Creazione rete segmentata in più VLAN con due switch

Oggi dimostro come implementare una rete segmentata in più VLAN e Subnetting su due switch.

1. Switch N.1 ospita 3 VLAN con subnetting diverse
- VLAN 2 (Segretaria) 2 host con IP 192.168.1.100 e 192.168.1.101
- VLAN 3 (Dottori) 2 host con IP 192.168.2.100 e 192.168.2.101
- VLAN 4 (Paghe) 2 host con IP 192.168.3.100 e 192.168.3.101

2. Switch N.2 ospita 1 VLAN
- VLAN 2 (Segretaria) 2 host con IP 192.168.1.102 e 192.168.1.103

I due switch sono collegati tra di loro tramite porta trunk per permettere il passaggio del traffico VLAN

Configurazione

Dopo aver configurato i PC con assegnazione di indirizzo IP e subnet mask diversi ho creato sullo switch N.1 le VLAN e ho assegnato ad ogni VLAN porte diverse:

- Alla VLAN 2 ho assegnato le porte FastEthernet 0/1 e FastEthernet 0/2
- Alla VLAN 3 ho assegnato le porte FastEthernet 0/3 e FastEthernet 0/4
- Alla VLAN 4 ho assegnato le porte FastEthernet 0/5 e FastEthernet 0/6

Sullo switch N.2 ho creato una VLAN e gli ho assegnato la porta:

- Alla VLAN 2 ho assegnato le porte FastEthernet 0/1 e FastEthernet 0/2

Gli switch sono stati collegati con GigabitEthernet sulla porta 0/1 e 0/2 in modalità Trunk
Non è presente un router quindi le VLAN non comunicano tra loro

VLAN(Virtual Local Area Network)

Una VLAN è una rete logica creata all'interno di una rete fisica, che permette di segmentare i dispositivi in gruppi indipendenti, anche se connessi allo stesso switch fisico. Le VLAN sono configurabili a livello di switch e router, e vengono spesso utilizzate per migliorare sicurezza, gestione e prestazioni della rete.

Vantaggi delle VLAN

1. **Segmentazione del traffico**

- Le VLAN permettono di separare il traffico di rete per dipartimenti, servizi o funzioni aziendali (ad esempio contabilità, marketing, produzione) senza necessità di infrastruttura fisica separata.
- Riduce il dominio di broadcast, limitando la quantità di traffico inutile che raggiunge tutti i dispositivi.

2. Miglioramento della sicurezza

- I dati all'interno di una VLAN sono isolati da altre VLAN, impedendo a utenti non autorizzati di accedere a risorse sensibili.
- Permette di creare VLAN dedicate per server critici o per accesso ospite, riducendo il rischio di attacchi laterali.

3. Flessibilità e scalabilità

- Gli utenti possono essere spostati da una VLAN all'altra con semplice configurazione software, senza modifiche fisiche dei cavi.
- Facilita l'espansione della rete in ambienti aziendali dinamici.

4. Ottimizzazioni delle prestazioni

- Riducendo il numero di dispositivi in un dominio di broadcast, si diminuisce il traffico inutile, migliorando l'efficienza complessiva della rete.
- Migliora la gestione della larghezza di banda tra reparti o servizi specifici.

5. Gestione centralizzata e semplificata

- Configurazioni come priorità QoS, access control e monitoraggio del traffico possono essere applicate per VLAN specifiche senza intervenire su tutta la rete.

6. Supporto per politiche aziendali

- Possibilità di implementare politiche di accesso basate su ruolo, dipartimento o servizio, aumentando il controllo sugli utenti e sui dispositivi.

Svantaggi delle VLAN

1. Complessità nelle configurazioni

- La progettazione di VLAN richiede una buona pianificazione della topologia, delle policy di routing e della sicurezza.
- Errori nella configurazione possono causare problemi di comunicazione tra dispositivi o vulnerabilità di sicurezza.

2. Necessità di switch gestiti

- Le VLAN richiedono switch che supportino 802.1Q o protocolli simili, generalmente switch "gestiti", più costosi rispetto agli switch non gestiti.

3. Limitazioni di broadcast e routing

- La comunicazione tra VLAN diverse richiede un router o un Layer 3 switch. Questo può introdurre un punto di congestione o latenza aggiuntiva se il traffico inter-VLAN è elevato

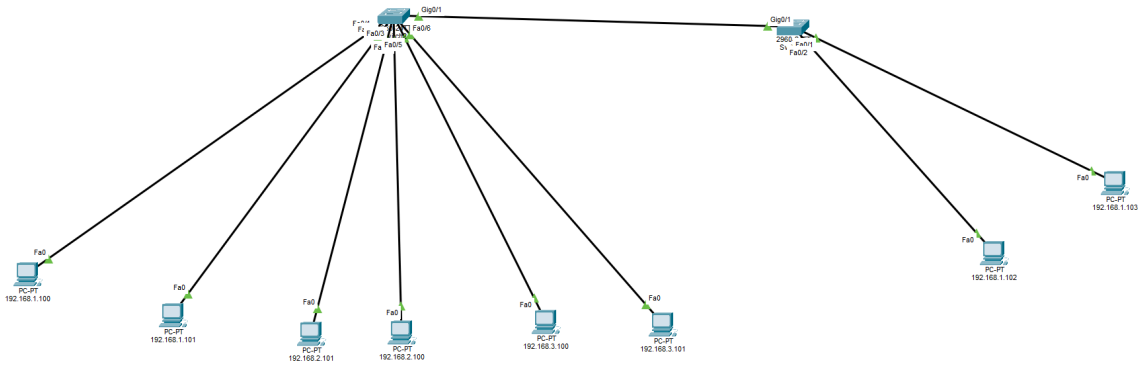
4. Possibili problemi di scalabilità
- In reti molto grandi, con molte VLAN, la gestione diventa complessa e la configurazione dei trunk tra switch può diventare difficile da mantenere.
- Ogni VLAN ha un ID numerico limitato, quindi reti molto vaste devono pianificare attentamente l'uso degli ID VLAN.

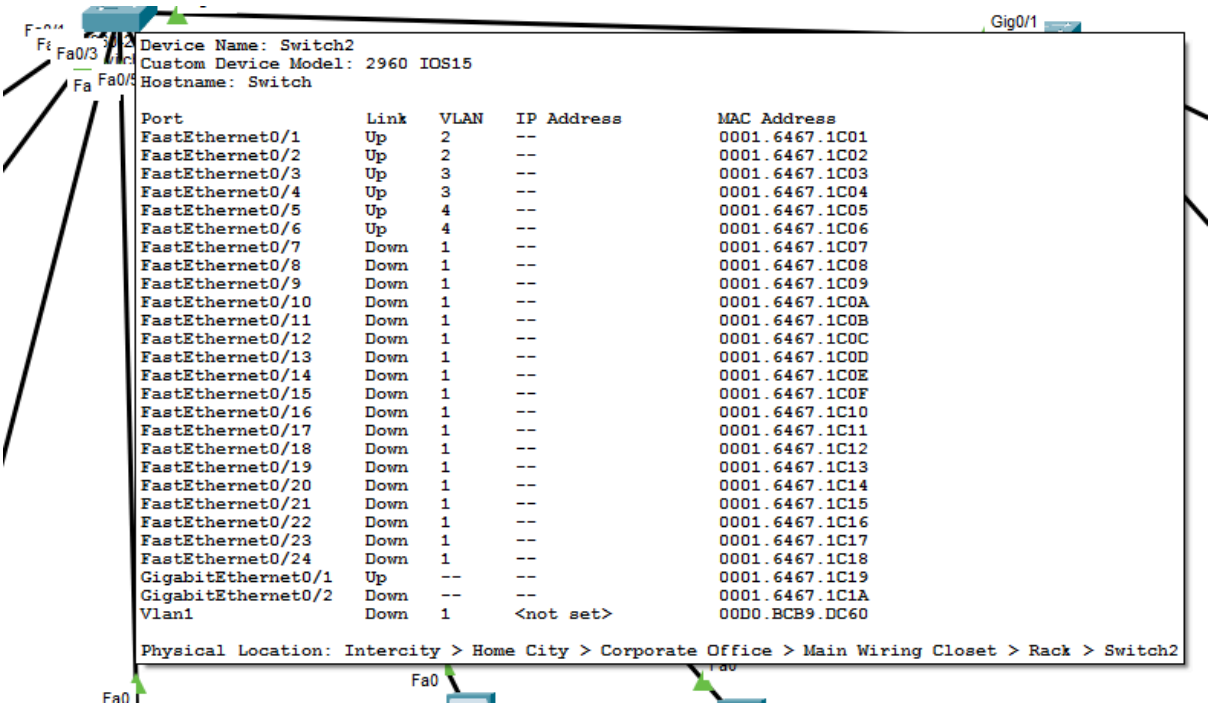
5. Rischi di sicurezza se mal configurati
- VLAN hopping: attacchi che permettono a un dispositivo di saltare da una VLAN all'altra se gli switch non sono configurati correttamente.
- La segmentazione logica non sostituisce completamente le politiche di sicurezza fisiche o firewall tra reti critiche.

Sintesi

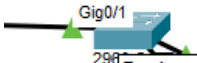
In sintesi possiamo dire che le VLAN sono uno strumento potente per isolare e ottimizzare il traffico di rete offrendo sicurezza, flessibilità e prestazioni migliori.

Schema grafico della configurazione

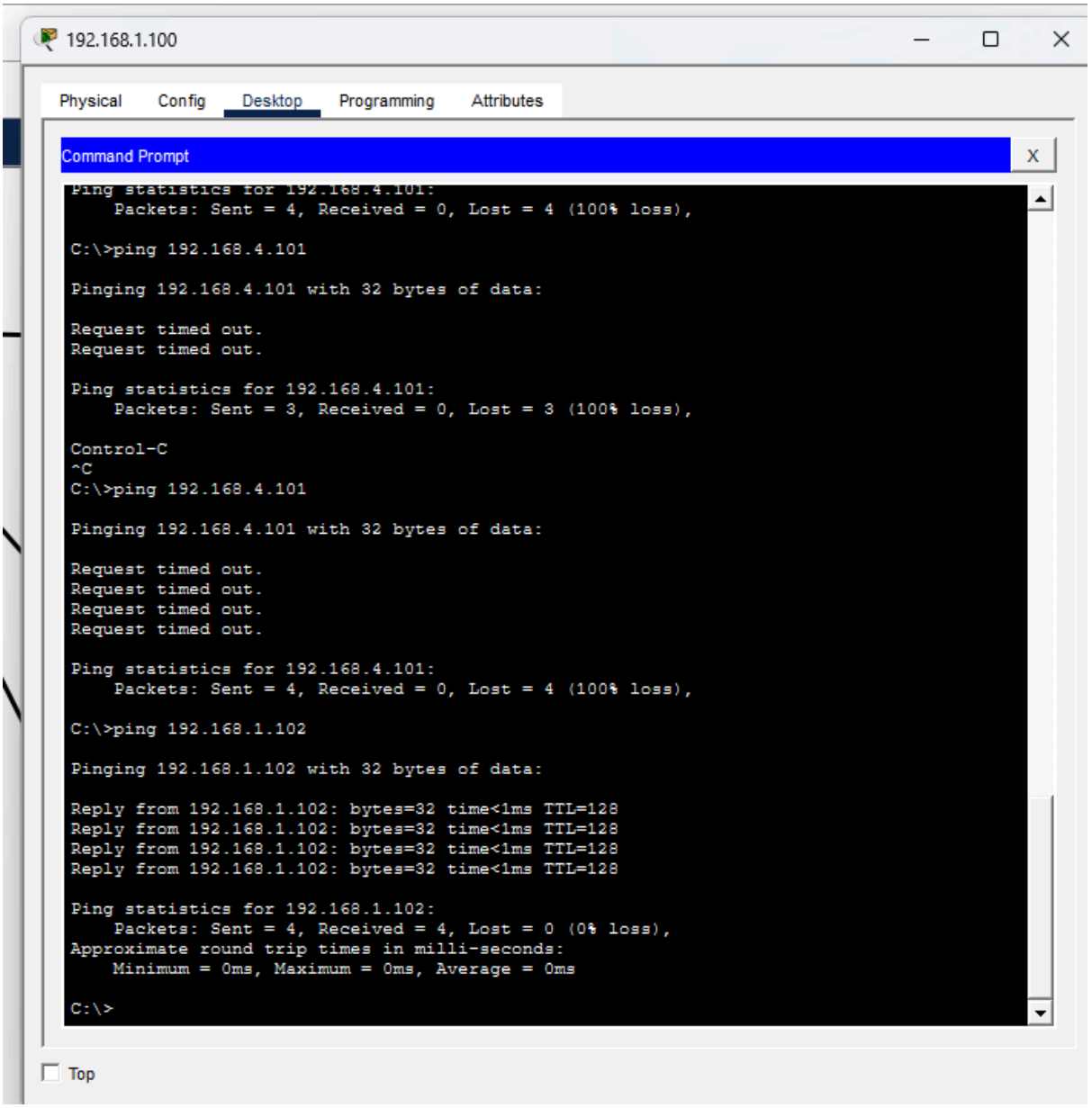





```
Device Name: Switch2
Custom Device Model: 2960 IOS15
Hostname: Switch

Port                 Link   VLAN   IP Address          MAC Address
FastEthernet0/1      Up     2      --                  0001.6467.1C01
FastEthernet0/2      Up     2      --                  0001.6467.1C02
FastEthernet0/3      Up     3      --                  0001.6467.1C03
FastEthernet0/4      Up     3      --                  0001.6467.1C04
FastEthernet0/5      Up     4      --                  0001.6467.1C05
FastEthernet0/6      Up     4      --                  0001.6467.1C06
FastEthernet0/7      Down   1      --                  0001.6467.1C07
FastEthernet0/8      Down   1      --                  0001.6467.1C08
FastEthernet0/9      Down   1      --                  0001.6467.1C09
FastEthernet0/10     Down   1      --                  0001.6467.1C0A
FastEthernet0/11     Down   1      --                  0001.6467.1C0B
FastEthernet0/12     Down   1      --                  0001.6467.1C0C
FastEthernet0/13     Down   1      --                  0001.6467.1C0D
FastEthernet0/14     Down   1      --                  0001.6467.1C0E
FastEthernet0/15     Down   1      --                  0001.6467.1C0F
FastEthernet0/16     Down   1      --                  0001.6467.1C10
FastEthernet0/17     Down   1      --                  0001.6467.1C11
FastEthernet0/18     Down   1      --                  0001.6467.1C12
FastEthernet0/19     Down   1      --                  0001.6467.1C13
FastEthernet0/20     Down   1      --                  0001.6467.1C14
FastEthernet0/21     Down   1      --                  0001.6467.1C15
FastEthernet0/22     Down   1      --                  0001.6467.1C16
FastEthernet0/23     Down   1      --                  0001.6467.1C17
FastEthernet0/24     Down   1      --                  0001.6467.1C18
GigabitEthernet0/1   Up     --     --                  0001.6467.1C19
GigabitEthernet0/2   Down   --     --                  0001.6467.1C1A
Vlan1                Down   1      <not set>           00D0.BCB9.DC60

Physical Location: Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > Switch2
```




```
Device Name: Switch3
Custom Device Model: 2960 IOS15
Hostname: Switch

Port                 Link   VLAN   IP Address          MAC Address
FastEthernet0/1      Up     2      --                  0002.17D6.3101
FastEthernet0/2      Up     2      --                  0002.17D6.3102
FastEthernet0/3      Down   1      --                  0002.17D6.3103
FastEthernet0/4      Down   1      --                  0002.17D6.3104
FastEthernet0/5      Down   1      --                  0002.17D6.3105
FastEthernet0/6      Down   1      --                  0002.17D6.3106
FastEthernet0/7      Down   --     --                  0002.17D6.3107
FastEthernet0/8      Down   1      --                  0002.17D6.3108
FastEthernet0/9      Down   1      --                  0002.17D6.3109
FastEthernet0/10     Down   1      --                  0002.17D6.310A
FastEthernet0/11     Down   1      --                  0002.17D6.310B
FastEthernet0/12     Down   1      --                  0002.17D6.310C
FastEthernet0/13     Down   1      --                  0002.17D6.310D
FastEthernet0/14     Down   1      --                  0002.17D6.310E
FastEthernet0/15     Down   1      --                  0002.17D6.310F
FastEthernet0/16     Down   1      --                  0002.17D6.3110
FastEthernet0/17     Down   1      --                  0002.17D6.3111
FastEthernet0/18     Down   1      --                  0002.17D6.3112
FastEthernet0/19     Down   1      --                  0002.17D6.3113
FastEthernet0/20     Down   1      --                  0002.17D6.3114
FastEthernet0/21     Down   1      --                  0002.17D6.3115
FastEthernet0/22     Down   1      --                  0002.17D6.3116
FastEthernet0/23     Down   1      --                  0002.17D6.3117
FastEthernet0/24     Down   1      --                  0002.17D6.3118
GigabitEthernet0/1   Up     --     --                  0002.17D6.3119
GigabitEthernet0/2   Down   --     --                  0002.17D6.311A
Vlan1                Down   1      <not set>           0060.3EEC.D35C

Physical Location: Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > Switch3
```


192.168.1.100
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
Ping statistics for 192.168.4.101:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 192.168.4.101
Pinging 192.168.4.101 with 32 bytes of data:
Request timed out.
Request timed out.
Ping statistics for 192.168.4.101:
Packets: Sent = 3, Received = 0, Lost = 3 (100% loss),
Control-C
^C
C:\>ping 192.168.4.101
Pinging 192.168.4.101 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 192.168.4.101:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 192.168.1.102
Pinging 192.168.1.102 with 32 bytes of data:
Reply from 192.168.1.102: bytes=32 time<1ms TTL=128
Reply from 192.168.1.102: bytes=32 time<1ms TTL=128
Reply from 192.168.1.102: bytes=32 time<1ms TTL=128
Reply from 192.168.1.102: bytes=32 time<1ms TTL=128
Ping statistics for 192.168.1.102:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>
Top