Title

switch command

Successfully pass the free certification exam at IW Academy and become an Infinet Certified Engineer.

To the certification exam

- Description
  - Switching rules
- Parameters
  - List management
  - Switch Group Management
  - Interface management
  - Switching rules management
  - Management commands
- Examples

Description

The "*switch*" command is used to configure MAC Switch.

CAUTION

Starting from "*MINT 1.22.0*" firmware version, switch mode is partially incompatible with other firmware versions. It is highly recommended to perform firmware upgrade for units working in switch mode. Compatibility for MINT protocol and routing is not disturbed. "Over The Air Firmware Upgrade" feature also can be used.

Syntax:

```
 MAC Switch V2.06
Usage:
________ LIST commands __________________________________

  switch list LISTNAME [{iface | mac | numrange | match}]
         {add | del} [VALUE ...]
         dump [name] [WILDCARD]
         rename  NEWNAME
         file   FILENAME
         [flush|remove]

________ GROUP commands _________________________________

  switch group ID {add | del} IFNAME[:{TAG|0}] ...
  switch group ID {repeater|trunk|unpaired} {on|off}
  switch group ID {(up|down)stream} {SCID|0}
  switch group ID [x]vlan {TAG|LIST|0} [[no]bidir]
  switch group ID nvlan {[on]|off}
  switch group ID info INFO_STRING
  switch group ID setid NEWID
  switch group ID stp { off | on | dump }
  switch group ID stp [vlan TAG]
  switch group ID stp priority [PRIO]             #(default: 57344, step: 4096)
  switch group ID stp forwarddelay [DELAY]        #(default: 15 sec)
  switch group ID stp maxage [TIME]               #(default: 20 sec)
  switch group ID stp port IFNAME priority [PRIO] #(default: 128, step 16)
  switch group ID stp port IFNAME cost [COST]     #(default: 200000(RSTP),
                                                             65535(STP))

  switch group ID igmp { off | on }
  switch group ID igmp static-add MCAST IF_NAME [MAC]
  switch group ID igmp static-del MCAST IF_NAME [MAC]
  switch group ID igmp dump [detail] [name]
  switch group ID igmp lmqt Value
  switch group ID igmp gmi Value
  switch group ID igmp router-port { off | on }
  switch group ID igmp flood-reports { off | on }
  switch group ID igmp zero-query-permit { off | on }
  switch group ID igmp srcip IP
  switch group ID igmp join-limit [IF_NAME] N [include $ACL] [except $ACL]
  switch group ID igmp querier [vlan N] {start|stop|clear}
  switch group ID igmp querier [[no]election] [source IP] [mcast X[,Y,...]]
  switch group ID igmp querier interval Value

  switch group ID dhcp-snooping { off | on }             #(default: off)
  switch group ID dhcp-snooping [no]trust IFNAME         #(default: notrust)
  switch group ID dhcp-snooping [no]verify-mac           #(default: verify)
  switch group ID dhcp-snooping option-82 [no]insert     #(default: insert)
  switch group ID dhcp-snooping option-82 format
    { string ASCII-string | hex HEX-string | mac }       #(default: mac)
  switch group ID dhcp-snooping option-82 untrusted-policy
    { drop | keep | replace }                            #(default: drop)

  switch group ID flood-unicast { off | on }
  switch group ID inband { off | on }
  switch group ID order N
  switch group ID set NEWNUMBER
  switch group ID [setpri|addpri PRIO] [qmch CHAN]
  switch group ID {deny | permit}
  switch group ID
         dump [interface] [WILDCARD]
         [dbdelete   MACADDRESS]
         {start [discard]| stop | remove | stat | showrules | showblack}
  switch group ID {in-trunk} [{ID|0}]

________ INTERFACE commands _____________________________

  switch interface IFNAME mac-limit N

________ RULES commands _________________________________

  switch {group ID | interface IFNAME} rule NUMBER
         [not]
         [src   LIST] [dst   LIST] [vlan  LIST]
         [iface LIST] [proto LIST] [match LIST]
         [ setpri|addpri PRIO ] [qmch CHAN]
         [ deny | permit ] [ remove ]

_______  CONTROL commands _______________________________

  switch resynchronize
  switch trace { off | on | verbose | filter "pcap expr"}
  switch stptrace { off | on }
  switch stpblock { off | on }
  switch stpmint { off | on }
  switch {dump [WILDCARD]|MACADDRESS}

  switch igmp[-snooping] dump [name] [detail]
  switch {start|stop|restart|destroy|dead-interval DEAD_INTERVAL[300]}
  switch stat[istics] [(clear|help|ID)]
  switch maxsources (MAXSOURCES|0) # default 5000
```

Search filters "*WILDCARD*" are used as arguments in various commands to form search queries that allow to describe certain groups of subjects. Following characters can be used:

- * - any number of any symbols (or empty);
- ~ - any symbol (just one).

Switching rules

Rules are used to select an appropriate switch group when packet is received through "*eth**" interface. Packet will be switched only by that group to which rules it fully satisfies. Chosen group decides whether this packet needs to be sent through one of the interfaces. The packet will only be sent if it satisfies the rules of this interface.

The rules consist of rules list and a decision by default (deny/permit). Each rule consists of a sequential number, condition and decision (deny/permit). While going through the list, the switch checks whether a packet matches the rule. If it matches the rule, the decision set for this rule is applied to the packet. Otherwise, the list of rules is viewed further. Rules are taken according to their sequential number in ascending manner. If a packet does not match to any rule, the default decision for this group or interface is taken.

The condition might consist of one or several parameters which are checked with the following packet parameters:

1. Source interface (iface)
2. Source MAC address (src)
3. Destination MAC address (dst)
4. VLAN tag (vlan)
5. Ethernet layer protocol number (proto)

For each parameter a corresponding list of values should be specified. Moreover, the condition may contain the PCAP filter. This expression will be considered as a packet "pseudo parameter" and is called "*match*". Therefore, the packet is considered to have matched the condition, if all of its parameters match to the corresponding acceptable values from the lists and/or the packet satisfies to the expression of "*match*" type. One or more parameters might be missing in a condition clause – in this case it will mean that packet satisfies to that part of the condition which is missing.

Parameters

Parameter	Description
List management	
list	Allows to manage list values. Lists are used as a set of acceptable values for rules.
LISTNAME	List name. Each list must have a unique name and must be one of these types: iface, mac, numrange, match. List name may consist of letters and digits, but should not start with a digit, is case-insensitive. If list name contains spaces, it should be put in quotes.
[{iface | mac | numrange | match}]	Each list must be assigned to one of the following types: • "*iface*" – list type which consists of network interfaces names. • "*mac*" – list type which consists of a set of MAC addresses. • "*numrange*" – list type that consists positive integer numbers ranges set. The range of numbers is specified as "*<min>[-<max>]"*. The range may consist of one number if "*<min>=<max>"*. If a range of numbers is added to existing list and two ranges values intersect, these ranges will be concatenated. When deleting a range that intersects with the existing one in the list, completely nested ranges are deleted and / or the overlapping intersections with the deleted one are removed. • "*match*" – by context, "*match"* expressions are identical to expressions lists but should consist of one element – the expression itself. The expression should be written in PCAP format. If an expression has spaces it should be put into quotes.
{add | del} [VALUE ...]	Parameters "*add"* and "*del"* are used to add or delete values to the specified list (except "*match").* • "*VALUE*" – one or several values to be added or deleted from the list.
dump [name] [WILDCARD]	Displays the list content. • "*name*" – list name. • "*WILDCARD"* – search filter.
rename NEWNAME	Renames the list. • "*NEWNAME*" – new list name.
file FILENAME	A source file can be specified for the list. The source file should contain the list of values with each value taking one line. The file can be located on an FTP server, to which the configured device has network access. The values are loaded into the list from the source automatically when the switch starts or when the source name changes.

[flush|remove]	• "*flush*" – clears the list content. • "*remove*" – deletes the list from the switch configuration.
Switch Group Management	
group	Allows to manage switch group.
ID	Numeric switch group identifier in range 1...4999.
{add | del} IFNAME[:{TAG|0}] ...	Adds or deletes specified interfaces to/from the switch group: • "*add|del"* – adds/deletes specified interfaces to/from the switch group. If "*add*" parameter is used and there is no switch group with ID identifier, it will be automatically created. • "*IFNAME"* – network interface name which should be added or deleted from the switch group. • "*TAG"* – allows different manipulations with VLAN tags of the packet when the packet is sent through this interface. The following options are available: ◦ "*TAG*" is specified for the interfaces and its value is >0. That means that any packet forwarded to the interface by the switch will be tagged with a VLAN tag "*TAG*". If the packet already had a tag, this tag will be retagged to "*TAG*". ◦ "*TAG*" is not specified. This means that the packet stays unmodified. ◦ "*TAG*" is specified and its value is zero. This means that the packet sent through this interface will be untagged if it was previously tagged or sent without any changes if it was not tagged.
{repeater|trunk|uncoupled} {on|off}	Enables/disables switching mode. The following modes are available in WANFleX: • "*repeater*" – group switches the packets simply by sending them to all the device's interfaces except the one the packet was received from. • "*trunk*" – the group switches all the packets received through "*eth**" interfaces in such a way that when packets are sent to "*rf**" interfaces, these packets are places in a group with a number corresponding to the packet's VLAN TAG. When receiving the packet from "*rf**" interfaces, trunk group sends these packets to "*eth**" interface tagging them with a switch group number this packet was received from. • "*uncoupled*" – if a ring/redundant network is connected to a core network in multiple points, STP loops can be formed in the core network. Thus, STP enabled switches may block some of the links and leed to inefficient network loading. Switch groups with "*uncoupled*" parameter blocks the traffic between each other even if they have the same switch group number. This does not affect the traffic to come into the wireless network. For the incoming traffic intermediate nodes only use the closest uncoupled node. This improves the effectiveness of network utilization.
{(up|down) stream} {SCID|0}	In order to deal with upstream multicast flows in video surveillance systems two additional parameters are introduced: • *"downstream"* – device is used to send downstream traffic. • "*upstream*" – device is used to upstream traffic. • *"SCID|0"* – switch link identifier 0, 1, 2. Must be equal on "*upstream"* and "*downstream"* devices.
in-trunk [{ID|0}]	Allows to create several disjoint trunk groups within the same network, with the VLAN flows inside. Is used on a subscriber station.
[x]vlan {TAG|LIST|0} [[no]bidir]	Defines that the group will switch the packets, which a VLAN tag has one of the following values: • "*TAG*" – VLAN tag is specified. • "*LIST*" – value is specified in a "*numrange*" list type. • "*0*" – cancels VLAN filtration. • "*bidir"* – enables ingress traffic classification by VLAN ID on each interface of the group (from the wired segment and from the wireless link). The option can be useful for a ring (or redundant) topology network transmitting multiple VLANs when the traffic with certain VLAN IDs is picked up at junction points. • *"[x]"* – allows the group to process packets without a VLAN tag. ⚠ **NOTE** When enabling this VLAN tag filter other rules do not work.
nvlan {[on]|off}	Defines that group will switch only the packets not tagged with VLAN tag.
info INFO_STRING	Allows adding comments to switch group description.

setid NEWID	Changes switch group ID.
dump [interface] [WILDCARD]]	Displays the database of all known MAC addresses. • "*interface"* – displays the database of all known MAC addresses by grouping them according to interfaces. • "*WILDCARD"* – the output will be filtered according to the selected criteria.
stat	Shows selected group statistic.
showrules | showblack	• "*showrules*" – displays detailed information about the group's classification rules, including the hits counter for each rule. • "*showblack*" – displays the list of MAC addresses that are blocked due to the indeterminacy of their owner.
dbdelete MACADDRESS	Deletes all records from MAC address database connected with a specified MAC address.
start [discard] |stop | remove	Starts/stops a specified switch group, deletes a specified group from the switch configuration.
stp { off | on | dump }	Enables/disables STP support for selected group. • "*dump*" – allows to see STP state of the group.
stp priority [PRIO]	Sets STP priority of a switch. • "*PRIO"* – priority value. If priority is not specified then default value (57344) is set. When setting priority value it will be automatically rounded down to a value divisible by 4096.
stp forwarddelay [DELAY]	Sets STP "*forward delay*" parameter, which determines a time that switch spend in "*listening*" and "*learning*" states. • "*DELAY"* – time value in seconds. If not specified default value is 15 seconds.
stp maxage [TIME]	Sets STP "*MAX age*" parameter, which determines time for switch to deliver BPDU-packet. • "*TIME"* – value in seconds. If not specified default value is 20 seconds.
stp port IFNAME priority [PRIO]	Sets the switch port STP priority. • "*IFNAME"* – interface name. • "*PRIO"* – port priority value. If not specified default value is 128. When setting priority value it will be automatically rounded down to a value divisible by 16.
stp port IFNAME cost [COST]	Sets STP "*cost*" parameter of switch port, which determines switch port cost. • "*COST"* – cost value. If not specified default value is 200000 for RSTP, 65535 for STP.
stp [vlan TAG]	Sets VLAN tag for STP in selected switch group.
igmp { off | on }	Enables/disables the "*IGMP-snooping*" function for the switch group.
setpri|addpri PRIO	Allows to set/increase the priority of packets passing through the group. • "*setpri"* – changes a priority to the value specified in the command. When using "*-1*" value a package priority is dropped to the lowest priority. • "*addpri"* – changes a priority only in case it is higher than the previous one (the smaller is the value the higher is the priority). So you can only increase priority using "*addpri*" parameter.
qmch CHAN	Allows to set service class "*CHAN*" to the Ethernet frame entering switch group. Service classes are created by "*qm chan*" command.
{deny | permit}	Permits/denies processing and sending out the packets which belong to this group.

igmp dump [detail] [name]	Displays IGMP hosts list which are subscribed to multicast group. • "*detail"* – shows detailed information on multicast-subscribers. • "*name*" – shows information for a specific gateway.
igmp lmqt Value	Sets "*Last Member Query Time*" value i.e. the maximum time during which the switch will wait for the answer from active subscribers after receiving "IGMP leave". If no answer is received the switch will stop Multicast packets delivery to the particular Gateway. Gateway is an Ethernet interface or radio interface with a device MAC address on the other side of the link.
igmp gmi Value	Sets "*Group Membership Interval*" value i.e. the amount of time that must pass before a Multicast Router decides there are no more clients subscribed to a Multicast group (no more "IGMP report" messages in the group).
igmp static-add MCAST IF_NAME [MAC]	Creates Multicast address static subscription.
igmp static-del MCAST IF_NAME [MAC]	Deletes Multicast address static subscription.
igmp router-port { off | on }	The switch to forward multicast streams not only to subscriber ports, but also to all router (querier) ports.
igmp flood-reports { off | on }	Enables IGMP report packets forwarding to all ports, not just the routers (querier) ports. By default is off.
igmp srcip IP	Replace a source IP address in IGMP Report packets on the address specified in the "*IP*" field of this parameter.
igmp zero-query-permit { off | on }	Enables processing for packets with 0.0.0.0 source IP address. By default is off.
igmp querier [vlan N] {start|stop|clear}	Enables/disables the "*Querier*" function, which substitutes the functions of Multicast Router in video systems with "*IGMP Snooping*" using. • "*vlan N"* – enables multicast packets transmittion with using VLAN. • "*clear"* – deletes "*IGMP Querier*" configuration.
igmp querier [[no]election] [source IP] [mcast X[,Y,...]]	• "*[no]election*" – when the IGMP Querier function is enabled, disables/enables the process of election of the IGMP Querier operating on the network segment. According to the standards, each network segment should have a single IGMP Querier, that has the lowest source IP address. By default is enabled. • "*source X"* – sets source IP address for Multicast packets. • "*mcast X[,Y,...]"* – sets concrete Multicast Group (or a number of groups) to be allowed for subscription.
igmp querier interval Value	Sets the interval to send IGMP Querier packets in seconds.
igmp join-limit [IF_NAME] N [include $ACL] [except $ACL]	Limits the number of active unique IGMP multicast group. Once the group limit is reached, subsequent join requests are rejected. • "*IF_NAME"* – network interface to make limitation. • "*include $ACL*" – list of addresses/networks covered by this limitation. • "*except $ACL*" – list of exceptions.
flood-unicast { off | on }	Enables/disables "*flood-unicast*" mode, allowing to send unicast packets as broadcast, sending them through all interfaces included in the switch group.
inband { off | on }	If the traffic sent by the switch group does not contain (should not contain) the information intended for this device (only transit flow), then the analysis of broadcast packets can be disabled, thus reducing the load on the processor. By default, analysis is enabled.
order N	In the process of data packets distribution to switch groups, the groups are viewed in order they are situated in the configuration. The first group that is suitable for a packet is chosen and the process is stopped. The parameter sets the order in which the concrete group will be run over during the assigning process.
dhcp-snooping { off | on }	Enables/disables DHCP snooping function, providing protection against attacks using a DHCP. By default is off.

dhcp-snooping [no]trust IFNAME	Marks the interface as trusted/untrusted. By default, all interfaces are marked as untrusted.
dhcp-snooping [no]verify-mac	Enables/disables checking for the sender MAC addresses correspondence with specified in the DHCP request.
dhcp-snooping option-82 [no] insert	Enables/disables adding Option 82 in DHCP request. By default is on.
dhcp-snooping option-82 format { string ASCII-string | hex HEX-string | mac }	Sets the DHCP relay identifier format in Option 82. - "*mac*" – MAC address by default. - "*ASCII-string*" – ASCII encoded identifier. - "*HEX-string*" – HEX encoded identifier.
dhcp-snooping option-82 untrusted-policy { drop | keep | replace }	Configures the action to be made if a packet containing Option 82 hits an untrusted interface. By default, packets are discarded.
Interface management	
interface IFNAME mac-limit N	Use to limit the number of dynamically learned MAC addresses per interface. Once the limit is reached no more MAC addresses will be learned. Traffic with source MAC addresses that have not been learned will be blocked.
Switching rules management	
group ID | interf ce IFNAME	Number of the group or interface name.
rule NUMBER	Sequential rule number.
set NEWNUMBER	Changes the rule number.
remove	Deletes the rule.
src, dst, vlan, iface, proto, match LIST	Specifies the lists of acceptable values for the corresponding parameter of the packet. For more information see the "Switching rules" subsection. - *"LIST*" – acceptable values list name.
deny | permit	Sets the decision for the corresponding rule.
setpri|addpri PRIO	Sets/increases the priority of packets passing through the group. - "*setpri" –* changes a priority to the value specified in the command. When using "*-1*" value a package priority is dropped to the lowest priority. - "*addpri" –* changes a priority only in case it is higher than the previous one (the smaller is the value the higher is the priority). So you can only increase priority using "*addpri*" parameter.
Management commands	
resynchronize	Forces to reload the acceptable values list contents, the data source of which is external file.
trace { off | on | verbose | filter "pcap expr"}	Disables/ enables logging the service information into the system log. - "*verbose*" – enables more detailed information logging. - "*filter "pcap expr*" – enables tracing how packets of the corresponding PCAP filter are being processed by the switch.

stptrace { off | on }	Disables/ enables logging of the STP service information such as changing the ports state, changing connections into the system log. By default is disabled.
stpblock { off | on }	- "*on*" – prevents STP frames forwarding in the switch mode when STP support is disabled. - "*off*" – allows STP frames forwarding.
stpmint { off | on }	Enables/disables the STP MINT mode. STP MINT mode is used to exclude the wired switches with the enabled STP protocol influence on the network operation. The mode blocks the BPDU frames of the STP protocol configured on wired switches so that the switch cannot detect the loop and block its ports. STP MINT mode in conjunction with the RSTP protocol enabled in the Infinet devices allows to break the loop and support the PRF protocol functioning that operates through the wired segment.
dead-interval <DEAD_INTERVAL_IN_SECONDS>	Switch MAC address database is a routing table of MAC layer which contains information on how the packet should be delivered to its destination (dst). Each switch group has an independent database. Records in the database are formed automatically based on the source address of the packet which was received by one of the interfaces included into a switch group. Moreover, the database always contains records corresponding with interfaces included into the switch group. These records are called local records. Each records has its life span. The parameter sets record "life span". If, during this life span, none of the interfaces have received a packet with a source address from this record, this record is deleted from the database. By default, life span is 300 seconds.
{start | stop | restart}	Starts/stops/restarts the switch.
{destroy}	Clears the switch configuration.
statistics [(clear|help|ID)]	Displays switch statistic. Shows the information on forwarded/flooded/dropped packets and records of the switch MAC address table (DB Records). Unicast, broadcast and flood packets statistic is made separately. - "*clear*" – clears the switch statistic. - "*help*" – shows a list of the drooped packets reasons descriptions used in the switch statistics command output. - "*ID*" – switch group ID. If specified the output displays separate packet stats for each VLAN that belongs to that switch group.
igmp[-snooping] dump [name] [detail]	Displays IGMP hosts list, which are subscribed to a multicast group from all groups. - "*detail"* – shows detailed information about subscribers. - "*name*" – shows the information for a specific gateway.
MACADDRESS	Displays the information for the specific MAC address.
maxsources (MAXSOURCES|0)	Sets the maximum allowed number of records in the switch MAC address table. The default number of records is 5000. If "0" value is used the number of records is set to minimum possible (500).

Examples

The following example shows how to use a wildcard template to display information about network interfaces "*eth0*" and "*eth1*". The "*eth~*" template using info rms the "*switch*" command to display information about interfaces which names started with "*eth*" and has any symbol in the end. "*Cost"* – the cost (metric) of the route. *"UsCNT"* – a counter indicating how many times this record has been used, i.e. how many packets were sent to this MAC address.

```
switch group 1 dump eth~
 Bridge group 1(normal), READY STARTED Interfaces : eth0(F) eth1(F) rf5.0(F)
 Total records 5
   DST MAC        L   Int.   GateWay MAC   Cost   UsCNT    Dead    Vlan
 ==============   =  ====  ========= ==    =====  =====    ====   =======
 001111144693       eth0   000000000000     0      3987     300       1
 000435018822    *  eth0   000000000000     0       0         0       1
 000435118822    *  eth1   000000000000     0       0         0       1
```

Create "*iface*" type list with name "*my_iface*" and add network interfaces "*eth0*" and "*rf5.0*".

```
switch list my_iface iface add eth0 rf5.0
```

Create a list of values ranges named "*vlans"* and add value 10, values range 20...30 and 40 value.

```
switch list vlans numrange add 10 20-30 40
```

Create "*match"* type list and add filter its effect will cover packets of all type protocol from "*195.38.45.64/26*" network.

```
switch list ip_mynet match add net 195.38.45.64/26
```

In the following example "*match"* type list is also created, but filter covers only IP packets from "*195.38.45.64/26*" network.

```
switch list ip_mynet match add ip net 195.38.45.64/26
```

Specify a text file as a values source.

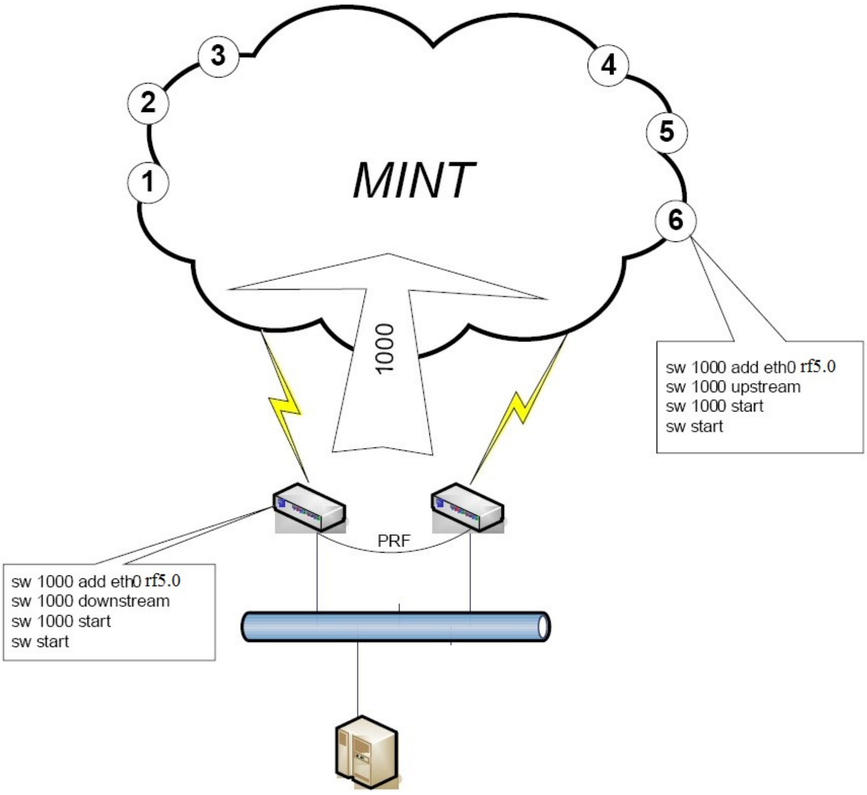
```
switch list MACGROUP1 file ftp://1.2.3.4/switches/list/macgroup1.txt
```

In the following example list "*macgroup1.txt*" may contain the following lines:

```
#
00:01:02:03:04:05  #
00:11:12:13:14:15  #
<EOF>
```

Title

Nodes with numbers 1, 2, 3, 4, 5 and 6 are connected to digital cameras which broadcast video traffic using multicast packets. All of these flows need to be transferred to a video server the best way without flooding the network with unnecessary broadcast packets.



```
sw 1000 add eth0 rf5.0
sw 1000 upstream
sw 1000 start
sw start
```

```
sw 1000 add eth0 rf5.0
sw 1000 downstream
sw 1000 start
sw start
```

Downstream (from server to camera) traffic, if any, is transferred in group number 1000 in which all the nodes are located. But upstream flows from each camera are transmitted directly to the nearest hub of the group.

A feature of this solution is the ability to set multiple switchs with the same group number. To address the problem broadcast storm that could arise from the fact that the switchs are included in the various ports switch of one wire in MINT restricted - Broadcast and downstream switchs never use each other to carry traffic. Furthermore, the availability of options "*upstream*" ensures that the terminal nodes will choose to send packages only one hub, but it is the shortest way to the nearest hub.

To make switch group 100 on a subscriber station a member of a trunk group 5, the following command should be added to subscriber station configuration:

```
switch group 100 in-trunk 5
```

Display current STP state using the "*switch group ID stp dump*" command.

```
switch 1 stp dump
 STP state for passive group 1:
 ID:       0000000000000000 Priority: 57344 ID ext: 0
 ROOT:     0000000000000000 Priority: 0     ID ext: 0
 Ports:
  Name  Prio    Cost    PVer    Role      State
 ====== ==== ========== ==== ========== ==========
 eth0    128    2000000 RSTP DISABLED   DISCARDING
 rf5.0   128     180844 RSTP DESIGNATED DISCARDING
```

In the following examples all packets switching by group 3 will be tagged with VLAN 10 tag when sending through "rf5.0" interface and tags will be removed when sending through the "eth0" interface.

> **NOTE**
>
> For all packets whose destination is the switch itself, the VLAN tag is always removed.

```
switch group 3 add rf5.0:10 eth0:0
```

Enable a trunk group on the device that will transmit several VLAN flows in different directions.

```
switch group 12 trunk on
```

On the subscriber devices "*in-trunk*" option must be used to specify which trunk group this group belongs to.

```
switch group 12 in-trunk 0
```

Group 10 will process packets with tags VLAN 100, 200, 300 and untagged packets which will be sent to the MINT network with 10 group number, tagged - with group numbers that match the VLAN tag.

```
switch list MYNET numrange add 100 200 300
switch group 10 xvlan MYNET
switch group 10 trunk on
```

Group 20 will process only tagged packets from MYNET list and changes the VLAN tag to the corresponding group number (and vice versa) before transmission.

```
switch list MYNET numrange add 100 200 300
switch group 20 vlan MYNET
switch group 20 trunk on
```

Group 30 will process only tagged packets from MYNET list and transmits without changing with the group number 30.

```
switch list MYNET numrange add 100 200 300
switch group 30 vlan MYNET
switch group 30 trunk off
```

Create switch group "*1*", enable STP for it and set the 36864 STP priority value.

```
switch group 1 add eth0 rf5.0
switch group 1 stp priority 36864
switch group 1 stp on
switch group 1 start
```

There are three switch group.

1. Create rule 10 in the switch group 5 to forbid packets with source MAC addresses (specified in the group MACGROUP1), belonging to certain VLAN (VLAN ID list belongs to VGROUP and consists of 10, 40 and range 20...30), in case if packets are IP and ARP, belonging to the network listed in IP_NET3845.
2. Create rule 20 in the switch group 5 to forbid packets with destination MAC addresses (specified in the group MACGROUP1), belonging to certain VLAN (VLAN ID list belongs to VGROUP and consists of 10, 40 and range 20...30), in case if packets are IP and ARP, belonging to the network listed in IP_NET3845.
3. Set priority 10 to packets in switch group 1.

```
switch list MACGROUP1 mac add 00:01:02:03:04:05 00:11:12:13:14:15
switch list VGROUP numrange add 10 20-30 40
switch list IP_NET3845 match add arp net 195.38.45.64/26 || ip net 195.38.45.64/26
switch group 5 rule 10 src MACGROUP1 vlan VGROUP match IP_NET3845 deny
switch group 5 rule 20 dst MACGROUP1 vlan VGROUP match IP_NET3845 deny
switch group 1 rule 1 setpri 10
```

Enable logging of packets with source MAC address "*00:11:22:33:44:55*" and "*1.2.3.0/24*" subnetwork processing by the switch.

```
sw trace filter "ether host 00:11:22:33:44:55"
sw trace filter "net 1.2.3.0/24"
```

Create three switch group. Group 5 switches packets with VLAN tags 10, 20-30 and 40. Group 15 switches packets with any VLAN tag with exception for those switched by group 5. Group 25 switches all packets without VLAN tag. In addition, group 25 will transmit inter-switch traffic.

```
switch list VGROUP numrange add 10 20-30 40

switch list ALL_VLAN numrange add 0-4999

switch group 5 add eth0 rf5.0
switch group 5 rule 10 vlan VGROUP permit
switch group 5 deny
switch group 5 start

switch group 15 add eth0 rf5.0
switch group 15 rule 10 vlan VGROUP deny
switch group 15 rule 11 vlan ALL_VLAN permit
switch group 15 deny
switch group 15 start

switch group 25 add eth0 rf5.0
switch group 25 rule 10 vlan ALL_VLAN deny
switch group 25 permit
switch group 25 start
switch start
```