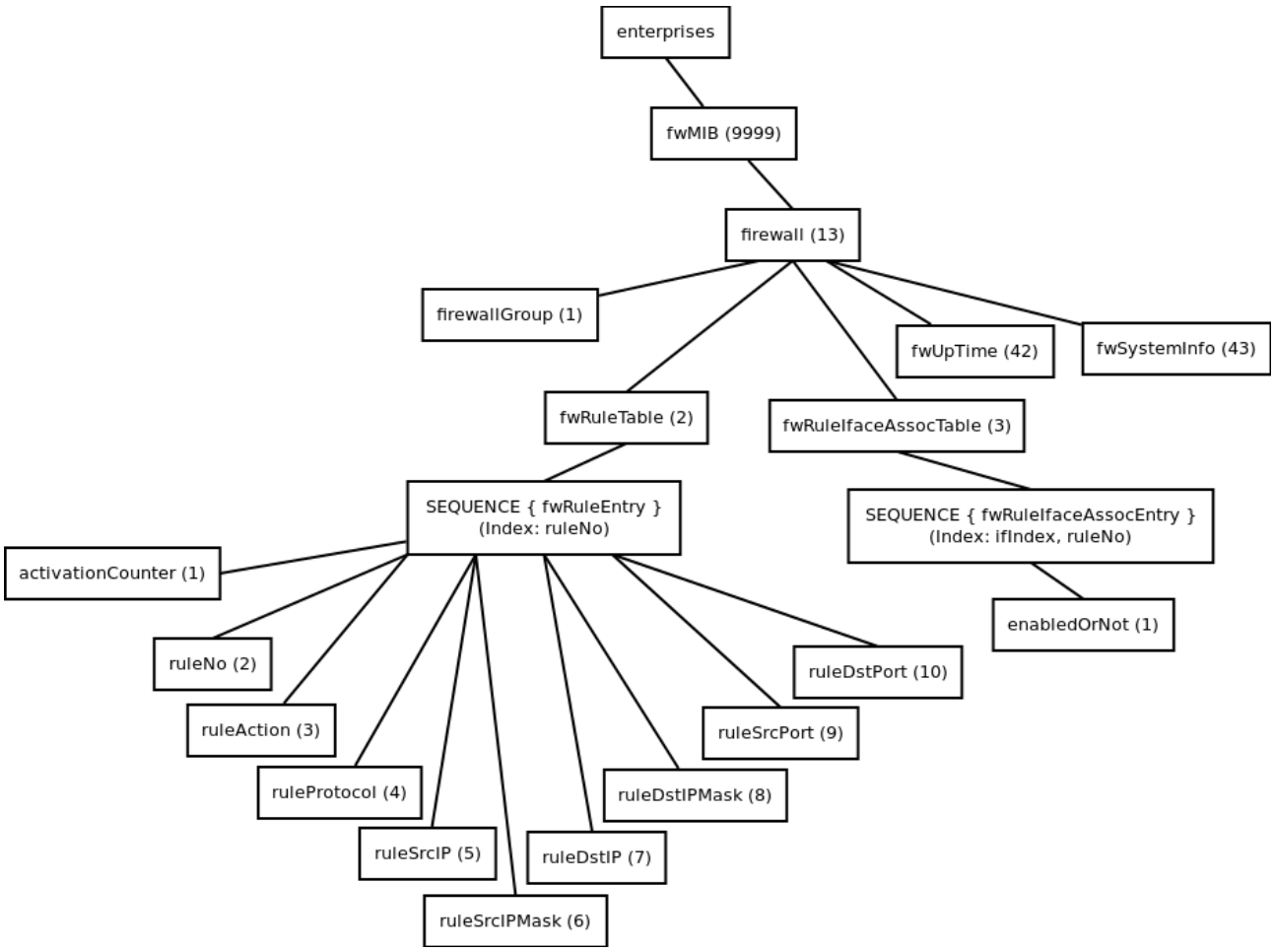
Διαχείριση Δικτύων – Ευφυή Δίκτυα

6η Ομάδα Ασκήσεων

Αλέξανδρος Μαυρογιάννης
Αριστοτέλης Πανάρας

Άσκηση 1

Παρατίθενται ο κώδικας του MIB module (στο τέλος της αναφοράς) και η σχηματική του απεικόνιση.
(Note: Το smilint βγάζει ένα error το οποίο δεν μπορούμε να διορθώσουμε:
./MIB_module:91: warning: SEQUENCE element #1 `ruleNo' does not match order of columnar objects under `fwRuleEntry')



Άσκηση 2.1

1. Έχουν οριστεί οι εξής ομάδες: NETMODE-Servers, NETMODE-Printers, NETMODE-Switches, Other-Servers και freebsd-servers.
Αυτό φαίνεται πηγαίνοντας στο path “>Host Groups”.

2. Παρακάτω φαίνονται οι ομάδες και οι συσκευές που ανήκουν σε αυτές:
NETMODE-Printers
{blondie, briki, dell5330}.netmode.ntua.gr
NETMODE-Servers
{averel, dolly, dragon, ghost, sheep, sofo, yankee}.netmode.ntua.gr
NETMODE-Switches
{cisco, hp, linksys}-sw.netmode.ntua.gr
Other-Servers
www.harvard.edu, www.imperial.ac.uk, www.otenet.gr
freebds-servers
localhost (maria.netmode.ntua.gr)

Στους hosts του group NETMODE-Switches παρακολουθούνται οι εξής υπηρεσίες: PING, Port 12 Link Status, Uptime.
Στον host του group freebsd-servers παρακολουθούνται οι υπηρεσίες Current Load, Current Users, HTTP, PING, Root Partition, SSH, Swap Usage, Total Processes.
Όσον αφορά το group NETMODE-Servers, στον host ghost.netmode.ntua.gr δεν παρακολουθείται καμία υπηρεσία (τι περιμέναμε άλλωστε;), ενώ στην dolly.netmode.ntua.gr έχουμε τις HTTP, IMAP, PING, POP, SMTP και SSH.
Στους hosts των groups NETMODE-Printers, Other-Servers και όλους τους άλλους μη αναφερθέντες hosts του NETMODE-Servers, παρακολουθείται μόνο η υπηρεσία PING.

3. Έχει οριστεί μόνο μία ομάδα υπηρεσιών, η pingservices. Σε αυτήν ανήκουν οι συσκευές {averel, dolly, dragon, sheep, sofo, yankee}.netmode.ntua.gr, www.harvard.edu, www.imperial.ac.uk και www.otenet.gr .
Αυτό φαίνεται στην καρτέλα “> Service Groups”.

4. Οι μόνες υπηρεσίες για τις οποίες δεν στέλνονται ειδοποιήσεις στο διαχειριστή, είναι οι HTTP και SSH στην maria.netmode.ntua.gr και οι HTTP, IMAP, POP, SMTP, SSH στην dolly.netmode.ntua.gr.

5, 6. Σε κατάσταση WARNING βρίσκεται η υπηρεσία PING στον κόμβο www.imperial.ac.uk, ενώ σε CRITICAL βρίσκονται πάλι οι υπηρεσίες PING στους hosts www.harvard.edu, www.otenet.gr, yankee.netmode.ntua.gr .

7. Αυτό φαίνεται στο path “> Process Info” από τα Program Start Time και Total Running Time και είναι 416d 18h 26m 15s, δηλαδή από 20-11-2012 11:24:24.

8. Τέλος, το scheduling των μετρήσεων για κάθε service φαίνεται στο “> Scheduling Queue”. Παρατηρούμε ότι για όλες τις υπηρεσίες που παρακολουθούνται, μετρήσεις λαμβάνονται κάθε 10 λεπτά, εκτός από όλες τις υπηρεσίες που υπάρχουν στον localhost (maria.netmode.ntua.gr).

Άσκηση 2.2

1. Τα WARNING ή CRITICAL state γίνονται trigger όταν το threshold ή packet loss ξεπεράσουν τα δηλωμένα όρια του αντίστοιχου command line switch (-w για warning και -c για critical αντίστοιχα). Εφόσον οι εντολές που χρησιμοποιούνται για να ελέγξουν την κατάσταση του κόμβου είναι η εξής μία: “check_ping -w 50.0,20% -c 100.0,60%”, όπως φαίνεται από το /usr/local/etc/nagios/objects/world.cfg, όταν ξεπεραστεί κάποια από τις 2 μετρικές εμφανίζεται το αντίστοιχο state.

2. Απαντήθηκε στο προηγούμενο ερώτημα, αλλά σε περίπτωση που έπρεπε να βρούμε τις τιμές των thresholds πειραματικά, θα έπρεπε είτε να κάνουμε poll τη σελίδα του nagios μέχρι να εμφανιστεί κάποιο διαφορετικό state output (εννοώντας διαφορετικό από τη σύνηθη τιμή του), και τότε να κάνουμε ένα binary search σε ένα πιθανό πεδίο ορισμού των thresholds, είτε να να πειραματιστούμε με τα thresholds χωρίς αυτή την πληροφορία. Στην πρώτη περίπτωση, πιθανότατα θα πέρναμε κάποιο tighter bound στο πεδίο των thresholds, ενώ στη δεύτερη θα πάρουμε κάποιο πιο χαλαρό όριο.

3.

```
======== /usr/local/libexec/nagios/check_tcp -H www.otenet.gr -p 80 | tee -a lab6_output.text ========
TCP OK - 0.002 second response time on port 80|time=0.002336s;;;0.000000;10.000000
======== /usr/local/libexec/nagios/check_fping unbearable_also.mooo.com | tee -a lab6_output.text ========
FPING OK - unbearable_also.mooo.com (loss=0%, rta=1.460000 ms)|loss=0%;;;0;100 rta=0.001460s;;;0.000000
======== /usr/local/libexec/nagios/check_fping unbearable.mooo.com | tee -a lab6_output.text ========
FPING CRITICAL - unbearable.mooo.com (loss=100% )|loss=100%;;;0;100
======== /usr/local/libexec/nagios/check_hpjd -H blondie | tee -a lab6_output.text ========
Printer ok - ("Ready          ")
======== /usr/local/libexec/nagios/check_http -H localhost -p 80 | tee -a lab6_output.text ========
HTTP OK: HTTP/1.1 200 OK - 363 bytes in 0.002 second response time |time=0.002339s;;;0.000000 size=363B;;;0
```

SOURCES

Το script για το ερώτημα 2.2.3:

```
#!/usr/bin/env bash

outfile="lab6_output.text"
path_prefix="/usr/local/libexec/nagios/"

#question_template: "command | tee -a $outfile"
questions=(
        "${path_prefix}"{'check_tcp -H www.otenet.gr -p 80','check_fping unbearable_also.mooo.com','check_fping
unbearable.mooo.com','check_hpjd -H blondie','check_http -H localhost -p 80'}" | tee -a $outfile"
)

function report () {
        echo "========" "$1" "========" >> $outfile
        eval "$1"
        echo -e "\n" >> $outfile
}

IFS=""
rm -f "$outfile"
for i in "${questions[@]}"
do
        report "$i"
done
echo "Finished!"
```

Ο κώδικας του MIB firewall module:

```
FIREWALL-MIB DEFINITIONS ::= BEGIN
	IMPORTS
		enterprises, OBJECT-TYPE, MODULE-IDENTITY, Integer32, Unsigned32, IpAddress, Counter32,
TimeTicks
			FROM SNMPv2-SMI
		OBJECT-GROUP
			FROM SNMPv2-CONF
		ifIndex
			FROM IF-MIB;

fwMIB MODULE-IDENTITY
	LAST-UPDATED		"201402242317Z"
	ORGANIZATION		"Me, Myself & I"
	CONTACT-INFO		"shit.happens@life.com"
	DESCRIPTION		"Firewall MIB module for netmg lab"
	REVISION		"201402242317Z"
	DESCRIPTION		"It's a new day!"
	::= { enterprises 9999 }

	firewall OBJECT IDENTIFIER ::= { fwMIB 13 }

	firewallGroup OBJECT-GROUP
		OBJECTS			{
			fwUpTime, fwSystemInfo,
			activationCounter,
			ruleNo, ruleAction, ruleProtocol,
			ruleSrcIP, ruleSrcIPMask, ruleDstIP, ruleDstIPMask, ruleSrcPort, ruleDstPort,
			enabledOrNot
		}
		STATUS			current
		DESCRIPTION	"The grouping happens here... :/"
		::= { firewall 1 }

	fwUpTime OBJECT-TYPE
		SYNTAX			TimeTicks
		MAX-ACCESS	read-only
		STATUS			current
		DESCRIPTION	"Uptime of firewall module (in 100ths of a second)"
		::= { firewall 42 }

	fwSystemInfo OBJECT-TYPE
		SYNTAX			OCTET STRING (SIZE(1..256))
		MAX-ACCESS	read-only
		STATUS			current
		DESCRIPTION	"Firewall system description"
		::= { firewall 43 }

	fwRuleIfaceAssocTable OBJECT-TYPE
		SYNTAX			SEQUENCE OF FwRuleIfaceAssocType
		MAX-ACCESS	not-accessible
		STATUS			current
		DESCRIPTION	"Association of rules with interfaces"
		INDEX		{ ifIndex, ruleNo }
		::= { firewall 3 }

	fwRuleIfaceAssocEntry OBJECT-TYPE
		SYNTAX			FwRuleIfaceAssocType
		MAX-ACCESS	not-accessible
		STATUS			current
```

```
		DESCRIPTION	"Association entry. The keys (indices) are the information, so only a dummy entry is needed."
		INDEX		{ ifIndex, ruleNo }
		::= { fwRuleIfaceAssocTable 1 }

	FwRuleIfaceAssocType ::=
		SEQUENCE {
			enabledOrNot			Unsigned32
		}

	enabledOrNot OBJECT-TYPE
		SYNTAX		Unsigned32
		MAX-ACCESS	read-only
		STATUS		current
		DESCRIPTION	"Dummy value for association of rules to interfaces"
		::= { fwRuleIfaceAssocEntry 1 }

	fwRuleTable OBJECT-TYPE
		SYNTAX		SEQUENCE OF FwRuleType
		MAX-ACCESS	not-accessible
		STATUS		current
		DESCRIPTION	"Firewall rule table"
		INDEX		{ ruleNo }				--This is not the place for indexing anymore. This is the independent table.
		::= { firewall 2 }

	fwRuleEntry OBJECT-TYPE
		SYNTAX		FwRuleType
		MAX-ACCESS	not-accessible
		STATUS		current
		DESCRIPTION	"A firewall rule entry"
		INDEX		{ ifIndex }				--{ ifIndex, ruleNo }	:: If I put ruleNo an index, I have to make it not-accessible...
		::= { fwRuleTable 1 }

	FwRuleType ::=
		SEQUENCE {
			ruleNo				Integer32,
			ruleAction			Unsigned32,		--	Unsigned32 { drop(1), pass(2) },
			ruleProtocol		Unsigned32,		--	Unsigned32 { ip(1), icmp(2), tcp(3), udp(4) },
			ruleSrcIP			IpAddress,
			ruleSrcIPMask		IpAddress,
			ruleDstIP			IpAddress,
			ruleDstIPMask		IpAddress,
			ruleSrcPort			OCTET STRING,
			ruleDstPort			OCTET STRING,
			activationCounter	Counter32
		}

	ruleNo OBJECT-TYPE
		SYNTAX		Integer32 (1 .. 2147483647)
		MAX-ACCESS	read-only
		STATUS		current
		DESCRIPTION	"Incremental rule number"
		::= { fwRuleEntry 2 }

	ruleAction OBJECT-TYPE
		SYNTAX		Unsigned32		--{ drop(1), pass(2) }
		MAX-ACCESS	read-only
		STATUS		current
		DESCRIPTION	"Pass or fail action under a rule"
```

```
        ::= { fwRuleEntry 3 }

    ruleProtocol OBJECT-TYPE
        SYNTAX          Unsigned32          --{ ip(1), icmp(2), tcp(3), udp(4) },
        MAX-ACCESS  read-only
        STATUS          current
        DESCRIPTION  "Packet protocol of packets that will match the rule"
        ::= { fwRuleEntry 4 }

    ruleSrcIP OBJECT-TYPE
        SYNTAX          IpAddress
        MAX-ACCESS  read-only
        STATUS          current
        DESCRIPTION  "Packet source IP address"
        ::=     { fwRuleEntry 5 }

    ruleSrcIPMask OBJECT-TYPE
        SYNTAX          IpAddress
        MAX-ACCESS  read-only
        STATUS          current
        DESCRIPTION  "Packet source IP mask"
        ::=     { fwRuleEntry 6 }

    ruleDstIP OBJECT-TYPE
        SYNTAX          IpAddress
        MAX-ACCESS  read-only
        STATUS          current
        DESCRIPTION  "Packet destination IP address"
        ::=     { fwRuleEntry 7 }

    ruleDstIPMask OBJECT-TYPE
        SYNTAX          IpAddress
        MAX-ACCESS  read-only
        STATUS          current
        DESCRIPTION  "Packet destination IP mask"
        ::=     { fwRuleEntry 8 }

    ruleSrcPort OBJECT-TYPE
        SYNTAX          OCTET STRING (SIZE(0..11))
        MAX-ACCESS  read-only
        STATUS          current
        DESCRIPTION  "Packet source port"
        ::= { fwRuleEntry 9 }

    ruleDstPort OBJECT-TYPE
        SYNTAX          OCTET STRING (SIZE(0..11))
        MAX-ACCESS  read-only
        STATUS          current
        DESCRIPTION  "Packet destination port"
        ::= { fwRuleEntry 10 }

    activationCounter OBJECT-TYPE
        SYNTAX          Counter32
        MAX-ACCESS  read-only
        STATUS          current
        DESCRIPTION  "Rule use counter"
        ::= { fwRuleEntry 1 }

END
```