Tue Apr 19 11:03:19 PDT 2005
by Andrew Gristina
thanks to Luca Deri and the ntop tea

This docu ent speci!ica""y addresses a subset o! interestin# net!"ow e$port situations to an ntop net!"ow co""ector insta""ed on %edora &ore 3 Linu$'

(hy ntop and net!"ow co""ection) There are any too"s !or #atherin# data !or network troub"eshootin#' * +TG can onitor inter!aces, bandwidth, and sn p counters such as &P - and e ory usa#e' . a#ios can onitor node a/ai"abi"ity' 0ys"o# can #i/e detai"ed in!or ation !or troub"eshootin#' . 1A+ can he"p c"assi!y tra!!ic' And network sni!!in# can #i/e a /ery detai"ed pro!i"e o! network tra!!ic and captures are in/a"uab"e too"s to he"p troub"eshoot network prob"e s' . et!"ow and . top can pro/ide !acets o! se/era" too"s and can be i p"e ented in situations where other too"s can not re"iab"y be used'

. top is e$ce""ent !or su ari2in# net!"ow in!or ation' . top reports can #i/e bandwidth su aries' . top can c"assi!y tra!!ic and pro/ide network pro!i"e' And . top can a"so a""ow you to #et a detai"ed pro!i"e o! network tra!!ic' 1y usin# net!"ow, . top can he"p c"assi!y and pro!i"e network tra!!ic on networks where spannin# ports or sni!!in# ay not be !easib"e due to sca"e or network architecture'

Installing ntop on a Fedora Core 3 Server

%irst, insta"" ntop on a %edora &ore 3 ser/er'

%or ease o! aintenance and insta""ation, down"oad the binary +P * s !ro 0ource!or#e:

`http://sourceforge.net/project/showfiles.php?group_id=17233&package_id=13248`

The %& 2 +P * s wi"" work on %& 3' %edora shou"d be binary co patib"e backward and !orward one /ersion 3 ore than that and you are askin# !or troub"e4'

To insta"" the rp   as root:

```
rpm -ivh ntop*
```

Then, copy the sa p"e con!i# to the "ocation o! the rea" con!i#:

```
cp /etc/ntop.conf/sample /etc/ntop.conf
```

5dit the ntop'con! !i"e'

6! ntop is not capturin# packets and is 7ust bein# used as a net!"ow co""ector, chan#e the inter!ace "istened on to none' . et!"ow on"y co""ection can he"p show the network tra!!ic patterns when taps or spans aren8t he"pin# or a/ai"ab"e' 9ust copy the "ine : ;) «inter!ace none= and paste it in, then re o/e the : ;)= that co   ents out the "ine:

```
--interface none
```

. e$t, chan#e the :< "oca" subnets= to inc"ude the network addresses that ntop shou"d re#ard as "oca"' This e$a p"e inc"udes the 10'$'$'$ network and u"ticast tra!!ic as "oca":

```
-m 10.0.0.0/8,224.0.0.0/4
```

This shou"d be a"" the chan#es needed to the con!i# !i"e' &heck the con!i# thorou#h"y to ake sure it re!"ects the en/iron ent'

1e!ore runnin# ntop, setup the ntop ad in user password' This password wi"" be used !or the web inter!ace' +un the !o""owin# co   and and !o""ow the pro pts:

```
/usr/bin/ntop -P /usr/share/ntop -u ntop -A
```

Docu ent the password' 6nsta""ation and initia" con!i#uration is now co p"ete'

6t is ti e to start ntop 3these co   ands are +edhat>%edora speci!ic and ay not be a/ai"ab"e on other "inu$ /ariants4:

```
/etc/init.d/ntop start
```

or

```
service ntop start
```

. e$t, ake sure ntop starts at boot 3these co   ands are +edhat>%edora speci!ic and ay not be a/ai"ab"e on other "inu$ /ariants4:

```
chkconfig ntop on
```

6! this succeeds, ntop is insta""ed and runnin# correct"y' &heck to see i! the ntop web pa#e is bein# ser/ed' -se a web browser to #o to the ntop ser/er8s ip address or hostna e and append port 3000 3i! the port the webser/er is "istenin# is not 3000 in the con!i#uration !i"e, use the new port instead4:

```
http://ntop.domain.local:3000
```

!

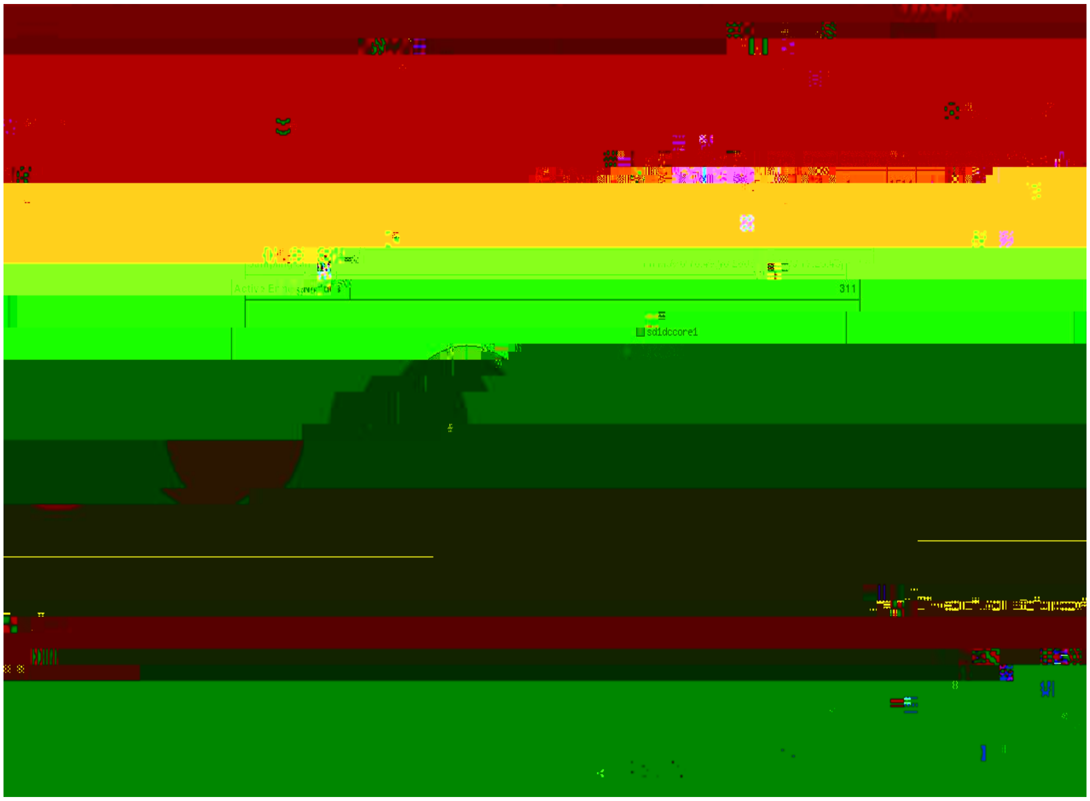
To con!i#ure ntop and net!"ow co""ection, use a web browser 3!ire!o$ works4 and connect to the ntop ser/er:

```
http://ntop.domain.local:3000
```

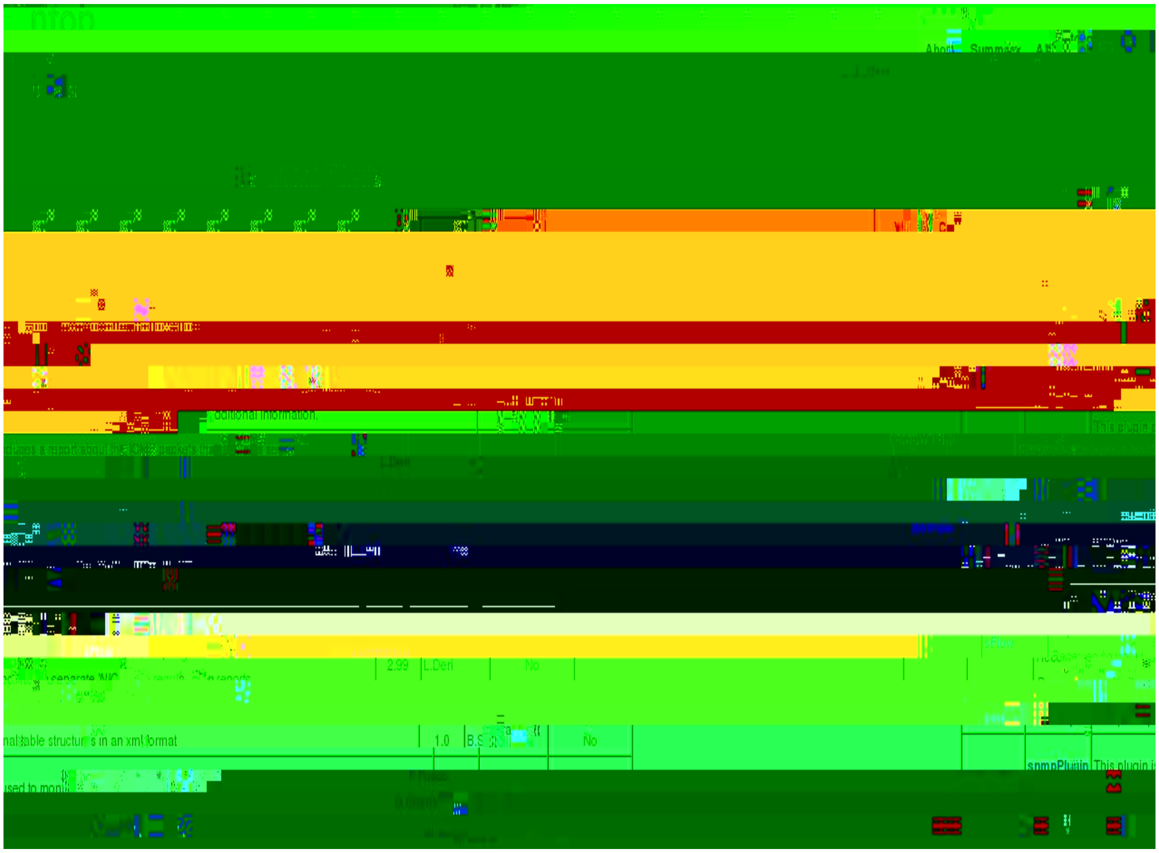
As a pd!, this docu ent inc"udes pictures that wi"" ake it easier to understand than the te$t !i"e /ersion'

&"ick Ad in: p"u#ins 3type in the web ad in password4'

Ad in<p"u#ins



This shou"d disp"ay the p"u#in pa#e shown be"ow:



Then, in the co"u   n "abe"ed :acti/e c"ick to to##"e= where it   eets the net!"ow row 3where the second :yes= is in the !i#ure abo/e4< c"ick the word :no= to to##"e the p"u#in acti/e' The screen shou"d "ook "ike the picture abo/e now and there shou"d be a :?es= in that s@uare'

Then c"ick net!"ow in the con!i#ure co"u   n'

This shou"d disp"ay the !o""owin# screen:

An this screen, add a net!"ow de/ice !or each net!"ow router or switch' &"ick the button "abe"ed :Add . et%"ow De/ice= and then proceed to the !o""owin# instructions'

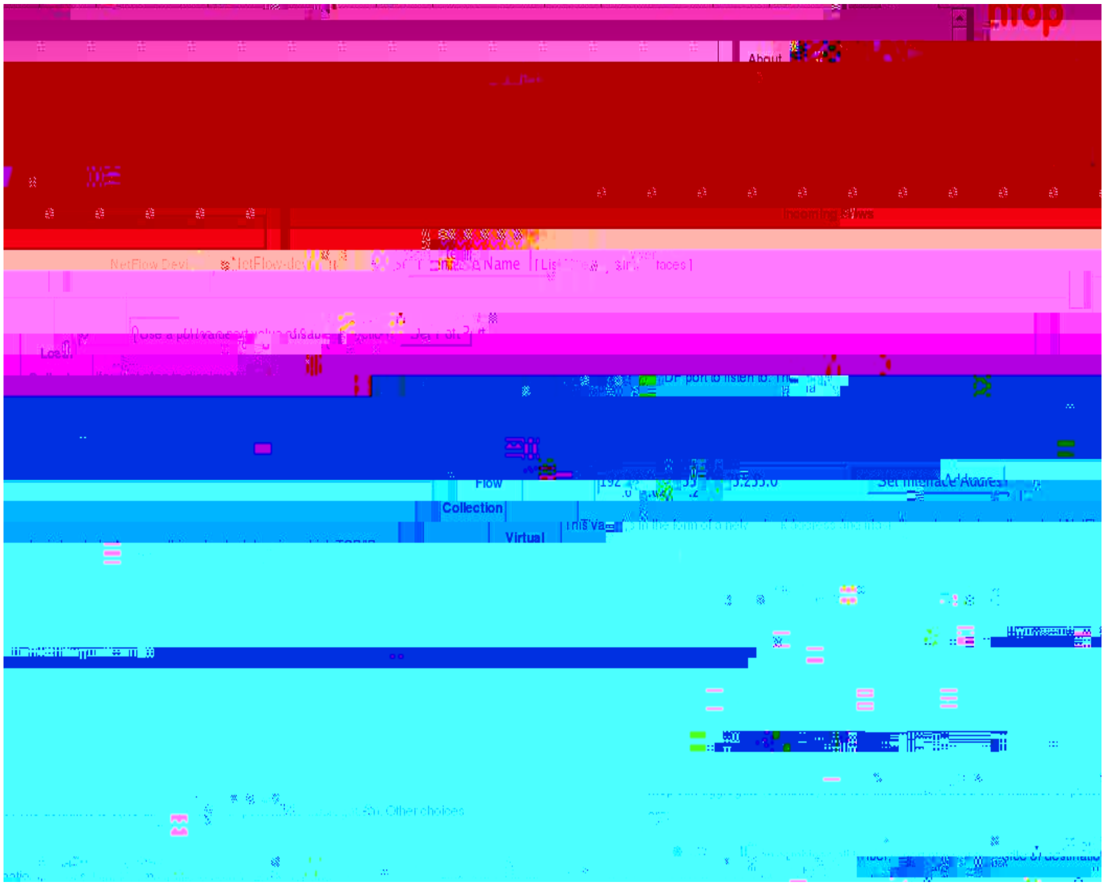
%i"" in the !o""owin# re@uired !ie"ds' A!ter !i""in# in each !ie"d, c"ick the set button !o""owin# that !ie"d' 6! the set button is not c"icked, that settin# wi"" be "ost or not chan#ed' Don8t !or#et to c"ick :set= a!ter each !ie"d' The !o""owin# are the ini u re@uired !ie"ds:

De/ice: any use!u" na e, the hostna e o! the net!"ow switch is reco ended'

Port: 2055 is the nor a" net!"ow port, i! there is on"y one de/ice sendin# !"ows to ntop, use 2055' 6! you are ha/in# u"tip"e de/ices that you want to keep separate, then use a di!!erent port !or each one'

. et!"ow address: use the inter!ace address, or 7ust put in a subnet !or what ntop shou"d re#ard as "oca" 3192'1BC'1'0>2D, 10'0'0'0>C or whate/er4' This ay be redundant with the < in the con!i# !i"e'

The rest o! the settin#s ay need ad7ust ent, but !or a basic net!"ow co""ector, that is a"" that is needed' 5$a p"e o! con!i#urin# net!"ow p"u#in:



" #

&heck &isco8s "atest docu ent !or the speci!ic /ersion 6A0 and hardware that net!"ow wi"" be enab"ed on' 0upE20 * 0%&s are auto atica""y in &5% ode' 1ut to do net!"ow on other hardware such as routers, the e@uip ent wi""" need to be in &5% ode' Fere is a sa p"e o! con!i#uration needed !or a B509 with supE20s:

```
ip flow-cache timeout active 5
ip flow-cache feature-accelerate
mls ip multicast flow-stat-timer 9
mls flow ip full
no mls flow ipv6
ip flow-export version 5
ip flow-export destination 10.10.10.10 2055
mls nde sender version 5
```

This wi"" send !"ows to the ntop co""ector at 10'10'10'10 on port 2055' 6! a subset o! the tra!!ic is a"" that is re@uired, use :   "s !"ow ip)= to disp"ay he"p on speci!yin# subsets 3not subnets4' ?ou can a"so "i   it net!"ow data to data !ro   a certain inter!ace:

```
int vlan 2
 ip route-cache flow
 mls netflow sampling
```

+outer con!i#uration:

An a router the . D5 portion 3network data e$port4 is not needed' &5% howe/er is re@uired !or net!"ow accordin# to docu   entation !or 6A0 12'2 and 12'3' The !o""owin# works on an C31 3and a"so on a 1E504 runnin# 12'2 train 6A0:

```
ip cef
ip flow-cache timeout active 5
ip flow-export version 5
ip flow-export destination 10.10.10.10 2055
```

And then, i! needed, turn net!"ow on the inter!ace desired:

```
int s 0/0:0
ip route-cache flow

int fa 0/0
ip route-cache flow
```

6! tra!!ic is !"owin# throu#h the de/ices, ntop shou"d be reportin# in!or   ation' &heck the webpa#e' 6! you ha/e   u"tip"e net!"ow co""ectors, use the :0witch . 6&= button to /iew the other co""ectors8 statistics'

Confirmation and Troubleshooting

Ance the net!"ow e$port is con!i#ured on the router or switch, test and /eri!y that ntop is seein# !"ows correct"y and that the ser/er is recei/in# the   ' 6! ntop is not showin# any data, /eri!y receipt o! the !"ow on the "inu$ bo$' Assu   in# the net!"ow is #oin# to port 2055, that is the de!au"t net!"ow port, you can use :tcpdu   p= to 7ust show tra!!ic to and !ro   port 2055:

```
tcpdump udp port 2055
```

6! :tcpdu   p= is insta""ed, there shou"d be p"enty o! data !ro   the router or switch' 6! no data is shown, the net!"ow data is not reachin# the "inu$ bo$ to be decoded' 6! you see data in the tcpdu   p output, but nothin# in ntop, the net!"ow p"u#in is probab"y not con!i#ured proper"y, ntop is not runnin# or you ha/e an iptab"es>!irewa"" b"ockin# the tra!!ic'

To check to see i! ntop is runnin#:

```
service ntop status
```

Then, ake sure it is "istenin# on the correct port :

```
netstat -an | grep 2055
```

Oubstitute any port you are sendin# to in p"ace o! 2055' 6t is beyond the scope o! this docu ent to troub"eshoot iptab"es, but as a @uick test disab"e the !irewa"" i! the security situation per its:

```
service iptables stop
```

or

```
/etc/init.d/iptables stop
```

Performance notes:

* onitorin# #i#abit networks with ntop 3or onitorin# on routers that are a"ready cpu ta$ed4 can cause per!or ance issues on the network de/ice and on the "inu$ bo$' 6! you don8t per!or ance base"ine your network e@uip ent, it is a #ood idea to do so' Fere are so e easy steps to base"ine 7ust !or the i pact o! ntop'

+un an app"ication to easure per!or ance "ike :top= on the "inu$ bo$ be!ore you turn on ntop and a#ain a!ter you turn it on' * ake so e notes so you ha/e a base"ine !or be!ore and a!ter' ?ou can cause so e &P - "oad on a bo$ with too uch net!"ow data #oin# to it'

Likewise do a Gshow proc cpu histG or :show proc= on the router 3or si i"ar4 be!ore and a!ter turnin# net!"ow on' * ake notes' Oendin# the net!"ow data takes a certain a ount o! &P - power and bandwidth, so base"ine per!or ance be!ore and a!ter startin# it' 6#nore these instructions i! there a"ready is a base"ine !or per!or ance o! the network e@uip ent and "inu$ bo$es'

6! ntop is usin# up too uch ra and !ai"in#, which can happen when onitorin# "ar#e networks or too any hosts 3"ike keepin# track o! a"" internet connections4, then tune the tracked hosts down by "i itin# trackin# to "oca" hosts 3you can inc"ude non<"oca" hosts in the "oca" hosts state ent to continue trackin# interestin# ip addresses4'

6n >etc>ntop'con! unco ent the "ine:

```
--track-local-hosts
```

Conclusion

Fope!u""y this #uide he"ps i p"e entation o! net!"ow co""ection !ro &isco 6A0 based products' . et!"ow can be an e$ce""ent too" !or c"assi!yin# and pro!i"in# networks' . top can he"p ake sense o! the net!"ow data, which can ake troub"eshootin# and ad inistration o! a network easier'