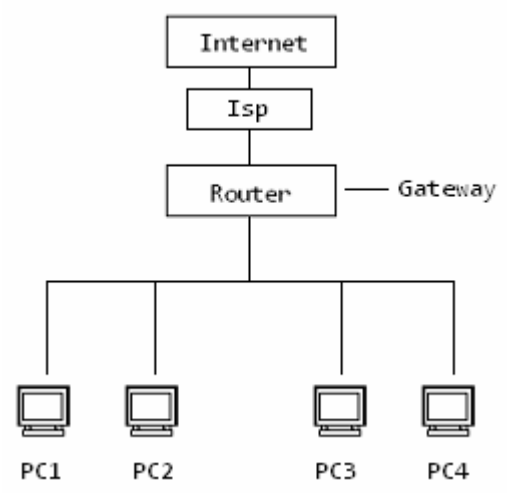
Routers and Routing process explanation through the Network Address Translation

0x100 – Router

0x110 – Cos’è?
Quello che nel gergo informatico viene chiamato Router (o Switch Router) è un dispositivo di rete che si occupa di dirigere il traffico lavorando solitamente sul livello 3 del modello OSI. Un Router, a differenza di uno Switch base che controlla i frame muovendosi sul livello 2, dirige i pacchetti lavorando sul livello 3. Tutto il traffico infatti viene trasmesso dal computer, cominciando dal livello 7 (la vostra applicazione di rete) sino al livello 1 (il livello fisico) ma per una spiegazione più dettagliata del funzionamento del networking ho scritto un altro paper. Comunque tramite il livello fisico il traffico raggiunge il medium di rete (network cablato oppure wireless). Se il traffico è su una Lan locale non passa attraverso un router. I router infatti funzionano soprattutto sul livello 3 ma devono intepretare almeno gli strati dall'1 al 3, nonostante tutto molti router riescono in qualche modo a interpretare anche i livelli dal 4 al 7. Al giorno d’oggi, quasi tutte la reti sono basate su Ethernet e IP. Quindi, solitamente, ogni pacchetto sulla vostra rete ha un indirizzo MAC Ethernet sorgente e destinazione, e un indirizzo IP sorgente e destinazione.

0x120 – Routing
L’azione che viene dunque denominata “routing” è l'instradamento dei pacchetti effettuato a livello di rete. Nel caso specifico del livello 3, i router utilizzano delle tabelle di routing (o tabelle di instradamento) che contengono blocchi di indirizzi IP che sono detti route (o rotte). Questo metodo è pertanto il migliore, in quanto un singolo elemento della tabella di instradamento può gestire un numero anche molto alto di host. I sistemi con cui questi blocchi vengono popolati, ovvero riempiti di dati, sono sostanzialmente tre: routing statico, routing dinamico, routing per reti dirette. Il primo è un metodo grezzo che obbliga un’impostanzione manuale delle tabelle. Il secondo è il più utilizzato ed è il più comodo. Infatti ci sono appositi protocolli che girano sui routers, come ad esempio il protocollo OSPF o BGP, che hanno la funzione di congiungere i vari dispositivi e consentire lo scambio di informazioni periodiche su come raggiungere le varie reti. Un router può consentire la connessione di reti di livello 2 eterogenee, come una LAN ethernet o ATM al contrario di uno switch che non è in grado di fare ciò. Inoltre molti router di ultima generazione destinati ai consumatori hanno funzioni di access point per reti wireless Wi-Fi e di firwall incorporato e tutto ciò concerne quindi le funzioni che andremo a vedere.



0x130 – Traffico e Funzionamento

La funzione più importante di un router è per l'appunto quella di occuparsi del traffico che lo attraversa. Per fare questo un router interpreta gli indirizzi Ethernet e IP, specialmente le destinazioni dei pacchetti. Prese le destinazioni le cerca nelle sue tabelle di routing e quando le trova prova ad individuare il percorso migliore e più veloce che i pacchetti devono prendere per raggiungere l'host. Se trova un solo percorso obbligato indirizza li i pacchetti, in questo caso si parla di "default route" (o "gateway of last resort") ovvero: "Se non ci sono percorsi migliori, inviali in questo". Gli utenti di routers domestici o di uffici, hanno sempre una sola "default route" perché gli indirizzi che il router deve controllare sono sempre molto pochi e tutto il traffico viene mandato all'ISP (Internet Service Provider). Ma nel caso di quest'ultimi i loro routers devono controllare moltissime migliaia di percorsi per decidere il migliore e queste operazioni vengono fatte in millisecondi tanto che a noi paiono istantanee anche se così proprio non sono. E' proprio dopo aver compiuto la ricerca nelle sue tabelle di routing, che un router decide come comportarsi. Se infatti il router non trova una via transitabile, elimina il nostro traffico e invia un messaggio chiamato ICMP (Internet Control Message Protocol) che indica Destinazione Irraggiungibile, se invece individua una via adatta procede effettuando le altre operazioni a sua disposizione: creare un NAT (funzione non sempre presente, ma frequentissima ultimamente nei routers domestici e di uffici), sostituire l'inidirizzo MAC con quello del router, e incapsulare i pacchetti per i protocolli WAN. Una volta immesso nella rete il pacchetto parte verso la sua destinazione finale. Ad ogni nuovo smistamento il suo TTL (Tempo di Vita) quando questo arriva a zero, se il pacchetto non ha ancora raggiunto la meta, viene scartato. Il router di destinazione dal canto suo non fa altro che eseguire le nostre stesse operazioni ma esattamente al contrario.

0x140 – In pratica

A questo punto non ci resta che esaminare la parte più pratica. Per avere un'idea di cosa consistono le tabelle di routing sia in ambiente Unix sia in ambiente Winzozz il comando da lanciare dal terminale è lo stesso: "netstat –nr". Su Windows esiste inoltre un ulteriore comando per ottenere lo stesso risultato che è "route print". Vediamo degli esempi di tabelle di routing su entrambi gli ambienti. La prima è una tabella di routing dalla console di Windows.

WINDOWS

```
C:\Documents and Settings\Saitek> netstat -nr

Tabella di Route
===========================================
Interface List
0x1 ...........................MS TCP Loopback interface n
0x2 ...00 50 56 c0 00 08 ...... VMware Virtual Ethernet Adapter for VMnet8
0x3 ...00 50 56 c0 00 01 ...... VMware Virtual Ethernet Adapter for VMnet1
0x4 ...00 16 eb 4e cf 40 ...... Realtek RTL8139/810x Family Fast Ethernet
===========================================
===========================================
Route attive:
Indirizzo rete   Mask             Gateway        Interfac.      Metric
0.0.0.0          0.0.0.0          192.168.1.1    192.168.1.33    20
127.0.0.0        255.0.0.0        127.0.0.1      127.0.0.1       1
169.254.0.0      255.255.0.0      192.168.1.33   192.168.1.33    30
192.168.1.0      255.255.255.0    192.168.1.33   192.168.1.33    20
192.168.1.33     255.255.255.255  127.0.0.1      127.0.0.1       20
192.168.1.255    255.255.255.255  192.168.1.33   192.168.1.33    20
192.168.47.0     255.255.255.0    192.168.47.1   192.168.47.1    20
192.168.47.1     255.255.255.255  127.0.0.1      127.0.0.1       20
192.168.47.255   255.255.255.255  192.168.47.1   192.168.47.1    20
192.168.126.0    255.255.255.0    192.168.126.1  192.168.126.1   20
192.168.126.1    255.255.255.255  127.0.0.1      127.0.0.1       20
192.168.126.255  255.255.255.255  192.168.126.1  192.168.126.1   20
224.0.0.0        240.0.0.0        192.168.1.33   192.168.1.33    20
224.0.0.0        240.0.0.0        192.168.47.1   192.168.47.1    20
224.0.0.0        240.0.0.0        192.168.126.1  192.168.126.1   20
255.255.255.255  255.255.255.255  192.168.1.33   192.168.1.33    1
255.255.255.255  255.255.255.255  192.168.47.1   192.168.47.1    1
255.255.255.255  255.255.255.255  192.168.126.1  192.168.126.1   1

Gateway predefinito:       192.168.1.1
===========================================
Route permanenti:
None Nessuno
```

La seconda è invece una tabella di routing sempre con lo stesso comando mostrata sul terminale Unix.

UNIX

```
$ netstat -nr
Tabelle di routing

Internet:
Destination Gateway Flags Refs Use Netif
default 10.0.0.1 UGS 2 146537336 fxp0
127.0.0.1 127.0.0.1 UH 0 3414961 lo0
10.0.0.1/26 link#1 UC 0 0 fxp0
10.0.0.2 00:02:b3:4c:65:27 UHLW 0 255732 lo0
10.0.0.1 00:02:7d:cc:3d:00 UHLW 1 0 fxp0 1087 10.0.0.1
```

Siete invece curiosi di sapere come funzionano delle tabelle di routing più ampie come quelle di un ISP? Bene possiamo fare anche questo abbastanza semplicemente. Per fare questo dobbiamo ottenere l’indirizzo

di un ISP come ad esempio quello di Tiscali(AS3257) che è: route-server.ip.tiscali.net
A questo punto non dobbiamo fare altro che collegarci dal telnet ed eseguire il comando “show ip route”.

```
Microsoft Telnet> open route-server.ip.tiscali.net
Connessione a route-server.ip.tiscali.net...

CCC

+------------------------------------------------------------------------+
|                                                                        |
|           TISCALI International Network - Route Monitor                |
|                              (AS3257)                                  |
|                                                                        |
|   This system is solely for internet operational purposes. Any         |
|   misuse is strictly prohibited. All connections to this router        |
|   are logged.                                                          |
|                                                                        |
|   This server provides a view on the TISCALI routing table that        |
|   is used in Frankfurt/Germany. If you are interested in other         |
|   regions of the backbone check out http://www.ip.tiscali.net/lg       |
|                                                                        |
|   Please report problems to noc@tiscali.net                            |
+------------------------------------------------------------------------+

route-server.ip.tiscali.net>show ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B – BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E – EGP
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route

Gateway of last resort is 213.200.64.93 to network 0.0.0.0

B    216.221.5.0/24 [20/5] via 213.200.64.93, 3d10h
B    210.51.225.0/24 [20/0] via 213.200.64.93, 2w1d
B    209.136.89.0/24 [20/0] via 213.200.64.93, 1w2d
B    209.34.243.0/24 [20/0] via 213.200.64.93, 1w2d
B    205.204.1.0/24 [20/0] via 213.200.64.93, 1w2d
B    204.255.51.0/24 [20/772] via 213.200.64.93, 2w1d
B    204.238.34.0/24 [20/0] via 213.200.64.93, 1w2d
B    204.221.17.0/24 [20/0] via 213.200.64.93, 1w2d
B    204.17.221.0/24 [20/0] via 213.200.64.93, 6d10h
B    203.255.52.0/24 [20/5] via 213.200.64.93, 21:04:52
B    203.238.37.0/24 [20/1365] via 213.200.64.93, 2w1d
B    203.170.97.0/24 [20/94] via 213.200.64.93, 17:15:11
--More--
```

In un protocollo di routing dinamico come spiegato in precedenza le tabelle di routing verranno modificate automaticamente. Ma si possono anche effettuare modifiche manuali tramite l’aggiunta di una route

statica ovvero un percorso predefinito che trasmette i pacchetti in tutto il network. In entrambi i sistemi operativi Winzozz e Unix il comando utilizzato gestire tutti i comandi di routing è: “route”. Poi vi verranno mostrate tutte le opzioni di routing. In particolare per entrambi i sistemi “route add” e “route change” permettono di aggiungere o modificare una route.

WINDOWS

```
C:\Documents and Settings\Saitek>route

Modifica le tabelle di routing della rete.

ROUTE [-f] [-p] [comando [destinazione]
[MASK netmask] [gateway] [METRIC passi] [interfaccia IF]

  -f           Cancella le tabelle di routing di tutte le voci gateway.
Se usato insieme ad uno dei comandi, le tabelle vengono cancellate prima
dell'esecuzione del comando.

  -p           Quando si usa con il comando ADD, mantiene una route
ad ogni avvio del sistema. Normalmente, invece, le route non sono conservate
quando si riavvia il sistema. Usato insieme al comando PRINT, mostra l'elenco
delle route permanenti registrate. Viene ignorato da tutti gli altri comandi,
che modificano sempre le route permanenti appropriate. Opzione non supportata
da Windows 95.

comando   Specifica uno dei quattro comandi:
PRINT     Stampa una route
ADD       Aggiunge una route
DELETE    Elimina una route
CHANGE    Modifica una route esistente destinazione Specifica l'host.
MASK      Se MASK viene specificato, l'argomento successivo viene
interpretato come la maschera di rete.
netmask      Specifica un valore maschera per la subnet da associare
alla voce di route. Se non specificato viene assunto

               255.255.255.255.
gateway      Specifica il gateway.  interfaccia  Numero di interfaccia per la
route specificata.

METRIC       Specifica i passi/costo per la destinazione
Tutti i nomi simbolici utilizzati come destinazione sono risolti nel file di
database NETWORKS. I nomi simbolici per il gateway sono risolti nel file di
database dei nomi di host HOSTS.

Se il comando è PRINT o DELETE, è possibile usare caratteri jolly (i caratteri
jolly sono specificati come "*") in destinazione o gateway, o omettere
l'argomento gateway.

Se Dest contiene * o ?, è considerato come un modello di shell e sono stampate
solo le route di destinazione corrispondenti. La "*" corrisponde a una stringa
qualsiasi e "?" corrisponde a un qualsiasi carattere.

Esempi: 157.*.1, 157.*, 127.*, *224*.
```

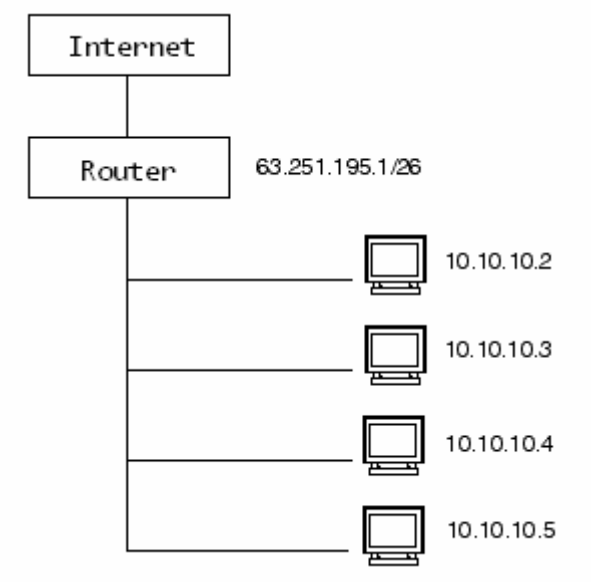
```
Note di diagnostica:
MASK non valido genera un errore quando (DEST & MASK) != DEST.
Esempio> route ADD 157.0.0.0 MASK 155.0.0.0 157.55.80.1 IF 1
L'aggiunta della route non è riuscita: il parametro mask specificato non è
valido. (Destinatione e Mask) != Destinazione.

Esempi: > route PRINT
> route ADD 157.0.0.0 MASK 255.0.0.0  157.55.80.1 METRIC 3 IF 2
destinazione^      ^mask      ^gateway     metric^    ^
Interfaccia^
Se IF non è data, viene cercata la migliore interfaccia per un dato gateway

> route PRINT
> route PRINT 157*          .... Stampa solo route corrispondenti 157*
> route CHANGE 157.0.0.0 MASK 255.0.0.0 157.55.80.5 METRIC 2 IF 2

      CHANGE è utilizzato solo per modificare gateway e/o metric.
> route PRINT
> routeDELETE 157.0.0.0
> route PRINT
```

UNIX

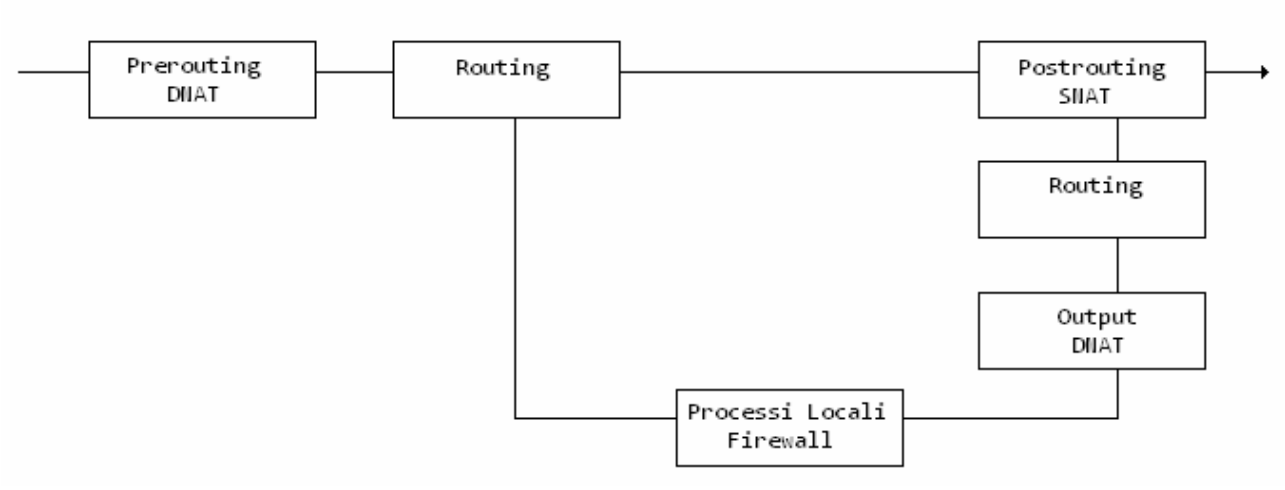
```
Saitek: $ Route add 192.168.3.101 10.0.0.1
Aggiungere host 192.168.3.101: gateway 10.0.0.1

Saitek: $ netstat -nr
Tabelle di routing
Internet:
Destinazione Gateway bandiere rif uso Netif Expire
...
192.168.3.101 10.0.0.1 UGHS 0 0 fxp0
...
```

0x200 – Nat

Il NAT (Network Address Translation) è una tecnica di network masquerading, spesso implementata in router o firewall, che modifica l'indirizzo IP dei pacchetti in transito nascondendo il vero IP interno dietro ad un altro IP. Internet ha bisogno di indentificare ogni singolo computer con un un indirizzo IP univoco. Però il numero degli indirizzi IP risulta limitato e quindi di solito gli ISP assegnano ad ogni sottoscrittore un solo indirizzo IP. Ma dato che alcune abitazioni e uffici presentano più computers avere un solo indirizzo IP può risultare un problema. Con Nat un piccolo gruppo di computers può condividere così lo stesso indirizzo IP. Questo permette inoltre maggiore sicurezza poiché l'IP dell'utente non viene diffuso attraverso il network, e solo l'ISP è in grado di rintracciare il vero indirizzo IP reindirizzando la richiesta direttamente all'utente interessato tramite l'utilizzo di specifiche porte. Il Nat può essere pensato anche come l'insieme di regole per modificare l'intestazione dei pacchetti, tenendo traccia delle manipolazioni eseguite ed operando l'operazione inversa sui pacchetti di risposta. Il Nat tiene conto per effettuare tutte le operazioni della tracciata delle connessioni. Infatti un router registra tutti gli scambi di pacchetti che lo attraversano. Il Nat è distinguibile in Snat se viene modificato l'indirizzo sorgente del pacchetto e Dnat se viene modificata la destinazione.



In un sistema Linux esistono anche delle componenti del kernel come “netfilter” che consente di intercettare e modificare i pacchetti che transitano attraverso la macchina. Per fare questo vengono utilizzate delle tabelle (iptables) al cui interno sono raggruppate delle catene (chain). Ogni tabella permette una diversa operazione sui pacchetti. Questo sistema è molto utile per spiegare il funzionamento generale del Nat. La tabella Nat infatti contiene tre catene predefinite: prerouting, postrouting, e output. Il Dnat è effettuato prima del routing, mentre lo Snat è effettuato dopo.



Nello schema soprastante è spiegato sinteticamente la funzione di routing suddivisa in prerouting, output e postrouting, i momenti nel quale devono essere eseguiti lo SNAT e il DNAT e quando interviene il lavoro del Firewall. Dnat è effettuato prima del routing e prima che i pacchetti siano filtrati invece Snat è eseguito dopo il filtraggio dei pacchetti. Anche su Windows è possibile modificare i pacchetti fino al livello MAC

ad esempio tramite Packet Builder che è un tool per Winzozz molto interessante che consente di scegliere il tipo di pacchetto da realizzare (ARP, IP, TCP, UDP), compilarlo in ogni campo e lanciarlo nella rete.

```
iptables -t nat -A PREROUTING -d 292.254.211.17 -j DNAT --to-destination 192.168.1.1

iptables -t nat -A POSTROUTING -s 192.168.1.1 -j SNAT --to-destination 292.254.211.17
```

Qui sopra è mostrato un esempio di full Nat comprendente Snat e Dnat eseguibile appunto da Linux tramite la componente “netfilter” presentata prima e le “iptables” (installabili da http://netfilter.kernelnotes.org). In seguito verranno mostrati altri esempi più specifici di Snat e Dnat.

0x210 – Snat

Lo SNAT (Source Network Address Translation) permette di modificare il campo sorgente del pacchetto. Praticamente lo Snat consente di modificare ad esempio l’indirizzo IP del mittente in quello pubblico del router o del provider. Questo processo avviene in postrouting ovvero immediatamente dopo la fase di routing, quindi dopo il filtraggio e poco prima che il pacchetto sia smistato nella rete. Questa operazione è utilizzata per l’appunto per il mascheramento della connessione, e in particolare è specifica per indirizzi statici. Non esiste uno Snat predefinito ma esistono vari tipi di Snat.

Un tipo di Snat è facilmente effettuabile con Linux sempre attraverso la componente netfilter e l’utilizzo delle iptables. Per fare ciò sono richieste naturalmente delle conoscenze nel campo di routing e di linux comunque vi illustrerò la sintassi del comando che è semplicissima. Il comando richiede le seguenti informazioni: tabella ('-t nat'), catena ('-A POSTROUTING'), obiettivo ('-j SNAT'), indirizzo sorgente che andrà a sostituire quello presente nel pacchetto ('--to' o '--to-source'). Esempio su unix di sostituzione del sorgente tramite comando al kernel:

```
iptables -t nat -A POSTROUTING -o eth0 -j SNAT --to 10.0.0.1
```

Con questo commando si comunica al kernel che tutti i pacchetti in uscita da eth0 devono essere modificati nel sorgente con 10.0.0.1. Vediamo un altro esempio molto simile di Snat.

```
iptables -t nat -A POSTROUTING -o eth0 -j SNAT --to 10.0.0.1-10.0.0.254
```

Questo è praticamente uguale ma si da più libertà nel sostituire il sorgente che può essere sia 10.0.0.1 sia 10.0.0.254.

0x211 – Napt

Il NAPT (Network Address Port Translation), conosciuto anche come PAT o IP Overloading, è una tecnica di IP masquerading, classificabile come Snat, che non solo nasconde l’indirizzo IP del richiedente ma anche la porta UDP o TCP da cui stanno transitando le connessioni. Questo servizio

consente di associare un IP e una porta di una rete locale ad un IP e una porta collocate in Internet, ad esempio la rete internet con una intranet. Quando un software richiede l'utilizzo di una porta, NAPT ne consente l'uso ma reindirizza la richiesta ad un'altra porta aperta. Con NAPT, tutti i computer della rete interna sono inaccessibili dall'esterno. Tuttavia se è necessario usare servizi pubblici dalla rete privata, ad esempio server Web, FTP o e-mail, è possibile configurare un router o un server per consentire l'accesso protetto. Con questo metodo, le connessioni verso l'esterno vengono ridirette su un host (il router) che esegue i servizi sulla rete privata.

0x220 - Dnat

Il DNAT differentemente dallo Snat, non modifica l'indirizzo del mittente bensì la destinazione, ovvero modifica la connessione in modo tale che vengano redirette verso indirizzi IP diversi da quelli originali. Ad esempio un Dnat può mutare l'indirizzo pubblico del router attraverso le regole basate sulle porte e reindirizzare verso il computer sul quale è presente il servizio da utilizzare. Questo avviene in fase di prerouting quindi subito prima della del routing, appena il pacchetto arriva dalla rete. Il Dnat può avere moltissimi usi, uno sicuramente che concerne appunto firewalls e routers è il port forwarding che tratteremo dopo. Una forma speciale di Dnat che viene chiamata Redirect (Reindirizzamento) consente di dirigere il traffico verso una determinata porta. Questo è lo stesso concetto utilizzato per un servizio di proxy dove il traffico viene rediretto su un host apposito denominato "proxy".

Sempre attraverso Linux e la componente "netfilter" andremo ad esaminare i comandi da lanciare per effettuare un Dnat. Per farlo sono richieste solitamente la tabella ('-t nat'), catena ('-A PREROUTING'), obiettivo ('-j DNAT'), interfaccia di provenienza ('-i eth0'), la porta che sostituirà quella presente nel pacchetto ('--to-port'), la destinazione ('--to-destination').

```
iptables -t nat -A PREROUTING -i eth0 -j DNAT --to 192.168.1.1
```

In quest'esempio l'indirizzo di destinazione del traffico proveniente da eth0 viene modificato nell'indirizzo 192.168.1.1.

```
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport www -j DNAT --to 192.168.1.1-192.168.1.2
```

In quest'altro esempio invece viene mostrato come a tutti i pacchetti tcp che vengono inviati verso la porta www (--dport www) viene modificata le destinazione verso i due host: 192.168.1.1 e 192.168.1.2

```
iptables -t nat -A PREROUTING -d 192.168.1.1 -j DNAT --to-destination 192.168.2.2
```

In questo esempio tutti i pacchetti che arrivano sul router con destinazione 192.168.1.1 verranno inviati dal router con destinazione 192.168.2.2.

Per quanto riguarda invece il tipo di Dnat che prima abbiamo accennato chiamato Redirect Dnat, la sintassi cambia leggermente e i dati solitamente richiesti sono la tabella ('-t nat'), la catena ('-A PREROUTING'), l'obiettivo ('-j REDIRECT'), l'interfaccia di provenienza

('-i eth0'), e la porta che andrà a sostituire quella presente nel pacchetto ('--to-port').

```
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport www -j REDIRECT --to-port 3128
```

In questo esempio per l'appunto tutto il traffico che da eth0 è diretto verso la porta www viene rediretto verso la porta 3128 dove, ad esempio, potrebbe essere in ascolto un proxy.

0x221 – Port Forwarding

Il Port Forwarding, spesso denominato anche Tunnelling, può essere considerato per certi aspetti una forma di Dnat. Questa operazione consente la trasmissione di dati da un dispositivo di rete ad un altro tramite l'uso di porte specifiche. Tutto questo viene comunemente fatto appunto utilizzando il Nat che viene eseguito da un server o un router o un altro computer all'interno della rete locale. Lo scopo principale di utilizzo del port forwarding è di consentire a un computer esterno ad una rete di raggiungere un computer con indirizzo privato all'interno di questa rete tramite l'utilizzo di una specifica porta.

Tornando ai nostri sistemi Linux è possibile eseguire il Port Forwarding aggiungendo alla tabella Nat del netfilter l'obiettivo Dnat e l'obiettivo Snat (visti in precedenza) nelle due corrispondenti catene.

0x300 – Common Routers Default Parameters

[Router]	[Modello]	[Dati di Default]	[Firwall and Port Forwarding]
	D-Link DSL-G624T	http://192.168.1.1 User: admin Passwd: admin	Setup/Advanced -> Port Forwarding Available Rules -> Add -> Apply Firewall non attivo di default.
	D-LINK DSL-302G	http://10.1.1.1 User: admin Passwd: admin	Service/NAT -> Nat Options -> Nat Rule Entry -> Add Firewall non attivo di default.
	LINKSYS WRT54G	http://192.168.1.1 User: “nessuno” Passwd: admin	Applications & Gaming -> Port Range Forward -> Save Settings. Firewall attivo di default.
	ATLANTIS WebShare A02-RA340	http://192.168.1.254 User: admin Passwd: atlantis	Configuration/Virtual Server -> Add Virtual Server -> Apply. Firewall attivo di default.
	ATLANTIS A02-RA141	http://192.168.1.254 User: admin Passwd: atlantis	Advanced Setup/Nat -> Many to One -> Edit Virtual Server -> Apply Firewall non attivo di default.
	ZyXEL P-660HW-D1	http://192.168.1.1 User: “nessuno” Passwd: 1234	Network/Nat/Port Forwarding -> Service Name -> User Define -> Apply. Firewall attivo di default.
	ZyXEL Prestige 660HW-61	http://192.168.1.1 User: admin Passwd: 1234	Advanced Setup/Nat -> SUA Only –> Edit Settings -> Save Firewall non attivo di default.
	NETGEAR DG834GIT	http://192.168.0.1 User: admin Passwd: password	Services -> Add Custom Service -> Apply. Firewall attivo di default.
	USRobotics 9108 SureConnect	http://192.168.1.1 User: admin Passwd: admin	Security/Virtual Servers -> Add -> Custom Server (V) -> Apply Firewall non attivo di default.
	USRobotics 9112	http://192.168.2.1 User: “nessuno” Passwd: 1234	Nat/Virtual Server -> Add Firewall non attivo di default.
	3COM Office Connect	http://192.168.1.1 User: “nessuno” Passwd: admin	Firewall -> Virtual Servers -> New -> Custom in Local Service -> Add Firewall non attivo di Default.
	Pirelli Netgate VOIP	http://192.168.1.1 User: user Passwd: user	Nat/Viertual Server -> Enable (V) -> Add Firewall non attivo di default.
	Pirelli Gate2Plus	http://192.168.1.1 User: “nessuno” Passwd: “nessuna”	Collegamento Lan -> Configura -> Virtual Server -> Aggiungi Firewall non attivo di default.
	SITECOM WL-536 WL-174	http://192.168.0.1 User: admin Passwd: admin	Advanced Setup/Nat/Virtual Server -> Single IP Account -> Save Firewall non attivo di default.

0x400 – Fonti
Scrivendo questa guida ho attinto da alcune fonti talune informazioni

www.wikipedia.it

0x500 - Conclusioni
Tutto ciò che ho spiegato in questa guida non è altro che una panoramica generale di quello che poi in realtà è il complesso sistema dei routers, del routing e dei vari protocolli. L’obiettivo che mi sono prefisso nello scrivere questo papers era quello di dare un’infarinata con qualche dettaglio didascalico qua e la dell’instradamento del traffico e dei suoi processi. Questa guida è stata scritta più che altro per fini teorici e non pratici. Grazie a tutti. Al prossimo paper.

Saitek
www.saitek.altervista.org
saitek_06@yahoo.it

"Apprendi e non smettere mai di farlo"