Indice

VLAN (Virtual Local Area Network)

Una VLAN consente di realizzare una LAN logica virtuale, grazie allo standard 802.1Q, su una infrastruttura di rete già esistente.

In poche parole, una VLAN consente di:

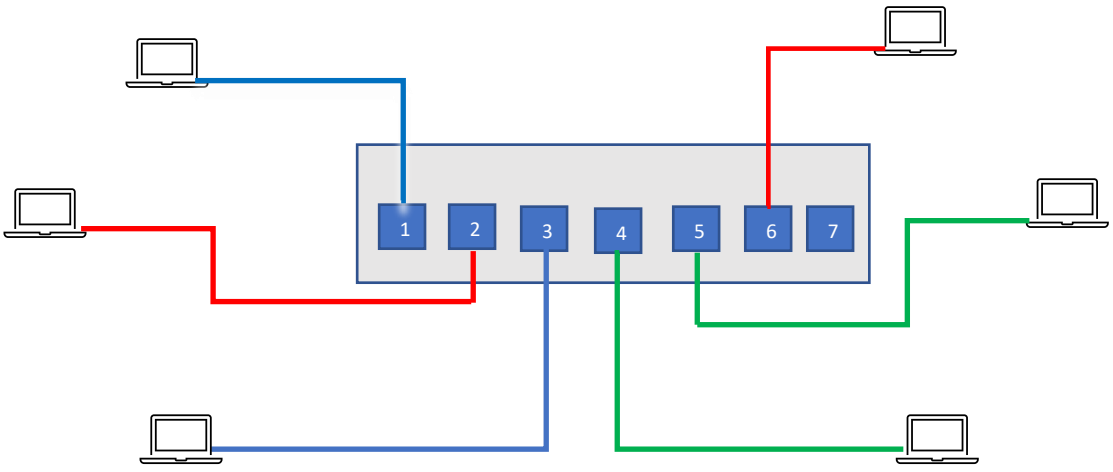
- Ad host distinti su reti separate (quindi con diversi indirizzi IP) di connettersi alla stessa rete logica condividendo lo stesso dominio di collisione;
- Di separare logicamente host appartenenti alla stessa rete fisica (quindi con lo stesso indirizzo IP), che condividono lo stesso dominio di broadcast, in diverse VLAN separando i domini di broadcast per ogni VLAN realizzata.

Per realizzare una VLAN bisogna intervenire sugli switch e bridge che devono osservare lo standard 802.1Q; vi sono due modalità per realizzare una VLAN:

1. **Port based VLAN (untagged)**
2. **VLAN 802.1Q (tagged)**

1. Port based VLAN (untagged).

Questa modalità viene anche detta *statica*: in questo caso, gli switch vengono 'divisi' in base alle porte, nel senso che un numero determinato di porte definiscono una VLAN, altre un'altra VLAN e così via (le porte devono essere configurate 'access')



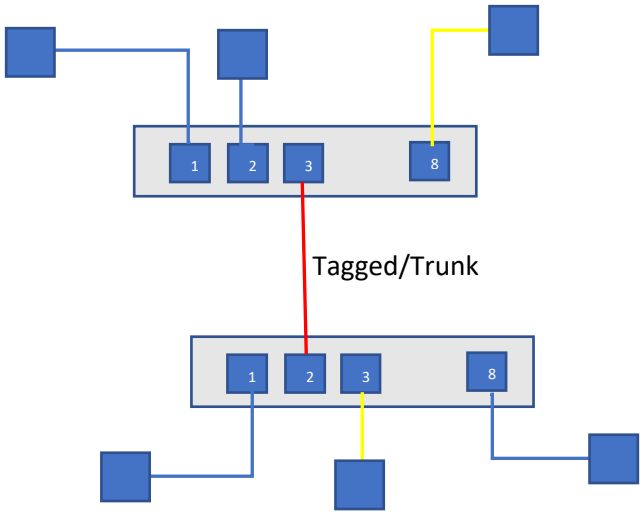
Nel disegno sono indicate tre VLAN che collegano due host ciascuna: la prima, di colore blu, collega le porte 1 e 3; la seconda, di colore rosso, collega le porte 2 e 6; la terza, di colore verde, collega le porte 4 e 5. Questa tipologia di VLAN è poco sicura: infatti ogni dispositivo collegato ad una porta dello switch appartiene alla corrispondente VLAN.

2. VLAN 802.1Q (tagged).

Questa modalità utilizza un protocollo (802.1Q appunto) che aggiunge un ***tag*** (un insieme di 4 bytes- due bytes detti **TPI -** Tag Protocol Identifier - gli altri due, **TCI** - Tag

Control Information, in cui 12 bit definiscono la VLAN e prendono il nome di **VID** – VLAN ID) ai frame e che specifica a quale VLAN appartengono. L'inserimento/decodifica del tag, viene effettuato da un'apposita porta dello switch configurata 'trunk'. Infatti, quando i frame viaggiano su VLAN in modalità basata sulle porte, è lo switch che li indirizza sulla porta della VLAN corrispondente, se viaggiano in modalità tagged l'informazione a quale VLAN appartengono deve essere inserita nel frame in modo che lo switch che riceve il frame sa dove questo deve essere indirizzato. In definitiva su una stessa porta trunk possono viaggiare frame appartenenti a VLAN differenti.

Non c'è una regola che determina quale modalità si deve usare per realizzare una VLAN, di solito per gli switch che collegano host si utilizza la metodologia basata sulle porte, mentre per il collegamento tra switch, si usa la tagged-trunk.



Dalla figura, si può notare come più VLAN possono essere collegate anche attraverso diversi switch: sulle porte tagged-trunk viaggiano, in definitiva, diversi frames appartenenti a diverse VLAN. Le porte tagged-trunk di uno switch, anche se accettano tutti i frames di tutte le VLAN, possono essere configurate per accettarne solo alcuni e questo meccanismo può essere applicato a tutti gli switch della rete, operazione onerosa e complessa per reti di grandi dimensioni. Il protocollo VTP (Virtual Trunking Protocol) della Cisco, consente di configurare tutte le VLAN attraverso un solo switch che, a sua volta, configura tutti gli switch ad esso collegati e che condividono delle VLAN (VTP domain).

Tale operazione può avvenire sugli switch Cisco, in tre modalità:

1. Server;
2. Client;
3. Transparent;

Su uno switch che opera in modalità ***Server***, l'amministratore ha la possibilità di modificare la configurazione delle VLAN (aggiungere/eliminare/modificare VLAN): una volta effettuata la modifica, tale modifica viene propagata a tutti gli switch appartenenti al dominio VTP.

La modalità ***Client*** permette ad uno switch di ricevere le modifiche effettuate sullo switch che opera in modalità Server: in questa modalità lo switch prima controlla se le modifiche

lo interessano, se sì modifica le informazioni memorizzate in un apposito database; quindi, inoltra le informazioni agli altri switch. Uno switch che opera in modalità client per determinare se le informazioni che riceve da un altro switch devono modificare quelle in suo possesso, controlla la versione (version number) che viene incrementata da uno switch server. Se la versione è maggiore rispetto la corrente, lo switch Client aggiorna le informazioni.

Gli switch che non appartengono al VTP domain operano in modalità ***Transparent***: propagano semplicemente le informazioni ricevute da uno switch agli altri switch ad esso collegati.

I messaggi che vengono prodotti dagli switch server e che si propagano nella rete prendono il nome di ***VTP ADVERTISEMENT***.

INTER-VLAN ROUTING.

Come scritto precedentemente, le VLAN si estendono anche oltre i collegamenti fisici di reti realizzate con switch. Possiamo realizzare VLAN anche tra dispositivi appartenenti a reti diverse. In questo caso la VLAN coinvolge necessariamente i router che, come sappiamo, consentono la 'navigazione' tra le reti differenti. Ricordiamo che il protocollo 802.1Q, inserisce nei frame le informazioni che indicano a quale VLAN il frame appartiene.

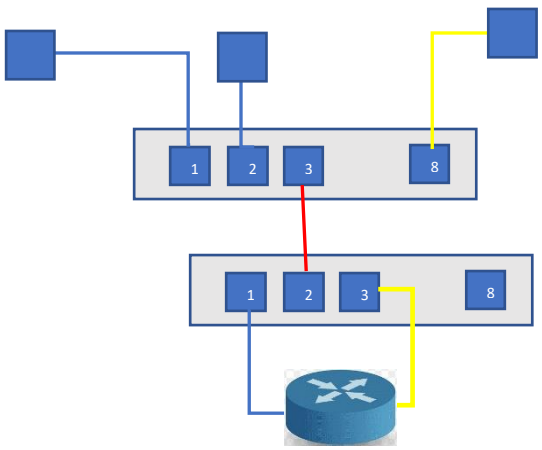
Per realizzare una Inter-VLAN Routing, vi sono tre soluzioni:

- Inter-VLAN tradizionale;
- 'Router-on-a-stick' Inter-VLAN;
- Switch based Inter-VLAN.

Inter-VLAN tradizionale

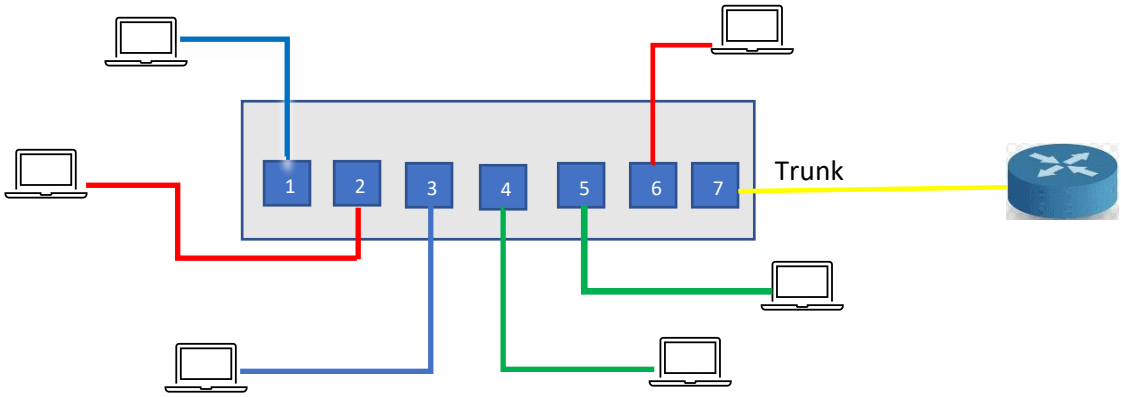
Per realizzare una Inter-VLAN tradizionale i diversi switch della LAN ove sono presenti le VLAN si collegano ad un router facendo attenzione che ogni VLAN deve essere connessa fisicamente ad una specifica porta del router. In definitiva il collegamento delle VLAN è basato sulle porte, una porta dello switch di una VLAN deve essere connessa ad una porta del router.

Es:



Router-on-a-stick Inter-VLAN

"Router on a stick" è il nome che si dà ad un router che ha il compito di effettuare routing tra VLAN diverse usando un'interfaccia in trunk su cui avviene il traffico delle VLAN interessate.

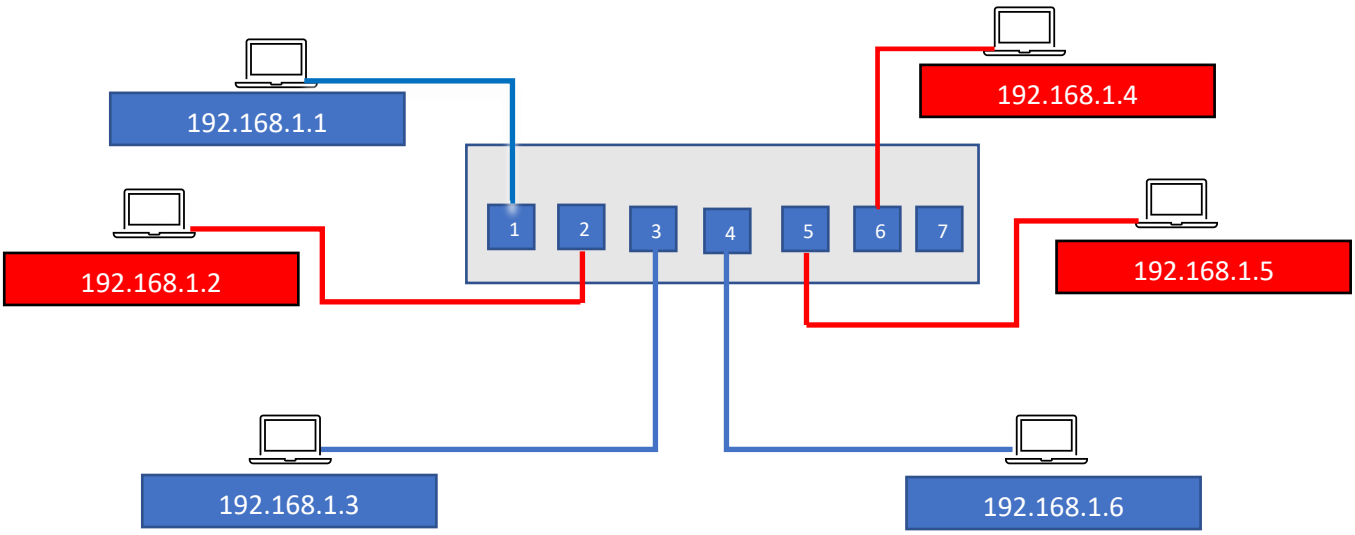


L'interfaccia fisica del router deve essere suddivisa in tante 'subinterfacce' logiche quante sono le VLAN.

Esempi.

Esempio 1. Realizzazione di due VLAN utilizzando un solo switch su 1 rete (port based).

Supponiamo di avere una rete composta come in figura con NetId 192.168.1.0 e nasce la necessità di suddividerla in due reti distinte in modo che una rete sia indipendente dall'altra.



Per ottenere il risultato richiesto dobbiamo agire sullo switch. Come prima operazione definiamo nella VLAN Database dello switch, le due VLAN assegnando al campo **VLAN Name**: *rete1* e al campo **VLAN Number**: *10*; quindi clicchiamo su ADD per aggiungere al database la VLAN. Analogamente ripetiamo l'operazione per la VLAN rete2: al campo **VLAN Name**: *rete2*, ed al campo **VLAN Number**: *20*. Clicchiamo nuovamente su ADD. Non ci resta che assegnare ad ogni porta cui abbiamo collegato un host, la VLAN di appartenenza.

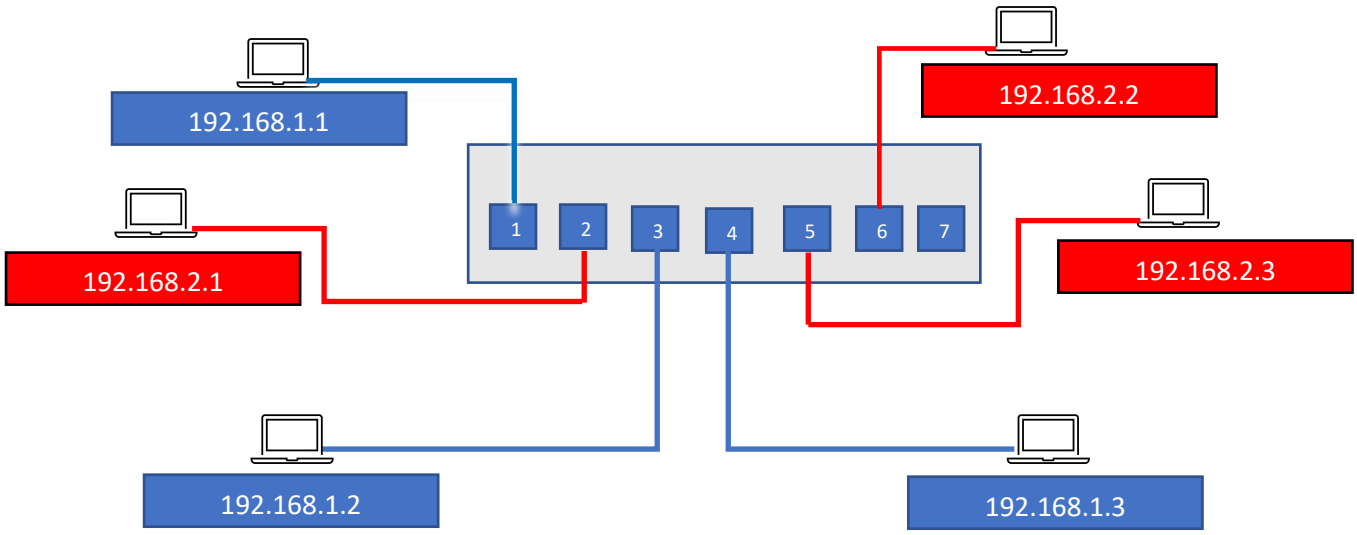
Quindi alle porte ethernet 1, 3 e 4 nella finestrella VLAN, che si ottiene cliccando sulla relativa interfaccia, selezioniamo la VLAN 10, mentre nelle porte 2, 5 e 6 la VLAN 20.

Esempio 2. Realizzazione di due VLAN utilizzando un solo switch con 2 reti (port based).

Supponiamo di voler realizzare due VLAN ognuna con tre host, la prima è la VLAN 'amministrazione' la seconda 'marketing'

Assegniamo ad ogni VLAN un indirizzo IP

NOME VLAN	INDIRIZZO IP	VID
Amministrazione	192.168.1.0	10
Marketing	192.168.2.0	20

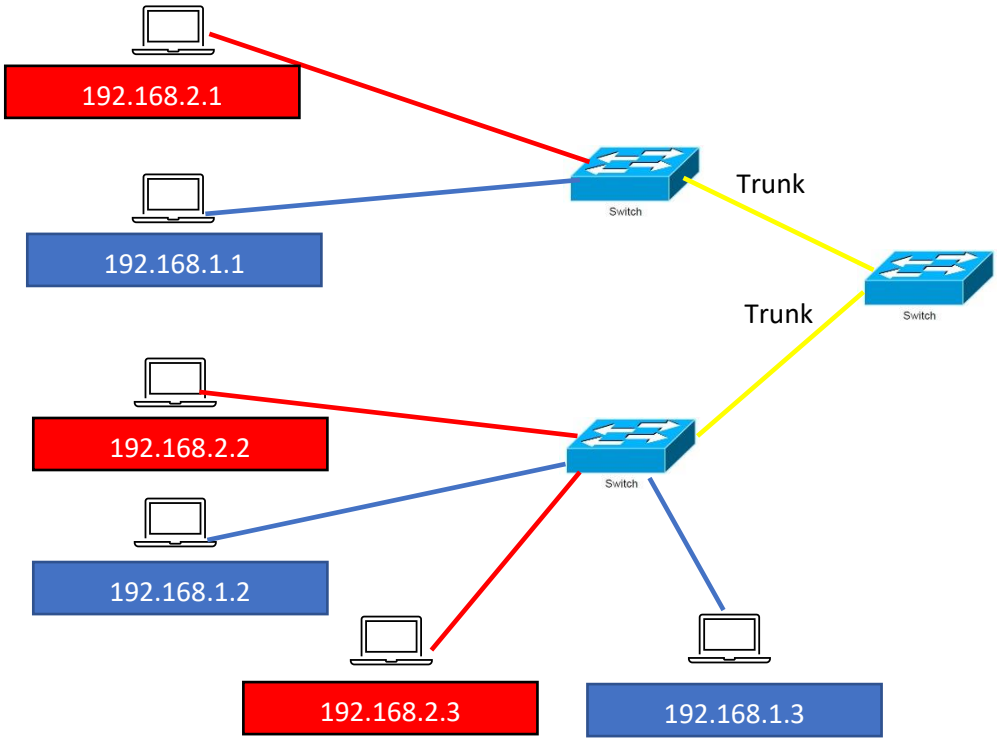


Nei rettangoli blu sono indicati gli indirizzi IP degli host della VLAN 'amministrazione', così nei rettangoli rossi sono indicati gli indirizzi IP degli host della VLAN 'marketing'.

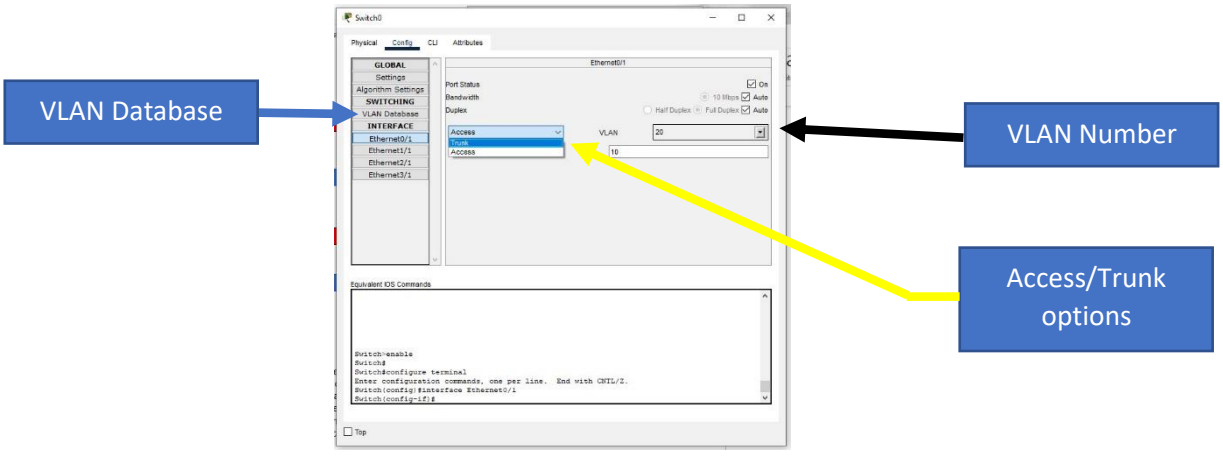
Ora dobbiamo agire sullo switch. Come prima operazione definiamo nella VLAN Database dello switch, le due VLAN assegnando al campo **VLAN Name**: *amministrazione* e al campo **VLAN Number**: *10*; quindi clicchiamo su ADD per aggiungere al database la VLAN. Analogamente ripetiamo l'operazione per la VLAN marketing: al campo **VLAN Name**: *marketing*, ed al campo **VLAN Number**: *20*. Clicchiamo nuovamente su ADD. Non ci resta che assegnare ad ogni porta cui abbiamo collegato un host, la VLAN di appartenenza. Quindi alle porte ethernet 1, 3 e 4 nella finestrella VLAN, che si ottiene cliccando sulla relativa interfaccia, selezioniamo la VLAN 10, mentre nelle porte 2, 5 e 6 la VLAN 20.

Esempio 3. Realizzazione di due VLAN utilizzando tre switch (port based – tagged-trunk)

Supponiamo ora, che i nostri 6 computer siano disposti in diversi piani dello stabile: ai piani alti, sono collocate le stanze dei dirigenti delle rispettive aree, mentre al pian terreno gli impiegati delle aree amministrazione e marketing. Ad ogni piano è situato uno switch, gli switch sono collegati tra loro tramite un altro switch.



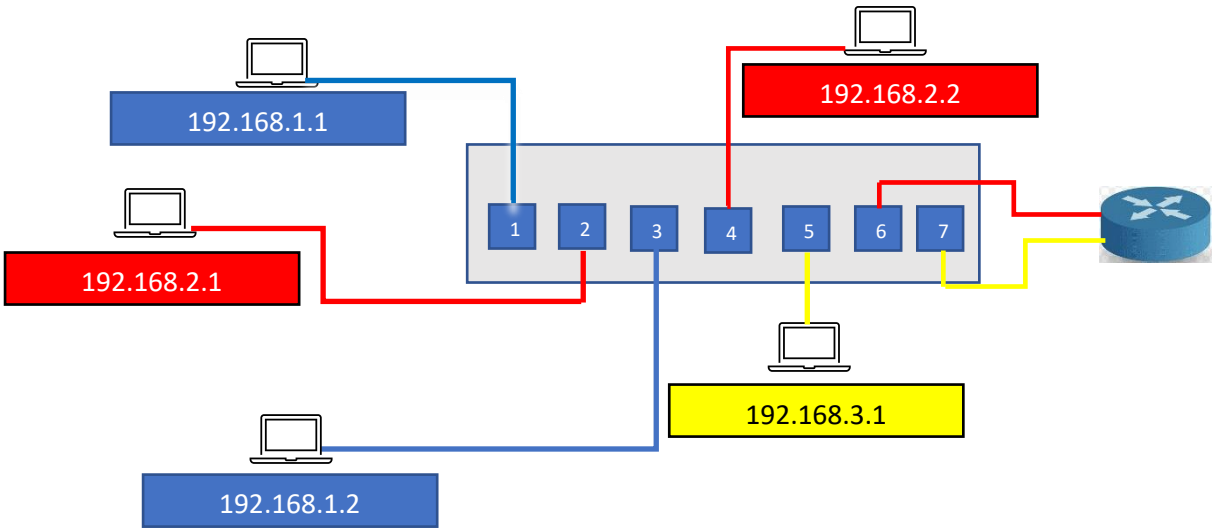
Come nell'esercizio precedente, bisogna configurare le VLAN database per i TRE switch, quindi per ogni switch definire la VLAN Name: *amministrazione* e VLAN Number: *10* ed aggiungerla al database, quindi la VLAN Name: *marketing* e VLAN Number: *20* e aggiungerla al database. Parimenti assegnare la VLAN 10 o 20 alle interfacce ethernet collegate agli host appartenenti alla VLAN amministrazione o alla VLAN marketing. Alle interfacce che collegano gli switch cambiare l'opzione 'Access' con l'opzione 'Trunk'.



Esempio 4. Realizzazione di due VLAN che comunichino tra loro e una terza a sé stante (Inter-VLAN Tradizionale).

Supponiamo di voler realizzare due reti logiche distinte che colleghino, una gli studenti un'altra i docenti. Il problema è che alcuni studenti utilizzano una rete con un indirizzo IP

diverso rispetto quello utilizzato da un altro gruppo di studenti. Vediamo come possiamo risolvere il problema. Supponiamo che la rete dei docenti è la 192.168.1.0, quelle degli studenti siano 192.168.2.0 e 192.168.3.0. Per i docenti possiamo utilizzare la metodologia port based vista negli esempi precedenti. Per gli studenti, uno switch di livello 2 non basta per risolvere il nostro problema. Per gli studenti dobbiamo usare o uno switch di livello 3 (che lavora a livello di indirizzi IP come un router, solo che non fa l'istradamento: Switch based Inter-VLAN) o con uno switch di livello 2 collegato ad un router. Utilizziamo la metodologia Inter-VLAN tradizionale.

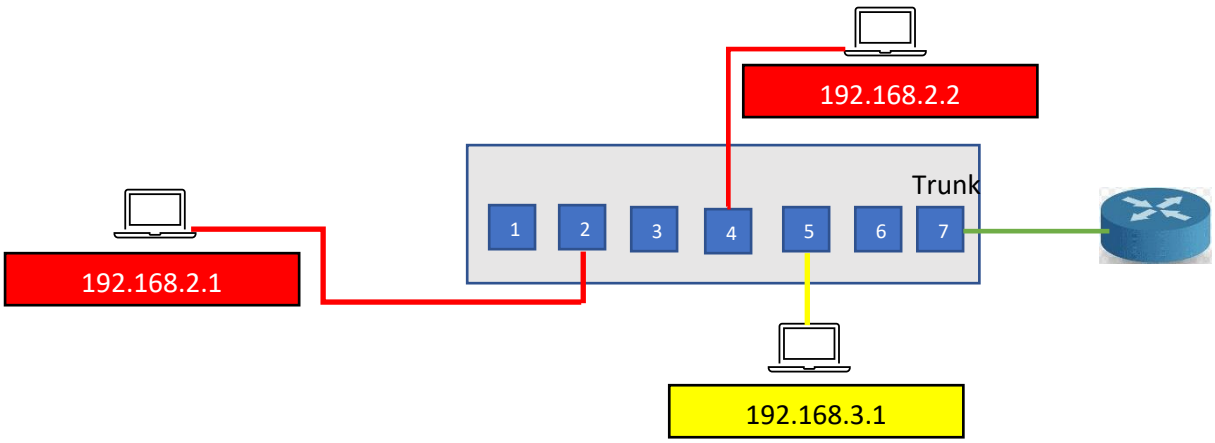


In definitiva realizziamo 3 VLAN la **blu** è quella dei docenti, la **rossa** e la **gialla** quella degli studenti. Inseriamo queste tre VLAN nel VLAN Database dello switch: VLAN Number: 10 e VLAN Name: Docenti, alla prima VLAN; VLAN Number: 20 e VLAN Name: Studenti1, alla seconda VLAN; VLAN Number: 30 e VLAN Name: Studenti2, alla terza VLAN; Quindi assegniamo alle porte 1 e 3 la VLAN 10; alle porte 2, 4 e 6 la VLAN 20; alle porte 5 e 7 la VLAN 30. N.B. le porte 6 e 7 sono le porte che vanno configurate con le VLAN da connettere al router. Alle interfacce del router a cui colleghiamo i cavi provenienti dalle porte dello switch, assegniamo gli indirizzi IP di gateway relativi alle reti 192.168.2.0 e 192.168.3.0 (ossia gli indirizzi 192.168.2.254 e 192.168.3.254) tali indirizzi vanno riportati nel gateway di default degli host appartenenti alle 2 VLAN rispettivamente.

Esempio 5. Router-on-a-stick Inter-VLAN.

Supponiamo di avere due VLAN con IP diversi. Nell'esercizio precedente abbiamo visto che usando due interfacce separate sia sullo switch che sul router, una per ogni VLAN, tramite Inter-VLAN tradizionale, possiamo far comunicare le VLAN tra di loro. Vediamo come possiamo fare la stessa cosa facendo però confluire tutte le VLAN su un'unica interfaccia dello switch del router.

Prendiamo l'esempio precedente; abbiamo due VLAN: VLAN Name: Studenti1 con VLAN Number: 20, Net IP: 192.168.2.0 e VLAN Name: Studenti2 con VLAN Number: 30, Net IP: 192.168.3.0.



Come fatto nell'esercizio precedente, assegniamo, quindi, alle porte 2 e 4 la VLAN 20; alla porte 5 la VLAN 30. L'interfaccia porta 7 diventa una porta Trunk, quindi che consente il passaggio di tutti i frame di tutte le VLAN e che verrà collegata alla porta del router R1, che ad esempio è una porta FastEthernet 0/0. Assegniamo gli indirizzi IP di gateway relativi alle reti 192.168.2.0 e 192.168.3.0 (ossia gli indirizzi 192.168.2.254 e 192.168.3.254) tali indirizzi vanno riportati nel gateway di default degli host appartenenti alle 2 VLAN rispettivamente.

Ora l'interfaccia FastEthernet 0/0, deve essere suddivisa in tante 'subinterfacce' logiche quante sono le VLAN che arrivano a questa porta (nel ns caso due): *FastEthernet0/0.1 e FastEthernet0/0.2*.

Questa operazione richiede la scrittura di qualche riga di comandi tramite la CLI (Command Line Interface) che riportiamo di seguito:

```
R1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)# int FastEthernet0/0
R1(config-if)# no ip address
R1(config-if)# int FastEthernet0/0.1
R1(config-subif)# encapsulation dot1q 20
R1(config-subif)# ip address 192.168.2.254 255.255.255.0
R1(config-subif)# int FastEthernet0/0.2
R1(config-subif)# encapsulation dot1q 30
R1(config-subif)# ip address 192.168.3.254 255.255.255.0
R1(config-subif)# end
R1#
```

Cerchiamo di spiegare ciò che è stato scritto. Innanzitutto, bisogna entrare in configurazione Terminale (conf t), quindi non assegniamo alcun indirizzo IP alla porta *FastEthernet 0/0* (*no ip address*) ma dichiariamo 2 subinterfacce, *int FastEthernet0/0.1* alla quale facciamo confluire la VLAN di Studenti 1, ossia la VLAN Number 20 (*encapsulation dot1q **20***) e l'indirizzo ip di Gateway con la relativa subnet mask: *ip address 192.168.2.254 255.255.255.0*, e *int FastEthernet0/0.2* alla quale facciamo confluire la VLAN di Studenti2 , ossia la VLAN Number 30 (*encapsulation dot1q **30***) e l'indirizzo ip di Gateway con la relativa subnet mask: *ip address 192.168.3.254 255.255.255.0.* Terminiamo l'operazione (*end*) ed il gioco è fatto!

CRITTOGRAFIA.

Crittografia simmetrica, asimmetrica e ibrida.

Il problema di nascondere messaggi da 'occhi indiscreti' è un problema noto da quanto è nata la scrittura, soprattutto in campo militare/commerciale.

Per risolvere il problema sono nate tecniche per: rendere 'invisibile' il messaggio (ad esempio l'uso di inchiostri 'simpatici' con i quali si scrive il messaggio che però è praticamente invisibile sul supporto ove è scritto e che, sottoposti a calore o a qualche sostanza, fanno sì che il messaggio diventa visibile), tecniche che nascondono il messaggio in un altro messaggio o che trasformano il messaggio in chiaro in un messaggio privo di senso. Negli ultimi due casi, il destinatario che riceve il messaggio deve conoscere la tecnica usata per nascondere/trasformare il messaggio dal mittente, così da poter risalire al messaggio originale.

Il problema si è notevolmente ampliato da quando è nato internet; oggi sulla rete facciamo: acquisti di beni e servizi, transazioni bancarie, contratti commerciali… informazioni che fanno gola a malintenzionati (hacker, cracker) che cercano di rubarle per motivi (illeciti) quali conoscere dati privati di terzi, svuotarci il conto corrente, manipolare le informazioni sottratte…

> *La differenza tra hacker e cracker è che un hacker tenta di esplorare i sistemi per violarli principalmente per motivi etici, dimostrativi, politici… il cracker è il vero cybercriminale che tenta di violare un sistema o la buonafede degli internauti per trarne profitto rubando dati o distruggendoli… spesso, però, i due termini sono fusi nel solo termine hacker.*

Il ramo della scienza che si occupa della trasformazione di un messaggio in chiaro in uno illeggibile e della sua trasformazione inversa (da messaggio illeggibile a messaggio in chiaro) è la **crittografia**.

Cominciamo a definire ***cifratura (o codifica)*** la tecnica che trasforma il messaggio in chiaro nel messaggio illeggibile e, quest'ultimo definiamolo, coerentemente alla definizione appena data, messaggio cifrato (o codificato). La tecnica per la cifratura è in realtà un ***algoritmo*** che riceve il messaggio in chiaro e lo trasforma in quello cifrato detto appunto *Algoritmo di cifratura*. La tecnica che compie il processo inverso, ossia dal messaggio cifrato lo trasforma nel messaggio in chiaro, è detta ***decodifica*** (o decifratura) e l'algoritmo che svolge questo compito prende il nome di *Algoritmo di decodifica*. Gli algoritmi per poter cifrare/decodificare un messaggio devono utilizzare uno o più *parametri* che regolano la trasformazione del messaggio. I parametri prendono il nome di ***chiavi***.

*Ad esempio, se volessimo inviare la parola CASE utilizzando la crittografia, dobbiamo per prima cosa pensare alla realizzazione di un algoritmo di cifratura che potrebbe essere "spostare di **n** lettere dell'alfabeto in avanti ogni lettera del messaggio"; quindi definire la chiave **n**. Con **n = 2** la parola 'CASE' diventerebbe 'FDVH': infatti F è due lettere avanti alla lettera C, D è due lettere avanti alla lettera A, V è due lettere avanti alla lettera S e H è due lettere avanti alla lettera E. Una volta trasmesso il messaggio cifrato, il destinatario deve avere l'Algoritmo di decodifica, che nel nostro caso sarebbe "spostare di **n** lettere dell'alfabeto indietro ogni lettera del messaggio" e la chiave **n = 2**.*

Nell'esempio, chi invia il messaggio e chi lo riceve utilizzano la stessa chiave per cifrare/decodificare il messaggio: in questo caso si parla di ***crittografia simmetrica (o pubblica)***:

Il problema della crittografia simmetrica è che coloro che vogliono comunicare tra loro devono essere in possesso della stessa chiave, chiave che, quindi, in un certo istante, deve essere inviata sulla rete. Se in quell'istante un malintenzionato riesce ad impossessarsi della chiave ha la possibilità di decifrare il messaggio cifrato che viaggia sulla rete. Ricordiamo che la rete è spesso 'controllata' da software detti 'sniffer' che permettono di catturare e analizzare i messaggi che vi viaggiano. È ovvio che questi software possono essere utilizzati da malintenzionati per rubare, intercettare e spiare informazioni che viaggiano sulla rete.

Gli algoritmi più importanti di crittografia simmetrica, di cui citiamo solo il nome, sono: il cifrario DES, il 3-DES, IDEA, AES.

Il problema su esposto viene risolto tramite l'utilizzo di due chiavi: l'algoritmo utilizza una chiave per crittografare il messaggio e una chiave per decodificare il messaggio. La chiave che crittografa il messaggio (chiave pubblica) viene inviata dal destinatario al mittente che deve inviare un messaggio al destinatario, il mittente nel momento che ha la necessità di inviare un messaggio, utilizzando la chiave pubblica in suo possesso, crittografa il messaggio. Il destinatario ha la chiave che lo decodifica (chiave privata) di conseguenza è il solo che può decodificare il messaggio.

B invia un messaggio cifrato con la chiave pubblica ricevuta da A, A lo decodifica con la sua chiave privata

D'altra parte, un messaggio codificato da A, tramite la sua ***chiave privata***, può essere decodificato da B tramite la sua ***chiave pubblica***. In questo caso non si garantisce la segretezza del messaggio ma la sua autenticità, ossia che il messaggio ricevuto da B sia stato prodotto da A. Per garantire la segretezza dei messaggi inviati tra A e B, bisogna usare 4 chiavi, una pubblica e privata di A (B conosce la pubblica di A) e una pubblica e privata di B (A conosce la pubblica di B).

Questa modalità di crittografia ove si utilizzano due chiavi (pubblica e privata), è nominata **crittografia asimmetrica (o a chiave pubblica)**.

L'algoritmo utilizzato nella crittografia asimmetrica, di cui citiamo solo il nome, è l'algoritmo RSA.

La crittografia asimmetrica è molto complessa nei calcoli che la rendono poco efficace soprattutto quando i file da crittografare sono di grandi dimensioni. Per questo motivo sono nati sistemi di **crittografia ibrida (o mista)**. Questi sistemi utilizzano la crittografia asimmetrica per lo scambio di una chiave (chiamata chiave di sessione) che viene poi utilizzata con la crittografia simmetrica per codificare e decodificare i messaggi.

Se la *crittografia* cerca di evitare che le informazioni viaggino in chiaro e facilmente accessibili a 'occhi indiscreti' sulla rete, la ***crittoanalisi*** è lo studio dei metodi per ottenere il significato di informazioni cifrate senza avere accesso alle informazioni segrete (algoritmi di decodifica/codifica, chiavi).

CERTIFICATI E FIRMA DIGITALE.

La cifratura e decodifica di un messaggio sono operazioni onerose dal punto di vista di calcolo e tempo. Spesso, però, non è necessario crittografare un documento: ciò che interessa è l'autenticità del documento e che il documento non sia stato modificato in modo arbitrario.

Per fare questo, il documento viene 'marchiato' da una sorta di 'impronta digitale' che indica chi ha prodotto il documento e che è conforme all'originale in modo inequivocabile.

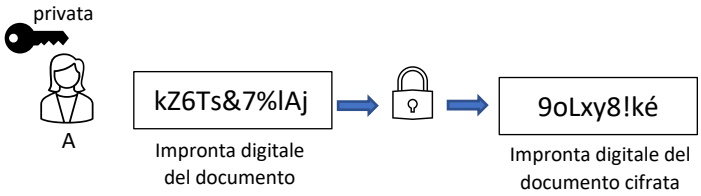
La firma digitale, in definitiva, si basa su un sistema di crittografia asimmetrica che consente:

- la sottoscrizione di un documento digitale;
- la verifica, da parte dei destinatari, dell'identità del soggetto sottoscrittore;
- la certezza che le informazioni contenute nel documento non siano state alterate.

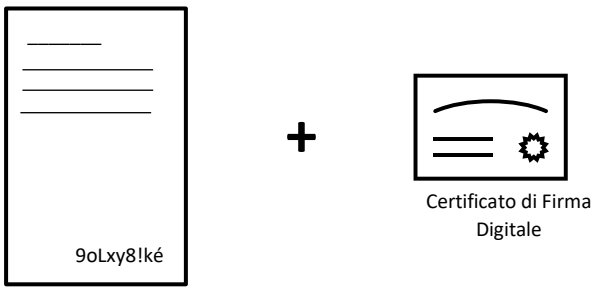
Vediamo ora come funziona la firma digitale.

Innanzitutto, dal documento su cui si vuole apporre la firma digitale, viene generata tramite un algoritmo (algoritmo di hash) *l'impronta digitale* del documento che altro non è che un insieme di caratteri che identifica ***univocamente*** il documento. Ciò significa che anche se si modifica un solo carattere al documento, l'impronta digitale sarà diversa.

Viene cifrata l'impronta digitale con la chiave privata dell'utente.



L'impronta digitale cifrata viene inserita nel documento originale



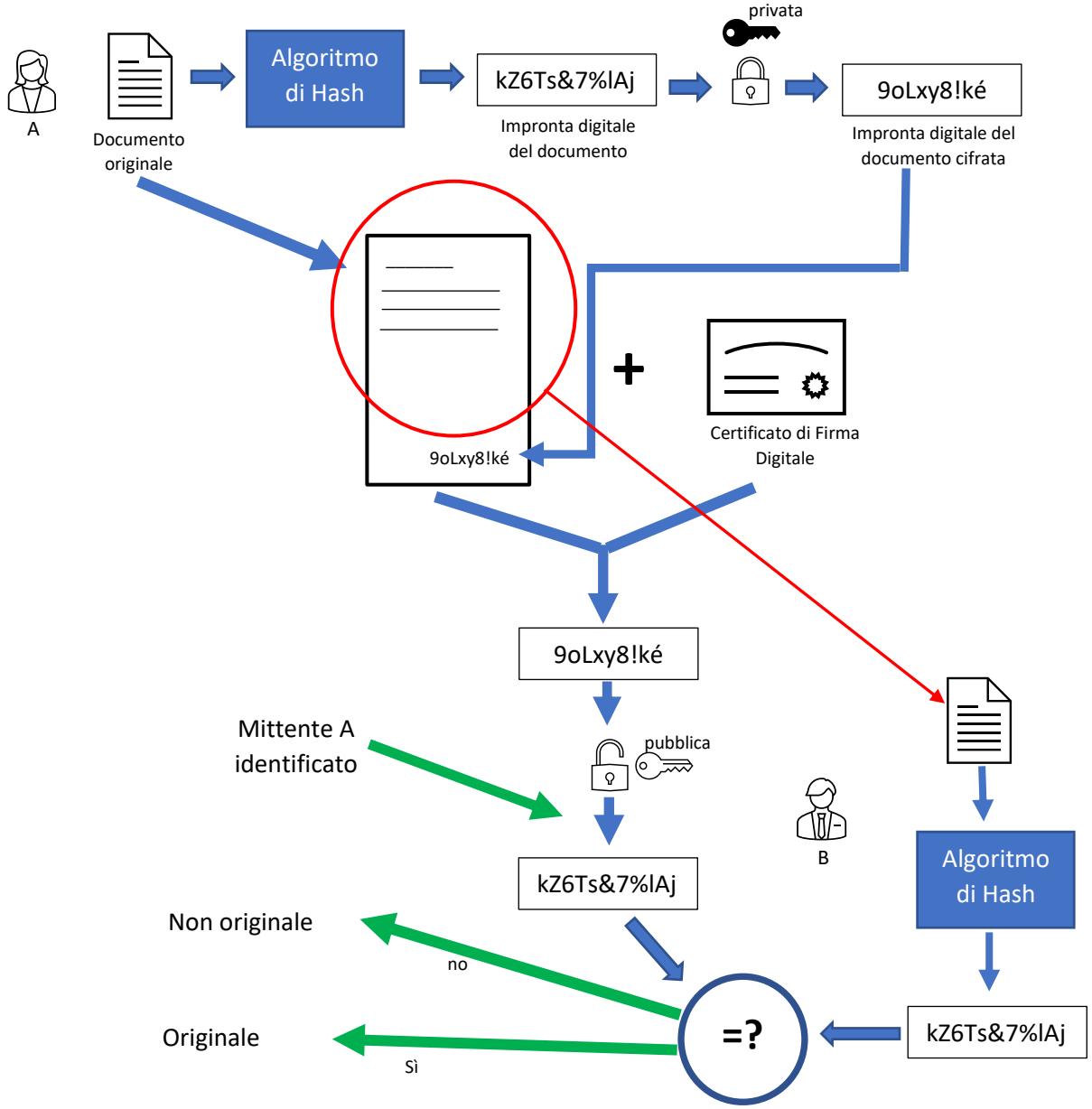
L'impronta digitale cifrata ci assicura sia l'autenticità del documento grazie la funzione Hash che ha generato l'impronta digitale, sia il sottoscrittore del documento grazie la cifratura con la chiave privata dell'impronta digitale generata.

Al documento così prodotto viene associato il certificato di firma digitale (vedi note sotto) ed entrambi inviati al destinatario. Tutto il processo di firma elettronica viene eseguito da software appositi.

Quando il destinatario aprirà il documento utilizzerà un apposito software per la verifica della firma digitale e acquisirà dal *certificato di firma digitale* associato al documento, la chiave pubblica del mittente (oltre altre informazioni). Tramite questa chiave, viene decifrata la stringa della firma digitale che produrrà come risultato l'impronta del documento. Il destinatario poi farà passare la funzione hash sul documento originario e genererà l'impronta: a questo punto se le due impronte coincideranno il destinatario sarà sicuro dell'integrità e dell'autenticità del documento ricevuto.

*Operativamente l'utente possiede un dispositivo di firma sicuro (**smart card**, **token USB**, **Business Key…**) rilasciato da appositi **enti certificatori**, e di un codice segreto, PIN - Personal Identification Number, con i quali firma digitalmente un documento. Le chiavi pubbliche e private, vengono consegnate dall'ente certificatore all'utente che richiede il servizio di Firma digitale. L'ente certificatore inoltre associa la chiave pubblica all'utente tramite il **certificato di firma digitale**. Come abbiamo visto nel paragrafo precedente, la chiave pubblica è in grado di decodificare l'impronta digitale, cifrata con chiave privata dall'utente sottoscrittore, il che garantisce l'identità del sottoscrittore del documento.*

Schema di invio/ricezione di un documento con firma digitale.



LA SICUREZZA NEI SISTEMI INFORMATIVI.

"*Potere è sapere*", questo detto riassume egregiamente l'importanza delle ***informazioni***: la conoscenza, il trattamento, la conservazione delle informazioni sono fondamentali e vitali per gli aspetti decisionali e strutturali di una organizzazione commerciale, militare, sociale…

Oggi le informazioni sono stoccate e trattate nei computer ed è necessario salvaguardare l'integrità e la protezione delle informazioni presenti sui supporti elettronici.

Con il termine **minacce alla sicurezza** indichiamo tutte le situazioni che possono compromettere l'integrità e la protezione delle informazioni.

Le **minacce alla sicurezza** si dividono in **naturali** ed **umane**:

Naturali sono quelle dovute alle calamità naturali (terremoti, inondazioni, incendi...); in questo caso bisogna effettuare preventivamente ***l'analisi dei rischi*** per valutare i costi/benefici nel realizzare le adeguate difese per proteggere le informazioni (ad esempio, per proteggere il computer di casa che non contiene informazioni particolarmente importanti, non è necessario costruire una stanza blindata, con un sistema elettrogeno di continuità…) basta, magari, fare ad intervalli di tempo regolari il backup dei dati su supporti di memorizzazione esterne. È ovvio che più i dati sono importanti più è necessario salvaguardare i supporti che li contengono e li trattano, in strutture adeguate e protette.

Umane sono quelle dovute all'intervento di soggetti che hanno interessi personali ad appropriarsi, modificare, distruggere le informazioni sui supporti ove sono conservate. Questi interventi vengono definiti **attacchi**. Gli attacchi si dividono in **attacchi interni** ed **attacchi esterni**.

Gli **attacchi interni** sono quelli che vengono effettuati da dipendenti o ex-dipendenti delle società per diversi motivi (ripicca, vendette, o semplicemente per soldi) e vanno dalla distruzione delle informazioni, alla loro manipolazione, allo spionaggio industriale. Queste persone sono facilitate dalla conoscenza della struttura e possono essere in possesso di badge per l'accesso a locali riservati, password…

Gli attacchi **esterni vengono** effettuati da hacker (cracker) con le modalità e per i motivi di cui abbiamo già discusso nel capitolo precedente.

Il problema degli attacchi informatici è aumentato con la connessione degli elaboratori alle reti soprattutto alla rete internet, si pone il problema quindi di come proteggersi dagli attacchi informatici, assicurare, cioè, la *sicurezza* dei dati e dei supporti informatici.

Per *sicurezza informatica* si intende l'insieme dei prodotti, dei servizi, delle regole organizzative e dei comportamenti individuali che proteggono i sistemi informatici di un'organizzazione (società commerciali, amministrazioni, …), di proteggere, in definitiva, da accessi indesiderati ai sistemi informativi al fine di garantire la riservatezza delle informazioni ed assicurare il funzionamento e la disponibilità dei servizi.

La sicurezza informatica viene spesso indicata con l'acronimo CIA (Confidentiality, Integrity, Availability – Riservatezza, Integrità, Disponibilità – ovviamente Riservatezza ed Integrità dei dati, Disponibilità dei sistemi). Per effettuare *l'analisi dei rischi*, gli aspetti che devono essere considerati sono:

Autenticazione – processo di riconoscimento delle credenziali dell'utente per riconoscerne l'identità;

Autorizzazione – l'utente autenticato e che quindi accede al sistema deve avere associalo l'insieme delle autorizzazioni ossia a quali informazioni può accedere e cosa può fare (o non può fare) di queste informazioni;

Riservatezza – agli utenti che non hanno le autorizzazioni per accedere alle informazioni, si deve impedire di intercettare e comprendere queste informazioni;

Disponibilità – i sistemi e le informazioni in essi contenuti devono essere disponibili con continuità agli utenti che hanno diritto all'accesso con le opportune autorizzazioni;

Integrità – la garanzia che le informazioni non siano state manipolate ed alterate in modo illecito da non autorizzati;

Paternità – ogni documento deve essere associato all'utente che lo ha prodotto senza che lui possa ripudiarlo o negarlo.

Inoltre, è spesso richiesta la *tracciabilità dei documenti* in modo da sapere chi e quando ha letto e consultato o effettuato l'accesso ad un archivio.

VALUTAZIONE DEI RISCHI

La valutazione del rischio informatico è un'analisi del sistema informativo, atta ad individuare le potenziali vulnerabilità che possono mettere a rischio la sicurezza dei dati dell'organizzazione.

Una volta individuate le potenziali vulnerabilità (o rischi) si procede con una stima probabilistica della verificabilità delle minacce (umane o naturali) e il grado di dannosità se si dovessero verificare. Per ogni minaccia si individuano e studiano le possibili contromisure per contrastarle valutandone i costi/benefici.

Principali tipologie di attacchi.

Malware

Il termine malware definisce software malevoli, ad esempio spyware, ransomware, virus e worm. Il malware viola una rete sfruttandone una vulnerabilità, in genere quando un utente seleziona un link pericoloso o apre un allegato ricevuto via e-mail che installa il software dannoso. Una volta all'interno del sistema, il malware può:

- Bloccare l'accesso ai componenti principali della rete (ransomware)
- Installare malware o altri software dannosi
- Ottenere informazioni di nascosto trasmettendo dati dal disco rigido (spyware)
- Interferire con alcuni componenti e rendere il sistema inutilizzabile

Phishing

Il phishing consiste nell'inviare comunicazioni fraudolente che sembrano provenire da una fonte affidabile, di solito una e-mail. L'obiettivo è quello di rubare dati sensibili come carte di credito e informazioni di accesso, o di installare un malware sul computer della vittima. Il phishing è una minaccia informatica sempre più comune.

Attacco man in the middle.

Gli attacchi man in the middle (MitM), noti anche come attacchi di intercettazione, si verificano quando gli hacker si inseriscono in una transazione fra due parti. Una volta che hanno interrotto il traffico, i criminali possono filtrare e rubare i dati.

I punti di ingresso comuni per gli attacchi MitM sono due:

1. Reti Wi-Fi pubbliche non sicure, dove gli hacker possono inserirsi tra il dispositivo di un visitatore e la rete. Senza saperlo, il visitatore passa tutte le informazioni all'hacker.
2. Una volta che il malware ha violato un dispositivo, un hacker può installare il software per elaborare tutti i dati della vittima.

Attacco denial-of-service (DoS)

Un attacco denial-of-service invia enormi flussi di traffico a sistemi, server o reti per esaurirne le risorse e la larghezza di banda. Di conseguenza, il sistema sotto attacco non è più in grado di soddisfare le richieste legittime. Per lanciare un attacco di questo tipo, gli hacker possono anche utilizzare più dispositivi compromessi. In questo caso di parla di attacco distributed-denial-of-service (DDoS).

SQL injection

Una SQL (Structured Query Language) injection si verifica quando un hacker inserisce codice malevolo in un server che utilizza SQL e lo forza a rendere pubbliche informazioni che normalmente dovrebbero rimanere riservate. Per effettuare una SQL injection, è sufficiente aggiungere del codice malevolo nella casella di immissione dati di un sito web vulnerabile.

Attacchi zero-day

Un attacco zero-day colpisce non appena viene scoperta una vulnerabilità nella rete, ma prima che sia possibile implementare una patch o una soluzione. Gli hacker prendono di mira la vulnerabilità rivelata durante questa finestra temporale.

Tunneling DNS

Il servizio DNS, che traduce il nome di dominio in un indirizzo IP, può essere utilizzato anche per creare dei "tunnel" tra due dispositivi che vogliono scambiarsi dei messaggi in una rete pubblica (internet) creando una sorta di comunicazione 'protetta' tra loro. Questo accade incapsulando il frame inviato da un client quando questo richiede (effettua una query) tramite il protocollo http ad un Server DNS di tradurre un nome di dominio nell'indirizzo IP (per creare una connessione protetta, è possibile incapsulare e crittografare un frame nel dominio, ad esempio in ***prova.it***, viene incapsulato il frame crittografato ***xyzthj.prova.it:*** è il server di destinazione che decrittografa il frame aggiunto al dominio). In definitiva, il tunneling DNS utilizza il protocollo DNS per trasmettere traffico non DNS sulla porta 53. Come prima accennato, esistono vari motivi legittimi per utilizzare il tunneling DNS. Tuttavia, i servizi di tunneling DNS su VPN (una modalità di tunneling) vengono usati anche per ragioni malevoli. Infatti, la comunicazione con i server DNS by-passano i firewall. Se un cybercriminale riesce ad intrufolarsi sfruttando la comunicazione DNS (dopo aver creato un dominio fake sul quale riesce a far confluire la comunicazione con un host di una rete) infetta l'host con il quale ha stabilito una connessione. A questo punto il gioco è fatto. Se l'uso è malevolo, le richieste DNS vengono manipolate per esfiltrare i dati da un sistema compromesso e dirottarli verso l'infrastruttura dell'hacker.

Sicurezza nei sistemi informativi distribuiti.

Si divide in:

- sicurezza sulla rete;
- sicurezza sugli host:
  - ✓ a livello di sistema operativo;
  - ✓ a livello di applicazione;

la suddivisione è in realtà estremamente sottile, in quanto un attacco sulla rete può estendersi sugli host e viceversa.

I tre pilastri della sicurezza sono:

prevenzione (avoidance) mediante la protezione dei sistemi e delle comunicazioni;

rilevazione (detection) mediante il controllo e monitoraggio degli accessi tramite autenticazione con password e certificati;

investigazione (investigation) tramite l'analisi dei dati, ecc, ...

Per quanto riguarda la prevenzione le tecniche adottate sono:

Uso della crittografia;

Autenticazione degli utenti: per garantire il riconoscimento dell'identità di chi accede al sistema informativo tramite il singolo host in locale attraverso password criptate e/o autenticazioni biologiche (impronte digitali, lettura della retina, …) o attraverso l'autenticazione dell'IP o MAC dell'host che si collega tramite la rete.

Firma elettronica;

Connessioni TCP tramite SSL: SSL (Secure Socket Layer) è un protocollo che offre servizi di sicurezza per l'autenticazione delle parti in comunicazione, integrità dei dati, riservatezza delle comunicazioni.

Firewall: è un servizio hardware e/o software di difesa perimetrale della rete che filtra il traffico dei pacchetti entranti/uscenti in base a delle regole definite in fase di configurazione del firewall secondo le seguenti modalità:

- default deny: tutti i servizi non esplicitamente permessi sono negati;
- default allow: tutti i servizi non esplicitamente negati sono permessi.

Il firewall può essere un router o un dispositivo hardware dedicato collegato ad un router, che filtra e monitora i pacchetti in entrata ed uscita tra la rete esterna (internet) e la rete locale.

Reti private e reti virtuali: è possibile acquistare presso gli operatori di reti pubbliche una linea ad uso esclusivo di un'azienda (rete private) come, ad esempio, la rete dei bancomat per il prelievo dei contanti. Ovviamente, queste reti sono molto costose; in alternativa si possono utilizzare reti private virtuali VPN (Virtual Private Network) che creano dei tunnel protetti sulle infrastrutture internet.

SERVIZI DI SICUREZZA PER LA POSTA ELETTRONICA

Il protocollo SMTP invia i messaggi di posta elettronica in chiaro: in questo modo non ci garantisce la riservatezza delle informazioni quando un messaggio attraversa la rete. Inoltre, sappiamo che può facilmente essere contraffatto il mittente: in poche parole il protocollo SMTP non garantisce né ***l'integrità*** del messaggio che può essere facilmente manipolato durante il suo viaggio, né ***l'autenticazione*** del mittente, né la ***riservatezza*** poiché viene inviato in chiaro e quindi leggibile da chiunque, di conseguenza, il ***non ripudio*** ossia l'impossibilità al mittente di negare la paternità del messaggio inviato.

Negli anni è stato sviluppato il protocollo S/MIME che fornisce i seguenti servizi di protezione per la posta elettronica:

- firma digitale
- crittografia del messaggio.

in particolare, il software di crittografia più celebre utilizzato principalmente nella codifica delle e-mail è il PGP (Pretty Good Privacy). Sia il protocollo S/MIME che il software PGP, assicurano un livello di sicurezza a livello applicativo.

LA SICUREZZA DELLE CONNESSIONI CON SSL/TLS

I protocolli TCP/IP e SMTP non sono sicuri e non tutti i servizi web possono utilizzare meccanismi di sicurezza a livello applicativo come accade per la posta elettronica. Sono stati introdotti, quindi, sistemi di protezione a livelli più bassi della pila TCP/IP, precisamente a livello di sessione. Lo standard più diffuso è ***SSL*** (Secure Socket Layer – successivamente integrato con il protocollo ***TLS*** – Transport Layer Security): si tratta di un insieme di protocolli crittografici che aggiungono funzionalità di cifratura ed autenticazione ai protocolli del livello di sessione, permettendo alle applicazioni client/server di internet di comunicare in modo sicuro.

Il protocollo SSL garantisce la sicurezza del collegamento tramite tre funzioni fondamentali:

- ***privatezza del collegamento***: garantita tramite la crittografia a chiave simmetrica
- ***autenticazione***: l'autenticazione dell'identità e della sicurezza di comunicare con il server corretto vengono garantiti tramite la crittografia a chiave asimmetrica.
- ***affidabilità***: il livello di trasporto include un sistema detto *MAC* (Message Authentication Code) che utilizza funzioni hash per la verifica dell'integrità dei dati spediti.

Il protocollo SSL viene accoppiato con protocolli del livello di applicazione come ***HTTPS:*** gli indirizzi dei siti protetti con SSL iniziano con ***https://*** ed hanno sulla loro sinistra un lucchetto. Cliccando sul lucchetto compare il certificato con le informazioni che certificano l'identità del gestore del sito (nome ed indirizzo del server così da controllare se coincide con quello a cui ci siamo collegati, chiave pubblica, ente certificatore).

Il protocollo TLS è suddiviso in due livelli:

1. TLS Record Protocol che:

   - Divide i messaggi in uscita in blocchi gestibili e riassembla i messaggi in ingresso.
   - Comprime i blocchi in uscita e decomprime i blocchi in ingresso (facoltativo).
   - Applica un *codice di autenticazione* (tipo impronta digitale) dei messaggi (MAC) ai messaggi in uscita e verifica dei messaggi in ingresso usando il MAC.
   - Crittografa i messaggi in uscita e decrittografa i messaggi in ingresso.

2. TLS Handshake (*) Protocol: è composto da un insieme di messaggi che vengono scambiati tra il server ed un client nel corso di 4 fasi:

   - Concordare la versione del protocollo da utilizzare.
   - Selezionare algoritmi crittografici.
   - Autenticarsi a vicenda scambiando e validando certificati digitali.
   - Utilizzare le tecniche di crittografia asimmetriche per generare una chiave segreta condivisa, che evita il problema della distribuzione chiave. TLS utilizza quindi la chiave condivisa per la crittografia simmetrica dei messaggi, che è più veloce della crittografia asimmetrica.

(*) Handshake significa letteralmente 'stretta di mano'.

LA DIFESA PERIMETRALE CON I FIREWALL

Abbiamo già definito un ***firewall*** (muro tagliafuoco) come uno o più dispositivi HW/SW capaci di filtrare il traffico proveniente(incoming)/uscente(outgoing) da/per internet dalla LAN aziendale/domestica secondo regole predefinite (difesa perimetrale). Non solo, i firewall possono filtrare il traffico anche all'interno della LAN, in modo tale che una minaccia proveniente da qualche dispositivo (al quale, ad esempio, è stata inserita una chiavetta USB infetta) non si propaghi all'interno della rete.

Inoltre, definiamo ***personal firewall*** i firewall che proteggono un singolo computer di solito *firewall software* già presenti nelle suites antivirus e gestiscono sia l'incoming che l'outgoing.

Con il termine ***network firewall*** definiamo i firewall che si interpongono tra la LAN ed internet per difendere tutti i dispositivi collegati alla LAN.

Inoltre, i firewall possono filtrare il traffico in base a quali tipi di pacchetto, indirizzi IP, porte logiche utilizzate, possono o non possono passare. In questo caso si parla di *filtri di pacchetto IP*.

Parliamo di *Server proxy*, firewall che si interpongono tra un client ed un sito/pagina in modo tale da 'mascherare' il client attraverso il server proxy che riceve ed invia le richieste del client e filtra le risposte del server del sito/pagina.

Network Firewall

Questi firewall possono essere formati da uno o più macchine dedicate al filtraggio del traffico tra internet e LAN.

- ✓ packet-filtering router
- ✓ circuit gateway
- ✓ proxy server

Packet filter firewall o stateless firewall

Un packet filter firewall o stateless firewall analizza ogni pacchetto che lo attraversa singolarmente, senza tenere conto dei pacchetti che lo hanno preceduto. In tale analisi vengono considerate solo alcune informazioni contenute nell'header del pacchetto, in particolare quelle appartenenti ai primi tre livelli del modello OSI più alcune del quarto. Le informazioni in questione sono l'indirizzo IP della sorgente, l'indirizzo IP della destinazione, la porta della sorgente, la porta della destinazione e il protocollo di trasporto. Su questi parametri vengono costruite le regole che formalizzano la policy del firewall e che stabiliscono quali pacchetti lasciar passare e quali bloccare (ACL – Lista di Controllo degli Accessi). Questo tipo di filtraggio è semplice e leggero ma non garantisce un'elevata sicurezza. Infatti, risulta vulnerabile ad attacchi di tipo IP spoofing (creazione di pacchetti IP che hanno un indirizzo di origine modificato per nascondere l'identità del mittente) in quanto non riesce a distinguere se un pacchetto appartenga o no ad una connessione attiva. Quindi, a causa della mancanza di stato, il firewall lascia passare anche i pacchetti il cui indirizzo IP sorgente originale, non consentito dalla policy del firewall, viene volutamente modificato con un indirizzo consentito. Inoltre, il filtraggio, basato solo sulle informazioni dei primi livelli del modello OSI, non permette al firewall di rilevare gli attacchi basati su vulnerabilità dei livelli superiori.

Stateful firewall o circuit-level gateway

Uno stateful firewall o circuit-level gateway svolge lo stesso tipo di filtraggio dei packet filter firewall e in più tiene traccia delle connessioni e del loro stato. Questa funzionalità, detta stateful

inspection, viene implementata utilizzando una tabella dello stato interna al firewall nella quale ogni connessione TCP e UDP viene rappresentata da due coppie formate da indirizzo IP e porta, una per ciascun endpoint (dispositivo in rete) della comunicazione. Vengono quindi memorizzati tutti i parametri che caratterizzano ogni singola connessione (ad esempio quando è iniziata la connessione, se è in corso o è terminata) Quindi uno stateful firewall bloccherà tutti i pacchetti che non appartengono ad una connessione attiva, a meno che non ne creino una nuova, o che non rispettino l'ordine normale dei flag nella comunicazione. La possibilità di filtrare i pacchetti sulla base dello stato delle connessioni previene gli attacchi di tipo IP spoofing ma comporta una maggiore difficoltà nella formulazione delle regole. Inoltre, gli stateful firewall non rilevano gli attacchi nei livelli OSI superiori al quarto e sono sensibili agli attacchi DoS che ne saturano la tabella dello stato. In generale, rispetto ai packet filter firewall, offrono una maggiore sicurezza ma sono più pesanti dal punto di vista delle performance.

Application firewall o proxy firewall o application gateway.

Un application firewall o proxy firewall o application gateway opera fino al livello 7 del modello OSI filtrando tutto il traffico di una singola applicazione sulla base della conoscenza del suo protocollo. Questo tipo di firewall analizza i pacchetti nella sua interezza considerando anche il loro contenuto (payload) ed è quindi in grado di distinguere il traffico di un'applicazione indipendentemente dalla porta di comunicazione che questa utilizza. Un'altra caratteristica che lo distingue da un packet filter firewall e da uno stateful firewall è che si inserisce nella connessione tra un host della rete che protegge e un host della rete esterna interrompendola di fatto, filtrando opportunamente la comunicazione tra di essi. Infatti, nelle comunicazioni svolge il ruolo di intermediario ed è quindi l'unico punto della rete che comunica con l'esterno, nascondendo così gli altri host che vi appartengono. Sebbene aumenti il livello della sicurezza, un application firewall è specifico per ogni applicazione e costituisce un collo di bottiglia per le performance della rete.

Next-generation firewall

Un next-generation firewall è una piattaforma che riunisce in un unico pacchetto diverse tecnologie per la sicurezza. Fra queste ci sono le tecnologie di filtraggio dei firewall presentati in precedenza ovvero il filtraggio stateless, la stateful inspection, l'analisi dei pacchetti a livello applicativo (deep-packet introspection) e altre funzionalità aggiuntive come il NAT (Network Address Translation - tecnica per 'mascherare' un indirizzo IP presente nell'header dei pacchetti in transito da e verso una LAN da parte dei Firewall e Router: in uscita l'indirizzo dell'host della LAN che accede ad internet viene mascherato con, di solito, con l'indirizzo del gateway; in ingresso viene effettuata l'operazione inversa) e il supporto alle VPN. Alcune delle altre caratteristiche tipiche di un next-generation firewall sono: il rilevamento e la prevenzione delle intrusioni, la definizione di policy specifiche per ogni applicazione, l'integrazione dell'identità dell'utente, l'acquisizione di dati di supporto per la sicurezza da fonti esterne, la qualità di servizio. L'obiettivo di questa tecnologia di firewall è la semplificazione di configurazione e gestione di un insieme eterogeneo di strumenti di sicurezza e allo stesso tempo il miglioramento del loro impatto sulle performance dell'intero sistema.

ACL - Access Control List

Le regole di cui abbiamo parlato in precedenza e che servono a regolare il traffico in ingresso ed uscita dalla rete locale tramite i firewall (packet filter e Statefull) vengono inserite in una lista chiamata ACL. Le ACL filtrano in base agli indirizzi IP sorgente o di destinazione, in base al protocollo o alla porta logica.

L'ACL può filtrare in due modi:

1. la lista contiene ciò che è vietato: in questo caso si parla di **Open Security policy** - tutto è permesso tranne ciò che è elencato nella lista;
2. la lista contiene ciò che è permesso: in questo caso si parla di **Closed Security policy** - tutto è vietato, è permesso ciò che è elencato nella lista;

ad esempio, vediamo come possiamo consentire la connessione con un solo server di indirizzo 65.104.3.12 a tutti gli Host di una LAN mediante il modo 2

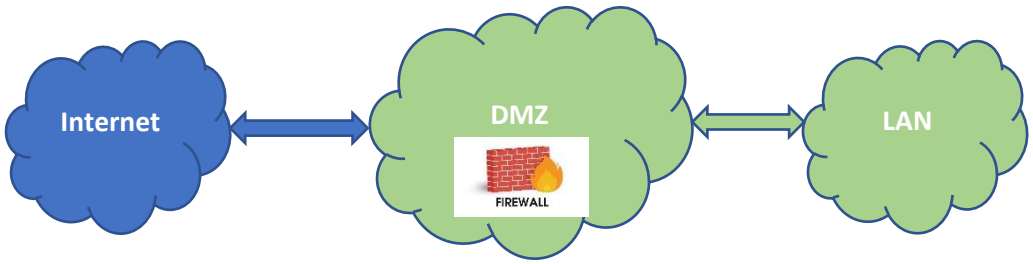
Nr regola	Azione	Source IP	Source port	Destination IP	Destination port
1	allow	65.104.3.12	80/TCP	Localhost	Any/TCP
2	allow	any	Any/TCP	65.104.3.12	80/TCP
3	Reject	Any	Any	Any	any

DMZ

La segmentazione delle reti informatiche è importante perché consente di separare sistemi che possono potenzialmente essere causa di problemi (infezioni, attacchi, ...) dal resto della LAN. Per segmentare la rete una possibile soluzione consiste nell'utilizzare le cosiddette VLAN. La funzionalità VLAN (Virtual LAN), prevista su router e switch professionali, consente di creare più sottoreti che tra loro non possono comunicare direttamente, con tutti i vantaggi in termini di sicurezza che ne derivano.

Con DMZ, dall'inglese *delimitarized zone* (zona demilitarizzata), si indica una rete di computer che funge, tra due reti (internet e LAN ad esempio), da zona cuscinetto con un proprio indirizzo IP e le delimita mediante regole di accesso rigide. I server (Web, Posta, DNS..) all'interno di una DMZ, seppur appartengano ad una rete locale aziendale, non sono collegati direttamente ai dispositivi connessi alla rete locale. L'esigenza di una DMZ nasce, quindi, quando si voglia condividere con altre reti non appartenenti alla rete locale aziendale (ad esempio Internet), un insieme di Servizi presenti su dispositivi (Server) della rete locale aziendale (ad esempio un sito web).

La DMZ la realizziamo, come detto, come una rete ***separata*** dalla LAN e, utilizzando i firewall, stabiliamo le regole di accesso sia da Internet che dalla LAN, alla DMZ.

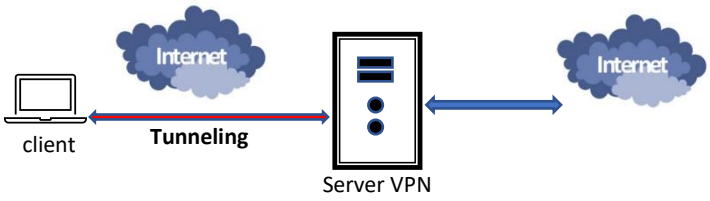


VPN (Virtual Private Network)

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

La connessione VPN indirizza i pacchetti di dati provenienti da un client direttamente ad un server VPN prima di essere inoltrati a terze parti sulla rete internet. Questa prima connessione viene effettuata dal client verso il Server (router) VPN che 'riconosce' (ad esempio tramite l'utilizzo di user e password) il client e stabilisce una connessione sicura con il client (ossia crea il tunneling) dei pacchetti da/verso il client.

È ovvio che le connessioni VPN possono essere usate anche dai privati per navigare in modo sicuro ed 'invisibile' su internet, in questo caso i server VPN fungono come una sorta di server proxy avanzato che oltre a mascherare l'indirizzo IP del client, nascondono i dati che vengono trasmessi tra il server VPN ed il client. Dopo aver creato il tunnel tra il server ed il client è il server VPN che inoltra, mascherando l'indirizzo IP del client, i pacchetti verso le altre destinazioni e riceve i dati provenienti da internet inviandoli, tramite il tunnel, al client sempre in modo protetto.

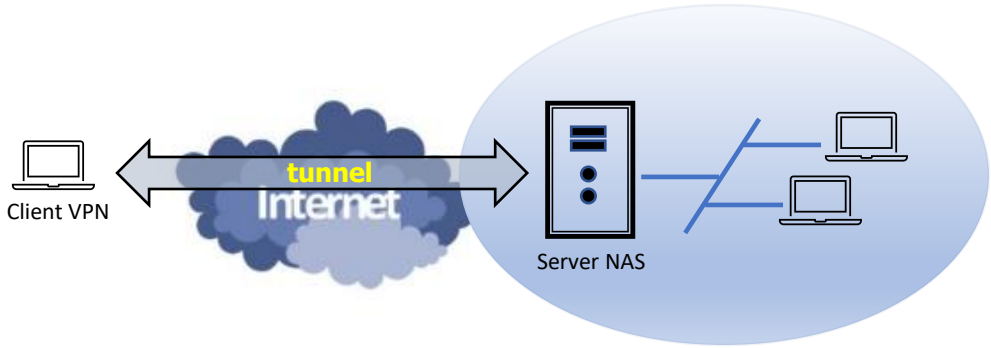


La modalità prima descritta è una tipologia che viene definita ***Private VPN***, le altre tipologie sono:

- ***Remote Access VPN***;
- ***Site to site VPN***.

Remote Access VPN.

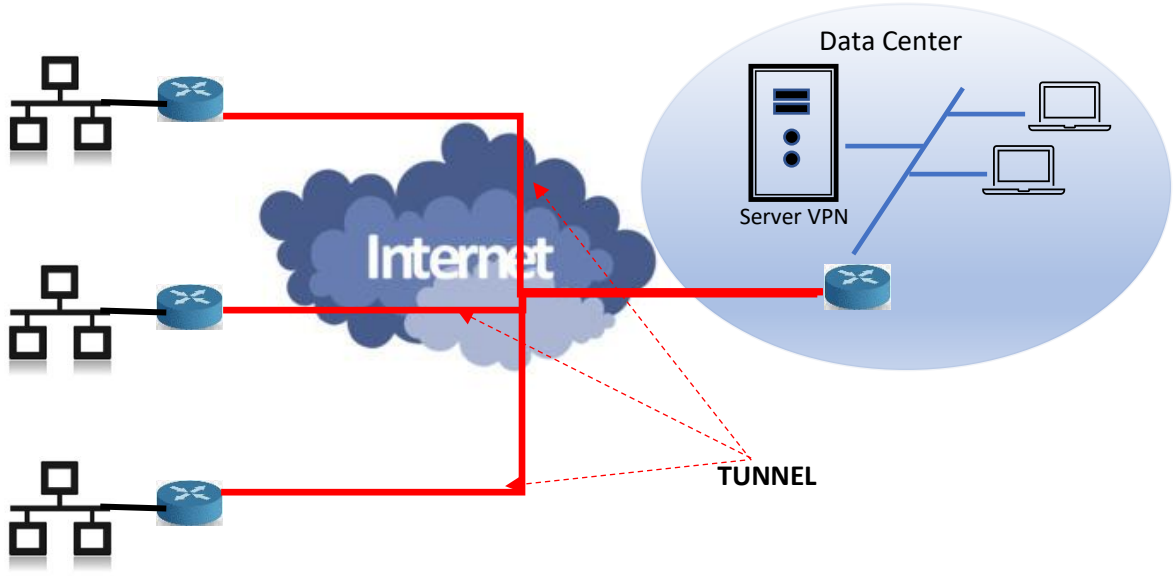
Le VPN ad accesso remoto consentono agli utenti che lavorano da casa (homeworking) o in movimento (teleworking) di accedere ad un server di una rete privata, attraverso una rete pubblica (Internet). Dal punto di vista dell'utente la VPN e come se fosse una connessione Point-to-Point tra il proprio computer (client VPN) ed il server aziendale detto NAS (Network Access Server) che richiede le credenziali di accesso tramite un processo proprio o avvalendosi di un Server AAA (Authentication, Authorization, Accounting).



Site to Site VPN

In questo caso tramite la VPN connettiamo due o più reti private, appartenenti ad una stessa organizzazione ma geograficamente distanti, come se appartenessero alla stessa rete privata, attraverso un tunnel in una rete pubblica (Internet).

In questo caso un server VPN della rete è situato nel data center dell'organizzazione al quale si collegano le varie reti private delle altre sedi, dislocate in luoghi geograficamente distanti. Ovviamente i collegamenti tra le reti private e il server VPN del data center avviene sulla rete pubblica, attraverso router opportunamente configurati (chiamiamoli router VPN): tra il router/server VPN del data center e i router VPN delle reti private si creano dei tunnel sicuri nei quali passano le informazioni.



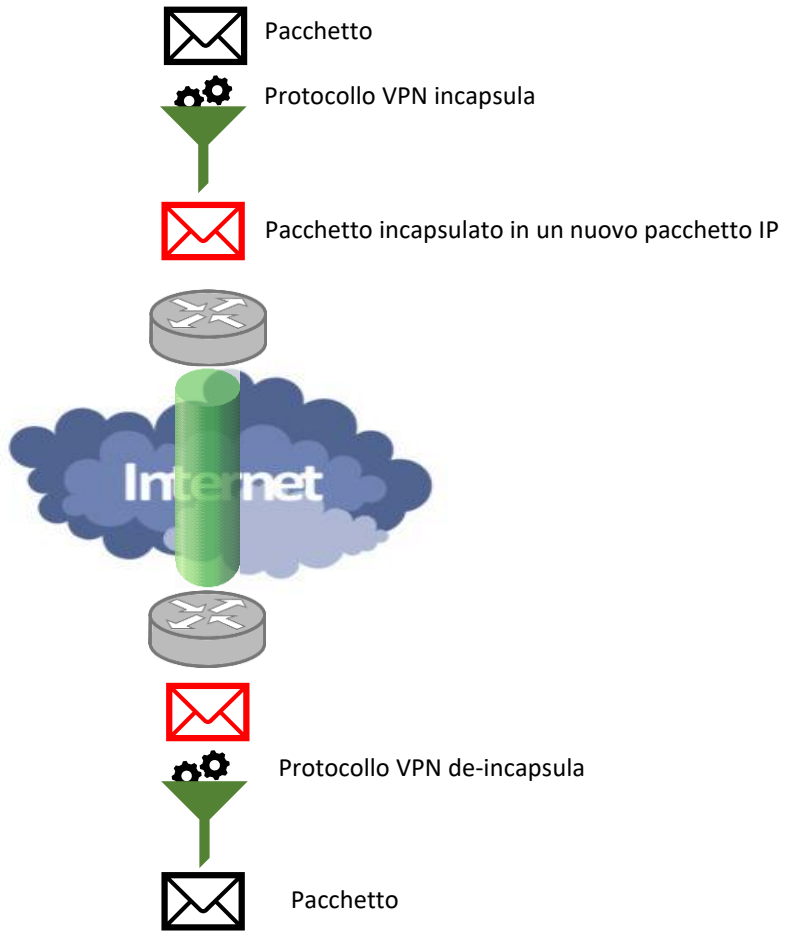
TUNNELING.

Abbiamo finora parlato di tunneling per stabilire una connessione protetta attraverso una rete pubblica. Ma cos'è e come si realizza il tunneling? È ovvio che questo tunnel non è un'infrastruttura 'fisica' che si estende tra due nodi della rete. È un processo 'logico' che fa si che due punti della rete non direttamente connessi e collegati mediante l'attraversamento di diversi nodi, è come se diventassero…. 'adiacenti'. Il segreto sta non solo nel crittografare le informazioni (dati) che sono contenuti nei pacchetti (PDU), ma anche nel 'camuffare' lo 'header' dei pacchetti che contiene, tra l'altro, le informazioni relative al mittente ed al destinatario del pacchetto.

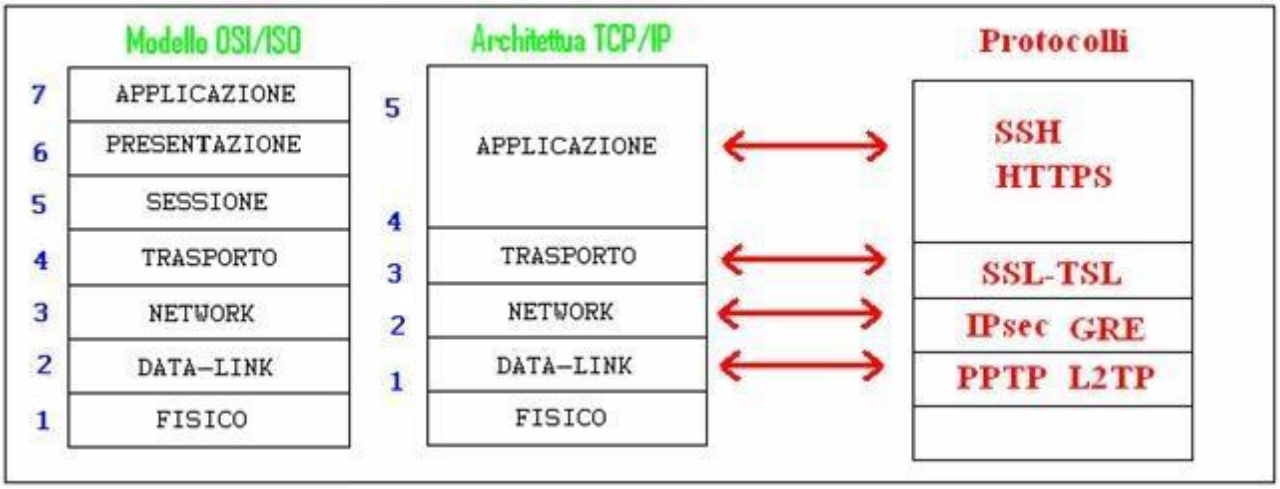
☞ *Ricordiamoci che ogni PDU è composto da due parti: l'intestazione (header) e la parte dati (body o data) in cui l'header è come se fosse la busta di una lettera che contiene la lettera stessa (body). Nel*

passaggio da un livello a quello successivo della pila ISO/OSI (TCP/IP) i vari protocolli imbustano (incapsulano) il PDU proveniente dal livello precedente in una loro 'busta'. Alla fine, però, l'header finale contiene le informazioni in chiaro di chi ha inviato il messaggio e del destinatario…

I protocolli che vengono usati per il VPN avvolgono in un'ulteriore busta tutto il PDU (compreso l'header) relativo al livello cui operano oltre a crittografare il contenuto. Alla fine, anche gli IP sorgente e destinatario sono mascherati: quando il pacchetto arriva al server VPN di destinazione solo allora viene de-incapsulato e l'header ritorna visibile.



Per poter realizzare la sicurezza delle trasmissioni mediante VPN esistono diversi protocolli di sicurezza, a vari livelli nella rete. In sostanza è possibile realizzare una VPN praticamente su ogni livello della pila OSI. La scelta di utilizzare un protocollo piuttosto che un altro dipende dai requisiti di sicurezza delle applicazioni e dalle necessità di sicurezza dell'utente, il quale deve decidere a che livello della pila deve essere implementata la sicurezza nelle trasmissioni su VPN. In alcuni casi, ha senso offrire alcuni di questi servizi/funzionalità ad un livello della pila e altri servizi/funzionalità ad un livello differente. Servizi e funzionalità che devono necessariamente essere implementate in alcuni livelli e non in altri, proprio per poter garantire la sicurezza e per la correzione degli errori.



Attenzione: i protocolli evidenziati sulla sinistra in rosso non sono da intendersi come "pila" di protocolli da usare per la sicurezza VPN; a seconda dei requisiti si adotterà una sicurezza tipicamente in un solo strato, e gli altri strati restano "normali"; per fare un esempio: IPsec non incapsula TSL, o usi IPsec o usi TSL.

I protocolli di tunneling più utilizzati sono i seguenti:

Protocollo	Livello	Cifrato
PPTP Point to Point Tunneling Protocol	Data-Link	*
L2TP (Layer two Tunneling Protocol) / L2F (Layer 2 Forwarding)	Data-Link	
GRE (Generic Routing Encapsulation)	Network	
IPSec (IP security)	Network	*
SSL-TSL (Secure Sockets Layer – Transport Layer Security)	Transport	*
SSH Secure Shell	Application	*

In ogni caso questi protocolli, ognuno con la propria tecnologia di sicurezza, utilizzano tutti dei meccanismi di tunneling e cifratura che incapsulano il pacchetto di dati creandogli attorno una protezione durante la trasmissione e lo de-incapsulano in ricezione. Tra questi il più sicuro è IPSEC, un protocollo completo per la comunicazione VPN; altri protocolli come L2TP e GRE non offrono servizi di cifratura e autenticazione, perciò, per garantire la sicurezza vengono usati in combinazione con IP Security (L2TP/IPSEC e GRE/IPSEC).

RETI WIRELESS

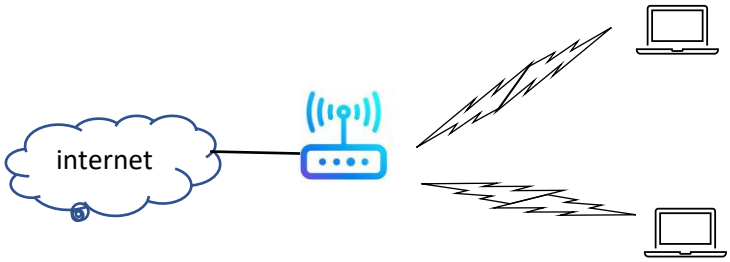
Il termine Wireless (senza fili) indica la possibilità di comunicazione tra dispositivi che utilizzano l'etere come mezzo trasmissivo nel quale fanno viaggiare onde radio, microonde, bluetooth… per inviare i messaggi ed effettuare la comunicazione.

Le reti wireless si suddividono in:

- **reti radiomobili;**
- **reti wireless LAN (WLAN).**

Le **reti radiomobili** consentono ad un dispositivo di spostarsi su un territorio senza perdere la connettività tramite una rete detta rete cellulare. La rete cellulare è composta da un insieme di ripetitori (antenne) il cui segnale copre un'area detta *cella*. Le celle dei ripetitori sono contigue: il dispositivo, spostandosi, si collega, di volta in volta, alla cella che attraversa senza perdere la connettività (questa tecnica viene detta ***handover*** o ***handoff***).

Le **reti WLAN** sono reti che hanno un raggio di copertura che va dai 100 a 500 mt e sono costituite da due tipi di dispositivi: STATION (STA) e ACCESS POINT (AP). La STA è un dispositivo (PC, Laptop, …) che ha una scheda di rete wireless non connessa direttamente alla rete ma che comunica con l'AP che è un dispositivo, anch'esso fornito di una scheda di rete wireless, ma connesso alla rete tramite un gateway



Oltre le reti WLAN, la topologia delle reti wireless si compone di:

BAN (Body Area Network) reti che si estendono per, al massimo, un paio di metri i cui dispositivi sono situati nelle 'vicinanze' del nostro corpo (body, appunto).

PAN (Personal Area Network) reti la cui copertura è di una decina di metri ad esempio in un locale.

WWLAN (Wireless Wide Area Network) reti la cui copertura è di una decina di Km, utilizzate principalmente in quelle zone difficili da raggiungere tramite cavi.

Il protocollo standard per le reti wireless e **l'IEEE 802.11** con le sue successive evoluzioni b, a, f. g, i, n, ac (802.11 b, …)

☞ *Le reti wireless per essere identificate trasmettono l'**SSID** (Service Set IDentifier). SSID in poche parole è il nome della rete che gli AP trasmettono periodicamente in frame dette beacon cosicché i dispositivi mobili di ricetrasmissione Wi-Fi possano creare un elenco delle reti wireless disponibili nella zona in cui essi si trovano. Tale elenco può poi essere mostrato all'utente affinché possa scegliere la rete a cui connettersi.*

LA CRITTOGRAFIA NELLE RETI WIRELESS

La crittografia LAN wireless serve a proteggere la rete wireless con un protocollo di autenticazione che richiede una password o una chiave di rete quando un utente o un dispositivo tenta di connettersi. Se la rete wireless non fosse protetta con un tipo di crittografia, utenti non autorizzati potrebbero accedere alla rete e ottenere informazioni personali o utilizzare la connessione Internet per attività dannose o illegali. Inoltre, se altre persone utilizzano la rete a insaputa del proprietario, è possibile si riducano le prestazioni o la velocità di rete.

Le seguenti informazioni illustrano i dettagli dei diversi tipi di crittografia LAN wireless, ad esempio WEP, WPA-WPA2, comunemente supportati dalla maggior parte dei dispositivi abilitati per il Wi-Fi, degli adattatori e dei router.

WEP: Wired Encryption Privacy o Wired Encryption Protocol

- Tipo di crittografia:

  Il suo funzionamento si basa su una password di protezione per accedere alla rete, la chiave WEP, che è la stessa tra tutti gli utenti che accedono alla rete. La chiave WEP è una password alfanumerica, impostata sul router, è può essere di diversa lunghezza, quali: 64, 128 e 256bit, più lunga sarà la chiave maggiore sarà il livello di crittografia dei dati e conseguentemente la protezione. D'altro canto, però una cifratura maggiore comporta un calo della velocità e delle prestazioni, a causa del maggiore onere di calcolo per crittografare dati con una chiave così lunga.

- Vantaggi:
  Facilità di configurazione.
  Sistema di sicurezza ampiamente supportato.
  Offre più protezione rispetto all'assenza completa di crittografia.

- Svantaggi:
  Crittografia non completamente sicura.
  Esistono altri protocolli di crittografia più sicuri.

WPA e WPA2: Wi-Fi Protected Access

- Tipo di crittografia:
  simile alla chiave WEP, ma ha un livello di protezione maggiore, poiché usa un algoritmo per l'offuscamento e la crittografia dei dati differente dal primo. Il WPA, sua forma certificata e più attuale WPA 2, è il principale sistema di sicurezza nelle reti senza fili. Solo recentemente alcuni hacker sono riusciti a violarlo. È stato proposto un nuovo standard evoluto chiamato WPA-AES che è tuttora lo standard più avanzato di sicurezza WLAN. L'uso dell'autenticazione con chiave WPA si sta allargando, e sicuramente andrà a sostituire quello con chiave WEP, bisogna inoltre aggiungere che i due sistemi non sono compatibili reciprocamente.

  Autenticazione Condivisa con chiave WPA-PSK: l'acronimo WPA-PSK (WiFi Protected Access – Pre Shared Key) indica che viene usata una chiave condivisa di autenticazione, come in WEP, basato su un metodo di cifratura però simile a WPA. È una di via di mezzo tra la chiave WEP e quella WPA. Offre maggiore protezione di WEP ma inferiore a WPA. Rispetto a quest'ultimo gode del vantaggio di avere un hardware più semplice e dai costi più ridotti.

- Vantaggi:
  Facilità di configurazione.
  Crittografia avanzata.
  Facilità di gestione.

- Svantaggi:
  Crittografia non supportata da tutti i dispositivi.

L'ARCHITETTURA DELLE RETI WIRELESS

Cominciamo ad elencare i componenti che fanno parte di una rete wireless (infrastruttura).

1. **Host Wireless**: laptop, PDA (palmari), telefoni IP;
2. **Stazione Base**: dispositivi collegati ad una rete cablata con funzione di ripetitori. Fungono da bridge tra la rete cablata su cui viaggiano i segnali (elettrici/ottici) trasformandoli in onde radio/infrarosse che utilizzano l'etere come mezzo trasmissivo (tipo AP);
3. **Collegamenti**: la connessione tra gli host e le stazioni base via etere e tra le stazioni base e le reti cablate.

Le reti wireless vengono definite ***con infrastruttura*** se esiste una o più stazioni base che collega/no gli host con la rete cablata; ***senza infrastruttura*** se gli host comunicano tra di loro senza la presenza delle stazioni base.

Lo standard 802.11 definisce due tipologie di rete:

- Reti IBSS (Independent Basic Service Set) o reti ad Hoc;
- Reti ESS (Extended Service Set)

Reti IBSS (ad Hoc)

Sono reti senza infrastruttura i cui host (STA) comunicano tra loro in modo peer-to-peer (P2P – ogni nodo della rete è sia Client che Server ossia può, sia chiedere un servizio ad un altro nodo della rete che fornire un servizio ad un nodo che ne fa richiesta).

Reti ESS.

Sono reti con infrastruttura in cui gli host si collegano ad una Stazione Base (AP) che ha un determinato raggio di copertura (cella); ogni singola infrastruttura formata da un AP e dagli Host che operano all'interno della cella, prende il nome di BSS (Basic Service Set). Per generare un'area di copertura maggiore si collegano più BSS. In questo caso la rete prende il nome di ESS. Gli host che si spostano tra una cella ed un'altra, grazie all'handoff, non perdono la connettività.