Quelques commandes qui te permettront de survivre dans un réseau hostile (ou pas)

Emmanuel Chaput, Yoann Couble, Dorin Rautu

Ethernet : les interfaces

Action	Commande
Observation d'une interface	`# ethtool eth0`
Repérer une interface	`# ethtool -p eth0`
Modifier le débit (en Mbps)	`# ethtool -s speed 100 eth0`

Ethernet : configuration d'un pont

Action	Net tools	IP route2
Créer un pont	`# brctl addbr pont`	`# ip link add pont type bridge`
Détruire un pont	`# brctl delbr pont`	`# ip link del pont type bridge`
Ajouter une interface	`# brctl addif pont eth0`	`# ip link set eth0 master pont`
Supprimer une interface	`# brctl delif pont eth0`	`# ip link set eth0 nomaster`
Choix de la priorité du pont	`# brctl setbridgeprio pont 42`	
Choix de la priorité d'une interface	`# brctl setportprio pont eth0 69`	`# bridge link set dev eth0 priority 69`
Ajouter une adresse		`# bridge fdb add c0:ff:ee:c0:ff:ee dev eth0 master temp`
Supprimer une adresse		`# bridge fdb del c0:ff:ee:c0:ff:ee dev eth0 master temp`
Etat de la base de données	`# brctl showmacs pont`	`# bridge fdb show`

Ethernet: les VLANs

Action	Net tools	IP route2	Cisco iOS
		Gestion des interfaces	
Ajouter une interface	`# vconfig add eth0 42`	`# ip link add link eth0 name eth0.42 type vlan id 42`	`(config-if)# switchport mode access` `(config-if)# switchport access vlan 42`
Supprimer une interface	`# vconfig del eth0 42`	`# ip link del link eth0 name eth0.42 type vlan id 42`	
		Configuration	
Création d'un VLAN			`(config) # vlan 42`
Destruction d'un VLAN			`(config) # no vlan 42`
		Aggrégation	
Configurer un port en trunk			`(config-if)# switchport mode trunk` `encapsulation dot1q`
Autroiser tous les VLANs			`(config-if)# switchport trunk allow all`
Autoriser certains VLANs		`# bridge vlan add vid 100 dev pont`	`(config-if)# switchport trunk allow 2-7,42`
Interdire certains VLANs		`# bridge vlan del vid 100 dev pont`	`(config-if)# switchport trunk remove 15,16`
		Observation	
Observation des VLANs		`# bridge vlan show`	`# show vlan	# show vlan brief`
Observation d'un VLAN			`# show vlan id 42`
Observer le trafic sur un commutateur			`(config) # monitor session 1 source interface` *`interface-id`* `both` `(config) # monitor session 1 destination interface` *`interface-id`* `encapsulation replicate`

Ethernet: le Spanning Tree

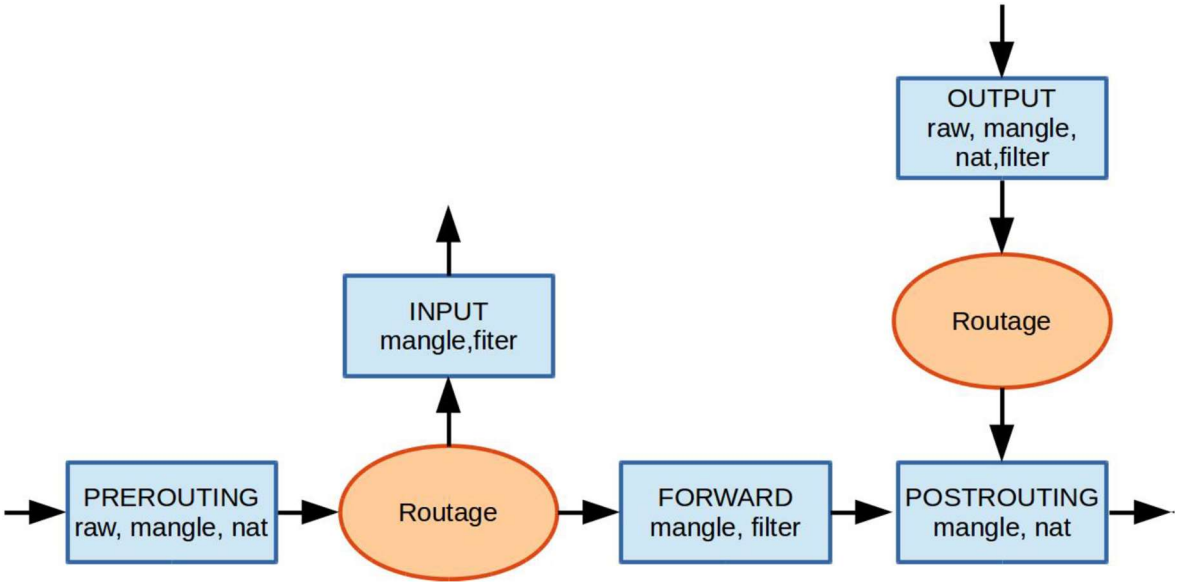
Action	Net tools	IP route2	Cisco iOS
		Configuration	
Activer le STP sur un VLAN	# brctl stp pont on		# spanning-tree vlan 42
Désactiver le STP	# brctl stp pont off		# no spanning-tree vlan 42
Désactiver le blocking sur un pont			(config-if)# spanning-tree portfast
Délai de forwarding	# brctl setfd pont 4		
Intervalle hello	# brctl sethello pont 1		
Age maximum	# brctl setmaxage pont 3		
Coût d'un lien	# brctl setpathcost pont eth1 243	# bridge link set dev eth1 cost 243	
Vieillissement des entrées en sec.	# brctl setageingtime pont 10		
Intervalle de test de la base en sec.	# brctl setgcint pont 5		
		Observation	
Etat du STP sur un VLAN			# show spanning-tree vlan 42
Etat du STP sur une interface			# show spanning-tree interface Fa0/0

IP: les interfaces

Action	Net tools	IP route2 (ip -6 : pour IPv6)	Cisco iOS
		Configuration	
Configurer une adresse	# ifconfig eth0 192.168.19.12/24	# ip addr add 192.168.19.12/24 dev eth0	(config-if)# ip address 192.168.19.12
Ajouter une adresse	# ifconfig eth0:1 192.168.20.12/24	# ip addr add 192.168.20.12/24 dev eth0	
Supprimer une adresse	# ifconfig eth0:1 down	# ip addr del 192.168.20.12/24 dev eth0	(config-if)# no ip address 192.168.19.12
Activer une interface	# ifconfig eth0 up	# ip link set dev eth0 up	
Désactiver une interface	# ifconfig eth0 down	# ip link set dev eth0 down	
		Observation	
Voir une interface	# ifconfig eth0	# ip addr show dev eth0	
Voir les interfaces actives	# ifconfig	# ip addr show	

IP: le routage

Action	Net tools	IP route2	Cisco iOS
		Configuration	
Activer le routage	# echo 1 > /proc/sys/net/ipv4/ip_forward		(config)# ip routing
Désactiver le routage	# echo 0 > /proc/sys/net/ipv4/ip_forward		(config)# no ip routing
		Paramétrage	
Ajouter une route	# route add -net 192.168.21.0/24 gw 192.168.20.1	# ip route add 192.168.21.0/24 via 192.168.20.1	(config)# ip route 192.168.21.0 255.255.255.0 192.168.20.1
Supprimer une route	# route del -net 192.168.21.0/24 gw 192.168.20.1	# ip route del 192.168.21.0/24 via 192.168.20.1	(config)# no ip route 192.168.21.0 255.255.255.0 192.168.20.1
Consultation des routes	# route	# ip route show	# show ip route



Action	Commande (à remplacer ce qui est entre <*>)
Source NAT d'une adresse	`# iptables -t nat -A POSTROUTING -o <eth0> -j SNAT --to <192.168.31.11>`
Source NAT d'une adresse pour un port	`# iptables -t nat -A POSTROUTING -p <tcp> --dport <80> -o <eth0> -j SNAT --to <192.168.31.11>`
Destination NAT d'une adresse pour un port	`# iptables -t nat -A PREROUTING -p <tcp> -d <147.127.0.0/16> -dport <80> -j DNAT --to <147.127.16.100:8080>`
Connecter un LAN à Internet	`# iptables -t nat -A POSTROUTING -o <eth1> -j MASQUERADE` `ethXXX – l'interface du routeur connecté à Internet`
Lister toutes les règles	`# iptables -L`
Changer la politique sur un chain	`# iptables –policy <INPUT | OUTPUT | FORWARD> <ACCEPT | DROP | REJECT | LOG>`
Vider toutes les tables	`# iptables -F`
Commande générique iptables	`# iptables -t <table> <-A -> append | -I position -> insert + position | -D -> supprimer> <CHAIN> -p <tcp | udp> <-s | d>` `<ipAddress/mask> -<-i | -o> <interface> -<sport | dport> <port> --state <NEW | ESTABLISHED> -j <TARGET>`
Tables	`raw, mangle, nat, filter`
CHAINS	`PREROUTING, INPUT, FORWARD, OUTPUT, POSTROUTING`
TARGETS	`ACCEPT, DROP, REJECT, LOG;` `Pour la table nat uniquement : SNAT, DNAT, MAQUERADE, REDIRECT (--to-ports #port | --to-destination @ip:port | --to @ip)`