Configurazione di una VLAN

- Creazione della VLAN con il relativo ID incrementale di 10 in 10 sugli switch interessati (`Vlan {num}`)
- Configurazione delle porte come access o trunk (`switchport mode trunk | access`)
- Configurazione degli ip assegnati alla VLAN (`VLAN {num} {ip sottorete}/{mask sottorete}`)

Configurazione di un router-on-a-stick

La configurazione di un router on a stick prevede che si imposti l'interfaccia di routing secondo i seguenti passi:

- Setting dell'interfaccia come interfaccia di livello 2 (`no ip address`)
- Configurazione di della sub-interfaccia (`interface FastEthernet0/0.x` con x = progressivo sub interfaccia per VLAN)
    - Setting dell'incapsulamento a 802.1q per la vlan (`encapsulation dot1q {vlan-num} native`)
    - Setting dell'IP address per la sub-interfaccia con un IP della VLAN `{vlan-num}` in considerazione (`ip address {IP vlan 1} 255.255.255.0`)
- Ripetere la configurazione per la n-esima sub-interfaccia

Esempio utilizzo di un IP pubblico con NAT

Disponete dell'indirizzo pubblico 196.20.76.1. Spiegate come lo utilizzereste per permettere ai PC della VLAN docenti di collegarsi a Inernet attraverso un gateway (Suggerimento: considerate un NAT sul router di connessione a Internet). E' possibile impedire l'accesso a Internet ai computer della VLAN "studenti"? Come?

Ipotesi: all'interno della rete si sta utilizzando l'indirizzo privato 192.168.0.0/24, subnettato in due subnet di indirizzo 192.168.0.0/25 e 192.168.0.128/25, rispettivamente affidati alla VLAN docenti e alla VLAN studenti.

Per permettere di utilizzare un indirizzo IP si configurerà il NAT sul gateway di accesso ad internet, in modo da assegnare il pool di indirizzi privati all'indirizzo pubblico di cui sopra.
Considerando un sistema di routing basato su linux, l'applicazione del seguente comando iptables può fare quanto richiesto:

```
iptables -t nat -A POSTROUTING -s  192.168.0.0/25 -j MASQUERADE
```

Questo presuppone che sul gateway sia abilitato il NAT basato su porte, in modo che si possa utilizzare un solo indirizzo pubblico ma sia possibile multiplexare e demultiplexare il traffico da/verso gli host interni alla rete (il router tiene una tabella di associazione tra indirizzo dell'host privato (ed eventuale porta) e relativo indirizzo pubblico (sempre uguale in questo caso) e porta).

Sempre ipotizzando un sistema di routing basato su linux, si potrà scegliere di scartare tutti i pacchetti in arrivo dalla sottorete 192.168.1.128/25, coi comandi seguenti

```
iptables -A INPUT -s 192.168.0.128/25 -d 192.168.0.0/24 ACCEPT
iptables -A INPUT -s 192.168.0.128/25 DROP
```

La prima regola specifica che tutti i pacchetti in arrivo dalla sottorete degli studenti e indirizzati alla super rete locale devono essere accettati, mentre la seconda specifica gli altri pacchetti provenienti dalla sottorete studenti che non fanno matching con la prima regola devono essere scartati.

Failure su IDLE RQ

- Si calcola Dimensione Frame * Probabilità errore bit
- Si stabilisce una probabilità di fallimento del frame Pf che sia abbastanza maggiore di del valore appena calcolato (Pf >> Ni*Pb)

- Si calcola U = (1 - Pf) / (1 + 2(Tp / Tix)), se bisogna calcolare il bitrate si imposta U = 1 e si calcola la banda come incognita in Tix

Tecniche per permettere il traffico solo dall'interno

Soluzione 1) Utilizzo del firewall sul router in modo da filtrare i pacchetti in arrivo dall'esterno, e quindi l'applicazione delle regole
iptables -A FORWARD -i {interfaccia_connessa_a_internet} -j DROP
iptables -A FORWARD -o {interfaccia_connessa_a_internet} -j ACCEPT

Soluzione 2)
Applicazione di una route di reject sul router
route add -net 0.0.0.0 netmask 0.0.0.0 reject

Soluzione 3)
Utilizzo del NAT, in quanto costruendo la tabella di connessioni a partire dalle connessioni create dall'interno, ogni pacchetto che proviene dall'esterno, se non appartiene ad una connessione giù creata, non può passare, perché il NAT non sa come tradurlo.

Calcolo Throughput

ByteDati = 1538 - 38 (overhead Frame Ethernet) - 20 (overhead minimo IP) - 20 (overhead minimo TCP)
RapportoTotSuDati = ByteDati / 1538
BandaEffettiva (o Throughput) = BandaNominale * RapportoTotSuDati

Es. TCP/IP/Ethernet 10Mbps.

Rapporto tra il massimo payload e la grandezza del frame ethernet = (1500-40)/(1500+38) = 0.9492 (95.92%)
Banda effettiva = 10^7 bit/s * 0.9492 = 9,49 Mbps

Calcolo throughput al cambiare della finestra

Tix + 2Tp = RTT
Di conseguenza il numero di segmenti (o W, come viene chiamato qui) è
RTT / Tix
ossia
RTT / (DimensionePacchetto / BitRateNominaleLinea)

Una volta calcolato quello, che fornisce il "limite superiore alla quantità di dati trasmissibili", si procede a calcolare step by step il crescendo della finestra fino al raggiungimento del limite.
Per il throughput si calcola la quantità di dati effettivamente trasmessa in quell'istante lì (scorporata di tutti gli overhead di protocollo) sui byte trasmessi (vedi formula sopra).

Complementi NAT

+ Il nat ***overloading*** (o PAT, o NAPT), è una forma di NAT dinamico che mappa più IP non registrati ad un singolo IP pubblico usando diverse porte. Nell'overloading, ogni computer sulla rete privata è tradotto nello stesso IP ma con una assegnazione di porta diverse.
+ Il ***dominio di stub*** è una LAN interna che usa gli gli IP al suo interno
+ Quando un ***pacchetto entra nel box NAT*** il suo indirizzo mittente è rimpiazzato dall'ip della compagnia e la porta sorgente è rimpiazzata da da un indice della tabella di traduzione del NAT. Questa tabella contiene per ogni riga l'ip e la porta originali
+ I ***pacchetti che arrivano nel NAT*** box dall'esterno subiscono lo stesso processo all'inverso

+ Quando si utilizza il NAT dinamico si crea una sorta di ***firewall***, in quanto il NAT permette solamente le connessioni che sono create all'interno del dominio di stub, e blocca le connessioni esterne
+ Al contrario, il ***NAT Statico*** permette di esporre un ip interno all'esterno, permettendo le connessioni dall'esterno per l'host interno esposto
+ I vantaggi dell'utilizzo del NAT sono
    + uso di un singolo IP per tanti host (fino a 64k)
    + creare reti nascoste
    + aumentare la sicurezza
    + semplicità e affidabilità
    + può essere usato per bilanciare il carico
    + trasferimento di server su altri host senza preoccupazione di broken links, sarà sufficiente cambiare il mapping interno nel router
    + NAT + RFC 1918 hanno rallentato l'esaurimento degli IPv4