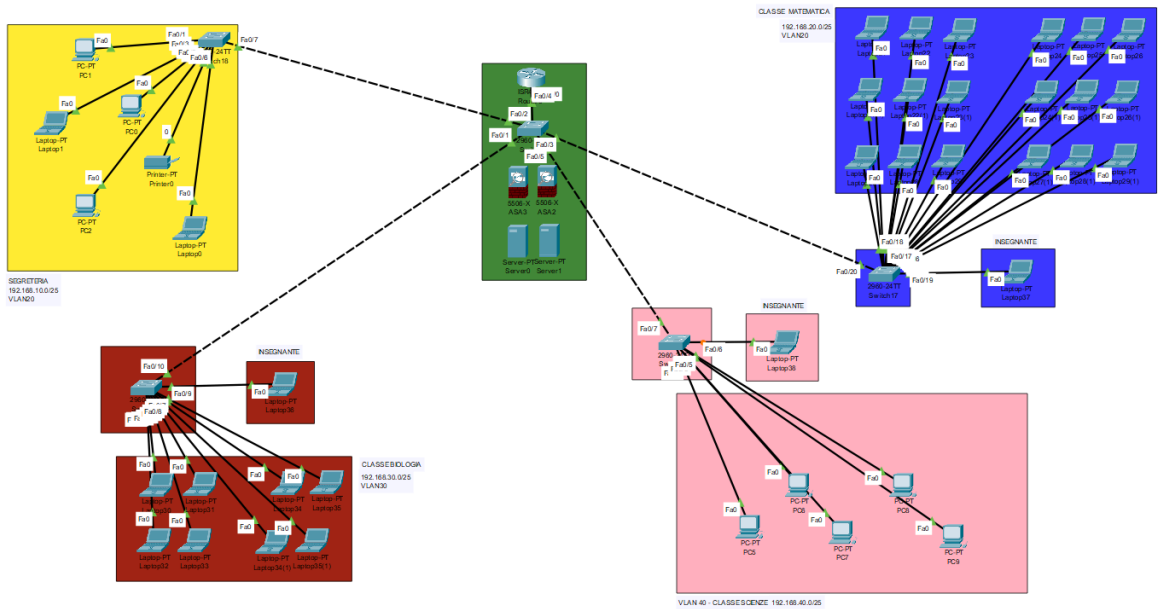
Progetto di Rete “Liceo Scientifico” – Relazione Tecnica

Introduzione

Il presente documento illustra la progettazione e configurazione di una rete locale segmentata per un istituto scolastico (Liceo Scientifico). Lo scopo del progetto è isolare logicamente i diversi reparti della scuola (segreteria amministrativa e tre aule didattiche di indirizzo: Matematica, Biologia, Scienze) mediante l’uso di VLAN, migliorando così l’organizzazione e la sicurezza della LAN. Ciascun gruppo dispone di una VLAN dedicata (Virtual LAN) che costituisce un distinto dominio di broadcast, separato dagli altri. Per permettere comunque la comunicazione controllata tra le reti dei vari reparti, è stato implementato il routing inter-VLAN tramite la tecnica *Router-On-A-Stick*. In pratica, un unico router fisico con un’unica interfaccia Ethernet trunk gestisce più sottointerfacce 802.1Q, fungendo da gateway per ogni VLAN distinta. Questo approccio consente di far comunicare reti IP diverse usando un solo collegamento verso il router, soddisfacendo le esigenze didattiche e di segmentazione della rete scolastica.

Topologia Logica

Figura: Topologia logica della rete con segmentazione in VLAN e instradamento inter-VLAN tramite Router-On-A-Stick

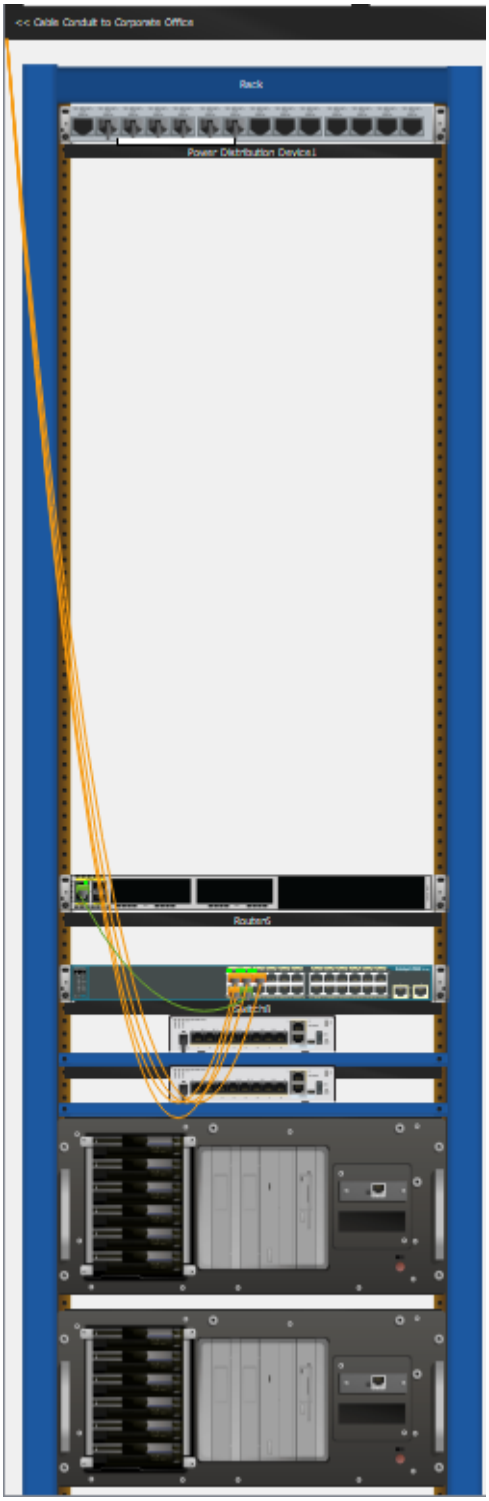


La topologia logica della rete (rappresentata in figura) prevede quattro VLAN separate su un’infrastruttura di switch e un router centrale. Le VLAN definite sono: **VLAN10 –**

Segreteria, **VLAN20 – Matematica**, **VLAN30 – Biologia** e **VLAN40 – Scienze**. Ognuna di esse corrisponde a una sottorete IP dedicata con maschera /25, rispettivamente: 192.168.10.0/25, 192.168.20.0/25, 192.168.30.0/25 e 192.168.40.0/25. I dispositivi (PC client) di ciascun reparto ricevono un indirizzamento IP appartenente alla propria subnet VLAN; ad esempio, i computer della Segreteria utilizzano indirizzi del tipo 192.168.10.x/25, mentre quelli dell'aula di Matematica utilizzano 192.168.20.x/25, e così via. Il router centrale è configurato con sottointerfacce (*sub-interfaces*) 802.1Q, ognuna associata a una VLAN e dotata di un indirizzo IP (tipicamente il primo indirizzo utile della subnet, es. 192.168.10.1 per VLAN10) che funge da *default gateway* per tutti i client di quella VLAN. In questo modo, tutto il traffico destinato fuori dalla propria VLAN viene inoltrato al router, il quale provvede a instradarlo verso la VLAN di destinazione appropriata. Dal punto di vista logico, le VLAN sono isolate di default (il traffico non può passare direttamente da una VLAN all'altra senza routing), garantendo separazione dei reparti; la comunicazione inter-VLAN avviene solamente attraverso il router, dove possono essere applicate eventuali regole di filtro. Completa la topologia un firewall Cisco ASA (già presente nello schema) collegato al router per la gestione sicura dell'accesso a Internet e future funzionalità di sicurezza perimetrale.

Topologia Fisica

Figura: Planimetria fisica della rete con la disposizione delle aule e connessioni cablate verso il rack centrale (router, switch core e server)



Dal punto di vista fisico, la rete è strutturata seguendo la planimetria dell'edificio scolastico. Ogni aula/laboratorio (Matematica, Biologia, Scienze) è dotata di uno switch di accesso ubicato nella stanza stessa, al quale sono collegati i PC della classe via cavo Ethernet. La Segreteria amministrativa dispone di alcune postazioni PC anch'esse collegate in rete, possibilmente tramite uno switch dedicato nell'ufficio oppure direttamente sullo switch centrale, a seconda della vicinanza al cabinet. Tutti gli switch periferici delle aule sono connessi tramite cablaggio strutturato all'**armadio di rete centrale**. Nell'armadio rack principale sono installati: **un router** (per instradare il traffico tra VLAN e verso l'esterno), **uno**

switch core di livello 2 (che aggrega le connessioni degli switch di aula e collega il router e il server), e **un server** locale. I collegamenti tra gli switch delle aule e lo switch core avvengono su porte trunk Gigabit Ethernet che corrono attraverso il cablaggio dell'edificio fino al rack centrale. In tal modo, ogni aula è fisicamente collegata al core in topologia a stella: lo switch core funge da concentratore e smista il traffico tra le varie tratte. Il server, posizionato anch'esso nel rack, è connesso allo switch core e può essere assegnato alla VLAN della Segreteria (o ad una VLAN dedicata, se previsto) per offrire servizi di rete interni. Il firewall ASA si trova all'esterno del router (collegato alla sua interfaccia WAN) e provvede all'eventuale collegamento verso Internet in sicurezza, ma non influisce sulla topologia interna delle VLAN.

Configurazione Dettagliata

Di seguito vengono elencati i principali passi di configurazione effettuati sui dispositivi di rete (switch e router) e sui terminali, con evidenza dei comandi Cisco IOS utilizzati.

- **Creazione delle VLAN sugli switch**: su *ogni switch* della rete (core e periferici) sono state create le quattro VLAN necessarie. In modalità di configurazione globale dello switch, i comandi utilizzati sono ad esempio:

```
Switch(config)# vlan 10
Switch(config-vlan)# name Segreteria
Switch(config-vlan)# vlan 20
Switch(config-vlan)# name Matematica
Switch(config-vlan)# vlan 30
Switch(config-vlan)# name Biologia
Switch(config-vlan)# vlan 40
Switch(config-vlan)# name Scienze
```

  Questo crea le VLAN 10, 20, 30, 40 e assegna a ciascuna un nome descrittivo corrispondente al reparto. I nomi servono solo a scopo documentativo (facilitano l'identificazione) mentre gli ID numerici VLAN sono ciò che definisce i domini di broadcast isolati all'interno degli switch.

- **Assegnazione delle porte in modalità access**: le porte degli switch che collegano i PC client sono state configurate in modalità *access* e assegnate alla VLAN corretta in base alla posizione. Ad esempio, sullo switch dell'aula di Matematica, le porte a cui sono connessi i PC di quella classe sono state configurate così:

```
SwitchMatematica(config)# interface range FastEthernet0/1-24
SwitchMatematica(config-if-range)# switchport mode access
SwitchMatematica(config-if-range)# switchport access vlan 20
```

In questo esempio tutte le porte FastEthernet da 0/1 a 0/24 sono impostate come porte di accesso appartenenti alla VLAN 20 (Matematica). Analogamente, sullo switch di Biologia le porte verso i client saranno in VLAN 30, e così via. Sullo switch core o sullo switch della Segreteria, le porte a cui sono collegati i PC della segreteria vengono messe in VLAN10. Questo garantisce che ciascun PC sia collegato solo con i dispositivi della propria VLAN e il suo traffico locale rimanga isolato dai PC di altre VLAN a livello 2.

- **Configurazione dei trunk tra switch**: i link di uplink che connettono ciascuno switch periferico allo switch core sono configurati come *trunk 802.1Q*. Una porta trunk è in grado di trasportare il traffico di tutte le VLAN (taggando i frame Ethernet con il rispettivo VLAN ID). Sullo switch periferico e sulla corrispondente porta dello switch core sono stati applicati i comandi:

```
Switch(config)# interface GigabitEthernet0/1
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk encapsulation dot1q   !
Switch(config-if)# switchport trunk native vlan 1         !
Switch(config-if)# switchport trunk allowed vlan 10,20,30,40
```

  In questo modo, la porta GigabitEthernet0/1 dello switch viene impostata in modalità trunk IEEE 802.1Q. La VLAN nativa è stata impostata sull'ID predefinito (1) oppure su una VLAN dedicata (ad esempio VLAN 99) uniformemente su tutti i trunk, per evitare disallineamenti. L'opzione `allowed vlan` restringe le VLAN trasportate sul trunk alle sole VLAN utilizzate (10,20,30,40), contribuendo a migliorare la sicurezza. I trunk consentono quindi al traffico di ciascuna VLAN di fluire dallo switch periferico al core e viceversa, mantenendo l'isolamento logico (i frame di VLAN diverse restano separati grazie al tag). Inoltre, è stato configurato un trunk analogo tra lo switch core e la porta del router a cui esso è collegato, poiché anche quel collegamento deve trasportare più VLAN contemporaneamente (verso le subinterface del router). Su tale porta dello switch core si utilizzano gli stessi comandi sopra indicati.

- **Configurazione del Router-On-A-Stick**: il router utilizza un'unica interfaccia fisica Ethernet (collegata allo switch core) per instradare il traffico di tutte le VLAN. Questa interfaccia (ad es. **GigabitEthernet0/0**) è stata suddivisa logicamente in sottointerfacce, una per ciascuna VLAN. Come primo passo, sull'interfaccia fisica si esegue `no ip address` e `no shutdown` (attivandola senza IP, poiché gli IP verranno assegnati alle subinterface). Poi, per ogni VLAN si configura una

subinterface dot1Q, ad esempio:

```
Router(config)# interface GigabitEthernet0/0.10
Router(config-subif)# encapsulation dot1Q 10
Router(config-subif)# ip address 192.168.10.1 255.255.255.128
Router(config-subif)# exit
Router(config)# interface GigabitEthernet0/0.20
Router(config-subif)# encapsulation dot1Q 20
Router(config-subif)# ip address 192.168.20.1 255.255.255.128
Router(config-subif)# exit
... (ripetuto per VLAN30 e VLAN40) ...
```

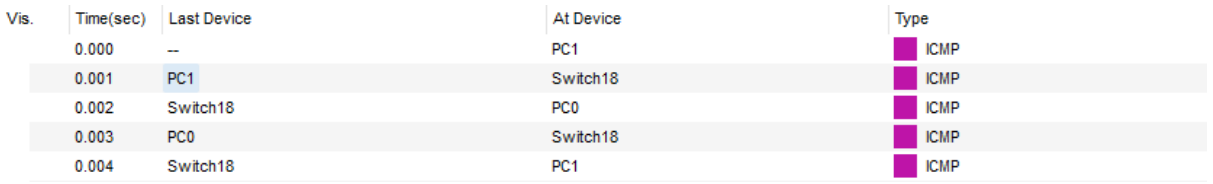
Ciascuna subinterface è identificata aggiungendo ".<VLAN_ID>" al nome dell'interfaccia fisica e viene istruita a fare *tagging* dei frame con l'ID VLAN corrispondente mediante il comando `encapsulation dot1Q <VLAN_ID>`. L'indirizzo IP assegnato su ogni subinterface rappresenta il gateway predefinito per la rispettiva VLAN (come mostrato nell'esempio sopra, 192.168.10.1/25 per VLAN10 Segreteria, 192.168.20.1/25 per VLAN20, ecc.). Una volta configurate tutte le subinterface, il router instaura con ciascuna VLAN una connessione di livello 3 direttamente connessa (come evidenziabile con `show ip route` che elenca le reti 192.168.10.0/25, 20.0/25, 30.0/25, 40.0/25 come "C" connected alle relative subinterface). In tal modo può effettuare l'instradamento tra queste reti. È importante notare che **la VLAN nativa** sul trunk non taggato (VLAN1 di default, se non modificata) andrebbe gestita con cautela: nel nostro caso non è stata utilizzata per traffico utenti, e si potrebbe configurare anche sul router una subinterface senza tag (`encapsulation dot1Q <ID> native`) se si volesse assegnare un IP anche alla VLAN nativa, ma ciò non è strettamente necessario poiché la VLAN1 non è usata per dispositivi finali in questo progetto.

- **Assegnazione degli IP e gateway sui PC**: i PC di ciascuna rete VLAN sono stati configurati con indirizzi IPv4 statici appartenenti alla subnet corretta e con il default gateway puntato all'IP della subinterface del router per quella VLAN. Ad esempio, un PC nell'aula di Biologia (VLAN30) potrebbe avere IP 192.168.30.10, netmask 255.255.255.128, gateway 192.168.30.1. Analogamente, un PC della Segreteria potrebbe essere configurato con IP 192.168.10.5/25 e gateway 192.168.10.1. Queste impostazioni assicurano che il traffico generato dal PC verso IP della stessa VLAN rimanga nel segmento locale, mentre qualsiasi traffico destinato a IP esterni (altra VLAN o Internet) venga inviato al router (gateway). **Nota**: attualmente, in assenza di un server DHCP, la configurazione IP è manuale su ogni postazione; in futuro si prevede di introdurre un servizio DHCP centralizzato per assegnare automaticamente gli indirizzi (vedasi sezione Miglioramenti Futuri).

Testing e Verifica

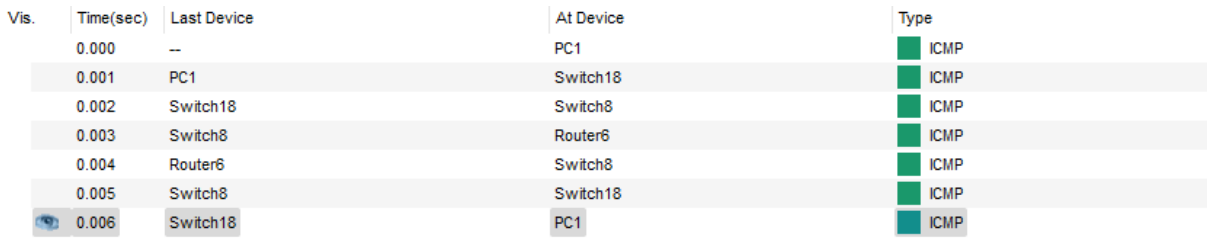
Dopo aver completato la configurazione, sono stati effettuati test di connettività per verificare il corretto funzionamento della rete VLAN e del routing inter-VLAN. In particolare, i seguenti test hanno dato esito positivo:

- **Ping intra-VLAN**: dispositivi all'interno della *stessa VLAN* sono in grado di comunicare tra loro. Ad esempio, due PC collegati alla VLAN20 (Matematica) riescono a pingarsi reciprocamente con successo, confermando che le porte sono correttamente assegnate e che gli switch inoltrano il traffico all'interno della VLAN senza filtrarlo. Lo stesso vale per PC appartenenti alle altre VLAN (es. due PC in Segreteria, due in Biologia, ecc.).



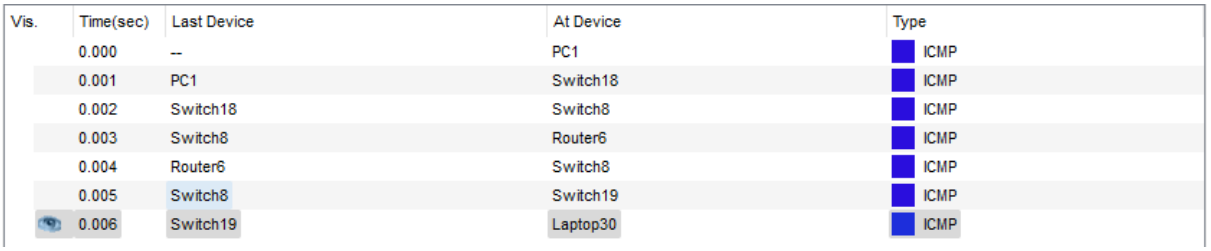
Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	PC1	ICMP
	0.001	PC1	Switch18	ICMP
	0.002	Switch18	PC0	ICMP
	0.003	PC0	Switch18	ICMP
	0.004	Switch18	PC1	ICMP

- **Ping inter-VLAN**: dispositivi appartenenti a *VLAN diverse* possono comunicare attraverso il router. È stato testato che un PC della VLAN10 (Segreteria) riesce a pingare l'indirizzo IP di un PC nella VLAN20 (Matematica) e ricevere risposta. Il percorso di questi pacchetti coinvolge il router (Router-On-A-Stick) che riceve il ping dalla VLAN10 e lo instrada verso la VLAN20, quindi la risposta viceversa. Il successo di questi test indica che il routing inter-VLAN è configurato correttamente e che le subinterface del router sono operative come gateway. Analogamente, è stata verificata la connettività tra tutte le coppie di VLAN previste dallo schema (ad esempio un PC in Biologia raggiunge un PC in Scienze, e così via).



Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	PC1	ICMP
	0.001	PC1	Switch18	ICMP
	0.002	Switch18	Switch8	ICMP
	0.003	Switch8	Router6	ICMP
	0.004	Router6	Switch8	ICMP
	0.005	Switch8	Switch18	ICMP
	0.006	Switch18	PC1	ICMP

- **Ping verso gateway e server**: ogni host è in grado di raggiungere il proprio gateway (la subinterface del router). Ad esempio, ciascun PC può eseguire con successo il ping del relativo indirizzo .1 della propria subnet VLAN, confermando che la configurazione IP del PC è corretta e che il router risponde su ogni VLAN. Inoltre, i PC delle varie VLAN riescono a pingare l'indirizzo del server centrale (se il server è collocato in una VLAN accessibile a tutti, come Segreteria, o se ha più interfacce su varie VLAN) – questo test conferma che anche le risorse condivise nella rete risultano raggiungibili. (Nel nostro caso, il server essendo nella VLAN10 è raggiungibile dai PC Segreteria direttamente e dalle altre VLAN tramite routing).



Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	PC1	ICMP
	0.001	PC1	Switch18	ICMP
	0.002	Switch18	Switch8	ICMP
	0.003	Switch8	Router6	ICMP
	0.004	Router6	Switch8	ICMP
	0.005	Switch8	Switch19	ICMP
	0.006	Switch19	Laptop30	ICMP

Considerazioni sulla Sicurezza

L'implementazione corrente fornisce una base di separazione del traffico tra i reparti, ma possono essere adottate ulteriori misure per migliorare la sicurezza della rete:

- **Isolamento tramite VLAN e native VLAN**: Già il fatto di aver suddiviso la LAN in VLAN costituisce un miglioramento della sicurezza e gestione, poiché limita il dominio di broadcast e isola il traffico di ciascun reparto ciscopress.com . Tuttavia, è importante configurare correttamente le VLAN native sui trunk. L'uso della VLAN1 come nativa è generalmente sconsigliato per motivi di sicurezza, in quanto è l'impostazione di default di tutti gli switch (potenziale vettore di attacchi VLAN hopping). Si raccomanda di impostare una VLAN nativa non utilizzata altrove (es. VLAN99) su tutti i trunk e di **non assegnare alcuna porta di accesso a tale VLAN nativa**. Questa accortezza elimina il rischio di traffico non taggato indesiderato e riduce la superficie di attacco. Inoltre, sui trunk andrebbero **permessi solo le VLAN necessarie** (come già fatto con `allowed vlan`), evitando di trasportare VLAN inutilizzate.

- **Controllo degli accessi agli switch**: Gli switch dovrebbero essere configurati con misure di sicurezza aggiuntive. Ad esempio, abilitare *port security* sulle porte di accesso per limitare il numero di indirizzi MAC connessi (impedendo che vengano collegati dispositivi non autorizzati a una porta, come switch o AP non previsti). Si possono configurare gli switch affinché disabilitino automaticamente (err-disable) una porta se viene rilevato un MAC non autorizzato o un flapping sospetto. Inoltre, è opportuno proteggere l'accesso di management agli switch: utilizzare credenziali robuste per console/SSH, definire un'apposita VLAN di management separata dalle VLAN utente, e filtrare l'accesso ai protocolli di gestione (ad es. limitando l'accesso SSH/Telnet ai soli IP autorizzati, come la postazione dell'amministratore di rete). Se supportato, si può implementare anche l'autenticazione centrale degli amministratori tramite RADIUS/TACACS+.

- **Filtraggio del traffico inter-VLAN**: Di default, con il router-on-a-stick ogni VLAN può comunicare con le altre senza restrizioni a livello 3. In un contesto scolastico, si potrebbe voler limitare o monitorare determinati traffici tra reparti (ad esempio, i PC degli studenti non dovrebbero raggiungere i sistemi amministrativi della Segreteria, se non necessario). A tal fine, si possono impostare **Access Control List (ACL)** sul router per filtrare il traffico tra specifiche VLAN

networklessons.com
. Le ACL permettono di definire politiche (ad esempio, consentire ai PC della segreteria di accedere alle VLAN didattiche ma non viceversa, oppure bloccare determinati protocolli/porte tra VLAN). Un'altra opzione, menzionata nel progetto, è l'uso di un firewall dedicato come l'ASA: l'ASA potrebbe essere configurato con interfacce su ciascuna VLAN in modalità *routed* o *transparent* e implementare regole di firewalling interne più avanzate. Nel nostro caso l'ASA è stato previsto principalmente per la protezione perimetrale verso Internet, ma in futuro potrebbe essere integrato anche per regolare il traffico interno tra VLAN se la sicurezza lo richiede.

- **Riduzione del dominio di fault**: La segmentazione in VLAN non solo migliora la sicurezza ma anche la resilienza: un eventuale loop di switching o tempesta di broadcast in una VLAN non si propaga alle altre. Per ulteriore sicurezza, si può considerare di abilitare funzionalità come **Storm Control** sugli switch (limitazione dei broadcast/multicast e unicast sconosciuti) per prevenire che saturazioni di traffico in un segmento impattino l'intera rete.

- **Integrazione con l'ASA**: Come accennato, il firewall Cisco ASA presente nello schema può essere sfruttato per migliorare la sicurezza generale. Esso potrebbe svolgere il ruolo di gateway verso Internet per tutte le VLAN (realizzando la separazione tra rete interna e WAN pubblica) e applicando politiche di NAT e ispezione del traffico in uscita/entrata. Inoltre, l'ASA può ospitare funzioni VPN per consentire accessi remoti sicuri, e in ambiente scolastico potrebbe essere usato per filtrare contenuti internet inappropriati attraverso funzionalità di URL filtering o integrazione con servizi appositi. Sebbene queste funzioni vadano oltre il perimetro del progetto VLAN interno, è importante pianificare l'architettura tenendo conto della loro implementazione futura.

Miglioramenti Futuri

Oltre alle misure di sicurezza sopracitate, sono stati identificati alcuni possibili sviluppi e miglioramenti realistici per evolvere la rete del Liceo Scientifico:

- **Introduzione di un server DHCP centralizzato**: Attualmente gli indirizzi IP sono configurati staticamente per ogni dispositivo. Una miglioria significativa sarebbe l'implementazione di un server DHCP in grado di gestire pool separati per ciascuna VLAN. Questo server potrebbe risiedere sul server già presente nel rack centrale (es. configurando un servizio DHCP su Windows Server o su Linux) oppure direttamente sul router Cisco (che supporta DHCP server per più pool). Ogni VLAN verrebbe associata a un pool IP distinto (es. pool 192.168.10.0/25 per Segreteria, 192.168.20.0/25 per Matematica, ecc.) e grazie al meccanismo di **DHCP relay (helper)** il router inoltrerebbe le richieste DHCP dai client al server centralizzato. Ciò semplificherebbe la gestione degli indirizzi, evitando conflitti e facilitando l'aggiunta di

nuovi dispositivi alla rete senza configurazione manuale.

- **Accesso a Internet con NAT**: Per fornire connettività Internet ai vari reparti in modo sicuro, si prevede di configurare la traduzione degli indirizzi (NAT) sull'apparato perimetrale. In pratica, il firewall ASA (o in alternativa il router stesso) effettuerà la **NAT overload (PAT)**, traducendo gli indirizzi privati delle VLAN interne in un pool di indirizzi pubblici (o in uno singolo, a seconda delle risorse disponibili) per l'accesso esterno. Questo permetterà a tutti i PC delle VLAN di navigare online utilizzando pochi indirizzi pubblici, mantenendo nascosta la rete interna. Contestualmente, andranno definite opportune regole firewall per filtrare il traffico in uscita e soprattutto in entrata, garantendo che solo il traffico autorizzato possa raggiungere la LAN scolastica dall'esterno.

- **Autenticazione e controllo accessi per gli utenti**: In un ambiente scolastico, potrebbe essere utile integrare meccanismi di autenticazione degli utenti nella rete. Un'idea è implementare **802.1X** sulle porte degli switch, associato a un server di autenticazione (es. RADIUS tramite un server Windows NPS o Cisco ISE). In questo modo, ogni dispositivo che si collega alla rete cablata (o Wi-Fi, se presente) deve autenticarsi con credenziali (ad esempio, le credenziali dell'utente studente o docente) prima di ottenere l'accesso alla LAN. A seconda dell'identità, si potrebbe anche assegnare dinamicamente la VLAN corretta (studenti vs personale) per applicare politiche differenti. Questo approccio aumenta la sicurezza impedendo accessi non autorizzati semplicemente collegando un dispositivo alla presa di rete. Se l'infrastruttura 802.1X risultasse troppo complessa, almeno una segregazione delle reti studenti/personale tramite VLAN separate e firewall/ACL tra di esse sarebbe un miglioramento (ad es. VLAN aggiuntive per "Studenti" e "Staff" indipendenti dai reparti fisici).

- **Logging e Monitoring**: Implementare un sistema di monitoraggio centralizzato per la rete. Si potrebbe configurare un server syslog dove router, switch e firewall inviano i propri log di eventi (es. tentativi di accesso, porte che vanno giù, violazioni di port security, messaggi ACL/Firewall, ecc.). Allo stesso tempo, attivare il protocollo SNMP sui dispositivi di rete per raccogliere statistiche di performance, stato delle interfacce e ricevere trap su eventi critici. Utilizzando una piattaforma di NMS (Network Management System) open source o commerciale, l'amministratore potrà avere una panoramica in tempo reale dello stato della rete e storicizzare dati utili per il troubleshooting. Anche il firewall ASA dovrebbe essere integrato nel monitoring per tracciare tentativi di intrusione o traffico anomalo. Infine, abilitare funzionalità di NetFlow/sFlow sul router (se supportato) consentirebbe di analizzare il traffico per individuare eventuali abusi (es. download massivi, streaming non autorizzato) e dimensionare meglio la banda internet.

- **Scalabilità e ridondanza**: Pensando al futuro, se la scuola dovesse espandersi, la topologia progettata è relativamente modulare: si potranno aggiungere nuove VLAN per altri reparti o servizi (es. una VLAN per laboratori informatici aggiuntivi, o per telecamere IP) senza stravolgere l'architettura, configurando ulteriori subinterface sul router e propagando le VLAN sugli switch. Per aumentare l'affidabilità, si potrà considerare l'uso di link ridondanti tra il core e gli switch di aula (configurando

protocolli Spanning Tree adeguati per prevenire loop) o l'adozione in futuro di uno switch core di livello 3 con routing interno (eliminando il single point of failure del router-on-a-stick, che in caso di guasto isolerebbe tutte le VLAN). Si potrebbe inoltre valutare un secondo dispositivo di routing/firewall in alta affidabilità (HSRP o failover ASA) per garantire la connettività anche in caso di guasto di un apparato critico.

Conclusione

In conclusione, la progettazione **segmentata tramite VLAN** si è rivelata fondamentale per strutturare la rete del Liceo Scientifico in modo ordinato, sicuro ed efficiente. Grazie alle VLAN, ogni dipartimento o aula opera su un segmento isolato, riducendo il traffico di broadcast e limitando l'ambito di eventuali problemi di rete. Al tempo stesso, l'implementazione del routing inter-VLAN con approccio *Router-On-A-Stick* ha permesso di mantenere la necessaria comunicazione tra i vari segmenti in modo centralizzato e controllato. Questo approccio modulare facilita la gestione della rete scolastica: nuove postazioni o reparti possono essere aggiunti assegnandoli a VLAN esistenti o creandone di nuove senza impattare sul resto dell'infrastruttura. La documentazione dei comandi e delle configurazioni eseguite garantisce la riproducibilità della configurazione e semplifica le attività di troubleshooting e manutenzione. In prospettiva, adottando le misure di sicurezza e miglioramenti proposti, la rete potrà evolvere ulteriormente, offrendo connettività Internet sicura, gestione centralizzata degli indirizzi e controllo degli accessi granulari. L'esperienza svolta evidenzia l'importanza della segmentazione tramite VLAN in ambienti didattici: essa bilancia efficacemente **isolamento** e **connettività**, fornendo una piattaforma di rete robusta su cui la scuola può fare affidamento per le proprie attività quotidiane.