potranno imparare il processo seguito, così da non doverlo scoprire ripartendo da zero. Se per esempio si lavora in un centro di assistenza o di controllo della rete, condividere questa documentazione aiuta a minimizzare i tempi di downtime del servizio.

Nella maggior parte dei casi, poi, la causa di un guasto è la più semplice, quindi è meglio non dare nulla per scontato e non iniziare subito con indagini complesse; è consigliabile, infatti, esaminare **prima gli elementi più banali** (il fatto che un computer non sia raggiungibile potrebbe essere semplicemente causato dal cavo di rete mal funzionante). Elementi come **firewall** e sistemi di sicurezza possono ostacolare la ricerca del guasto, quindi è necessario verificare le loro configurazioni.
Nel truobleshooting è consigliabile usare **pochi strumenti** di network management, in modo da conoscerli e saperli gestire molto bene, piuttosto che molti strumenti usati in modo confusionario.

Esistono varie modalità di affrontare il troubleshooting, e la scelta di un approccio o di un altro spesso dipende dal livello di esperienza del tecnico chiamato a risolvere il problema.
Nel riquadro sotto si presentano le tecniche più diffuse.

IN ENGLISH PLEASE

Structured Troubleshooting Approaches

- **Top-down**: the troubleshooter works from the TCP/IP stack's Application Layer down to the Physical Layer.
- **Bottom-up**: this approach starts from the TCP/IP stack's Physical Layer and moves up toward the Application Layer.
- **Divide-and-conquer**: the troubleshooter starts in the middle of the TCP/IP stack (usually the Network Layer), and then, based on his findings, he moves up or down the stack.
- **Follow-the-path**: this approach is based on the path that packets take through the Network from source to destination.
- **Spot-the-differences**: this approach compares Network devices or processes that are operating correctly to devices or processes that are not operating as expected and gathers clues by spotting significant differences. In case the problem occurred after a change on a single device was implemented, the spot-the-differences approach can pinpoint the problem cause by focusing on the difference between the device configurations, before and after the problem was reported.
- **Move-the-problem**: the strategy of this approach is to physically move components and observe whether the problem moves with the moved components.

Per un tecnico non esperto nell'attività di troubleshooting può essere utile seguire i passi indicati nella TABELLA 5 che riflettono l'ordine dei livelli dello stack TCP/IP. La complessità delle strutture aumenta man mano che si va verso l'alto e la padronanza di come funzionano i protocolli ai vari livelli costituisce una solida base per comprendere e risolvere i problemi che si presentano nelle applicazioni usate dagli utenti.

Entità	Problemi relativi a...
Protocolli di trasporto e applicazioni	funzionalità di alto livello (cosa succede dopo che si è effettuato il trasferimento dati tra due host?)
Tecnologia WAN	connessione end-to-end
Protocolli di rete	connettività dalla scheda di rete al primo router
Protocolli di accesso al mezzo	connettività dalla scheda di rete al primo switch (o hub)
Cablaggio	mezzi fisici usati per il collegamento

TABELLA 5 Elementi su cui focalizzare l'analisi e il troubleshooting secondo l'ordine dello stack TCP/IP

6.4 L'Intelligenza Artificiale e i sistemi esperti per il troubleshooting

I sistemi esperti (**Expert System**) sono una branca dell'Intelligenza Artificiale che studia lo sviluppo di sistemi in grado di emulare il comportamento di uno specialista umano in un processo di problem solving (un tipico esempio sono i sistemi esperti per le diagnosi mediche). Un sistema esperto utilizza una base dati, denominata **knowledge base**, in cui sono memorizzate moltissime informazioni che vengono elaborate per trovare la soluzione. La base di conoscenza è sviluppata con l'aiuto di esperti umani che forniscono la loro competenza ed esperienza nel settore in cui dovrà lavorare il sistema esperto. Inoltre, questi sistemi sono in grado di aumentare la propria knowledge base sulla base di un processo di autoapprendimento che li differenzia dai programmi di automazione realizzati per rendere automatica un'attività.

A partire dagli anni Ottanta sono stati sviluppati dei sistemi esperti nell'ambito della diagnostica dei guasti nelle reti a supporto dell'attività di **#help desk** che però non hanno avuto molto successo: le capacità di troubleshooting dei tecnici umani, ben preparati e con grande esperienza nel settore, continuavano a essere superiori.

Uno dei fattori frenanti nello sviluppo dei sistemi esperti, nei vari campi di applicazione, è stata la difficoltà di gestire enormi quantità di dati e la carenza di tecniche adeguate per la loro elaborazione.

L'attuale sviluppo di tecniche di **deep learning** e la maturità della tecnologia dei **big data** sta fornendo la soluzione a questo problema. L'applicazione di queste tecniche potrà portare ad avere reti che si auto-configurano e auto-riparano grazie alla raccolta di un'elevata quantità di dati sullo stato della rete.

#techwords

Il servizio di **help desk** fornisce un supporto al cliente per la risoluzione di problemi su prodotti acquistati. Si avvale di un software per la gestione delle chiamate.
Si distinguono due tipologie di helpdesk tecnico: quella di I livello e quella di II livello. Nel primo caso, l'operatore telefonico ha il compito di risolvere i problemi più semplici del cliente. Se invece il problema è complesso interviene l'assistenza di II livello.

FISSA LE CONOSCENZE

- Spiega come si possono applicare tecniche di problem solving nell'attività di controllo della rete e dei sistemi che ne fanno parte.
- Qual è la metodologia migliore da seguire nella ricerca del guasto?
- Spiega il ruolo della documentazione nell'attività di troubleshooting.
- Una mancanza di connettività tra la scheda di rete e lo switch quali protocolli coinvolge?

Esercizio commentato
Troubleshooting

7 STRUMENTI PER IL TROUBLESHOOTING

LEZIONE ONLINE

COMANDI PER IL TROUBLESHOOTING

Si descrivono i comandi più comunemente utilizzati per il troubleshooting nei sistemi Windows e Linux.

7.1 Troubleshooting su computer Windows e Linux

In questa Lezione vengono presentati alcuni comandi utili per il troubleshooting, che possono essere utilizzati con la maggior parte dei sistemi operativi.

Nella Lezione e nei Laboratori online si fa riferimento ai sistemi operativi Windows e Linux, ma le applicazioni presentate (chiamate spesso comandi) sono disponibili anche su molti altri sistemi. Per la sintassi completa dei comandi e la descrizione di tutte le opzioni previste è necessario fare riferimento all'help in linea e alla manualistica online.

```
C:\>netstat ?

Visualizza statistiche relative ai protocolli e informazioni sulle
connessioni di rete TCP/IP correnti.

NETSTAT [-a] [-b] [-e] [-f] [-n] [-o] [-p proto] [-r] [-s] [-t] [interval]

  -a            Visualizza tutte le connessioni e le porte di ascolto.
  -b            Visualizza il file eseguibile utilizzato per la creazione
                di ogni connessione o porta di ascolto. Alcuni file
                eseguibili conosciuti includono più componenti indipendenti.
                In tali casi viene visualizzata la sequenza dei componenti
                utilizzati per la creazione della connessione o porta di
                ascolto e il nome del file eseguibile viene visualizzato
                in fondo, tra parentesi quadre ([]). Nella parte superiore
                è indicato il componente chiamato e così via, fino al
                raggiungimento di TCP/IP. Se si utilizza questa opzione,
                l'esecuzione del comando può richiedere molto tempo e
                riuscirà solo se si dispone di autorizzazioni sufficienti.
  -e            Visualizza le statistiche Ethernet. Può essere utilizzata
                insieme all'opzione -s.
  -f            Visualizza i nomi di dominio completi (FQDN, Fully Qualified
                Domain Name) per gli indirizzi esterni.
  -n            Visualizza indirizzi e numeri di porta in forma numerica.
  -o            Visualizza l'ID del processo di origine associato a ogni
                connessione.
  -p proto      Visualizza le connessioni relative al protocollo specificato
                da "proto", che può essere TCP, UDP, TCPv6 o UDPv6.
                Se utilizzato insieme all'opzione -s per le statistiche per
                protocollo, "proto" può essere: IP, IPv6, ICMP, ICMPv6, TCP,
                TCPv6, UDP o UDPv6.
  -r            Visualizza la tabella di routing.
  -s            Visualizza le statistiche per protocollo. Per impostazione
                predefinita, vengono visualizzate le statistiche per IP,
                IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP e UDPv6. Per specificare
                un sottoinsieme dei valori predefiniti, è possibile
                utilizzare l'opzione -p.
  -t            Visualizza lo stato di offload della connessione corrente.
  interval      Ripete la visualizzazione delle statistiche selezionate,
                con una pausa di un numero di secondi pari a "interval"
                dopo ogni visualizzazione. Per interrompere la ripetizione
                della visualizzazione delle statistiche, premere CTRL+C.
                Se questa opzione viene omessa, le informazioni di
                configurazione correnti verranno visualizzate una volta sola.
```

FIGURA 12 ▲ Sintassi del comando netstat su Windows

Per **Windows** è sufficiente digitare nella finestra **Prompt dei comandi** il nome del comando senza parametri oppure seguito da un punto interrogativo, per ottenerne la sintassi e la descrizione delle opzioni. Per esempio in FIGURA 12 si mostra il risultato per il comando netstat.

Per **Linux** si utilizzano le man pages ossia la manualistica installata: dalla finestra terminale si scrive **man** seguito dal nome del comando di interesse. Per esempio in FIGURA 13 si mostra il risultato del comando:

```
$ man netstat
```

```
File  Edit  View  Search  Terminal  Help
NETSTAT(8)                Linux Programmer's Manual                NETSTAT(8)

NAME
       netstat  - Print network connections, routing tables, interface statis-
       tics, masquerade connections, and multicast memberships

SYNOPSIS
       netstat  [address_family_options]  [--tcp|-t]  [--udp|-u]  [--raw|-w]
       [--listening|-l]  [--all|-a]  [--numeric|-n]  [--numeric-hosts]
       [--numeric-ports]  [--numeric-users]  [--symbolic|-N]
       [--extend|-e[--extend|-e]]  [--timers|-o] [--program|-p] [--verbose|-v]
       [--continuous|-c]

       netstat              {--route|-r}              [address_family_options]
       [--extend|-e[--extend|-e]]  [--verbose|-v]  [--numeric|-n]
       [--numeric-hosts] [--numeric-ports] [--numeric-users] [--continuous|-c]

       netstat {--interfaces|-i} [--all|-a] [--extend|-e[--extend|-e]] [--ver-
       bose|-v]  [--program|-p]  [--numeric|-n]  [--numeric-hosts] [--numeric-
       ports] [--numeric-users] [--continuous|-c]

       netstat      {--groups|-g}      [--numeric|-n]      [--numeric-hosts]
       [--numeric-ports] [--numeric-users] [--continuous|-c]
Manual page netstat(8) line 1 (press h for help or q to quit)
```

FIGURA 13 ▶ Sintassi del comando netstat su Linux Ubuntu

7.2 I comandi principali

La TABELLA 6 riassume le utility per il controllo di reti e sistemi sia in ambienti Windows sia in ambienti Linux.
Le utility specifiche per i sistemi Windows e Linux verranno descritte nella Lezione online "Comandi per il troubleshooting".

TABELLA 6 Principali utility di Windows e Linux

Applicazione su Windows	Applicazione su Linux	Scopo	Esempio di comando su Windows	Esempio di comando su Linux	Quando si usa
ipconfig	ip	Gestione della configurazione IP della macchina.	ilpconfig /all	ip link	Per verificare le informazioni sull'indirizzamento IP.
arp	ip	Esamina e configura la ARP cache locale.	arp -a	ip n	Per controllare il contenuto della ARP cache.
netstat	ip	Mostra le statistiche di protocollo e lo stato delle connessioni.	nestat -r	ip r	Per controllare lo stato delle connessioni di rete e il contenuto della routing table.
ping	ping	Invia e riceve un messaggio di test verso un host destinatario.	ping www.google.it	ping www.google.it	Per testare la connettività di rete e verificare se l'host è raggiungibile.
tracert	traceroute	Traccia il percorso da un host mittente a un host destinatario.	tracert www.google.it	traceroute www.google.it	Per raccogliere informazioni di routing.
nslookup	dig	Controlla l'operatività del DNS.	nslookup www.google.it	dig www.google.it	Per verificare la correttezza delle operazioni del DNS Server.

LABORATORIO ONLINE

TROUBLESHOOTING NEI SISTEMI WINDOWS

Attività di troubleshooting su un sistema Windows che non si connette alla rete. Analisi dell'attività della scheda Wi-Fi.

LABORATORIO ONLINE

TROUBLESHOOTING NEI SISTEMI LINUX

Attività di troubleshooting su un sistema Linux Ubuntu che non si connette alla rete locale tramite wi-fi. Verifica indirizzi IP e impostazioni del DNS.

FISSA LE CONOSCENZE

- Come si consulta la sintassi di un comando su un sistema Windows?
- Che cosa sono le man pages presenti nei sistemi Linux?
- Quale comando si usa nei sistemi Linux per visualizzare le man pages?

RIPASSIAMO INSIEME

1 La gestione delle reti

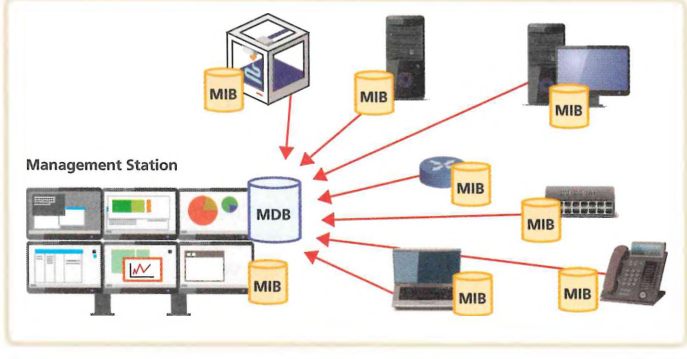
Le reti sono entità complesse, formate da molteplici componenti connesse tra loro. Per gestirle al meglio l'amministratore di rete deve svolgere un insieme di attività definito network management. È importante poter disporre della documentazione dettagliata della rete e di strumenti specifici (network management tools).

2 La gestione di reti TCP/IP

Le reti TCP/IP sono reti eterogenee, interconnesse tra loro, pertanto la loro gestione è svolta a livello Application così da essere indipendente dalla rete fisica e logica. Il modello implementato è manager-agent: il software manager è installato sulla stazione di gestione, il software agent è sul dispositivo da gestire. IETF ha definito un framework gestionale che si compone di 3 parti: il protocollo di comunicazione SNMP, una base di dati (MIB) che contiene le informazioni sui dispositivi da gestire e un linguaggio (SMI) per la definizione formale degli oggetti della MIB.

3 L'organizzazione dei dati da gestire

Le informazioni riguardanti i dispositivi della rete da gestire sono memorizzate come oggetti della MIB e scritti secondo le regole del linguaggio di definizione SMI. Ogni oggetto è identificato in modo univoco tramite un Object Identifier (OID) che fa parte di un namespace definito in ambito ISO e ITU e ha una struttura gerarchica.



4 Il protocollo SNMP

È il protocollo di livello Application usato per la gestione delle reti. Definisce le modalità di scambio di informazioni tra una stazione manager e gli host della rete (agent) e consente di tenere sotto controllo l'operatività e le prestazioni della rete.

6 Problem solving e troubleshooting

L'attività di analisi e troubleshooting di una rete richiede una conoscenza approfondita del funzionamento delle reti TCP/IP. La documentazione deve essere sempre aggiornata così da ridurre i tempi di individuazione e risoluzione delle anomalie. La manutenzione preventiva della rete e degli host è importante per prevenire guasti che potrebbero causare un'interruzione del servizio agli utenti.

7 Strumenti per il troubeshooting

Nei sistemi operativi Windows e Linux sono presenti alcune utility che vengono usate per svolgere l'attività di troubleshooting. Si tratta di applicazioni che si richiamano da terminale.

VERIFICA DI FINE UNITÀ

Test
Svolgi il **test interattivo**

Quali delle seguenti affermazioni sono vere (V) e quali false (F)?

1. Nel modello Client-Server adottato in SNMP, l'agent è il client e il manager è il server. V F
2. Gli oggetti della MIB sono definiti usando il linguaggio XML. V F
3. Dal punto di vista della sicurezza, SNMPv3 supporta solo il controllo degli accessi. V F
4. SNMPv2c usa il concetto di community come unico meccanismo di sicurezza. V F
5. I messaggi trap sono inviati dall'SNMP Manager all'SNMP Agent. V F
6. Un produttore può definire delle MIB specifiche per la gestione SNMP dei propri apparati. V F
7. L'applicazione MRTG è usata per monitorare il traffico di rete. V F
8. Nella gestione proattiva della rete si interviene tempestivamente su un guasto appena è segnalato. V F
9. Nel troubleshooting è consigliabile applicare tutte insieme le modifiche ipotizzate e poi verificare se il problema è risolto. V F
10. Il troubleshooting può avvantaggiarsi di tecniche di Intelligenza Artificiale. V F

Domande a scelta multipla (una sola è la risposta esatta)

1. **Tra le variabili specificate nella MIB c'è la *ifNumber* che specifica:**
   - A il numero delle interfacce di rete
   - B il numero di IP datagram inoltrati
   - C il numero di segmenti TCP ricevuti
   - D il numero di UDP datagram ricevuti

2. **Con bottleneck si intende:**
   - A il monitoring dei livelli di traffico nella rete
   - B l'individuazione di punti di congestione
   - C il controllo sull'utilizzo del software
   - D il controllo sull'utilizzo dell'hardware

3. **Su quale protocollo di trasporto e su quali porte si basa SNMP?**
   - A Protocollo FTP e porte 20 e 21
   - B Protocollo UDP e porte 160 e 161
   - C Protocollo TCP e porte 1 e 2
   - D Protocollo HTTP e porte 80 e 81

4. **Il troubleshooting è:**
   - A il processo di ricerca delle anomalie
   - B una tecnica per migliorare la fault-tolerance
   - C il processo di ricerca del percorso migliore
   - D una tecnica per nascondere gli indirizzi

Ascolta le **risposte**

PREPARATI PER IL COLLOQUIO ORALE

1. LEZIONE 1 **Descrivi alcune tipiche attività che rientrano nel network management.**
2. LEZIONE 1 **Perché è importante avere una documentazione della rete completa e aggiornata?**
3. LEZIONE 2 **Descrivi le componenti dell'architettura definita in ambito IETF per la gestione delle reti TCP/IP.**
4. LEZIONE 3 **Quale ruolo svolge la MIB nella gestione di un apparato?**
5. LEZIONE 3 **Come sono identificati i nomi degli oggetti definiti nelle MIB?**
6. LEZIONE 4 **Quali sono le principali funzionalità offerte dal protocollo SNMP?**
7. LEZIONE 4 **Quali funzionalità di sicurezza sono state introdotte con SNMPv3?**
8. LEZIONE 5 **Descrivi qualche applicazione che utilizza SNMP come protocollo di comunicazione per il monitoring della rete.**
9. LEZIONE 6 **Descrivi la metodologia di Root Cause Analysis (RCA).**
10. LEZIONE 6 **Descrivi quali sono le tipiche attività del troubleshooting.**
11. LEZIONE 6 **Descrivi la successione di azioni da svolgere per la ricerca di un guasto e la sua risoluzione.**
12. LEZIONE 7 **Descrivi alcune utility che spesso sono utilizzate per il controllo di reti e sistemi.**

IN ENGLISH, PLEASE

CLIL

Ascolta la **pronuncia del testo** e verifica la **traduzione**

ABSTRACT

Network and system management

Network management is the process of operating, monitoring and controlling the network to make sure it works as intended.
TCP/IP networks are managed with the Simple Network Management Protocol (SNMP), an Application Layer protocol that collects information from a network device. The architecture of SNMP is based on client-server model with management stations (on client side) that monitor and control network elements, and management agents (on server side) that perform the management functions requested by management stations. The network information is stored in MIB (Management Information Base).
Network troubleshooting requires to follow a standard procedure to address the causes of malfunctions in a network or system. We can use some tools to analyze networks and device's configuration in order to quickly identify the cause of a problem.

EXERCISES

Use the appropriate number to match words and meanings.

...	Help desk	1	A software component within a managed device.
...	Redundancy	2	It is issued by agent to asynchronously report events to the manager.
...	Agent	3	The ability to continue operations even after a failure.
...	Self-adaptive	4	A system that controls and monitors the activities of network hosts.
...	Manager	5	Duplication of resources or data paths.
...	Fault-tolerance	6	It manages the customer requests, answers to them and solves known problems.
...	Get-Request	7	System's ability to modify automatically its behavoir
...	Trap	8	It is issued by the manager to monitor devices.

GLOSSARY

Downtime: a period of time when a network is unavailable to users.
Expert system: a computer system emulating the decision-making ability of a human expert.
Managed device: a piece of network equipment (including its software) that resides on a managed network. In each managed device runs a process, called agent.
MIB: Management Information Base, it is the information set that each manageable device stores to reflect its status.
Monitoring: the activity of constantly checking a computer network for slow or failing components.
Network Administrator: a person responsible for network management and support.
Network Management: the activities, methods, procedures and tools that pertain to the operation, administration, maintenance and provisioning of network resources.
Polling: it allows to monitor the status of various MIB variables. It consists of periodic SNMP requests sent to the SNMP agent.
Root cause: the underlying problem that sets in motion a cause-and-effect reaction leading to malfunction or failures.
Traffic shaping: a performance management technique used to assure timely delivery of the most important traffic while offering the best possible performance for all users.
Troubleshooting: a logical, systematic search for the source of a problem so that it can be fixed and network or devices can resume operation.

LAVORARE PER COMPETENZE

COMPETENZE IN GIOCO

Competenze disciplinari

- Scegliere gli strumenti più adeguati per monitorare la rete.
- Mettere in atto procedure per rendere la rete affidabile.
- Saper descrivere e documentare le soluzioni adottate.
- Utilizzare le reti e gli strumenti informatici nelle attività di studio, ricerca e approfondimento disciplinare.

Competenze chiave di cittadinanza

- Interpretare il testo.
- Risolvere problemi.
- Comunicare.
- Competenza digitale.

obiettivi formativi

- Stimolare l'approfondimento e la ricerca disciplinare.
- Consultare fonti Internet.
- Contestualizzare in un caso reale le nozioni teoriche acquisite studiando.
- Esporre i risultati della ricerca alla classe.

tempi

- Preparazione: 2 ore.
- Presentazione dei risultati e dibattito: 1 ora.
- Autovalutazione: 10 minuti.

strumenti

- Libro di testo.
- Dispositivo connesso a Internet.
- Software PowerPoint.
- Proiettore collegato al computer in classe o in laboratorio.

TEMA PROPOSTO

Una scuola superiore intende aggiornare la sua infrastruttura di rete per adeguarla alle esigenze della Didattica Digitale Integrata (DDI) al fine di:

- offrire una piattaforma interna per la didattica multimediale e per servizi in streaming, accessibile sia dalla rete locale interna alla scuola sia tramite Internet;
- garantire la sicurezza della rete interna da possibili minacce, sia interne che esterne.

Analizzare le problematiche di gestione della piattaforma multimediale e le misure necessarie a prevenire possibili interruzioni nel servizio.

SVOLGIMENTO

Le piattaforme multimediali per la scuola sono ambienti di apprendimento online (e-learning) che consentono di condividere materiale multimediale (documenti, immagini, filmati, ecc.) tra docenti e studenti.
Sono molte le piattaforme open source per la didattica multimediale che rispondono alle esigenze dell'e-learning. Le migliori permettono al docente di caricare lezioni e video lezioni, di fare verifiche online, di monitorare il lavoro a casa degli studenti e modellare i corsi in base alle proprie esigenze.

moodle

#prendinota

Moodle
È una delle piattaforme di e-learning più diffuse al mondo, che meglio si adatta alle esigenze delle scuole e delle università.
È un progetto open source che offre a insegnanti e studenti un sistema integrato e personalizzabile.

Stabilita la piattaforma da utilizzare occorre organizzare il sistema in modo da garantire che il servizio funzioni adeguatamente, cercando di prevenirne le possibili cause di interruzione.

Elenchiamo alcuni dei principali motivi che possono portare all'interruzione di un servizio offerto online e le soluzioni più comuni per prevenirli o limitarli:

- interruzione dell'alimentazione: si previene fornendo la rete di un gruppo di continuità UPS (Uninterruptible Power Supply);
- guasto della macchina server: si riesce a limitare la durata dell'interruzione utilizzando server di backup ridondanti o, se i server sono virtualizzati, clonandoli;
- interruzione della connessione Internet: si previene mediante una seconda linea gestita da un ISP (Internet Service Provider) diverso;
- eccesso di traffico con punti di congestione e successiva perdita di pacchetti: si tiene sotto controllo il traffico mediante una serie di strumenti di network management che permettono di avere una supervisione dell'intera rete. Per esempio, se analizzando le statistiche di utilizzo della rete si rileva che un router è particolarmente lento e corre il rischio di essere congestionato dal traffico, l'amministratore può intervenire sulla CPU e sul buffer del router oppure può sostituirlo con un router maggiormente performante, il tutto prima che gli utenti della piattaforma sperimentino dei rallentamenti;
- in ambito LAN scolastica, le modalità di realizzazione della rete wired e wireless, la scelta degli switch e degli access point risultano fondamentali nella gestione del traffico di rete;
- server sovraccarico di richieste con rallentamento e successivo blocco del servizio (system crash) in certi orari: anche in questo caso sono i network management tools che permettono di monitorare gli accessi al server e in generale alle risorse di rete e quindi permettono di intervenire tempestivamente. Se il rallentamento si verifica di frequente, una soluzione può essere decidere per un server dedicato (non condiviso) da configurare su una macchina server dalle elevate prestazioni. Se invece il rallentamento si verifica occasionalmente, è sufficiente l'intervento dell'amministratore di rete che può, per esempio, diminuire il TTL (Time To Live) dei pacchetti in attesa. Fondamentale è anche il controllo del throughput della banda di trasmissione da parte dell'amministratore della rete (bandwidth management);
- attacchi informatici: gli attacchi tipo DoS (Denial of Service), che mirano a bombardare il server di richieste fino a bloccarlo completamente, si possono anch'essi limitare mediante l'utilizzo dei network management tools. Il filtraggio dei pacchetti in arrivo (campionamento e analisi) consente di individuare in tempo utile i flussi da bloccare.

Come si è visto, sono soprattutto le attività di network management che consentono a una rete e ai servizi che essa offre di funzionare correttamente.

Comunque, prima di intervenire sulla rete o anche solo di effettuare delle previsioni sul suo stato, è importante che l'amministratore conosca bene la sua struttura fisica e logica e come funziona in condizioni normali. Tutte le informazioni devono entrare a far parte della documentazione di rete che deve sempre essere aggiornata e messa a disposizione dei tecnici sistemisti.

In caso di reti che gestiscono elevati volumi di traffico, per garantire la continuità di un servizio è bene affidarsi alle tecniche di **traffic shaping**.
Le tecniche di traffic shaping implementate possono riguardare il rallentamento del traffico meno critico, l'aumento della priorità del traffico più importante e la limitazione della quantità di traffico che attraversa un'interfaccia in uno specifico intervallo di tempo.
Per esempio, l'amministratore della rete scolastica potrebbe limitare il traffico legato alle attività svolte nei laboratori (rete wired) e dare maggior banda al traffico generato dalle applicazioni legate alla didattica in aula (rete wireless).

Una soluzione che libererebbe la scuola dal problema di garantire il funzionamento della piattaforma multimediale è quella di usufruire di servizi di hosting a pagamento che garantiscano la continuità del servizio.

A CASA

- Effettua una ricerca in Internet sulle piattaforme multimediali specifiche per la didattica; esaminando i diversi esempi trovati concentrati su:
  – tipologie di piattaforme multimediali;
  – cause di interruzione del funzionamento di una piattaforma online;
  – misure necessarie per prevenire le interruzioni del servizio.
- Individua quali, tra gli esempi trovati, risulta affine al contesto illustrato nel tema proposto.
- Leggi l'esempio di svolgimento proposto per verificare se le tue ipotesi si adattano al caso preso in esame e se la trattazione proposta risulta completa nell'ottica dei risultati della tua ricerca.
- Raccogli i tuoi risultati in una presentazione in PowerPoint (massimo 5 slide) evidenziando i casi trovati, la relazione con il contesto proposto, eventuali modifiche o aggiunte da effettuare alla soluzione proposta nell'esempio di svolgimento.

IN CLASSE

- Condividi la presentazione dei tuoi risultati con i compagni.
- Confronta e discuti con i compagni i casi che sono stati presentati.
- Stabilite quale caso rappresenta l'esempio migliore per completezza e realisticità nell'ottica della realizzazione delle misure necessarie richieste nel tema d'esame.
- Procedi con l'autovalutazione.

AUTOVALUTAZIONE

ATTIVITÀ	LIVELLO			
	INIZIALE	BASE	INTERMEDIO	AVANZATO
Ho compreso senza difficoltà le richieste dell'attività proposta?	Ho compreso solo alcune delle richieste aiutato dal docente. ☐	Con la guida del docente e la collaborazione dei compagni ho compreso quasi tutte le richieste. ☐	Ho compreso le richieste e in parte le ho svolte autonomamente. ☐	Ho identificato le richieste e le ho svolte senza difficoltà. ☐
Ho reperito le informazioni in rete senza difficoltà?	Ho reperito solo alcune delle informazioni utili aiutato dal docente. ☐	Con la guida del docente e la collaborazione dei compagni ho reperito quasi tutte le informazioni. ☐	Ho reperito le informazioni utili autonomamente e le ho elaborate. ☐	Ho identificato le informazioni utili e le ho elaborate senza difficoltà. ☐
L'analisi dello scenario mi ha permesso di definire modifiche e miglioramenti allo svolgimento proposto?	A partire dalla mia analisi, non sono stato in grado di individuare nessun punto critico nello svolgimento proposto. ☐	A partire dalla mia analisi, sono stato in grado di individuare alcuni punti critici nello svolgimento proposto con l'aiuto del docente. ☐	A partire dalla mia analisi, sono stato in grado di individuare i punti critici e alcune modifiche apportabili nello svolgimento proposto con l'aiuto del docente. ☐	A partire dalla mia analisi, sono stato in grado di individuare i punti critici e definire le modifiche apportabili in modo dettagliato e completo. ☐

UNITÀ 9

ARDUINO E RASPBERRY Pi PER IoT

IN QUESTA UNITÀ

Guarda la **presentazione** dell'unità

DDI+ Didattica Digitale Integrata Plus

conoscenze	abilità	competenze
Conoscere le caratteristiche delle schede wireless e bluetooth.	Saper scegliere le schede di rete più adatte.	Configurare le schede di rete per Arduino in base alle specifiche richieste.
Conoscere le prestazioni delle varie schede.	Saper configurare le schede in base alle specifiche del progetto.	Configurare una rete con la scheda Raspberry Pi.
	Saper configurare le schede in base ai dispositivi esterni.	Valutare le prestazioni e la funzionalità della rete realizzata.

FLIPPED CLASSROOM

A casa

- Leggi la Lezione 1 e rivedi quanto studiato sui parametri di rete;
- valuta la configurazione necessaria per leggere un parametro fisico e trasmetterlo a distanza.

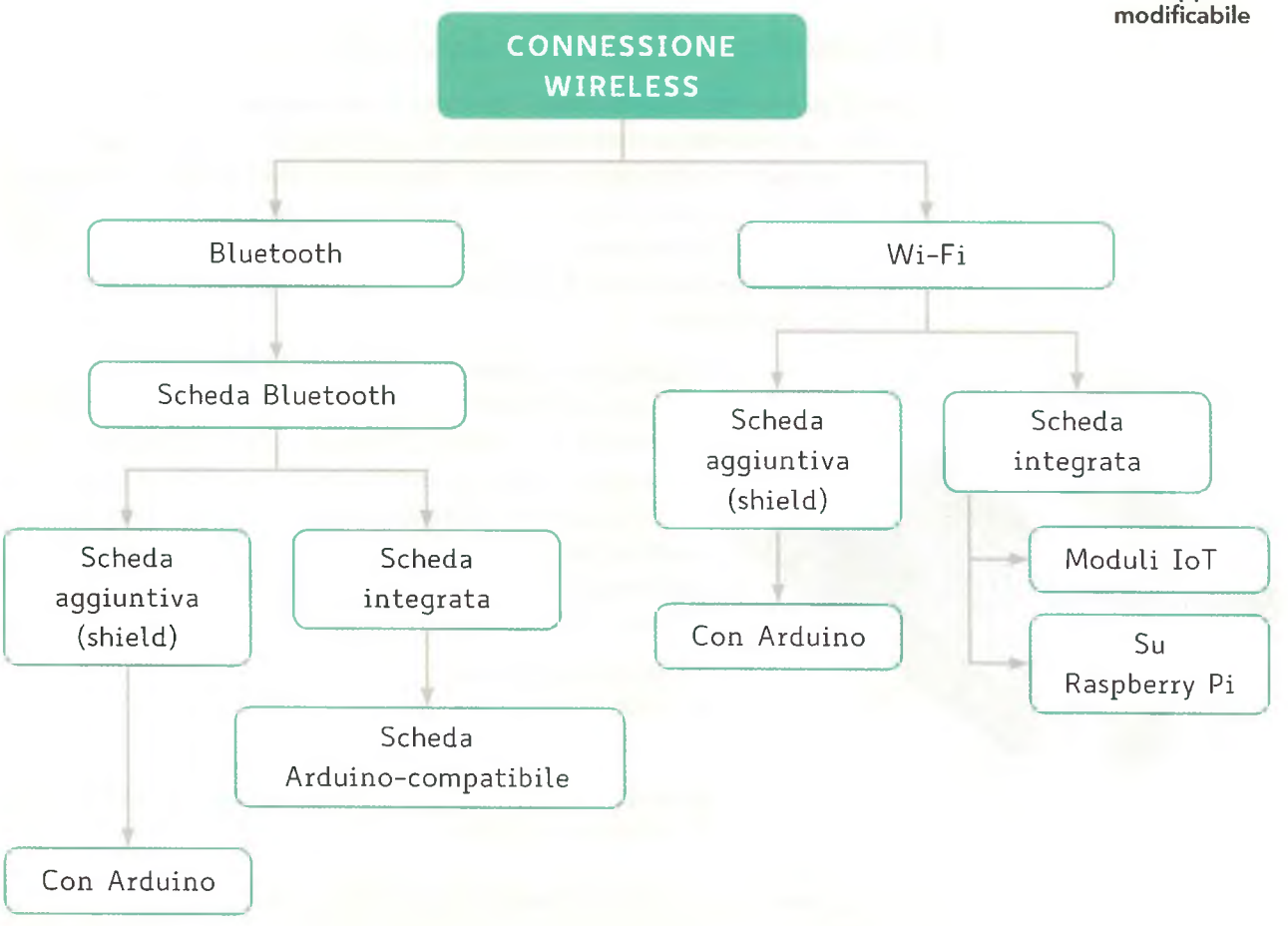
In classe

- Confrontate le soluzioni tecniche trovate;
- discutete quali possono essere le soluzioni tecniche migliori;
- valutate i limiti delle soluzioni tecniche scartate.

MAPPA CONCETTUALE

DIDATTICA INCLUSIVA

Mappa modificabile

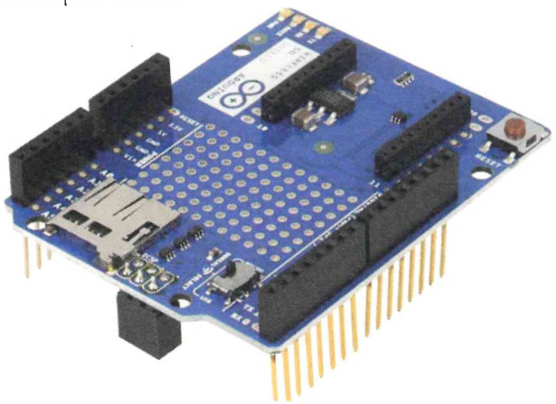


1 ARDUINO PER IoT

1.1 Arduino e le connessioni wireless

In questa Lezione verranno illustrate le modalità di connessione della scheda Arduino con la rete. La crescente necessità di connettere vari dispositivi senza collegamenti via cavo ha spinto le varie aziende a sviluppare schede con la classica filosofia Arduino di essere alla portata di tutti, a basso costo, perfettamente compatibili con il software di programmazione di Arduino, ma con dimensioni molto ridotte e consumi energetici adatti all'inserimento di tali moduli dentro involucri poco ingombranti, alimentando il tutto con batterie.

FIGURA 1 Scheda di rete Wi-Fi per Arduino



Il gruppo di sviluppo di Arduino, che inizialmente aveva realizzato solo uno shield Wi-Fi (FIGURA 1), proprio a causa dell'enorme crescita del settore IoT, ha messo a punto alcune schede che non rispettano più le classiche dimensioni della scheda Arduino Uno, ma sono di dimensioni ridotte e dotate di connessioni wireless. Stanno progressivamente sostituendo la Wi-Fi shield in quanto, in uno spazio ridotto, è presente sia il microcontrollore sia la scheda Wi-Fi.

Le più utilizzate sono:

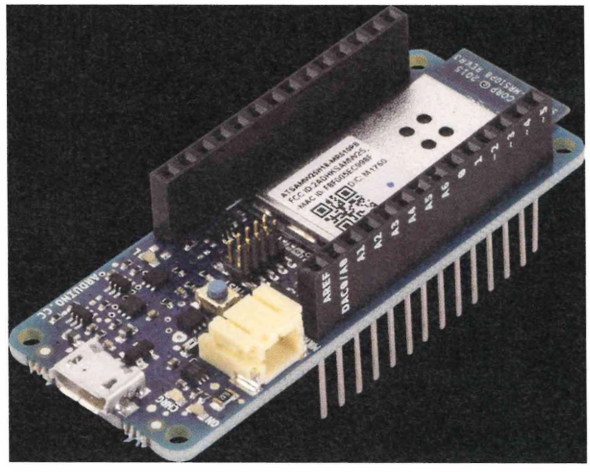
- Arduino Nano IoT
- Arduino MKR1010

Si riportano qui, a titolo di esempio, le caratteristiche della scheda Arduino MKR1010.

Microcontroller (datasheet)	SAMD21 Cortex®-M0+ 32bit low power ARM MCU
Radio module	u-blox NINA-W102 (datasheet)
Board Power Supply (USB/VIN)	5 V
Secure Element	ATECC508 (datasheet)
Supported Battery	Li-Po Single Cell, 3.7 V, 1024 mAh Minimum
Circuit Operating Voltage	3.3 V
Digital I/O Pins	8
PWM Pins	13 (0, ..., 8, 10, 12, 18 / A3, 19 / A4)
UART	1
SPI	1
I2C	1
Analog Input Pins	7 (ADC 8/10/12 bit)
Analog Output Pins	1 (DAC 10 bit)
External Interrupts	8 (0, 1, 4, 5, 6, 7, 8, 16 / A1, 17 / A2)
DC Current per I/O Pin	7 mA
CPU Flash Memory	256 kB (internal)
SRAM	32 kB
EEPROM	no
Clock Speed	32.768 kHz (RTC), 48 MHz
LED_BUILTIN	6
USB	Full-Speed USB Device and embedded Host

Come si può notare dalle caratteristiche, la scheda (FIGURA 2) è predisposta per l'alimentazione da batterie Li-Po proprio per la necessità di avere batterie di dimensioni ridotte. Il microprocessore è di tipo a basso consumo con tensione di alimentazione a 3,3 V, anche se mantiene la compatibilità con segnali logici a 5 V in ingresso.

FIGURA 2 Scheda Arduino MKR1010



Gli standard di comunicazione Wi-Fi sono aggiornati anche per la parte relativa alla crittografia, fattore particolarmente importante per la sicurezza delle comunicazioni wireless.

1.2 Laboratorio Arduino wireless

Qui di seguito sono riportati e commentati (oltre ai commenti originali) alcuni esempi prelevabili e utilizzabili direttamente dal programma *arduino.exe*; tali programmi, inoltre, sono disponibili sul sito *www.arduino.cc*.

esempio

Accendere un LED via web

File sorgenti
Scarica il file

Materiale necessario:
- scheda Arduino + Wi-Fi shield oppure Arduino MKR1010;
- cavo USB per Arduino Uno oppure cavo microUSB per Arduino MKR1010;
- LED + Resistore 180 Ohm (collegati in serie tra PIN 9 e GND).

```
/*
  Wi-Fi Web Server LED Blink
  A simple web server that lets you blink a LED via the web.
  This sketch will create a new access point (with no password).
  It will then launch a new server and print out the IP address
  to the Serial monitor. From there, you can open that address in a web browser
  to turn on and off the LED on pin 13.
  If the IP address of your board is yourAddress:
    http://yourAddress/H turns the LED on
    http://yourAddress/L turns it off
  created 25 Nov 2012
  by Tom Igoe
  adapted to Wi-Fi AP by Adafruit
 */

#include <SPI.h>
#include <WiFiNINA.h>
#include "arduino_secrets.h"
///////please enter your sensitive data in the Secret tab/arduino_secrets.h
char ssid[] = SECRET_SSID;        // your network SSID (name)
char pass[] = SECRET_PASS;    // your network password (use for WPA, or use as key
                              // for WEP)
int keyIndex = 0;                // your network key Index number (needed only for WEP)

int led =  LED_BUILTIN;
int status = WL_IDLE_STATUS;
```

Libreria Wi-Fi

Libreria gestione password

→

```
Wi-FiServer server(80);

void setup()
{
 //Initialize serial and wait for port to open:
 Serial.begin(9600);
 while (!Serial)
  {
   ; // wait for serial port to connect. Needed for native USB port only
   }
 Serial.println("Access Point Web Server");
 pinMode(led, OUTPUT);      // set the LED pin mode
 // check for the Wi-Fi module:
 if (Wi-Fi.status() == WL_NO_MODULE)
   {
    Serial.println("Communication with Wi-Fi module failed!");
    // don't continue
    while (true);
   }
  String fv = Wi-Fi.firmwareVersion();
  if (fv < Wi-Fi_FIRMWARE_LATEST_VERSION)
   {
   Serial.println("Please upgrade the firmware");
   }
    // by default the local IP address will be 192.168.4.1
    // you can override it with the following:
    // Wi-Fi.config(IPAddress(10, 0, 0, 1));
    // print the network name (SSID);
    Serial.print("Creating access point named: ");
    Serial.println(ssid);
    // Create open network. Change this line if you want to create a WEP network:
    status = Wi-Fi.beginAP(ssid, pass);
    if (status != WL_AP_LISTENING)
     {
      Serial.println("Creating access point failed");
      // don't continue
      while (true);
      }
  delay(10000);    // wait 10 seconds for connection:
  server.begin();  // start the web server on port 80
  printWi-FiStatus();  // you're connected now, so print out the status
}

void loop()
 {
  // compare the previous status to the current status
  if (status != Wi-Fi.status())
    {
     // it has changed update the variable
     status = Wi-Fi.status();
     if (status == WL_AP_CONNECTED)
      {
       Serial.println("Device connected to AP");    // a device has connected to the AP
```

Verifica la presenza di un modulo Wi-Fi

Verifica che il firmware della scheda sia aggiornato

L'IP predefinito è 192.168.4.1, ma è possibile modificarlo con l'istruzione che nel listato è messa come commento

Attende di connettersi alla rete Wi-Fi

Utilizza una funzione (vedi in fondo al listato) per visualizzare i parametri di connessione

Verifica che la connessione non sia terminata

```
  } else
     {
      // a device has disconnected from the AP, and we are back in listening mode
      Serial.println("Device disconnected from AP");
     }
}
Wi-FiClient client = server.available();  // listen for incoming clients
 if (client)                              // if you get a client,
 {
  Serial.println("new client");          // print a message out the serial port
  String currentLine = "";               // make a String to hold incoming data from the
                                         // client
  while (client.connected()) {           // loop while the client's connected
  if (client.available())                // if there's bytes to read from the client,
    {
     char c = client.read();             // read a byte, then
     Serial.write(c);                    // print it out the serial monitor
     if (c == '\n')                      // if the byte is a newline character
      {
      // if the current line is blank, you got two newline characters in a row
      // that's the end of the client HTTP request, so send a response:
      if (currentLine.length() == 0)
       {
        // HTTP headers always start with a response code (e.g. HTTP/1.1 200 OK)
        // and a content-type so the client knows what's coming, then a blank line:
        client.println("HTTP/1.1 200 OK");
        client.println("Content-type:text/html");
        client.println();
        // the content of the HTTP response follows the header:
        client.print("Click <a href=\"/H\">here</a> turn the LED on<br>");
        client.print("Click <a href=\"/L\">here</a> turn the LED off<br>");
        // The HTTP response ends with another blank line:
        client.println();
        // break out of the while loop:
        break;
       }
      else      // if you got a newline, then clear currentLine:
       {
        currentLine = "";
       }
    }
    else if (c != '\r')
          {   // if you got anything else but a carriage return character,
            currentLine += c;      // add it to the end of the currentLine
          }
    // Check to see if the client request was "GET /H" or "GET /L":
    if (currentLine.endsWith("GET /H"))
     {
      digitalWrite(led, HIGH);              // GET /H turns the LED on
      }
    if (currentLine.endsWith("GET /L"))
     {
      digitalWrite(led, LOW);               // GET /L turns the LED off
```

Rimane in attesa di una richiesta

Genera una pagina web per consentire l'accensione e lo spegnimento del LED

In base al carattere ricevuto provvede ad accendere o spegnere il LED

→

```
      }
    }
  }
  // close the connection:
  client.stop();
  Serial.println("client disconnected");
 }
}
```

Funzione che visualizza i parametri di connessione della scheda

```
void printWi-FiStatus()
 {
  // print the SSID of the network you're attached to:
  Serial.print("SSID: ");
  Serial.println(Wi-Fi.SSID());
 // print your Wi-Fi shield's IP address:
 IPAddress ip = Wi-Fi.localIP();
 Serial.print("IP Address: ");
 Serial.println(ip);
// print where to go in a browser:
Serial.print("To see this page in action, open a browser to http://");
Serial.println(ip);
}
```

esempio

File sorgenti
Scarica il file

Wi-Fi Web Server

Materiale necessario:
- scheda Arduino + Wi-Fi shield oppure Arduino MKR1010;
- cavo USB per Arduino Uno oppure cavo microUSB per Arduino MKR1010;
- potenziometro collegato tra Vcc e GND con cursore collegato al PIN A0.

```
/*
 Wi-Fi Web Server

 A simple web server that shows the value of the analog input pins.
 This example is written for a network using WPA encryption. For
 WEP or WPA, change the Wi-Fi.begin() call accordingly.
 Circuit:
 * Analog inputs attached to pins A0 through A5 (optional)

 created 13 July 2010 by dlf (Metodo2 srl)
 modified 31 May 2012
 by Tom Igoe

 */
#include <SPI.h>
#include <Wi-FiNINA.h>
#include "arduino_secrets.h"

///////please enter your sensitive data in the Secret tab/arduino_secrets.h
char ssid[] = SECRET_SSID;        // your network SSID (name)
char pass[] = SECRET_PASS;    // your network password (use for WPA, or use as key
```

```
                                // for WEP)
int keyIndex = 0;               // your network key Index number (needed only for WEP)
int status = WL_IDLE_STATUS;
Wi-FiServer server(80);

void setup()
 {
  //Initialize serial and wait for port to open:
  Serial.begin(9600);
  while (!Serial)
       {
            ; // wait for serial port to connect. Needed for native USB port only
       }

  // check for the Wi-Fi module:
  if (Wi-Fi.status() == WL_NO_MODULE) {
    Serial.println("Communication with Wi-Fi module failed!");
    // don't continue
    while (true);
  }

  String fv = Wi-Fi.firmwareVersion();
  if (fv < Wi-Fi_FIRMWARE_LATEST_VERSION)
   {
    Serial.println("Please upgrade the firmware");
   }

  // attempt to connect to Wi-Fi network:
  while (status != WL_CONNECTED)
    {
    Serial.print("Attempting to connect to SSID: ");
    Serial.println(ssid);
    // Connect to WPA/WPA2 network. Change this line if using open or WEP network:
    status = Wi-Fi.begin(ssid, pass);
    delay(10000);      // wait 10 seconds for connection:
    }
 server.begin();
  // you're connected now, so print out the status:
  printWi-FiStatus();
}


 void loop()
  {
  // listen for incoming clients
  Wi-FiClient client = server.available();
  if (client)
    {
    Serial.println("new client");
    // an http request ends with a blank line
    boolean currentLineIsBlank = true;
    while (client.connected())
      {
```

Predispone all'utilizzo della porta 80

Predispone all'utilizzo della porta 80

Richiama la funzione che visualizza i parametri di connessione

→

```
    if (client.available())
     {
      char c = client.read();
      Serial.write(c);
      // if you've gotten to the end of the line (received a newline
      // character) and the line is blank, the http request has ended,
      // so you can send a reply
      if (c == '\n' && currentLineIsBlank)
       {
        // send a standard http response header
        client.println("HTTP/1.1 200 OK");
        client.println("Content-Type: text/html");
        client.println("Connection: close");  // the connection will be closed after
                                              // completion of the response
        client.println("Refresh: 5");  // refresh the page automatically every 5 sec
        client.println();
        client.println("<!DOCTYPE HTML>");
        client.println("<html>");
        // output the value of each analog input pin
        for (int analogChannel = 0; analogChannel < 6; analogChannel++)
          {
            int sensorReading = analogRead(analogChannel);
            client.print("analog input ");
            client.print(analogChannel);
            client.print(" is ");
            client.print(sensorReading);
            client.println("<br />");
          }
        client.println("</html>");
        break;
       }
      if (c == '\n')
        {
         // you're starting a new line
         currentLineIsBlank = true;
        } else if (c != '\r')
                {
                 // you've gotten a character on the current line
                 currentLineIsBlank = false;
                }
     }
    }
    // give the web browser time to receive the data
    delay(1);

    // close the connection:
    client.stop();
    Serial.println("client disconnected");
  }
}

void printWi-FiStatus()
  {
```

Genera una pagina web

Effettua la lettura di 5 ingressi analogici da A0 ad A5

Funzione che visualizza i parametri di connessione

```
// print the SSID of the network you're attached to:
Serial.print("SSID: ");
Serial.println(Wi-Fi.SSID());
// print your board's IP address:
IPAddress ip = Wi-Fi.localIP();
Serial.print("IP Address: ");
Serial.println(ip);
// print the received signal strength:
long rssi = Wi-Fi.RSSI();
Serial.print("signal strength (RSSI):");
Serial.print(rssi);
Serial.println(" dBm");
}
```

1.3 Altre schede per IoT

La necessità di avere moduli di dimensioni molto contenute e consumi ridottissimi ha portato allo sviluppo di schede che hanno un numero ridotto di pin, ma più che sufficiente per pilotare semplici dispositivi o acquisire dati. La tipologia di schede che ha avuto maggior successo è quella chiamata Famiglia ESP8266 (FIGURA 3) perché si basa sull'integrato SOC ESP8266. Le schede sono programmabili con comandi AT, ma sono stati sviluppati firmware i quali consentono l'interfacciamento tramite il programma *Arduino.exe* che utilizzando le librerie dedicate consente una programmazione più immediata e la possibilità di utilizzare i listati esistenti per Arduino, con piccoli adattamenti dovuti al numero ridotto di pin e alcuni altri parametri.
Il collegamento deve avvenire , per i moduli che non prevedono la presa microUSB, tramite un adattatore con la porta USB, un debugger seriale (FIGURA 4) il cui collegamento è mostrato in FIGURA 5.

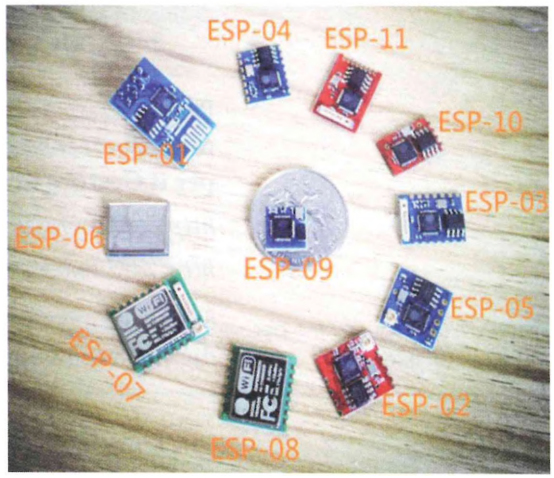


FIGURA 3 Famiglia ESP8266

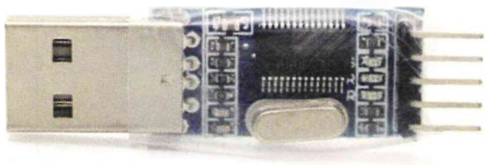


FIGURA 4 Debugger seriale

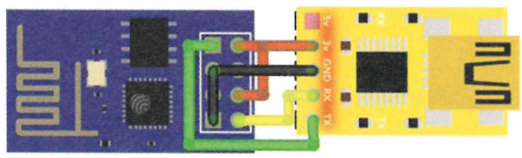


FIGURA 5 Collegamento con modulo ESP8266

Un'altra famiglia di schede è la ESP32 (FIGURA 6), un'evoluzione della ESP8266, che rispetto a quest'ultima ha la possibilità di collegarsi al computer per la programmazione utilizzando una connessione con microUSB. La configurazione esterna si mantiene, ma cambiano notevolmente le prestazioni in base al microcontrollore utilizzato.

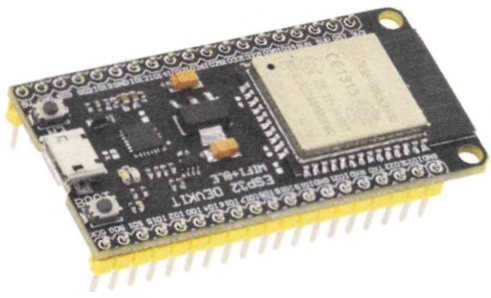


FIGURA 6 ESP32

Qui di seguito i parametri dei modelli più utilizzati

MICROPROCESSORE	Tensilica Xtensa dual-core 32-bit LX6	Tensilica 32-bit RISC CPU Xtensa LX106
ARCHITETTURA	32 BIT	32 bit
CORE	2	1
CPU	240 MHz	80 MHz
Wi-Fi	IEEE 802.11 b/g/n	IEEE 802.11 b/g/n
BLUETOOTH	4.2	/
RTC	Sì	/
RAM	512 kB	24 kB
MEMORIA FLASH	4 MB	4 MB
PIN GPIO	36	16
INTERFACCIA	CAN, I2C, SPI, UART	I2C, SPI, UART
TENSIONE OPERATIVA	3,3 V	3,3 V

Per utilizzare *Arduino.exe* per la programmazione occorre modificare le impostazioni (FIGURA 7): inserendo dal **Menu File > Impostazioni...** nel campo **URL aggiuntive per il Gestore di schede** uno dei seguenti link:

https://dl.espressif.com/dl/package_esp32_index.json (scheda ESP32)

http://arduino.esp8266.com/stable/package_esp8266com_index.json (scheda ESP8266)

Successivamente (FIGURA 8) occorre andare in **Strumenti > Scheda > Gestione schede**, digitare **esp32** oppure **esp8266** e cliccare su **Installa**.

FIGURA 7 Configurazione per ESP32 e ESP8266

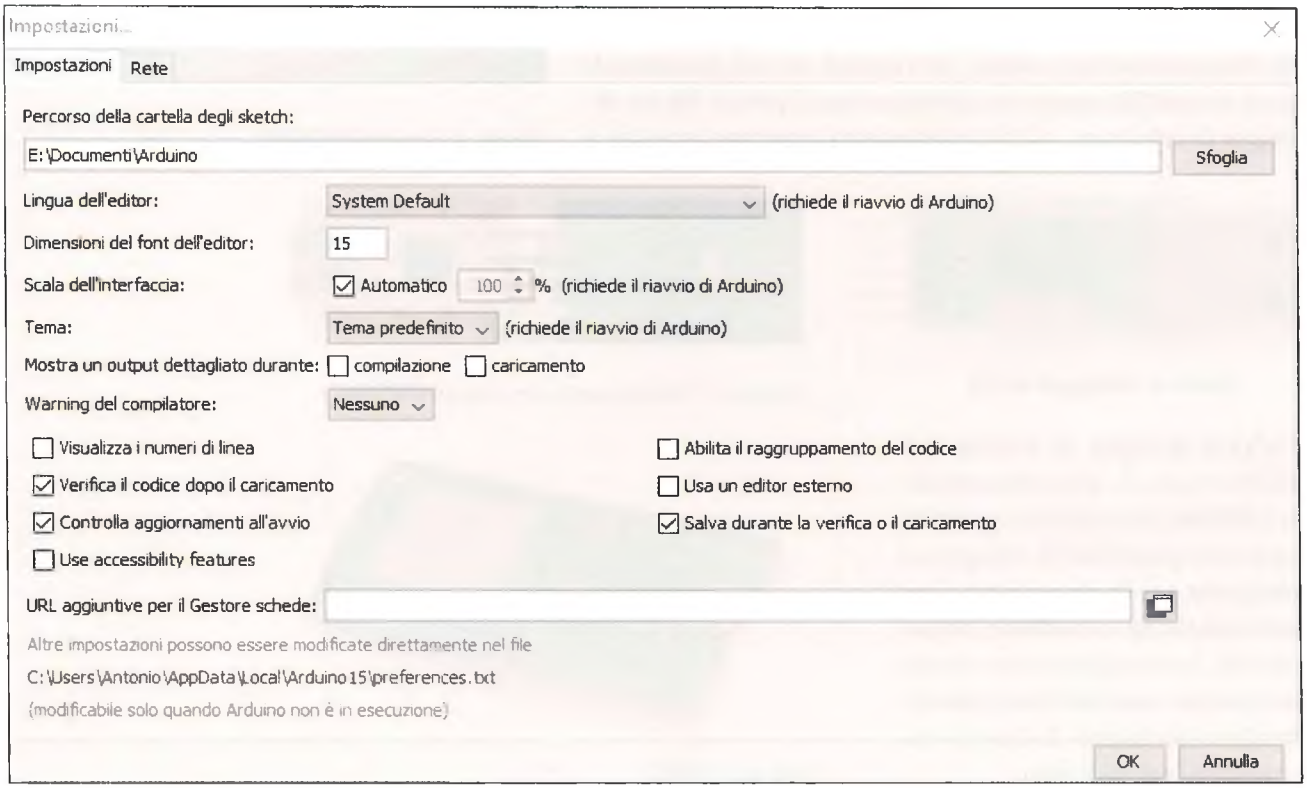


FIGURA 8 Finestra di dialogo per installazione libreria ESP32

Al termine dell'installazione, tra le schede installabili comparirà la famiglia ESP32 tra cui scegliere quella da collegare. Per poter programmare la ESP32 è sufficiente il collegamento tramite cavo USB A – microUSB, mentre per la scheda ESP8266 occorre ricorrere a un piccolo accorgimento: collegare un condensatore da 10 µF tra il pin EN (terminale positivo del condensatore) e GND (terminale negativo del condensatore) per abilitare la programmazione (FIGURA 9). Durante il normale uso il condensatore non deve essere utilizzato.

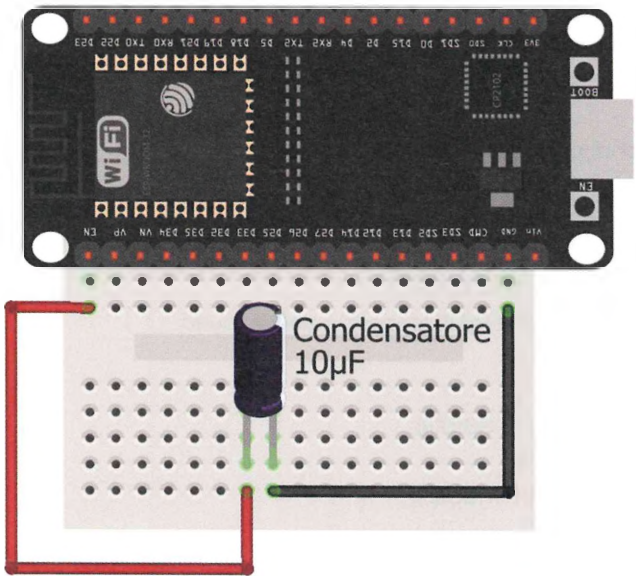


FIGURA 9 Collegamento per programmazione ESP8266

esempio

Scansione reti Wi-Fi

File sorgenti
Scarica il file

Materiale necessario:
– scheda ESP32 (oppure ESP8266);
– cavo USB A - microUSB;
– condensatore 10 µF / 10 V (se si utilizza ESP8266);
– basetta millefori;
– filo rigido.

```
/*
 * This sketch demonstrates how to scan Wi-Fi networks.
 * The API is almost the same as with the Wi-Fi Shield library,
 * the most obvious difference being the different file you need to include:
 */
#include "Wi-Fi.h"

void setup()
{
  Serial.begin(115200);
  // Set Wi-Fi to station mode and disconnect from an AP if it was previously connected
  Wi-Fi.mode(Wi-Fi_STA);
  Wi-Fi.disconnect();
  delay(100);
  Serial.println("Setup done");
}
void loop()
{
  Serial.println("scan start");

  // Wi-Fi.scanNetworks will return the number of networks found
  int n = Wi-Fi.scanNetworks();
  Serial.println("scan done");
  if (n == 0)
   {
     Serial.println("no networks found");
   } else {
          Serial.print(n);
          Serial.println(" networks found");
          for (int i = 0; i < n; ++i) {
      // Print SSID and RSSI for each network found
      Serial.print(i + 1);
      Serial.print(": ");
      Serial.print(Wi-Fi.SSID(i));
      Serial.print(" (");
      Serial.print(Wi-Fi.RSSI(i));
      Serial.print(")");
      Serial.println((Wi-Fi.encryptionType(i) == Wi-Fi_AUTH_OPEN)?" ":"*");
      delay(10);
    }
  }
  Serial.println("");

  // Wait a bit before scanning again
  delay(5000);
}
```

Quando rileva la presenza di reti Wi-Fi inizia la scansione, visualizzando i nomi sul monitor seriale di *Arduino.exe*

esempio

Utilizzo UDP tramite Wi-Fi

File sorgenti
Scarica il file

Materiale necessario:
- scheda ESP32 (oppure ESP8266);
- cavo USB A - microUSB;
- condensatore 10 µF / 10 V (se si utilizza ESP8266);
- basetta millefori;
- filo rigido.

```
// This sketch sends random data over UDP on ESP32 device

#include <Wi-Fi.h>
#include <Wi-FiUdp.h>

// Wi-Fi network name and password:
const char * networkName = "your-ssid";
const char * networkPswd = "your-password";

//IP address to send UDP data to:
// either use the ip address of the server or
// a network broadcast address
const char * udpAddress = "192.168.0.255";
const int udpPort = 3333;

//Are we currently connected?
boolean connected = false;

//The udp library class
Wi-FiUDP udp;

void setup()
 {
 Serial.begin(115200);                          // Initialize hardware serial:
   connectToWi-Fi(networkName, networkPswd);   //Connect to the Wi-Fi network
 }

void loop()
{
 if(connected) //only send data when connected
   {
    //Send a packet
     udp.beginPacket(udpAddress,udpPort);
      udp.printf("Seconds since boot: %lu", millis()/1000);
      udp.endPacket();
    }
 //Wait for 1 second
 delay(1000);
}
```

Libreria UDP Wi-Fi

Richiama la funzione che effettua la connessione

→

Richiama la funzione che legge i parametri della rete a cui è connesso

```
void connectToWi-Fi(const char * ssid, const char * pwd)
    {
     Serial.println("Connecting to Wi-Fi network: " + String(ssid));
     // delete old config
     Wi-Fi.disconnect(true);
     //register event handler
     Wi-Fi.onEvent(Wi-FiEvent);
    //Initiate connection
     Wi-Fi.begin(ssid, pwd);
    Serial.println("Waiting for Wi-Fi connection...");
  }     //Wi-Fi event handler

void Wi-FiEvent(Wi-FiEvent_t event){
   switch(event)
     {
       case SYSTEM_EVENT_STA_GOT_IP:
            //When connected set
            Serial.print("Wi-Fi connected! IP address: ");
            Serial.println(Wi-Fi.localIP());
           //initializes the UDP state
           //This initializes the transfer buffer
           udp.begin(Wi-Fi.localIP(),udpPort);
           connected = true;
           break;
       case SYSTEM_EVENT_STA_DISCONNECTED:
            Serial.println("Wi-Fi lost connection");
            connected = false;
            break;
     default: break;
   }
}
```

FISSA LE CONOSCENZE

- La Wi-Fi shield è una scheda autonoma? Perché?
- Una scheda ESP32 è una scheda Wi-Fi autonoma? Perché?
- Quali parametri rendono l'ESP32 più adatto all'IoT?
- La scheda ESP8266 è programmabile direttamente tramite cavo USB?

2 RASPBERRY Pi PER IoT

La filosofia che guida lo sviluppo dell'IoT ha come obiettivo quello di ottenere che apparecchiature di uso comune (elettrodomestici, lampade, impianti audio-video, oggetti indossabili) siano in grado di dialogare con l'utente per consentirgli di configurarle e utilizzarle mediante un computer o uno smartphone, un assistente vocale (per esempio Google Home o Amazon Alexa) e la rete Internet, senza l'utilizzo di cavi di collegamento. Ciò può essere ottenuto inserendo delle schede dotate di connessione Wi-Fi all'interno degli elettrodomestici stessi.

Occorre quindi che la scheda utilizzata sia poco ingombrante, dotata di una discreta potenza di calcolo e, nel caso di apparati portatili, consumi molto poco per non incidere sulla durata delle batterie del dispositivo portatile.

La scheda Raspberry Pi soddisfa i criteri relativi alla potenza di calcolo e alla connessione Wi-Fi, ma ha dei consumi non trascurabili, poco adatti a un'alimentazione a batteria. Tale limite ha portato da una parte a utilizzare la scheda Raspberry Pi all'interno di apparecchiature alimentate costantemente dalla rete elettrica, dall'altra allo sviluppo di schede Raspberry a bassissimo consumo a scapito della potenza di calcolo, come la scheda Raspberry PI Zero (FIGURA 10), oltre a un prezzo bassissimo. Le configurazioni di tale scheda differiscono per la presenza o meno di alcuni connettori pre-saldati.

Dati tecnici Raspberry PI Zero WH

Broadcom BCM2835
– processore ARM11 a core singolo 1 GHz
– RAM 512 MB

Connettività wireless
– 802.11 b/g/n wireless LAN
– Bluetooth 4.1
– Bluetooth Low Energy (BLE)

Connettore GPIO 40 Pin pre-saldato

Slot scheda di memoria micro SD

MiniHDMI port (uscita video)

Porta microUSB di alimentazione

Porta microUSB dati OTG

CSI camera connector

Uscita video RCA

Connettore di reset

Dimensioni: 65 mm x 30 mm x 11.6 mm

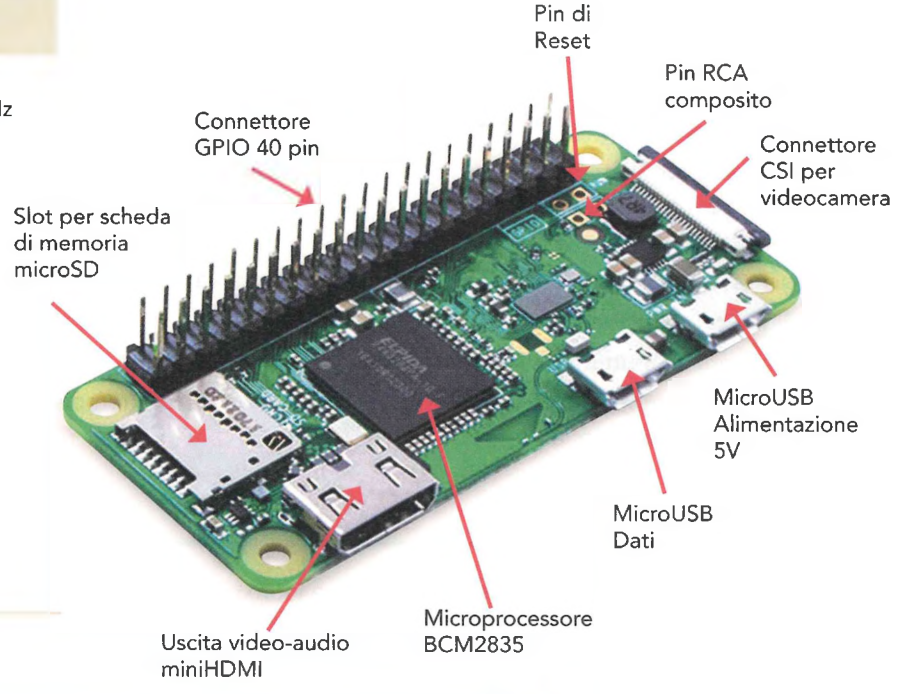


FIGURA 10 Raspberry Pi Zero

FISSA LE CONOSCENZE

- Per quale motivo i dispositivi IoT indossabili devono avere bassissimi consumi elettrici?
- Quale connessione utilizzano più frequentemente i dispositivi IoT?
- In che cosa differisce una normale scheda Raspberry PI dalla versione Zero?

LAVORARE PER COMPETENZE

COMPETENZE IN GIOCO

Competenze disciplinari

- Conoscere i parametri di una scheda di rete per Arduino.
- Configurare la scheda di rete in base alla rete a cui è collegata.

Competenze chiave di cittadinanza

- Interpretare il testo.
- Risolvere problemi.
- Comunicare.
- Competenza digitale.

obiettivi formativi

- Consultare fonti Internet.
- Esporre i risultati della ricerca alla classe.

tempi

- Ricerca di informazioni in rete sul tema proposto: 1 ora.
- Personale risoluzione del tema proposto: 1 ora.
- Preparazione di una presentazione con la propria soluzione: 1 ora.
- Illustrazione dei risultati e dibattito in classe: 1 ora.
- Autovalutazione: 10 minuti.

strumenti

- Libro di testo.
- Dispositivo connesso a Internet.
- Carta e penna.
- Software per le presentazioni.
- Proiettore o LIM in classe o in laboratorio.

TEMA PROPOSTO

Occorre monitorare la temperatura, umidità e luminosità ambientale di un laboratorio in cui si studia la crescita di alcune piante e trasmettere le informazioni su una pagina web di monitoraggio tramite connessione Internet wireless.

File sorgenti
Scarica il file

- Scegliere i sensori adeguati alle esigenze (intervallo di valori da rilevare, precisione).
- Configurare opportunamente la scheda di rete.
- Determinare la struttura della pagina web.
- Determinare la modalità di memorizzazione delle informazioni (tempistiche, memorie di massa da utilizzare, tipologia di rappresentazione grafica).

SVOLGIMENTO

- Individuare su siti Internet i sensori più adatti e i loro costi.
- Ricercare esempi disponibili in rete per l'acquisizione, la visualizzazione e la memorizzazione delle singole grandezze.
- Disegnare uno schema dei vari blocchi utilizzati.
- Disegnare lo schema dei collegamenti elettrici.
- Verificare il funzionamento del software con i singoli sensori tramite simulatore on line.
- Costruire una pagina HTML di prova e determinare i comandi necessari per la visualizzazione dei parametri richiesti.
- Integrare i vari listati in modo da gestire contemporaneamente le varie grandezze.
- Simulazione complessiva del programma e gestione della pagina web.
- Ricerca di possibili ottimizzazioni.
- Stesura della relazione.

A CASA

- Predisposizione del progetto in modo completo, inserendo la valutazione dei costi dei vari dispositivi utilizzati.
- Valutazione delle possibili migliorie al sistema.

IN CLASSE

- Condividi la presentazione dei tuoi risultati con i compagni.
- Confrontate e discutete insieme i casi che sono stati presentati.
- Stabilite quale caso rappresenta l'esempio migliore sia dal punto di vista tecnico, sia dal punto di vista economico per completezza e che meglio si adatta alla soluzione del tema proposto.
- Procedi con l'autovalutazione.

AUTOVALUTAZIONE

ATTIVITÀ	LIVELLO			
	INIZIALE	BASE	INTERMEDIO	AVANZATO
Ho compreso senza difficoltà le richieste dell'attività proposta?	Ho compreso solo alcune delle richieste aiutato dal docente. ☐	Con la guida del docente e la collaborazione dei compagni ho compreso quasi tutte le richieste. ☐	Ho compreso le richieste e in parte le ho svolte autonomamente. ☐	Ho identificato le richieste e le ho svolte senza difficoltà. ☐
Ho reperito in rete le informazioni su come configurare il modulo Wi-Fi scelto ed ottimizzare la visualizzazione dei dati acquisiti?	Ho reperito solo alcune delle informazioni utili. ☐	Con la guida del docente e la collaborazione dei compagni ho reperito quasi tutte le informazioni. ☐	Ho reperito le informazioni utili autonomamente e le ho elaborate. ☐	Ho identificato le informazioni utili e le ho elaborate senza difficoltà. ☐
Sono riuscito a realizzare una presentazione convincente?	Ho preparato una presentazione di 3 slide con poche informazioni. ☐	Ho preparato una presentazione con molte informazioni un po' confuse. Non sono riuscito a spiegarmi bene. ☐	Ho preparato una presentazione con molte informazioni abbastanza strutturate. Non sono riuscito a spiegarmi bene. ☐	Ho preparato una presentazione con molte informazioni ben strutturate. Sono riuscito a far capire a tutti i concetti che volevo esprimere. ☐

RISPOSTE AI QUESITI DI FINE UNITÀ

UNITÀ 1 TECNICHE DI CRITTOGRAFIA PER L'INTERNET SECURITY

Vero (V) o falso (F) pag. 26
1. V 2. F 3. V 4. V 5. F 6. V 7. V 8. V 9. F

Domande a scelta multipla pag. 26
1. C 2. A 3. A 4. C 5. A 6. C

In English, please pag. 27
7 5 8 6 3 2 1 4

UNITÀ 2 EFFICIENZA E SICUREZZA NELLE RETI LOCALI

Vero (V) o falso (F) pag. 76
1. V 2. V 3. V 4. F 5. V 6. V 7. V 8. F 9. V 10. V

Domande a scelta multipla pag. 76
1. B 2. D 3. C 4. B

In English, please pag. 77
4 8 1 5 7 2 3 6

UNITÀ 3 LE RETI PRIVATE VIRTUALI (VPN)

Vero (V) o falso (F) pag. 112
1. F 2. V 3. V 4. F 5. F 6. V 7. F 8. V

Domande a scelta multipla pag. 112
1. C 2. B 3. C 4. B

In English, please pag. 113
4 6 2 1 3 5 8 7

UNITÀ 4 LE RETI WIRELESS

Vero (V) o falso (F) pag. 142
1. F 2. V 3. V 4. V 5. V 6. V 7. F 8. V

Domande a scelta multipla pag. 142
1. B 2. A 3. D 4. A 5. A 6. D

In English, please pag. 143
6 4 8 1 7 2 5 3

UNITÀ 5 RETI IP E RETI CELLULARI PER UTENTI MOBILI

Vero (V) o falso (F) pag. 179
1. V 2. V 3. V 4. F 5. V 6. F 7. V 8. V 9. V 10. F

Domande a scelta multipla pag. 179
1. A 2. B 3. C 4. B

In English, please pag. 180
6 4 8 1 7 2 5 3

UNITÀ 6 PROGETTARE STRUTTURE DI RETE: DAL CABLAGGIO AL CLOUD

Vero (V) o falso (F) pag. 215
1. F 2. V 3. V 4. V 5. F 6. V 7. F 8. V 9. V

Domande a scelta multipla pag. 215
1. D 2. B 3. C 4. A

In English, please pag. 216
8 4 6 7 2 3 1 5

UNITÀ 7 ARCHITETTURE WEB: SERVIZI, APPLICAZIONI, AMMINISTRAZIONE

Vero (V) o falso (F) pag. 251
1. V 2. V 3. F 4. V 5. F 6. V 7. F 8. V

Domande a scelta multipla pag. 251
1. C 2. A 3. C 4. A

In English, please pag. 252
2 7 1 6 8 5 4 3

UNITÀ 8 LA GESTIONE DELLA RETE E DEI SISTEMI

Vero (V) o falso (F) pag. 283
1. F 2. F 3. F 4. V 5. F 6. V 7. V 8. F 9. F 10. V

Domande a scelta multipla pag. 283
1. A 2. B 3. B 4. A

In English, please pag. 284
6 5 1 7 4 3 8 2

LEGENDA IMMAGINI

APPARATI DI RETE

Router

Router Firewall

Switch

Hub

Router-Switch

Firewall

Antenna mobile

Modem-Router-Switch-
Access point Rete domestica

Access point aziendale

END SYSTEM

Computer desktop

Computer laptop

Tablet

Smartphone

Telefono IP

Stampante

Server

Server rack

Proxy Firewall

Database

REFERENZE ICONOGRAFICHE

Archivio GettyImages

ArtemSam
Audy_indy
Balck_jack3D
bwzenith
David Malan
Dean Mitchell
Dimitri Otis
DrAfter123
ilbusca
inarik
Jacob Ammentorp Lund
Jesussanz
John Lamb
John Lund
Mitrija
olaser
paYoshimi
Radachynskyi
ryasick
serts
SolStock
VladCa
wwing
Yuri_Arcurs

SOFTWARE CITATI NEL TESTO

Software utilizzati

Cisco Packet Tracer 7.3.1
Wireshark 3.x
Processing
NGINX e PHP per Raspberry Pi4

Sistemi Operativi affrontati

Windows 10 (desktop)
Windows Server 2019
GNU/Linux (UBUNTU 20.04 LTS desktop e server)
Cisco IOS
Raspberry Pi4 (Raspberry Pi OS)

Software/marchi citati

Cisco
Cisco Prime Infrastructure
Cisco FindIT Network Manager
Microsoft
Office365
Hyper-V
PowerShell
Active Directory
Visual Studio Code
NetBios
SQL Server
Azure
Internet Information Services (IIS)
Apple
Parallels desktop
Symantec
Software Virtualization Solution (SVS)
Apache
Android
Java
Oracle VM VirtualBox
VMware
VMware Worstation Pro e Workstatio Player
VMware Fusion Pro e Fusion Player
Microsoft App-V
Parallel Desktop
Citrix Virtual Apps and desktops
Altervista
Hostinger
Netsons
Ilbello
Amazon Web Services (AWS)
Google cloud
Gmail
Aruba Jelastic Cloud
Dell
HP
IBM
McAfee
Samba
Avaya Unified Communication Management
HPE Intelligent Management Center
CA Unified Infrastructure Management
Solarwinds NP
Net-SNMP
Nagios
ZABBIX
Multi Router Traffic Grapher (MRTG)
Netflix, Spotify