

KATHARA COMMANDS:

KATHARA V-COMMANDS

- *vstart*: starts a new device
- *vconfig*: attaches network interfaces to a running device
- *vclean*: halts a device

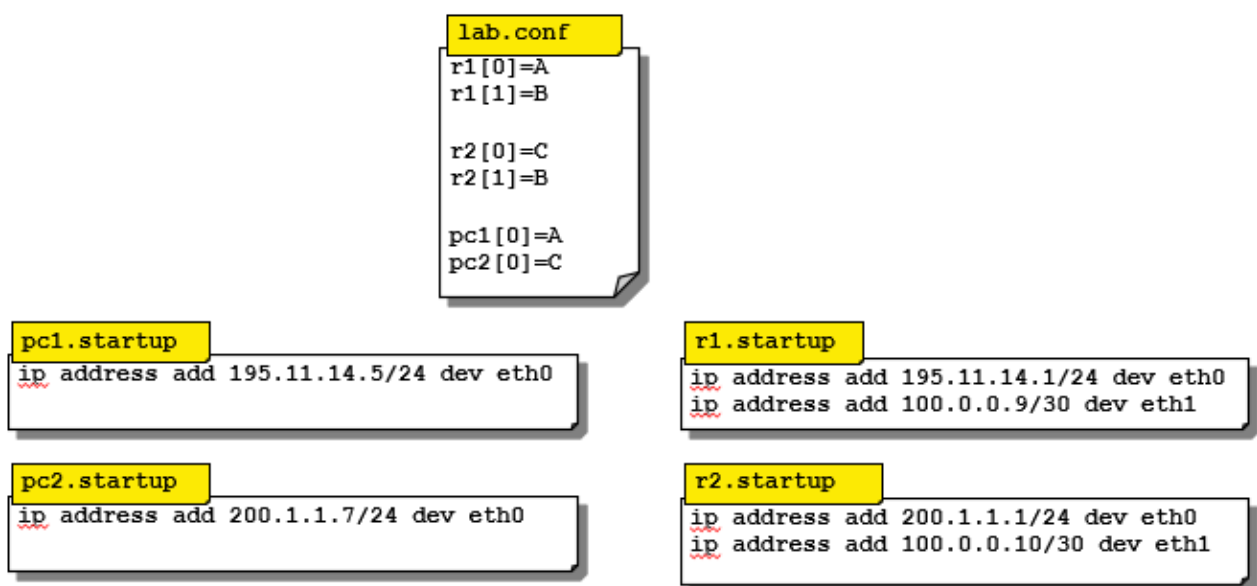
KATHARA L-COMMANDS

- *lstart*: starts a Kathará lab
- *lclean*: halts all the devices of a lab
- *lconfig*: manage the network interface of a running lab
- *lrestart*: halts all the devices of a lab and start them again
- *linfo*: provides information about a lab

KATHARA GLOBAL COMMANDS

- *check*: Check your system environment
- *connect*: Connect to a running Kathará machine
- *list*: Show all running Kathará machines of the current user
- *settings*: Show and edit Kathará settings
- *wipe*: Delete all Kathará machines and links, optionally also delete settings

STATIC-ROUTING:



- *ip route*
mostra la tabella di instradamento della macchina
- *pc1.startup*
 - *ip address add 100.1.0.13/30 dev eth0*
associa un indirizzo IP a ciascuna porta eth della macchina
 - *ip route add default via 10.0.0.2/24 dev eth0*
aggiunge la rotta di default verso la macchina specificata tramite indirizzo IP, attraverso la porta specificata eth0.
- *lab.conf*
 - *r1[0]="A"*
r1[1]="B"
r1[image]="kathara/frr"
associa il nome di una LAN (stringa) al numero di porta del router.
L'immagine dichiara i demoni da lanciare (*base, frr, named*).

FRRouting - RIP:

- *r1/etc/frr/daemons*
file *daemons*: configurazione iniziale di frr, si sceglie quale demone di routing lanciare. Da copiare.
- *r1/etc/frr/frr.conf*
 - *router rip*
redistribute connected
network 100.1.0.0/24
inserisce configurazioni per il protocollo RIP. Definisce qual è la rete di riferimento per il protocollo RIP.
 - *log file /var/log/frr/frr.log*
- *r1/etc/frr/vtysh.conf*
 - *service integrated-vtysh-config*
permette di inserire tutte le configurazione nel singolo file frr.conf
- *r1.startup*
 - *ip address add 100.1.0.13/30 dev eth0*
associa un indirizzo IP a ciascuna porta eth della macchina
 - *systemctl start frr*
permette di lanciare il demone frr ed eseguire i protocolli di routing.
- ***vttysh***
comando che permette di interagire direttamente con frr all'interno di una macchina. Tasto '?' permette di mostrare i possibili comandi disponibili.

- *show ip route*
mostra le rotte del protocollo IP del demone Zebra in data plane.
selected (>): se disponibili più opzioni per una specifica rotta, se ne seleziona solamente una.
FIB (*): tabella di instradamento del kernel (control plane)
- *show running-config*
mostra la configurazione corrente frr. In particolare, mostra la configurazione che è stata appresa, non mostra le configurazioni errate inserite in frr.conf
- *configure terminal*
entra in modalità configurazione
 - *router rip*
permette di entrare nella modalità configurazione per il protocollo di routing specificato.
 - *route 0.0.0.0/0*
condivide la rotta di default con gli altri router del protocollo. Indica il router come possessore della default, deve instradare tali pacchetti verso l'internet. Da inserire in frr.conf sotto la dichiarazione di *router rip*.
- *show ip rip*
tabella di routing specifica del demone rip
- *tcpdump -tnni eth2 -v*
permette di lanciare uno sniffer sulla porta indicata (eth2).
- *ip link set eth1 down*
comando che permette di spegnere un'interfaccia di un router.

FRRouting – OSPF:

- *r1/etc/frr/frr.conf*
 - *interface eth0*
ospf cost 21
indica che l'interfaccia eth0 ha un costo per il protocollo ospf pari a 21. Valore 10 di default.
 - *router ospf*
network 10.0.0.0/16 area 0.0.0.0
dichiara l'utilizzo del protocollo di routing ospf. Dichiara che la LAN con indirizzo 10.0.0.0/16 fa parte dell'area con nome 0.0.0.0 (non è un indirizzo IP ma l'identificativo dell'area).

- *redistributed connected*
log file */var/log/frr/frr.log*
- **vtysh**
 - *show ip route*
mostra la tabella di instradamento Zebra, mostra le rotte alternative, ma non scelte, anche per le LAN direttamente connesse, in quanto ospf le calcola lo stesso.
[110/10]: [costi di Zebra / costi di OSPF], le rotte direttamente connesse non hanno costo, OSPF ha costo 110 per Zebra.
 - *show ip ospf route*
mostra le rotte calcolate dal demone ospf. Diviso in due sezioni: network e router routing table.
 - *show ip ospf interface*
mostra informazioni aggiuntive sulle interfacce della macchina.
State DR: indica che all'interno della LAN in questione, l'interfaccia relativa rappresenta il Designated Router. Il secondo arrivato durante le elezioni ha stato di Backup. Il numero IP del DR è utilizzato per identificare una LAN. È inoltre usato per evitare di instaurare un numero di connessioni quadratiche rispetto al numero di macchine, in una LAN si parla solo con il DR, gli altri link fisicamente esistono, ma non vengono usati dai demoni OSPF. Il traffico normale passa ovunque.
 - *show ip ospf database*
database che ha permesso a ospf di calcolare le rotte. Ad ogni router è assegnato un ID. Le LAN sono rappresentate da nodi e indicate da ID, il nome della LAN è il DR della LAN stessa. ADV Router è il router che ha fornito tale informazione.
 - *show ip ospf database router*
mostra tutte le informazioni dettagliate di tutti i router della rete, incluse le reti LAN a cui sono collegati.
 - *show ip ospf database network*
mostra tutte le informazioni sulle LAN.

FRRouting – OSPF multiarea:

- *r1/etc/frr/frr.conf:*
 - *interface eth0*
ospf cost 21

- *router ospf*
network 10.0.0.0/16 area 0.0.0.0
network 100.0.0.0/30 area 1.1.1.1
- *area 1.1.1.1 stub*
indica che l'area 1 è stub, l'area 0 è indicata come backbone di default.
Da inserire solamente nei router di frontiera
- *redistributed connected*
log file /var/log/frr/frr.log

DNS – configurazioni:

nuove macchine definite come *dnsroot*, *dnsorg* che sono autorità rispettivamente su root e org. *localuni* e *localstart* sono resolver locali usati dalle macchine pc, a cui si affidano per scoprire i nomi di interesse.

- *pc2/etc/resolv.conf*
contiene le informazioni sul resolver locale:
 - *nameserver 192.168.0.110*
 - *search uniroma3.it* : uniroma3.it corrisponde al dominio di ricerca
- *dnsuni/etc/bind/named.conf*
contiene la configurazione del demone named.
 - *include "/etc/bind/named.conf.options";*
include un altro file di configurazione per definire le opzioni di bind.
 - *zone "." {*
type hint;
file "/etc/bind/db.root";
};
da aggiungere in tutti i nameserver del lab, tutti devono sapere dove sta ".", l'unico server che non ha questo comando è il server "." Autorità. Da informazioni (hint) su dove trovare il nameserver di root.
 - *zone "uniroma3.it" {*
type master;
file "/etc/bind/db.it.uniroma3";
};
indica che il server è autorità su uniroma3.it
- *dnsuni/etc/bind/db.root*
 - . IN NS ROOT-SERVER.

ROOT-SERVER IN A 192.168.0.5

il dominio "." ha come nameserver una macchina di nome ROOT-SERVER. Il secondo record associa un indirizzo IP al nome della macchina (glue record).

- *dnsuni/etc/bind/db.it.uniroma3*

- *@ IN SOA dnsuni.uniroma3.it.*

record Start of Authority. @ indica un puntatore al record indentificato nel campo, in questo caso punta a uniroma3.it (definito in *zone "uniroma3.it"*).

- *root.dnsuni.uniroma3.org (...)*

campi da copiare

- *@ IN NS dnsuni.uniroma3.it*

dnsuni.uniroma3.it. IN A 192.168.0.11

pc1.uniroma3.it. IN A 192.168.0.111

indica chi è il server autorità su @ (uniroma3.it) e aggiunge il glue record relativo al suo indirizzo IP. Record di PC1 con il relativo indirizzo IP. Il nameserver deve conoscere tutte le macchine incluse nel suo dominio. I resolver locali non hanno nome, ma solo indirizzo IP, non appaiono nei nameserver autorità.

- *dnsit/etc/bind/db.it*

- *(...)*

- *uniroma3.it. IN NS dnsuni.uniroma3.it.*

dnsuni.uniroma3.it IN A 192.168.0.11

il **nameserver di it** delega il controllo di uniroma3.it al nameserver autorità su quel dominio, aggiunge il gluerecord con indirizzo IP.

- *localuni/etc/bind/named.conf.options*

- *options {*

directory "/var/cache/bind";

allow-recursion { 192.168.0.0/24; };

dnssec-validation no;

};

il **resolver locale** possiede hint a root (nel named.conf).

Possiede le informazioni di *allow-recursion*, indica quali sono gli indirizzi IP autorizzati a chiedere informazioni a tale resolver.

dnssec-validation no disattiva le richieste dnssec firmate.

- *dig pc2.startup.net*
permette di eseguire query al DNS per risolvere il nome
- *dig +trace pc2.startup.net*
mostra tutta la gerarchia di risposte per risolvere il nome

WEB SERVER:

- *server.startup*
 - *systemctl start apache2*
per avviare un web server
- *server/var/www/html/index.html*
file html che viene stampato dal web server
- *ps aux*
mostra i processi attivi sulla macchina, permette di indentificare se apache2 è stato lanciato correttamente. Da eseguire sul server
- *links http://10.0.0.1*
permette di lanciare il browser da linea di comando e di accedere al sito web indicato tramite indirizzo IP.

BGP - peering:

- frr.conf
 - *router bgp <my-as-number>*
indica al router di parlare bgp con il relativo AS number.
 - *neighbor <neighbor-ip> remote-as <neighbor-as-number>*
identifica un vicino con il quale parlare BGP con il relativo ip, appartiene ad un AS remoto con il numero specificato. Per ciascun vicino occorre scrivere un comando neighbor.
 - *neighbor <neighbor-ip> description <text>*
comando con valore di commento, associa una funzione al neighbor dichiarato.
- *show ip bgp summary* (in vtysh)
mostra informazioni su bgp, incluse le informazioni sui neighbor e peering attivi.

BGP - announcement:

- frr.conf
 - *network <network-ip/network-mask>*
Si occupa di annunciare il prefisso delle proprie LAN ai vicini. Necessita di un security filter per l'annuncio. Verifica se il router ha tale prefisso nella forwarding table, se non è vero il comando non ha effetto
 - *no bgp network import-check*
disabilita il check sull'esistenza del prefisso nella tabella del kernel, maggiore libertà di fare annunci. Permette di annunciare LAN più grandi non direttamente connesse.
 - *no bgp ebgp-requires-policy*
disabilita il check sull'esistenza di filtri associati ai peer.

BGP – prefix filtering:

- frr.conf
 - *neighbor <neighbor-ip> prefix-list <p-list-name> in*
 - *neighbor <neighbor-ip> prefix-list <p-list-name> out*
applica la prefix list per gli annunci in ingresso o in uscita
 - *ip prefix-list <p-list-name> permit <network/mask>*
 - *ip prefix-list <p-list-name> deny <network/mask>*
permettono di accettare in ingresso (o in uscita) solamente una serie di prefissi specificati. Le prefix-list sono ordinate per sequence number,

numeri più bassi vengono eseguiti prima, viene applicata solo la prima che fa matching

BGP – stub as:

- frr.conf
 - *neighbor <network-ip> default-originate*
permette di originare la default e mandarla ad un neighbor
 - *network 0.0.0.0/0*
inserisce una rotta di default nella tabella bgp del router, non implica la presenza nella tabella di instradamento. Necessita di *no bgp ebgp-requires-policy*. Usato nella gerarchia alta per propagare i pacchetti verso il basso, non dovrebbe essere usata nei livelli intermedi.

BGP – multi homed stub:

- frr.conf
 - *neighbor <ip-address> route-map <name> in/out*
permette di modificare gli attributi di un annuncio in entrata o in uscita
 - *route-map <name> permit 10*
definisce la route map, il permit indica la priorità delle operazioni da eseguire
 - *match ip address <name>*
permette di fare il matching con gli indirizzi ip specificati nell'access-list indicata con il nome
 - *set <attribute> <value>*
se viene riconosciuto il matching precedente setta la metrica a 10 (es. *set metric 10*). *Metric* permette di sfavorire una LAN in uscita, metrica più bassa ha priorità maggiore; *local-preference* invece permette di sfavorire una LAN in ingresso, local-preference più alta ha maggiore priorità.
 - *access-list <name> permit <ip-network/netmask>*
definisce l'access list facendo passare esclusivamente gli indirizzi provenienti dalla LAN specificata

BGP – multi homed stub large:

- frr.conf
 - *router rip*
 - *network <network-address/netmask>*
 - *redistribute bgp*
permette di ridistribuire all'interno della rete interna RIP le informazioni ricevute da BGP.