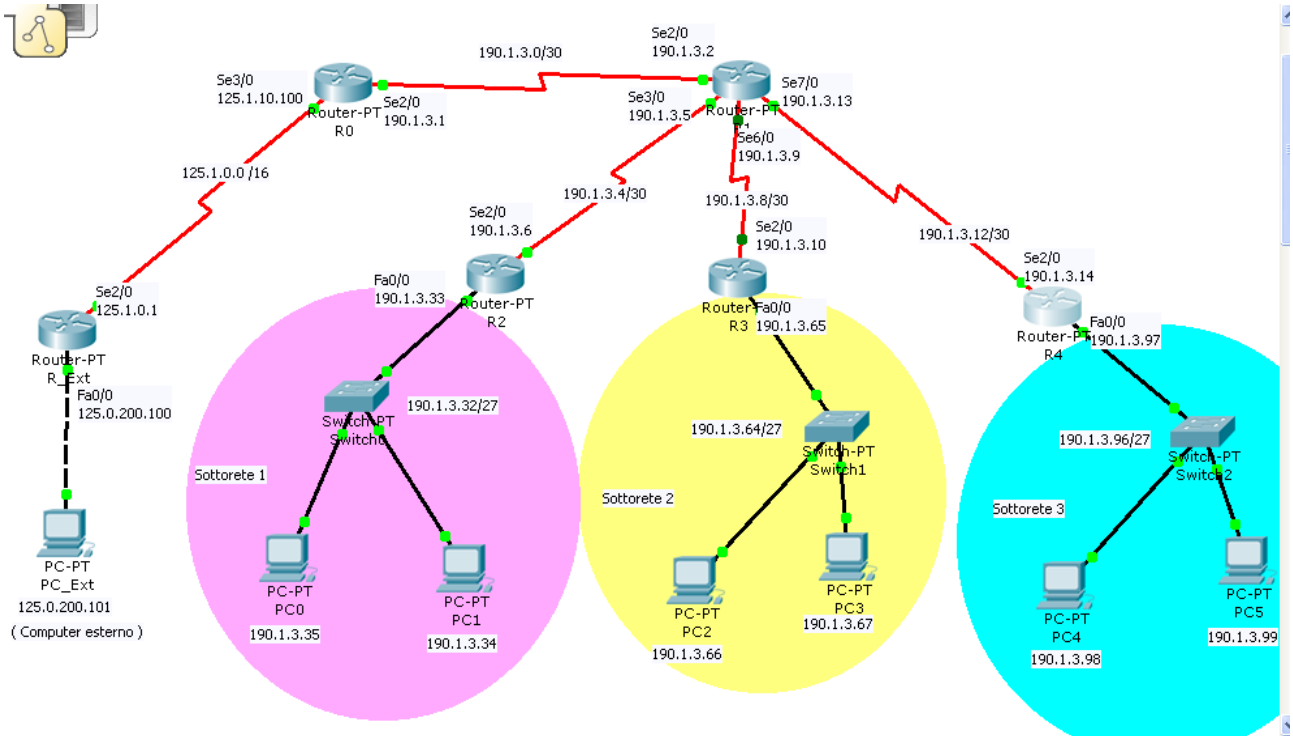
Rete suddivisa in subnet + esempio di ACL

Il problema

Considerato lo spazio di indirizzamento 176.16.3.0 /24, avente ampiezza di 255 possibili numeri IP, si consideri la rete sottostante. Scopo della rete disegnata è quello di suddividere in tre sottoreti i numeri di IP della rete principale. I raggruppamenti presenti (nell'esecutivo schematizzati) sono tre, ciascuno di ampiezza massima effettiva di 30 host (32 numeri di IP – 2)[1].

La suddivisione ordinata degli indirizzi IP in vari sottogruppi, formanti delle sottoreti, permette:

- un assegnazione metodica ed ordinata dei numeri di IP
- di avere tabelle di instradamento nei router ridotte al minimo
- instradare in una sola direzione per tutto un gruppo di indirizzi



La suddivisione degli indirizzi di 190.1.3.0 / 24 è:

Rete	CIDR	Indirizzo inizio	Indirizzo finale	N° host
190.1.3.0	/24	190.1.3.1	190.1.3.255	(255)
Suddivisi come:				
190.1.3.0	/30	190.1.3.1	190.1.3.2	2
190.1.3.4	/30	190.1.3.5	190.1.3.6	2
190.1.3.8	/30	190.1.3.9	190.1.3.10	2
190.1.3.12	/30	190.1.3.13	190.1.3.14	2
Inutilizzati		190.1.3.16	190.1.3.31	(16)
190.1.3.32	/27	190.1.3.33	190.1.3.62	30

1 In questo conto si deve considerare che al numero complessivo di numeri di IP si deve sottrarre 2 indirizzi, 1 per la rete (il cosiddetto indirizzo di rete) ed 1 che deve implementare l'indirizzo broadcast (sulla rete indicata in viola 190.1.3.63).

190.1.3.64	/27	190.1.3.65	190.1.3.94	30
190.1.3.96	/27	190.1.3.97	190.1.3.127	30
Inutilizzati (per espansioni future)		190.1.3.129	190.1.3.255	(128)

Come si può osservare un largo blocco di tali indirizzi (da 190.1.3.129 a 190.1.3.255) è rimasto libero, per scopi ed utilizzi futuri.

I primi 128 indirizzi del blocco ipotizzato sono invece stati usati per definire indirizzi nei tronchi di connessione e soprattutto nelle sottoreti stesse. Esse (schematicamente rappresentate con due calcolatori attaccati) hanno la possibilità di averne fino a 30 ognuna.

Le regole di routing inserite in modo statico nei vari router di tale rete sono:

Router	Instradamento verso rete	Comando di routing
R1	190.1.3.32 / 27	ip route 190.1.3.32 255.255.255.224 Se3/0
R1	190.1.3.64 / 27	ip route 190.1.3.64 255.255.255.224 Se6/0
R1	190.1.3.96 / 27	ip route 190.1.3.96 255.255.255.224 Se7/0
R1	0.0.0.0 / 0	ip route 0.0.0.0 0.0.0.0 Se2/0

Tali regole permettono a tutti i pacchetti ricadenti nell'ambito dei numeri di IP relativi ad una delle 3 sottoreti considerate di essere instradati in modo opportuno verso il ramo della rete connesso alla relativa sottorete.

Si pone subito dopo, semmai, un altro problema , ossia se ognuna delle sottoreti possa vedere le altre.

Inoltre anche nel router R1 è inserita la regola, che indica che il pacchetto deve essere inoltrato all' esterno della rete se l'indirizzo di destinazione indicato non è quello richiesto.

Con i settaggi definiti sopra nessuna delle sottoreti poteva vedere le altre sottoreti, in dalla tabella di instradamento definita prima, solo R1 è istruito a smistare opportunamente i pacchetti verso le sottoreti. Viceversa un pacchetto proveniente dalla sottorete 1 che debba andare alla sottorete 3, incontrerà sulla sua strada il router R2 non opportunamente istruito sulla posizione della sottorete 3. Tuttavia indicando genericamente a ciascuno di questi router di instradare i pacchetti "sconosciuti" (instradamento di default) verso R1, il problema della comunicazione fra le varie sottoreti e', se ci si pensa, risolto.

Per i router subito sottostanti ad R1 che permette l'accesso a tutta la sottorete, ossia R2, R3 ed R4 che sono quelli di accesso alle singole sottoreti 190.1.3.32/27, 190.1.3.64/27, 190.1.3.96/27, si definiranno quindi le regole di routing (statiche):

Router	Instradamento verso rete	Comando di routing
R2	190.1.3.32 / 27	Nessuno - collegata
R2	190.1.3.4 / 30	Nessuno - collegata
R2	0.0.0.0 /0	ip route 0.0.0.0 0.0.0.0 Se2/0 (instradamento di default in uscita verso altra rete)

In modo analogo si regolano i router R3 ed R4. Ad esempio per R3:

Router	Instradamento verso rete	Comando di routing
R3	190.1.3.64 / 27	Nessuno - collegata
R3	190.1.3.8 / 30	Nessuno - collegata
R3	0.0.0.0 /0	ip route 0.0.0.0 0.0.0.0 Se2/0 (instradamento di default in uscita verso altra rete)

Si noti che eventuali pacchetti partenti dalla sottorete 1 e viaggianti verso la sottorete 3, con queste regolazioni prima saliranno verso R1, per poi essere redirezionati, se necessario, opportunamente, verso la sottorete opportuna. Se viceversa risulta che il pacchetto non è indirizzato verso le sottoreti anzidette, esso proseguirà verso l'esterno della sottorete (come, ad esempio, nel caso sia diretto al PC 125.0.200.1).
In questo modo le sottoreti sono tutte in comunicazione incondizionata tra loro.
Se si volesse controllare questa comunicazione o evitarla bisognerebbe a questo punto fare ricorso alle famose ACL (access Control List), che definiscono appunto liste di permessi di accesso opportunamente.

Esempio di ACL applicate a questa rete (vd. file .pkt con ACL)

Le ACL, come avremo modo di analizzare piu' in dettaglio sono regole applicabili ai router per limitare le comunicazioni transitanti nei router stessi. Non sempre infatti è desiderabile che qualunque parte di rete sia in connessione con tutte le altre. Le Access Control List presenti nei router sono adeguate a risolvere molti di questi problemi, permettendo transiti selettivi di pacchetti riguardo a protocollo, porte, indirizzi IP di partenza (specifici o di gruppo), indirizzi IP di destinazione (specifici o di gruppo), tutto questo regolato su specifiche porte del router.
Esistono diversi tipi di ACL, ma sostanzialmente le più comunemente utilizzate sono di duetipi; le ACL standard, meno potenti e complete e le ACL estese che permettono controlli più flessibili.
Le ACL standard si limitano a controllare l'IP sorgente dei pacchetti.
Le ACL estese possono controllare l'IP sorgente, l'IP di destinazione (anche come opportuni gruppi di IP), il tipo di protocollo (ossia essere selettive solo per alcuni protocolli usati, ad esempio HTTP o ICMP), essere selettive solo su alcune porte, ed altro.
Nel nostro specifico caso andremo ad utilizzare le ACL estese, in quanto ci interessa inserire nel controllo un gruppo di IP di destinazione e un gruppo di IP sorgenti (quelli della sottoreti 1 e 3). Non useremo invece la possibilita' di controllo relative ad uno specifico protocollo o alle porte.
La metodica delle ACL prevede di:

- creare la / le ACL da applicare (che sono a tutti gli effetti regole) su un certo router
- applicare tali regole alle opportune interfacce del router

I comandi per creare le ACL sono già riportati sullo schema PT, vale a dire[2]:

```
R1(config)#access-list 101 deny ip 190.1.3.96 0.0.0.31 190.1.3.32 0.0.0.31
```

2 Si noti il numero 101. Le ACL standard in Cisco IOS hanno numeri da 1 a 99, quelle estese da 100 a 199

```
R1(config)#access-list 101 permit ip any any
```

Si crea una ACL estesa che impedisce il transito di pacchetti provenienti dalla rete 190.1.3.96 /27 e indirizzati verso la rete 190.1.3.32 /27. In realtà le maschere di rete utilizzate possono lasciare perplessi, ed infatti non sono maschere di rete, ma i loro negati. Si ricordi che /27 ha come maschera di rete 255.255.255.224; si provi a fare il negato di questo numero:

255.255.255.224 = 11111111 11111111 11111111 11100000

negando (NOT) 00000000 00000000 00000000 00011111

vale a dire la wilcard è: 0.0.0.31

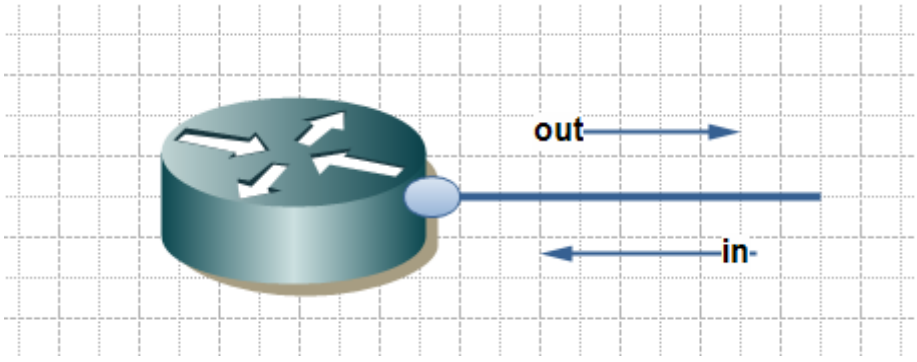
ed otterremo la cosiddetta wildcard, che và indicata a fianco del numero di IP, quando parliamo di gruppi di IP.

La seconda regola specifica che tutti gli altri pacchetti devono essere lasciati transitare. Essa potrebbe sembrare a prima vista contraddittoria, ma non lo è. Le regole valgono nella sequenza in cui sono inserite, quindi se il pacchetto non sottostà alla prima regola di divieto, si passerà ad analizzare questa seconda regola, che permette agli altri di passare. Senza questa ulteriore specifica, i pacchetti di default, in mancanza di regole che permettano il loro passaggio, sono bloccati.

Una volta creata la ACL la si può applicare alla porta Se7/0 del router R1, che è poi quella che collega al resto della rete la sottorete 3. Si deve ricordare che in questo caso bisognerà specificare se il controllo avviene in ingresso o in uscita (con le indicazioni in o out). Dalla documentazione Cisco risulta che:

In— Traffico che arriva sull'interfaccia e in seguito passa attraverso il router. La sorgente si intende da dove proviene il pacchetto e la destinazione è dove esso và, ossia dall'altro lato del router.

Out – Traffico che è già passato attraverso il router e lascia il dispositivo. La sorgente è da dove esso proviene, dall' altra parte del router, prima del router, e la destinazione è dove stà andando.



Dopo aver detto tutto ciò la ACL viene applicata quindi alla Se7/0 con i comandi:

```
R1(config)#int Se7/0
R1(config-if)#ip access-group 101 in
```

In modo analogo, ma simmetrico si è proceduto a filtrare l'interfaccia Se3/0 del router collegata alla sottorete 1, che si voleva isolare dalla sottorete 3. Il risultato, constatabile, è che le sottoreti 1 e 3 non sono più in comunicazione, ma isolate tra loro, mentre tutto il resto del traffico da e per esse, e per ogni altra destinazione resta possibile.