Lesson Module Status

- Slides – draft
- Properties - done
- Flashcards – I wish
- 1st minute quiz – NA
- Web Calendar summary – done
- Web book pages –
- Commands –
- Howtos –
- Skills pacing - NA
- Lab – done
- Depot (VMs) – NA

Tim Childers - guest speaker on LDAP at 6:30PM

Course history and credits

Jim Griffin

- Jim created the original version of this course
- Jim's site: http://cabrillo.edu/~jgriffin/

Rick Graziani

- Thanks to Rick Graziani for the use of some of his great network slides
- Rick's site: http://cabrillo.edu/~rgraziani/

Joe A.

Joe P.

Teach & Confer is a live interactive classroom to meet with your students.

www.cccconfer.org
dial-in: 888-886-3951
passcode: 439080

John

Junious

Robert

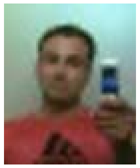
Kay

Chuck

Lieven

Rich

Jesus



Josh

Edgar

Joe B.

Casady

Chris H.

Edwin

Julio

Jack

Brynden

Ryan

VMs for tonight

(Revert, 384MB RAM and Power up)

Celebrian

Email me (risimms@cabrillo.edu) a relatively current photo of your face for 3 points extra credit

No more quizzes!

Management tools and utilities

Objectives	Agenda
• Identify, isolate, and correct malfunctions in a computer network.	• Questions on previous material • Housekeeping • T3 review • Troubleshooting exercise • LDAP - guest speaker Tim Childers • Various tools • Prepping for the final • Lab and final prep workshop • Wrap

Questions on previous material

Questions?

- Previous lesson material
- Lab assignment

Housekeeping

The Final - Thursday, June 3

Is there **anyone** who cannot take the final at our usual class time (which starts at 5:30pm)?

- Any conflicts with finals in another class?

Note, according to the college schedule, our final exam is supposed to take place from 4-6:50pm!

Unless there is a conflict with another class ***I'd like to propose we start the final instead at 5:30pm*** *which is our normal class starting time. Plan for three hours but if you need extra time you may stay longer.*

Extra credit labs are due midnight June 3

Five forum posts are due midnight June 3

Test 3 Results

Test 3 Results

Questions missed on test:

```
 1
 2 xxxx
 3 xxxx
 4
 5 xxx
 6 xxxx
 7
 8 xxxx
 9 xxxx
10
11
12 xxxxx
13
14 x
15 xxxxxxx
16 xxxxx
17 xx
18 xxxxxx
```

Q2. What is the difference between an iterative DNS query and a recursive DNS query? How could you demonstrate the type of queries (recursive or iterative) done by a DNS client (the resolver) vs. the type of queries done by a DNS server using our class VM's?

Difference: *Iterative queries request the "best" answer, the response may be a referral to another name server. Recursive queries request "final" answers only.*

Demonstrate by: *Setting up one VM as a DNS server and another as a DNS client using the first VM as it's nameserver (in /etc/resolv.conf). Monitor outgoing DNS queries for (hopefully not cached) hostnames with Wireshark from both VMs.*

Examine the "Recursion Desired" flag in a Wireshark capture of the DNS query or just observer whether or not iterative queries are taking place.

The DNS client will make recursive queries and the DNS server will make non-recursive (iterative) queries.

Q3. Locate the “.” zone file on Hershey used by the installed DNS software. Look for the root server operated by IANA. What is the fully qualified domain name and IP address of that root server according to Hershey’s zone file?

FQDN: *L.ROOT-SERVERS.NET.*
IP Address: *198.32.64.12*

Partial credit if you were "close" (m or k server)

From /etc/named.conf on Hershey:

```
zone "." IN {
        type hint;
        file "named.ca";
};
```

From /var/named/named.ca on Hershey:

```
;
; operated by IANA
;
.                       3600000      NS     L.ROOT-SERVERS.NET.
L.ROOT-SERVERS.NET.     3600000      A      198.32.64.12
;
; housed in Japan, operated by WIDE
;
.                       3600000      NS     M.ROOT-SERVERS.NET.
M.ROOT-SERVERS.NET.     3600000      A      202.12.27.33
; End of File
```

Q5. Which exported directory on Hershey has access restricted to the systems in room 2501 (172.30.1.0/24)?

/backup/centos

```
[rsimms@hershey rsimms]$ /usr/sbin/showmount -e localhost
Export list for localhost:
/home          *
/install/rh    *
/install/suse  *
/install/rhel  *
/backup/centos 172.30.1.0/255.255.255.0
[rsimms@hershey rsimms]$
```

*Use **showmount -e hershey** on Hershey or one of your Linux VMs to list exported directories*

Q6. A firewall was inadvertently clobbered on a CentOS (Red Hat) system preventing remote access to the CUPS service. It now has only the following:

```
[root@arwen ~]# iptables -nL RH-Firewall-1-INPUT --line-numbers
Chain RH-Firewall-1-INPUT (2 references)
num  target     prot opt source          destination
1    ACCEPT     all  --  0.0.0.0/0       0.0.0.0/0
2    ACCEPT     icmp --  0.0.0.0/0       0.0.0.0/0       icmp type 255
3    ACCEPT     esp  --  0.0.0.0/0       0.0.0.0/0
4    ACCEPT     ah   --  0.0.0.0/0       0.0.0.0/0
5    ACCEPT     udp  --  0.0.0.0/0       224.0.0.251     udp dpt:5353
6    ACCEPT     all  --  0.0.0.0/0       0.0.0.0/0       state RELATED,ESTABLISHED
7    ACCEPT     tcp  --  0.0.0.0/0       0.0.0.0/0       state NEW tcp dpt:22
8    REJECT     all  --  0.0.0.0/0       0.0.0.0/0       reject-with icmp-host-prohibited
[root@arwen ~]#
```

What complete iptables command(s) would insert the necessary rules for remote access to the CUPS service?

iptables -I RH-Firewall-1-INPUT 6 -p udp -m udp --dport 631 -j ACCEPT
iptables -I RH-Firewall-1-INPUT 6 -p tcp -m tcp --dport 631 -j ACCEPT

Tip: Look at the output of ***cat /etc/sysconfig/iptables*** *on any of the CentOS VMs*

Note: Be sure and use the I (insert) rather than A (append). Appending a new rule would be ineffective. The rule on line 8 will reject any packet. Any rules (appended) after line 8 would be ignored.

```
[root@elrond ~]# cat /etc/sysconfig/iptables
# Generated by iptables-save v1.3.5 on Sun May 17 14:13:55 2009
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [237:32096]
:RH-Firewall-1-INPUT - [0:0]
-A INPUT -j RH-Firewall-1-INPUT
-A FORWARD -j RH-Firewall-1-INPUT
-A RH-Firewall-1-INPUT -i lo -j ACCEPT
-A RH-Firewall-1-INPUT -p icmp -m icmp --icmp-type any -j ACCEPT
-A RH-Firewall-1-INPUT -p esp -j ACCEPT
-A RH-Firewall-1-INPUT -p ah -j ACCEPT
-A RH-Firewall-1-INPUT -d 224.0.0.251 -p udp -m udp --dport 5353 -j ACCEPT
-A RH-Firewall-1-INPUT -p udp -m udp --dport 631 -j ACCEPT
-A RH-Firewall-1-INPUT -p tcp -m tcp --dport 631 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A RH-Firewall-1-INPUT -p udp -m state --state NEW -m udp --dport 53 -j ACCEPT
-A RH-Firewall-1-INPUT -p tcp -m state --state NEW -m tcp --dport 80 -j ACCEPT
-A RH-Firewall-1-INPUT -p tcp -m state --state NEW -m tcp --dport 21 -j ACCEPT
-A RH-Firewall-1-INPUT -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A RH-Firewall-1-INPUT -j REJECT --reject-with icmp-host-prohibited
COMMIT
# Completed on Sun May 17 14:13:55 2009
[root@elrond ~]#
```

Q8. What is the name of the printer being shared by the Samba service on Hershey?

hpdesk, lazer

```
[rsimms@hershey rsimms]$ smbclient -L localhost
added interface ip=172.30.1.20 bcast=172.30.1.255 nmask=255.255.255.0
added interface ip=172.30.4.20 bcast=172.30.4.255 nmask=255.255.255.0
Password:
Anonymous login successful
Domain=[WORKGROUP] OS=[Unix] Server=[Samba 2.2.7a]

        Sharename      Type      Comment
        ---------      ----      -------
        depot          Disk      Public files on Hershey
        IPC$           IPC       IPC Service (Most Cool Samba Server)
        ADMIN$         Disk      IPC Service (Most Cool Samba Server)
        hpdesk         Printer
        lazer          Printer

        Server               Comment
        ---------            -------
        CIS-SERVER           Buffalo NAS server
        DV2000
        HERSHEY              Most Cool Samba Server

        Workgroup            Master
        ---------            -------
        CIS-MUD              STATION09
        TOLKIEN              SNICKERS
        WORKGROUP            HERSHEY
[rsimms@hershey rsimms]$
```

Q9. Your organization has decided to set SELinux to enforcing mode on all systems. This caused access problems to the Samba docs share on a system named Celebrian. Users can no longer access the share with SELinux set to enforcing mode. You review the share information and see the following:

From smb.conf:

```
[docs]
     comment = Public documents
     path = /var/shares/docs
     guest ok = Yes
```

Need to change this context type for this directory to be shared by Samba

A long lising of the directory being shared:

```
[root@celebrian var]# ls -ldZ shares/docs
drwxr-xr-x  cis192 users root:object_r:var_t             shares/docs
```

What single command would fix this problem so users could again access the share with SELinux set to enforcing mode?

*chcon -R -t samba_share_t /var/shares/docs/**

(see Lab 8 or Lesson 11 for sharing directories using Samba)

Q12. On Hershey what file would you edit and what line number would you modify to reconfigure sendmail to use a different alias file? (You can assume the make would be done and the service restarted after your changes were made)

File to edit (use absolute filename): */etc/mail/sendmail.mc*
Line number to modify: *26 which is define(`ALIAS_FILE', `/etc/aliases')dnl*

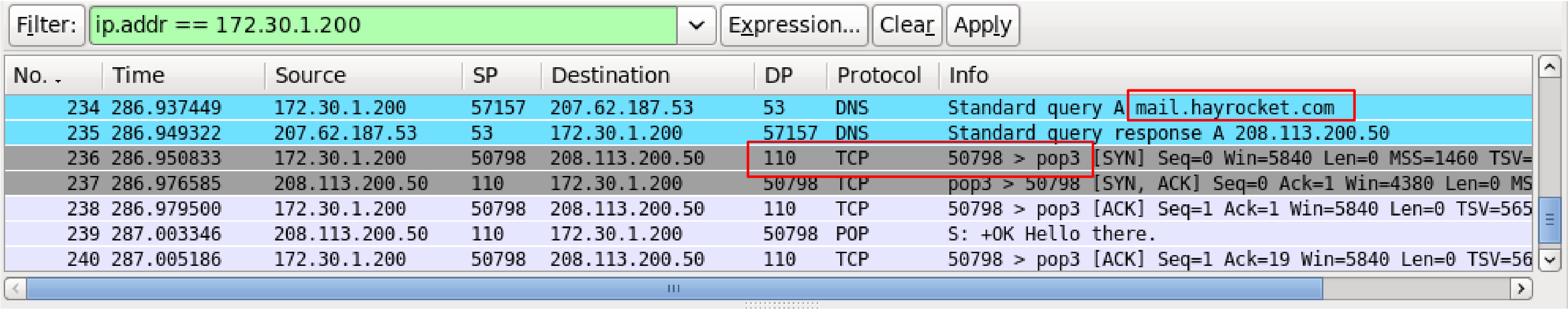
```
[rich@hershey rich]$ cat /etc/mail/sendmail.mc | grep -n  /etc/aliases
26:define(`ALIAS_FILE', `/etc/aliases')dnl
[rich@hershey rich]$
```

Q15. What are the two NIS maps on Hershey that hold the domain wide hosts information (hostname-IP pairs) for the cis-mud.net domain? (give the absolute filenames)

/var/yp/cismud.net/hosts.byaddr
/var/yp/cismud.net/hosts.byname

```
[rsimms@hershey rsimms]$ ls /var/yp
binding      hosts.00   nicknames  shadow      yp.conf
cismud.net   Makefile   passwd     shadow--    ypserv.conf
hosts        Makefile-  passwd--   shadow.OLD  ypservers
[rsimms@hershey rsimms]$ ls /var/yp/cismud.net/
group.bygid   hosts.byname   protocols.byname    services.byservicename
group.byname  passwd.byname  protocols.bynumber  ypservers
hosts.byaddr  passwd.byuid   services.byname
[rsimms@hershey rsimms]$
```

Q16. (2 point) What command was typed on Elrond (172.30.1.200) that resulted in this Wireshark capture?



Filter: ip.addr == 172.30.1.200

No.	Time	Source	SP	Destination	DP	Protocol	Info
234	286.937449	172.30.1.200	57157	207.62.187.53	53	DNS	Standard query A mail.hayrocket.com
235	286.949322	207.62.187.53	53	172.30.1.200	57157	DNS	Standard query response A 208.113.200.50
236	286.950833	172.30.1.200	50798	208.113.200.50	110	TCP	50798 > pop3 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 TSV=
237	286.976585	208.113.200.50	110	172.30.1.200	50798	TCP	pop3 > 50798 [SYN, ACK] Seq=0 Ack=1 Win=4380 Len=0 MS
238	286.979500	172.30.1.200	50798	208.113.200.50	110	TCP	50798 > pop3 [ACK] Seq=1 Ack=1 Win=5840 Len=0 TSV=565
239	287.003346	208.113.200.50	110	172.30.1.200	50798	POP	S: +OK Hello there.
240	287.005186	172.30.1.200	50798	208.113.200.50	110	TCP	50798 > pop3 [ACK] Seq=1 Ack=19 Win=5840 Len=0 TSV=56

telnet mail.hayrocket.com 110

Using telnet to dialog with a POP server

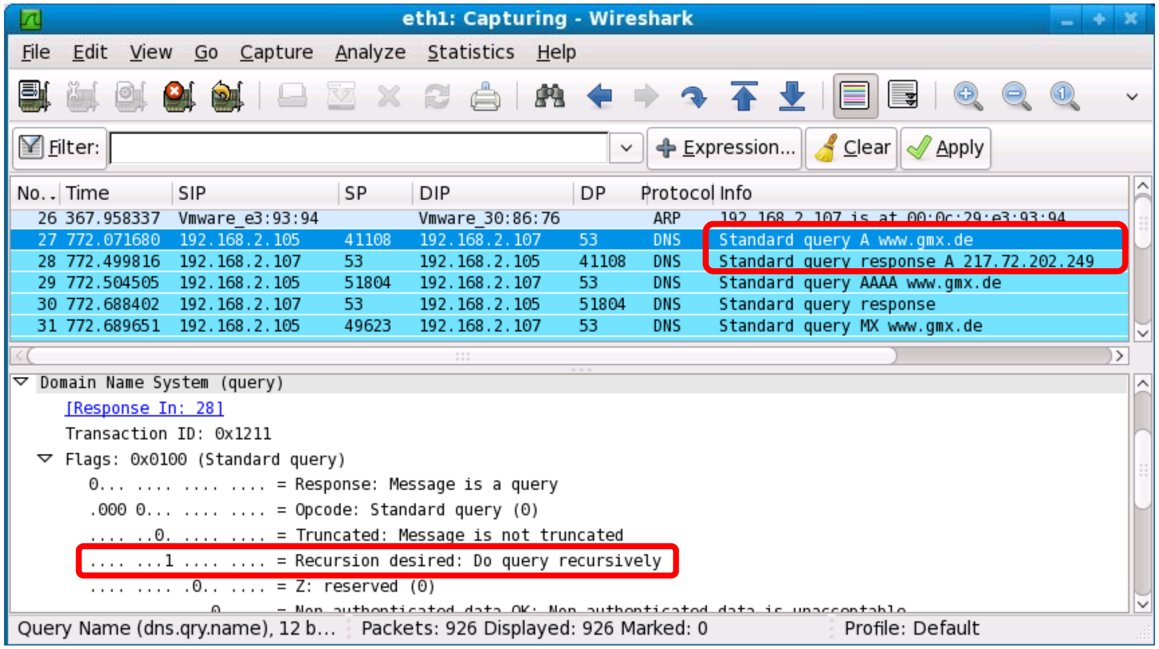
Note that initial DNS queries which indicates a hostname rather than a IP address was used for the command

Q17. (1 point) On a CentOS 5.4 system what type of DNS queries are used by the client resolver when attempting to resolve hostnames into IP addresses? (circle one)

a) Iterative
[✓ b) Recursive]
c) Ad-hoc
d) Wildcard

Use Q2 to demonstrate to yourself that this is what happens.

*The **DNS client** resolver does a recursive query to the name server for www.gmx.de. The response immediately follows with the IP address "answer"*



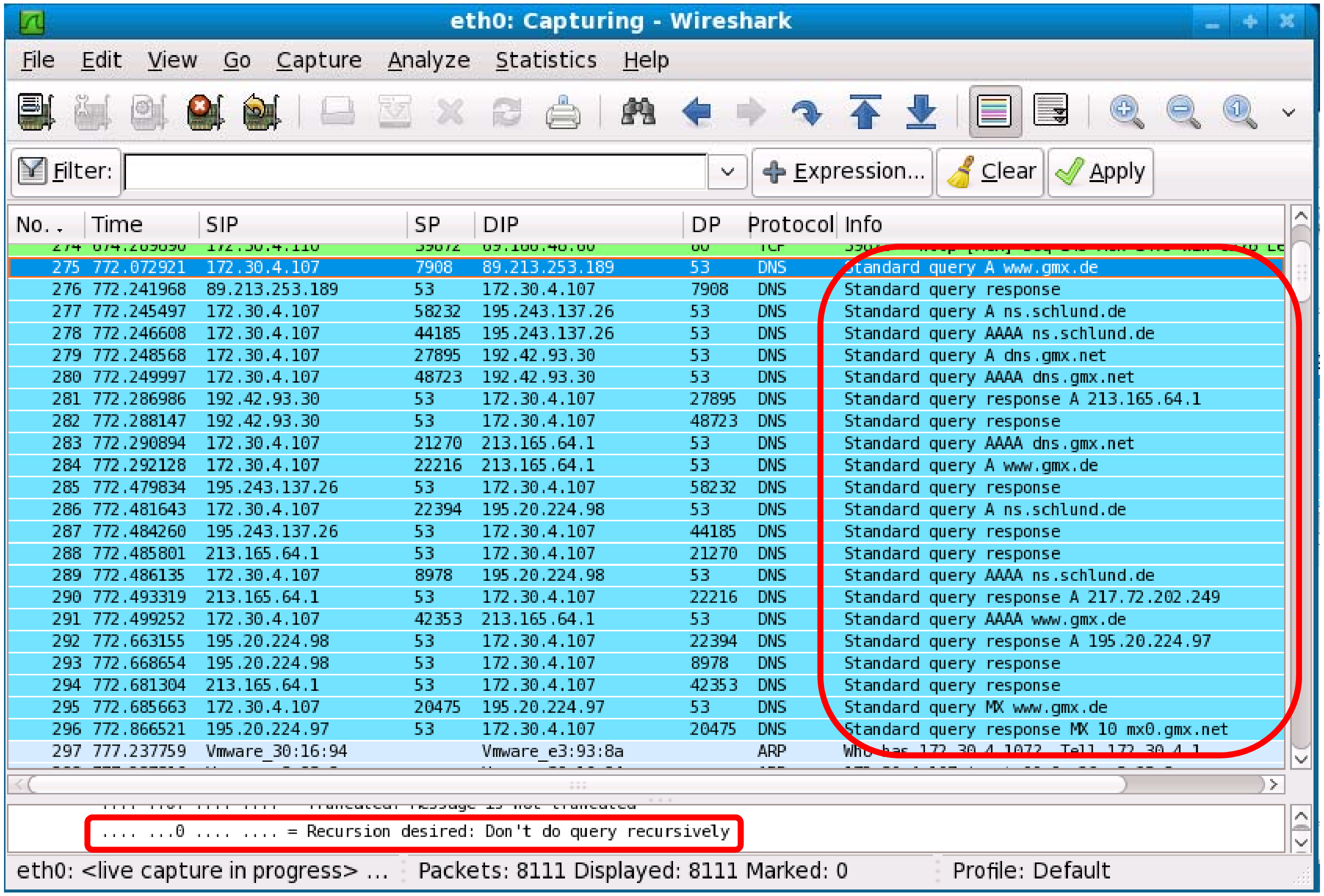
```
No..  Time        SIP              SP     DIP              DP     Protocol Info
  26 367.958337  Vmware_e3:93:94         Vmware_30:86:76         ARP      192.168.2.107 is at 00:0c:29:e3:93:94
  27 772.071680  192.168.2.105    41108  192.168.2.107    53     DNS      Standard query A www.gmx.de
  28 772.499816  192.168.2.107    53     192.168.2.105    41108  DNS      Standard query response A 217.72.202.249
  29 772.504505  192.168.2.105    51804  192.168.2.107    53     DNS      Standard query AAAA www.gmx.de
  30 772.688402  192.168.2.107    53     192.168.2.105    51804  DNS      Standard query response
  31 772.689651  192.168.2.105    49623  192.168.2.107    53     DNS      Standard query MX www.gmx.de
```

```
▽ Domain Name System (query)
    [Response In: 28]
    Transaction ID: 0x1211
  ▽ Flags: 0x0100 (Standard query)
      0... .... .... .... = Response: Message is a query
      .000 0... .... .... = Opcode: Standard query (0)
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... .0.. .... = Z: reserved (0)
      .... .... ...0 .... = Non-authenticated data OK: Non-authenticated data is unacceptable
```

Query Name (dns.qry.name), 12 b... Packets: 926 Displayed: 926 Marked: 0 Profile: Default

Q17. (continued)

*The **DNS server** makes iterative queries to resolve www.gmx.de which involves talking to some intermediate "best answer" referrals*



eth0: Capturing - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply

```
No. .  Time        SIP               SP     DIP              DP     Protocol Info
274 674.269690  172.30.4.110      39072  69.160.46.60     80     TCP
275 772.072921  172.30.4.107      7908   89.213.253.189   53     DNS   Standard query A www.gmx.de
276 772.241968  89.213.253.189    53     172.30.4.107     7908   DNS   Standard query response
277 772.245497  172.30.4.107      58232  195.243.137.26   53     DNS   Standard query A ns.schlund.de
278 772.246608  172.30.4.107      44185  195.243.137.26   53     DNS   Standard query AAAA ns.schlund.de
279 772.248568  172.30.4.107      27895  192.42.93.30     53     DNS   Standard query A dns.gmx.net
280 772.249997  172.30.4.107      48723  192.42.93.30     53     DNS   Standard query AAAA dns.gmx.net
281 772.286986  192.42.93.30      53     172.30.4.107     27895  DNS   Standard query response A 213.165.64.1
282 772.288147  192.42.93.30      53     172.30.4.107     48723  DNS   Standard query response
283 772.290894  172.30.4.107      21270  213.165.64.1     53     DNS   Standard query AAAA dns.gmx.net
284 772.292128  172.30.4.107      22216  213.165.64.1     53     DNS   Standard query A www.gmx.de
285 772.479834  195.243.137.26    53     172.30.4.107     58232  DNS   Standard query response
286 772.481643  172.30.4.107      22394  195.20.224.98    53     DNS   Standard query A ns.schlund.de
287 772.484260  195.243.137.26    53     172.30.4.107     44185  DNS   Standard query response
288 772.485801  213.165.64.1      53     172.30.4.107     21270  DNS   Standard query response
289 772.486135  172.30.4.107      8978   195.20.224.98    53     DNS   Standard query AAAA ns.schlund.de
290 772.493319  213.165.64.1      53     172.30.4.107     22216  DNS   Standard query response A 217.72.202.249
291 772.499252  172.30.4.107      42353  213.165.64.1     53     DNS   Standard query AAAA www.gmx.de
292 772.663155  195.20.224.98     53     172.30.4.107     22394  DNS   Standard query response A 195.20.224.97
293 772.668654  195.20.224.98     53     172.30.4.107     8978   DNS   Standard query response
294 772.681304  213.165.64.1      53     172.30.4.107     42353  DNS   Standard query response
295 772.685663  172.30.4.107      20475  195.20.224.97    53     DNS   Standard query MX www.gmx.de
296 772.866521  195.20.224.97     53     172.30.4.107     20475  DNS   Standard query response MX 10 mx0.gmx.net
297 777.237759  Vmware_30:16:94          Vmware_e3:93:8a         ARP   Who has 172.30.4.107?  Tell 172.30.4.1
```

```
.... ...0 .... .... = Recursion desired: Don't do query recursively
```

```
eth0: <live capture in progress> ...   Packets: 8111 Displayed: 8111 Marked: 0   Profile: Default
```

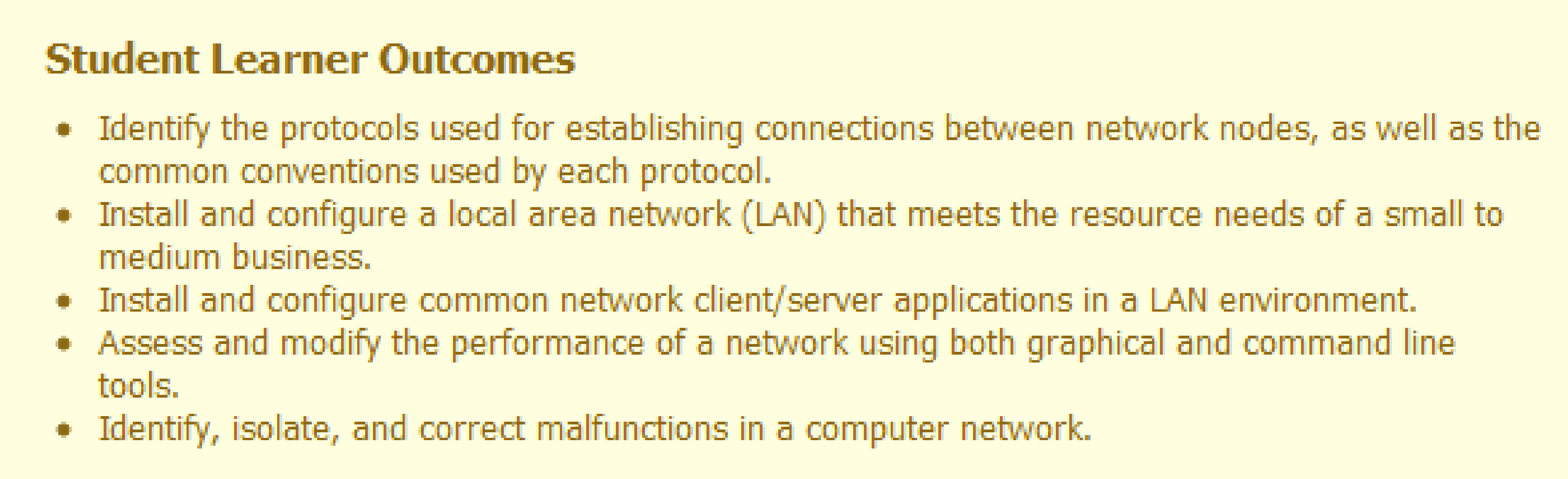
Q18. By examining the email message headers, fill in the blanks below:

Name of computer used to create the message: *shrekster*
IP Address of the computer used to create the message: *63.249.103.10*
MUA that created the email (name of product): *Outlook Express*
MTA that sent the email (fully qualified hostname): *mail.cruzio.com*

```
Return-Path: <dog@mystery.com>
X-Original-To: rich@hayrocket.com
Delivered-To: rsimms@spaceymail-mx1.g.dreamhost.com
Received: from mail.cruzio.com (mail.cruzio.com [63.249.95.37])
    by spaceymail-mx1.g.dreamhost.com (Postfix) with ESMTP id 58307CE77F
    for <rich@hayrocket.com>; Sat, 16 May 2009 20:51:06 -0700 (PDT)
Received: from shrekster (dsl-63-249-103-107.dhcp.cruzio.com [63.249.103.107])
    by mail.cruzio.com with SMTP id n4H3p3CI050144
    for <rich@hayrocket.com>; Sat, 16 May 2009 20:51:05 -0700 (PDT)
Message-ID: <03C11112625C44FEAC1FB1033FF9A951@shrekster>
From: "Mystery Dog" <dog@mystery.com>
To: <rich@hayrocket.com>
Subject: Who am I
Date: Sat, 16 May 2009 20:51:03 -0700
MIME-Version: 1.0
Content-Type: multipart/alternative;
    boundary="----=_NextPart_000_0006_01C9D668.06DF9A70"
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 6.00.2900.5512
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2900.5579
```

SLO Assessments

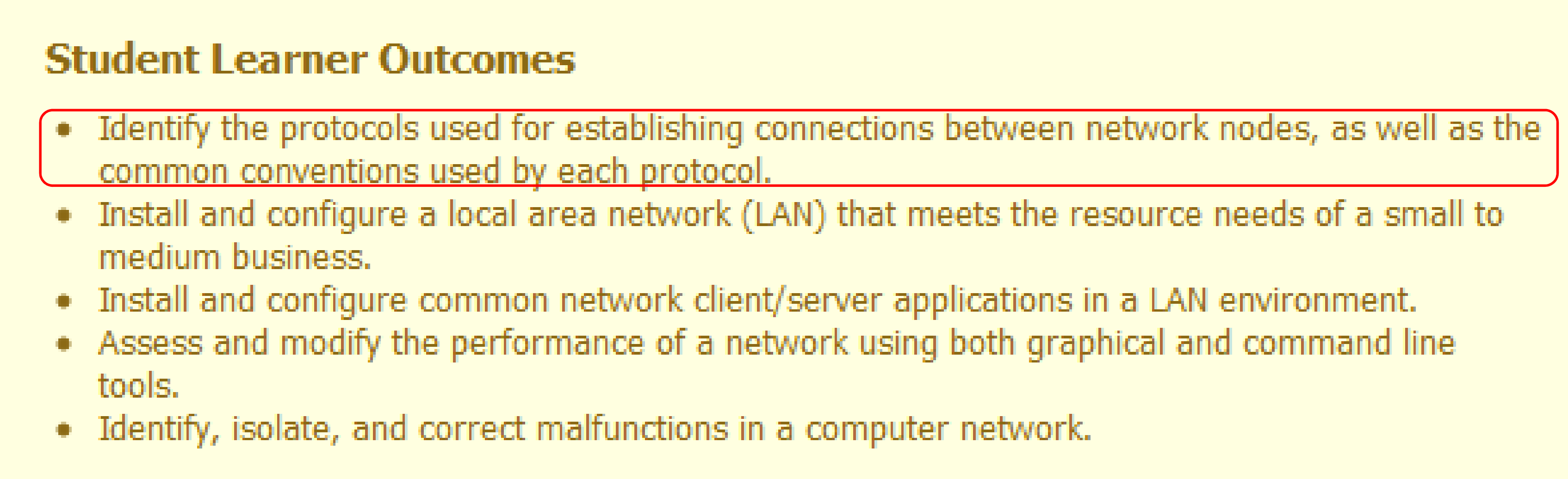
http://simms-teach.com/cis192home.php



Student Learner Outcomes

- Identify the protocols used for establishing connections between network nodes, as well as the common conventions used by each protocol.
- Install and configure a local area network (LAN) that meets the resource needs of a small to medium business.
- Install and configure common network client/server applications in a LAN environment.
- Assess and modify the performance of a network using both graphical and command line tools.
- Identify, isolate, and correct malfunctions in a computer network.

http://simms-teach.com/cis192home.php



Student Learner Outcomes

- Identify the protocols used for establishing connections between network nodes, as well as the common conventions used by each protocol.
- Install and configure a local area network (LAN) that meets the resource needs of a small to medium business.
- Install and configure common network client/server applications in a LAN environment.
- Assess and modify the performance of a network using both graphical and command line tools.
- Identify, isolate, and correct malfunctions in a computer network.

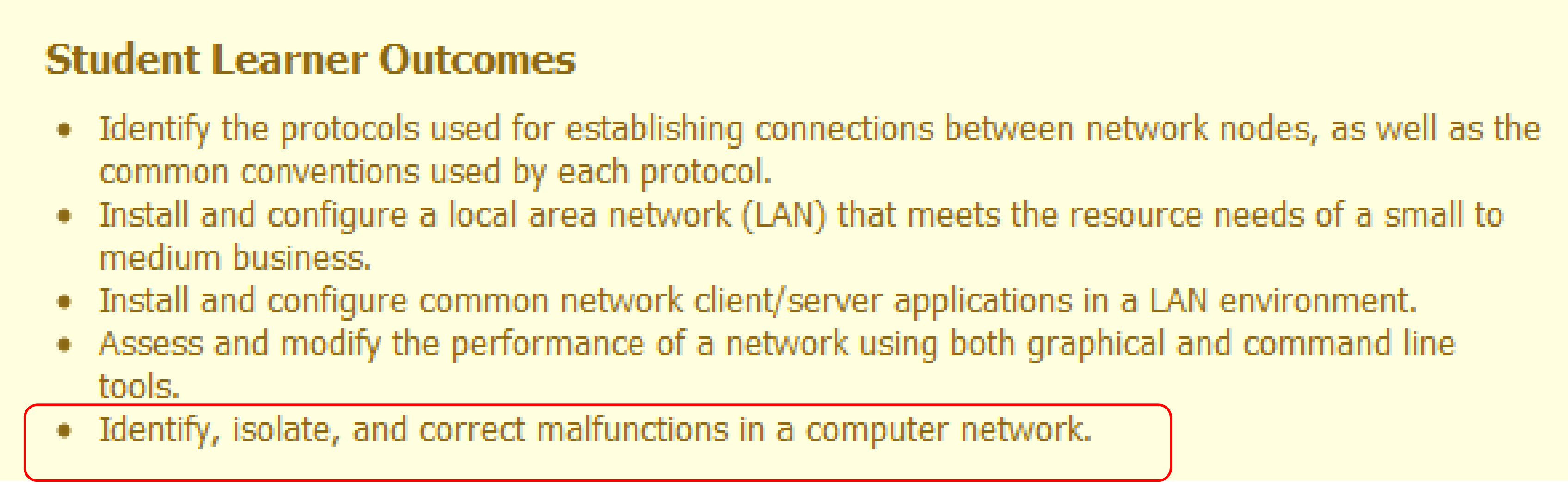
Protocols Assessment

SLO: Identify the protocols used for establishing connections between network nodes, as well as the common conventions used by each protocol.

Please browse to the following link and take the anonymous survey:

http://www.surveymonkey.com/s/X9SJQYV

http://simms-teach.com/cis192home.php



Student Learner Outcomes

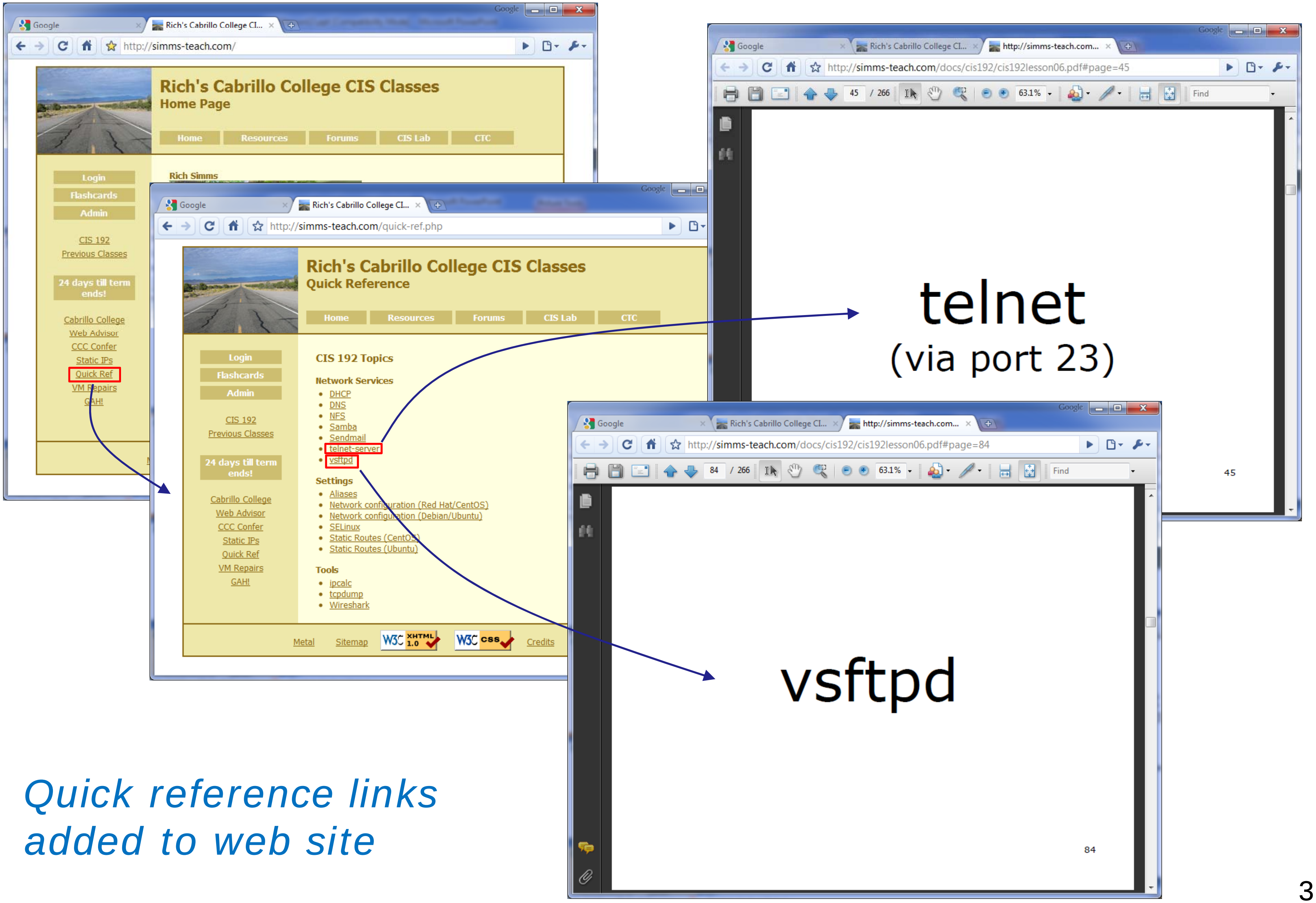
- Identify the protocols used for establishing connections between network nodes, as well as the common conventions used by each protocol.
- Install and configure a local area network (LAN) that meets the resource needs of a small to medium business.
- Install and configure common network client/server applications in a LAN environment.
- Assess and modify the performance of a network using both graphical and command line tools.
- Identify, isolate, and correct malfunctions in a computer network.

SLO: Identify, isolate, and correct malfunctions in a computer network

***The problem**: The FTP and Telnet services on Celebrian are no longer are available and customers are getting very irritated.*

***History**: The server went down during a power failure. However after the server was started up again both the Telnet and FTP services no longer are working.*

***Situation**: The original administrator who configured the server has left the company. As a consultant you have just signed a Professional Services Agreement get both these services back online.*



http://simms-teach.com/

Rich's Cabrillo College CIS Classes
Home Page

Rich Simms

http://simms-teach.com/quick-ref.php

Rich's Cabrillo College CIS Classes
Quick Reference

CIS 192 Topics

Network Services

- DHCP
- DNS
- NFS
- Samba
- Sendmail
- telnet-server
- vsftpd

Settings

- Aliases
- Network configuration (Red Hat/CentOS)
- Network configuration (Debian/Ubuntu)
- SELinux
- Static Routes (CentOS)
- Static Routes (Ubuntu)

Tools

- ipcalc
- tcpdump
- Wireshark

http://simms-teach.com/docs/cis192/cis192lesson06.pdf#page=45

telnet
(via port 23)

45

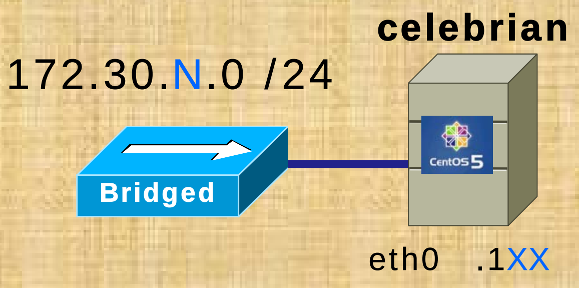
http://simms-teach.com/docs/cis192/cis192lesson06.pdf#page=84

vsftpd

84

Quick reference links added to web site

Troubleshooting Assessment



.1XX is based on your station number and the IP Table
N=1 for the classroom and N=4 for the CIS lab or CTC
http://simms-teach.com/docs/static-ip-addrs.pdf

- Revert and power-up Celebrian
- Cable as shown
- Use **dhclient eth0** for an initial IP address
- **scp *logname*@opus.cabrillo.edu:/home/cis192/scripts/down* .**
- **chmod 700 download-scripts-packages** (use tab complete)
- **./download-scripts-packages** (and download everything)
- **cd bin**
- **./do-act13A-celebrian**
- Repair the problem(s) and get the Telnet and FTP services back online
- Verify your fix by accessing these services from another VM

LDAP

Lightweight Directory Access Protocol (LDAP)

- NIS is the historical solution for synchronizing files on the network and enabling a common login mechanism.
- NIS is easy to setup and administer however it does not scale up well (domains cannot be linked) and is only minimally secure.
- Microsoft uses LDAP as part of their Active Directory solution.
- Sites today are migrating to LDAP which enables a common solution across Windows, Linux and UNIX.
- Besides sharing files and printers, Samba can be configured as a Domain Controller to fit within an Active Directory environment.
- Tim Childers has set up a reference implementation of LDAP and Samba on the System Pod in 2504. Centralized user account information allows domain logins from both Windows and Linux.

LDAP
Guest Speaker

Tim Childers
Intel Corporation
(and previous Cabrillo College student)

NSM
Tools

Troubleshooting Tools

Applications and Ports	telnet *app-port* (Lesson 13) netstat -utln (Lesson 5)
Routes and Connectivity	traceroute *ip-addr* or mtr *ip-addr* (Lesson 2) route -n (Lesson 3) ping *ip-addr* (Lesson 1)
Connection	arp -a (Lesson 2) ifconfig (Lesson 1)

Basic troubleshooting tools we have been using in this course

Monitoring Tools

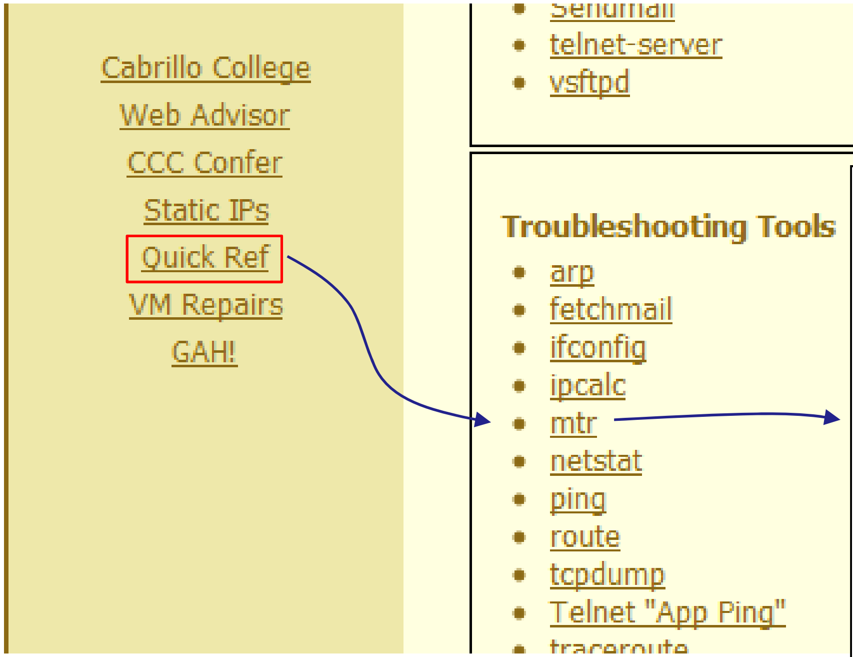
wireshark - graphical packet sniffer (Lesson 2)

tcpdump - text based packet sniffer (Lesson 2)

arpwatch - collect IP MAC pairs (Lesson 2)

Packet and ARP level monitoring

Troubleshooting and Monitoring Tool Examples

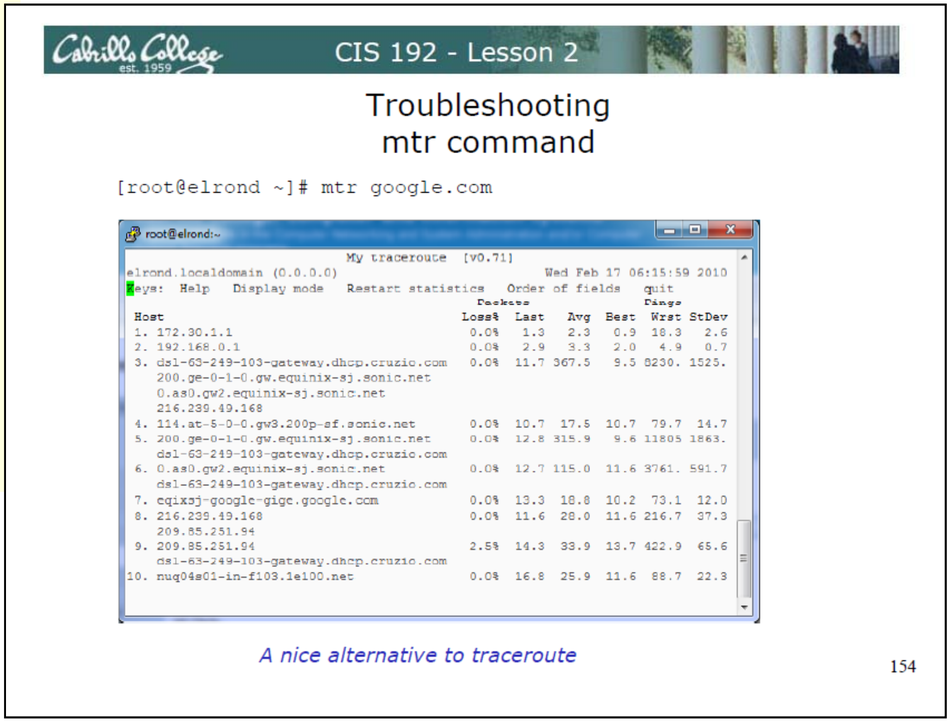


- Cabrillo College
- Web Advisor
- CCC Confer
- Static IPs
- Quick Ref
- VM Repairs
- GAH!

- sendmail
- telnet-server
- vsftpd

Troubleshooting Tools

- arp
- fetchmail
- ifconfig
- ipcalc
- mtr
- netstat
- ping
- route
- tcpdump
- Telnet "App Ping"
- traceroute



Cabrillo College est. 1959 CIS 192 - Lesson 2

Troubleshooting
mtr command

```
[root@elrond ~]# mtr google.com
```

```
                             My traceroute  [v0.71]
elrond.localdomain (0.0.0.0)                           Wed Feb 17 06:15:59 2010
Keys:  Help   Display mode   Restart statistics   Order of fields   quit
                                             Packets               Pings
 Host                                      Loss%   Last   Avg  Best  Wrst StDev
 1. 172.30.1.1                              0.0%    1.3   2.3   0.9  18.3   2.6
 2. 192.168.0.1                             0.0%    2.9   3.3   2.0   4.9   0.7
 3. dsl-63-249-103-gateway.dhcp.cruzio.com  0.0%   11.7 367.5   9.5 8230. 1525.
    200.ge-0-1-0.gw.equinix-sj.sonic.net
    0.as0.gw2.equinix-sj.sonic.net
    216.239.49.168
 4. 114.at-5-0-0.gw3.200p-sf.sonic.net      0.0%   10.7  17.5  10.7  79.7  14.7
 5. 200.ge-0-1-0.gw.equinix-sj.sonic.net    0.0%   12.8 315.9   9.6 11805 1863.
    dsl-63-249-103-gateway.dhcp.cruzio.com
 6. 0.as0.gw2.equinix-sj.sonic.net          0.0%   12.7 115.0  11.6 3761. 591.7
    dsl-63-249-103-gateway.dhcp.cruzio.com
 7. eqixsj-google-gige.google.com           0.0%   13.3  18.8  10.2  73.1  12.0
 8. 216.239.49.168                          0.0%   11.6  28.0  11.6 216.7  37.3
    209.85.251.94
 9. 209.85.251.94                           2.5%   14.3  33.9  13.7 422.9  65.6
    dsl-63-249-103-gateway.dhcp.cruzio.com
10. nuq04s01-in-f103.1e100.net              0.0%   16.8  25.9  11.6  88.7  22.3
```

A nice alternative to traceroute

154

The Quick Ref page on the web site has been updated with examples showing the troubleshooting tools

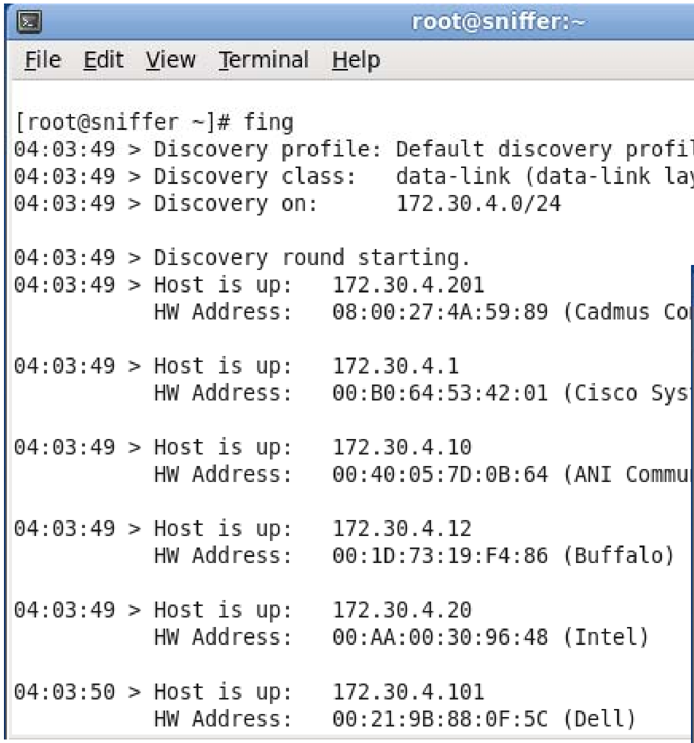
Network and System Management Tools

fing
nmap
Nagios
Cacti
Webmin
HP SIM
many more ...

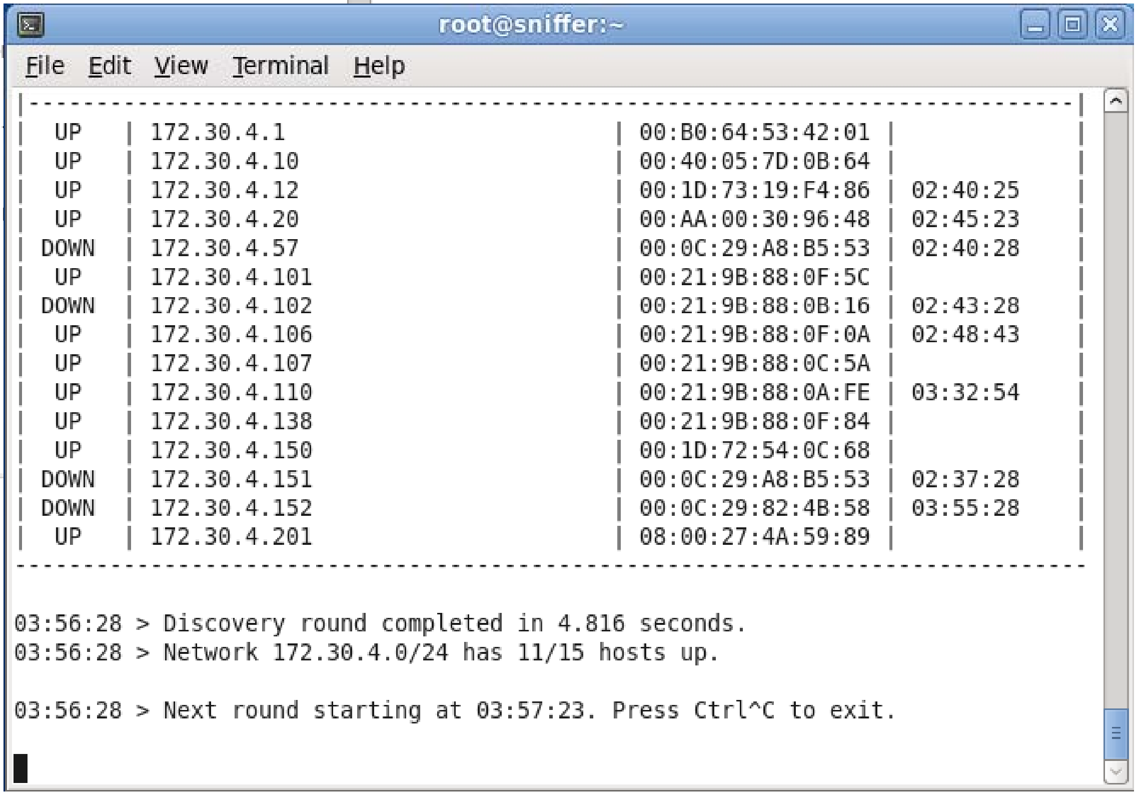
Free tools that run on Linux

Network and System Management Tools

fing
network discovery and
scanning tool



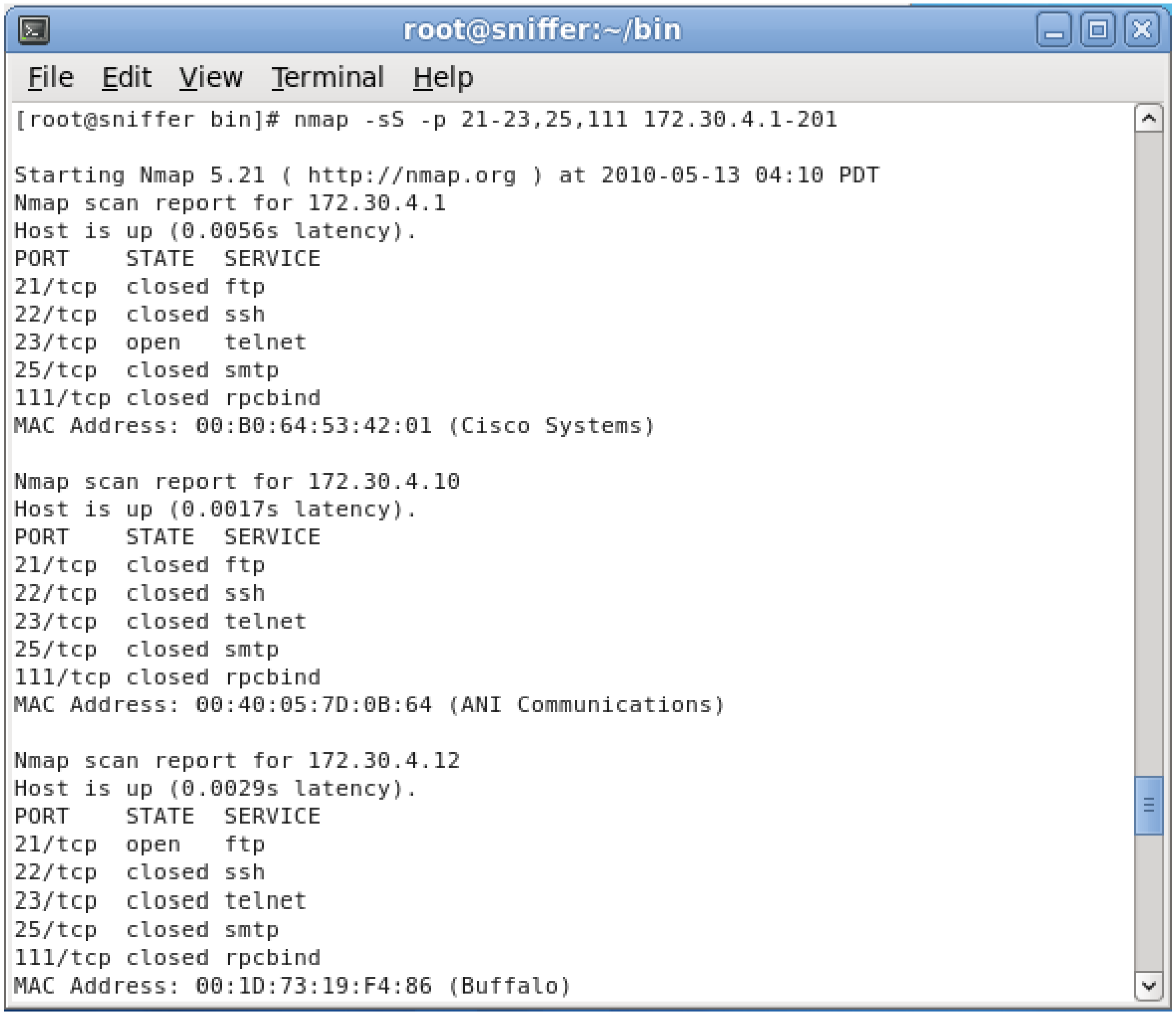
```
[root@sniffer ~]# fing
04:03:49 > Discovery profile: Default discovery profile
04:03:49 > Discovery class:   data-link (data-link layer)
04:03:49 > Discovery on:      172.30.4.0/24

04:03:49 > Discovery round starting.
04:03:49 > Host is up:   172.30.4.201
           HW Address:   08:00:27:4A:59:89 (Cadmus Co

04:03:49 > Host is up:   172.30.4.1
           HW Address:   00:B0:64:53:42:01 (Cisco Sys

04:03:49 > Host is up:   172.30.4.10
           HW Address:   00:40:05:7D:0B:64 (ANI Commu

04:03:49 > Host is up:   172.30.4.12
           HW Address:   00:1D:73:19:F4:86 (Buffalo)

04:03:49 > Host is up:   172.30.4.20
           HW Address:   00:AA:00:30:96:48 (Intel)

04:03:50 > Host is up:   172.30.4.101
           HW Address:   00:21:9B:88:0F:5C (Dell)
```



```
|--------------------------------------------------------------------------|
|  UP   | 172.30.4.1                      | 00:B0:64:53:42:01 |            |
|  UP   | 172.30.4.10                     | 00:40:05:7D:0B:64 |            |
|  UP   | 172.30.4.12                     | 00:1D:73:19:F4:86 | 02:40:25   |
|  UP   | 172.30.4.20                     | 00:AA:00:30:96:48 | 02:45:23   |
| DOWN  | 172.30.4.57                     | 00:0C:29:A8:B5:53 | 02:40:28   |
|  UP   | 172.30.4.101                    | 00:21:9B:88:0F:5C |            |
| DOWN  | 172.30.4.102                    | 00:21:9B:88:0B:16 | 02:43:28   |
|  UP   | 172.30.4.106                    | 00:21:9B:88:0F:0A | 02:48:43   |
|  UP   | 172.30.4.107                    | 00:21:9B:88:0C:5A |            |
|  UP   | 172.30.4.110                    | 00:21:9B:88:0A:FE | 03:32:54   |
|  UP   | 172.30.4.138                    | 00:21:9B:88:0F:84 |            |
|  UP   | 172.30.4.150                    | 00:1D:72:54:0C:68 |            |
| DOWN  | 172.30.4.151                    | 00:0C:29:A8:B5:53 | 02:37:28   |
| DOWN  | 172.30.4.152                    | 00:0C:29:82:4B:58 | 03:55:28   |
|  UP   | 172.30.4.201                    | 08:00:27:4A:59:89 |            |
----------------------------------------------------------------------------

03:56:28 > Discovery round completed in 4.816 seconds.
03:56:28 > Network 172.30.4.0/24 has 11/15 hosts up.

03:56:28 > Next round starting at 03:57:23. Press Ctrl^C to exit.

█
```

http://www.over-look.com/site/index.php/download

Network and System Management Tools

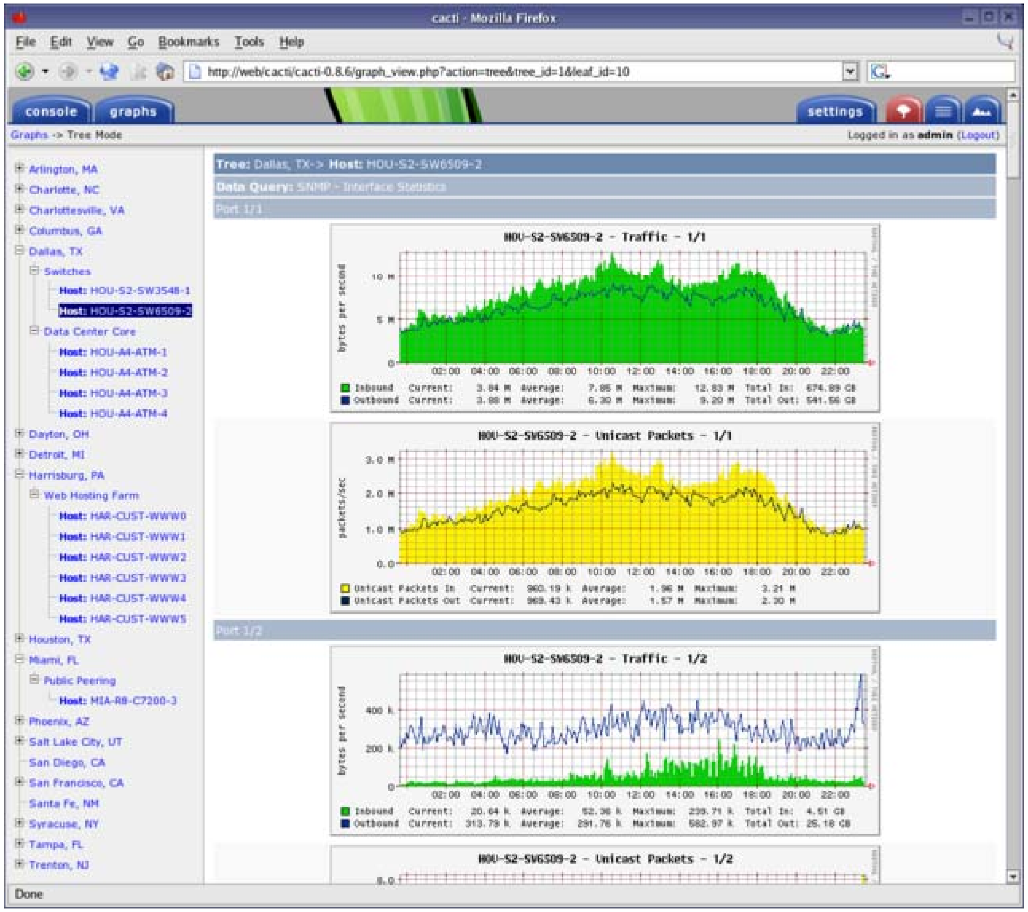


```
[root@sniffer bin]# nmap -sS -p 21-23,25,111 172.30.4.1-201

Starting Nmap 5.21 ( http://nmap.org ) at 2010-05-13 04:10 PDT
Nmap scan report for 172.30.4.1
Host is up (0.0056s latency).
PORT    STATE  SERVICE
21/tcp  closed ftp
22/tcp  closed ssh
23/tcp  open   telnet
25/tcp  closed smtp
111/tcp closed rpcbind
MAC Address: 00:B0:64:53:42:01 (Cisco Systems)

Nmap scan report for 172.30.4.10
Host is up (0.0017s latency).
PORT    STATE  SERVICE
21/tcp  closed ftp
22/tcp  closed ssh
23/tcp  closed telnet
25/tcp  closed smtp
111/tcp closed rpcbind
MAC Address: 00:40:05:7D:0B:64 (ANI Communications)

Nmap scan report for 172.30.4.12
Host is up (0.0029s latency).
PORT    STATE  SERVICE
21/tcp  open   ftp
22/tcp  closed ssh
23/tcp  closed telnet
25/tcp  closed smtp
111/tcp closed rpcbind
MAC Address: 00:1D:73:19:F4:86 (Buffalo)
```

nmap
network scanning tool

yum install nmap

Network and System Management Tools



```
Inbound   Current:   3.84 M  Average:   7.85 M  Maximum:  12.83 M  Total In:  674.89 GB
Outbound  Current:   3.88 M  Average:   6.30 M  Maximum:   9.20 M  Total Out: 541.56 GB
```

```
Unicast Packets In   Current:  960.19 k  Average:  1.96 M  Maximum:  3.21 M
Unicast Packets Out  Current:  969.43 k  Average:  1.57 M  Maximum:  2.30 M
```

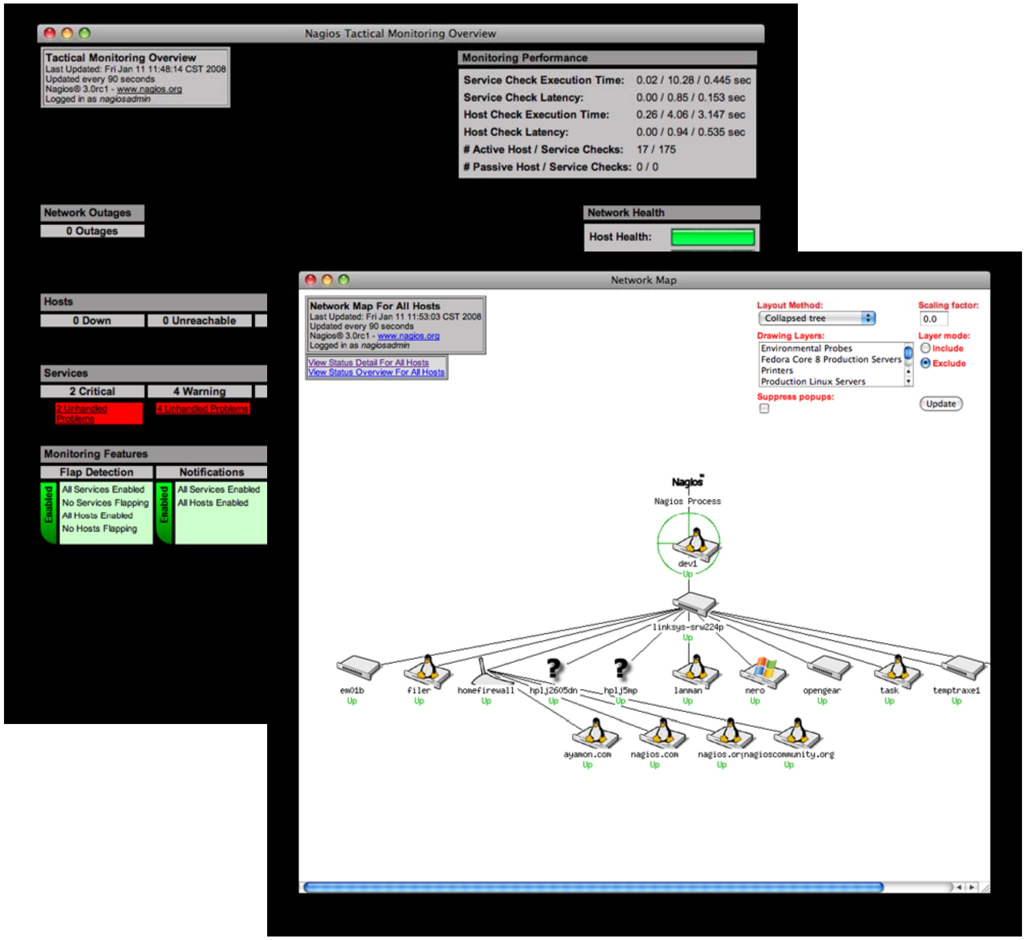
```
Inbound   Current:   20.64 k  Average:   52.36 k  Maximum:  239.71 k  Total In:  4.51 GB
Outbound  Current:  313.79 k  Average:  291.76 k  Maximum:  582.97 k  Total Out: 25.18 GB
```

Cacti

Open source graphing tool for RRDTool data

http://www.cacti.net

Network and System Management Tools



Nagios Tactical Monitoring Overview

Tactical Monitoring Overview
Last Updated: Fri Jan 11 11:48:14 CST 2008
Updated every 90 seconds
Nagios® 3.0rc1 - www.nagios.org
Logged in as *nagiosadmin*

Monitoring Performance

Service Check Execution Time:	0.02 / 10.28 / 0.445 sec
Service Check Latency:	0.00 / 0.85 / 0.153 sec
Host Check Execution Time:	0.26 / 4.06 / 3.147 sec
Host Check Latency:	0.00 / 0.94 / 0.535 sec
# Active Host / Service Checks:	17 / 175
# Passive Host / Service Checks:	0 / 0

Network Outages
0 Outages

Network Health
Host Health: 🟩

Hosts
0 Down | 0 Unreachable

Services
2 Critical | 4 Warning
2 Unhandled Problems | 4 Unhandled Problems

Monitoring Features

Flap Detection		Notifications	
Enabled	All Services Enabled No Services Flapping All Hosts Enabled No Hosts Flapping	Enabled	All Services Enabled All Hosts Enabled

Network Map

Network Map For All Hosts
Last Updated: Fri Jan 11 11:53:03 CST 2008
Updated every 90 seconds
Nagios® 3.0rc1 - www.nagios.org
Logged in as *nagiosadmin*

View Status Detail For All Hosts
View Status Overview For All Hosts

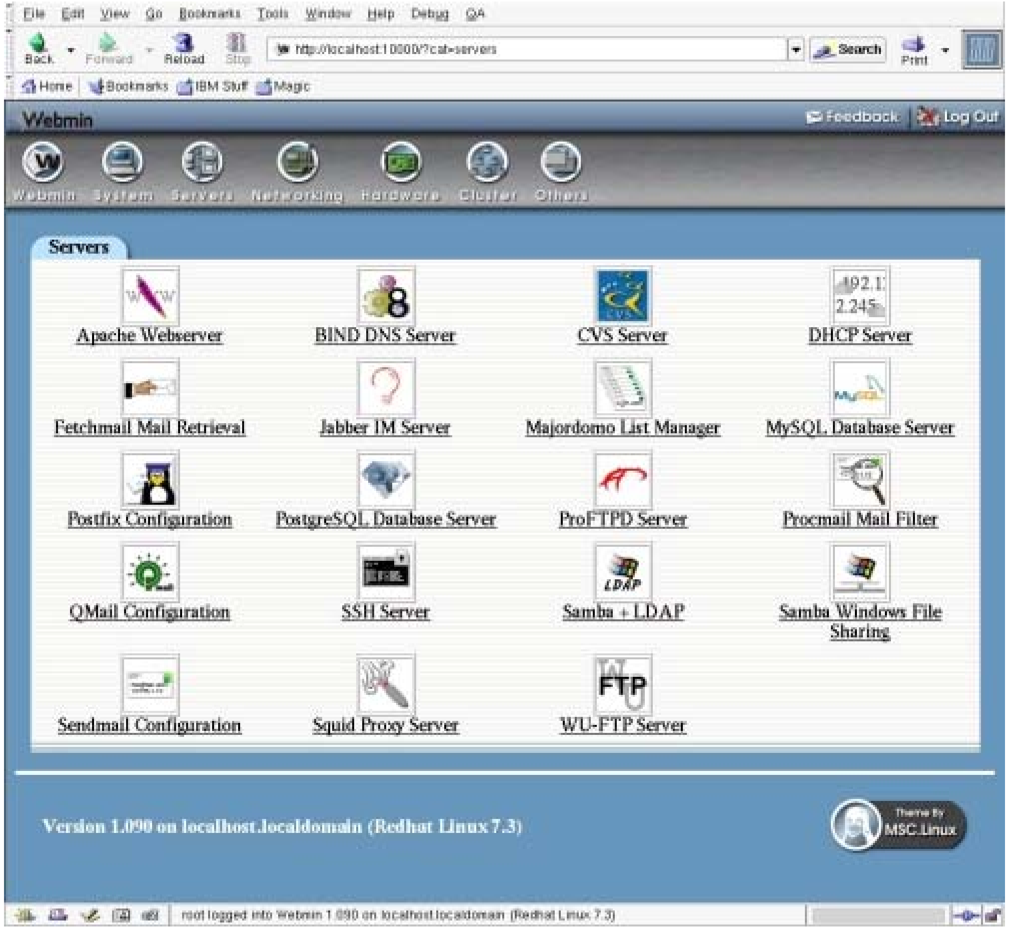
Layout Method: Collapsed tree
Scaling factor: 0.0
Drawing Layers: Environmental Probes, Fedora Core 8 Production Servers, Printers, Production Linux Servers
Layer mode: ○ Include ● Exclude
Suppress popups: □
Update

Nagios

Open source system and network monitoring tool

http://www.nagios.org

Network and System Management Tools



Version 1.090 on localhost.localdomain (Redhat Linux 7.3)

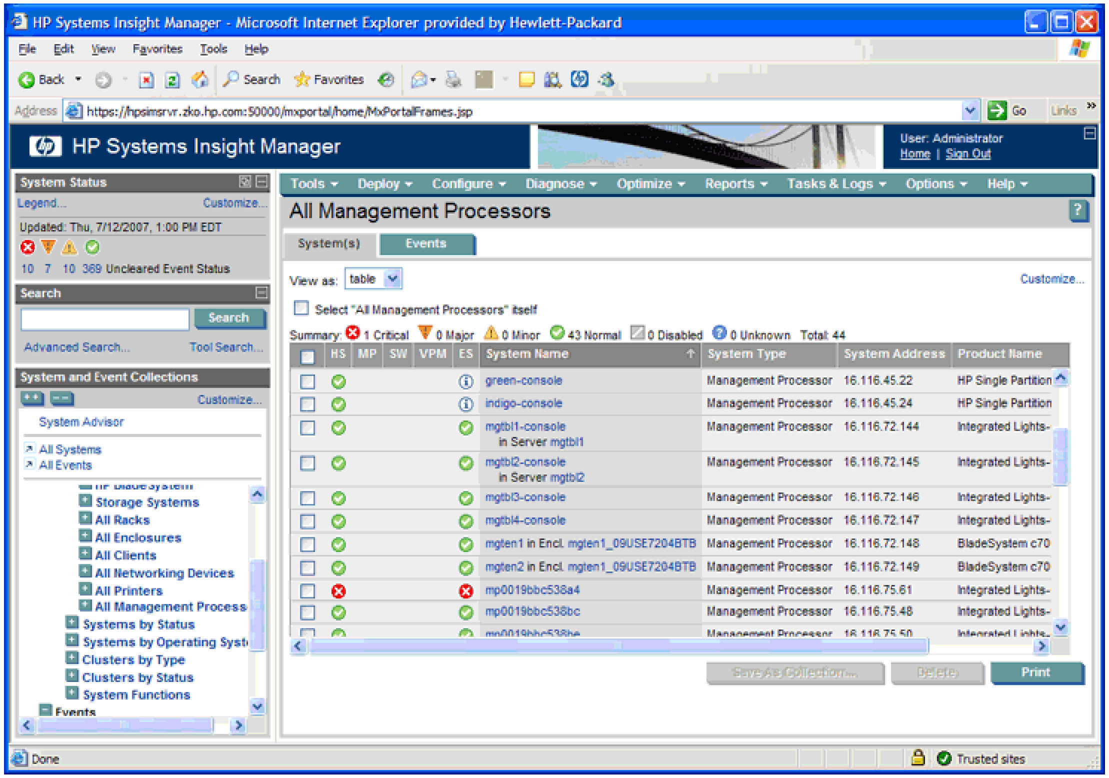
root logged into Webmin 1.090 on localhost.localdomain (Redhat Linux 7.3)

webmin

Web based system administration tool

http://www.webmin.com/

Network and System Management Tools


HP Systems Insight Manager - Microsoft Internet Explorer provided by Hewlett-Packard
File Edit View Favorites Tools Help
Back Search Favorites
Address https://hpsimsrvr.zko.hp.com:50000/mxportal/home/MxPortalFrames.jsp
Go Links
HP Systems Insight Manager
User: Administrator
Home | Sign Out
System Status
Legend... Customize...
Search
Search
Advanced Search... Tool Search...
System and Event Collections
Customize...
System Advisor
All Systems
All Events
HP BladeSystem
Storage Systems
All Racks
All Enclosures
All Clients
All Networking Devices
All Printers
All Management Process
Systems by Status
Systems by Operating Syst
Clusters by Type
Clusters by Status
System Functions
Events
Tools Deploy Configure Diagnose Optimize Reports Tasks & Logs Options Help
System(s) Events
Customize...
Save As Collection... Delete Print
Done
Trusted sites

Updated: Thu, 7/12/2007, 1:00 PM EDT

10 7 10 369 Uncleared Event Status

All Management Processors

View as: table

□ Select "All Management Processors" itself

Summary: 1 Critical 0 Major 0 Minor 43 Normal 0 Disabled 0 Unknown Total: 44

□	HS	MP	SW	VPM	ES	System Name	System Type	System Address	Product Name
□	✓				ⓘ	green-console	Management Processor	16.116.45.22	HP Single Partition
□	✓				ⓘ	indigo-console	Management Processor	16.116.45.24	HP Single Partition
□	✓				✓	mgtbl1-console in Server mgtbl1	Management Processor	16.116.72.144	Integrated Lights-
□	✓				✓	mgtbl2-console in Server mgtbl2	Management Processor	16.116.72.145	Integrated Lights-
□	✓				✓	mgtbl3-console	Management Processor	16.116.72.146	Integrated Lights-
□	✓				✓	mgtbl4-console	Management Processor	16.116.72.147	Integrated Lights-
□	✓				✓	mgten1 in Encl. mgten1_09USE7204BTB	Management Processor	16.116.72.148	BladeSystem c70
□	✓				✓	mgten2 in Encl. mgten1_09USE7204BTB	Management Processor	16.116.72.149	BladeSystem c70
□	☒				☒	mp0019bbc538a4	Management Processor	16.116.75.61	Integrated Lights-
□	✓				✓	mp0019bbc538bc	Management Processor	16.116.75.48	Integrated Lights-
□	✓				✓	mp0019bbc538be	Management Processor	16.116.75.50	Integrated Lights-

HP SIM

Web based system administration tool

http://www.hp.com/go/hpsim

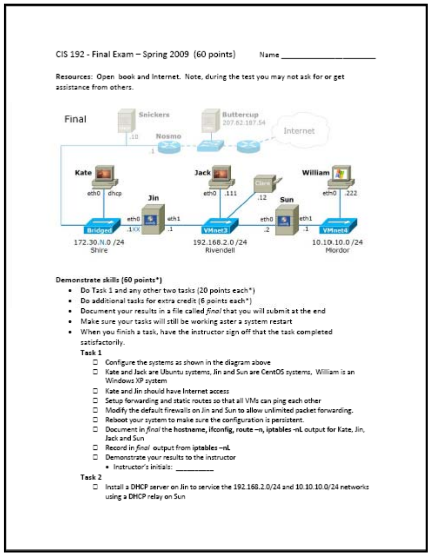
Network and System Management Tools

OpenView
Tivoli
CA-Unicenter
many more ...

Final

Final - 60 points

- Meet at the normal class time and location
- There are 8 possible tasks to implement from scratch during the final exam. The description of these task requirements will be available one week prior to the exam.
- One task is mandatory (20 points). Two additional tasks of your choice make up the rest of the exam (20 points each)
- Any additional tasks completed during the exam will earn 6 points of extra credit each. These extra credit points are not subject to the extra credit cap for the course.
- You may use the forum and work with other students to prepare in advance of the final. During the final you must work by yourself.
- The exam is open, book, open notes and open computer. Your are not allowed to ask for or give assistance during the exam.



CIS 192 - Final Exam – Spring 2009 (60 points) Name ____________________

Resources: Open book and Internet. Note, during the test you may not ask for or get assistance from others.

Demonstrate skills (60 points*)

- Do Task 1 and any other two tasks (20 points each*)
- Do additional tasks for extra credit (6 points each*)
- Document your results in a file called *final* that you will submit at the end
- Make sure your tasks will still be working aster a system restart
- When you finish a task, have the instructor sign off that the task completed satisfactorily.

Task 1

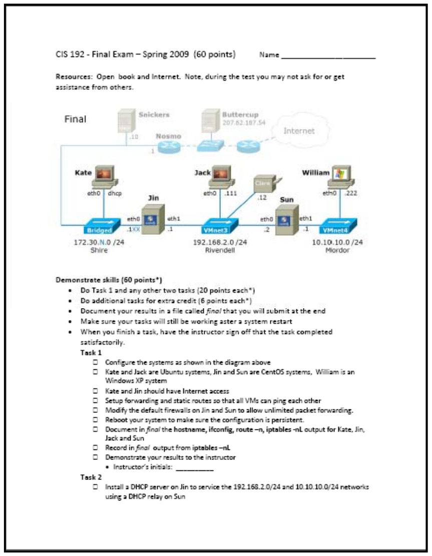
□ Configure the systems as shown in the diagram above
□ Kate and Jack are Ubuntu systems, Jin and Sun are CentOS systems, William is an Windows XP system
□ Kate and Jin should have Internet access
□ Setup forwarding and static routes so that all VMs can ping each other
□ Modify the default firewalls on Jin and Sun to allow unlimited packet forwarding.
□ Reboot your system to make sure the configuration is persistent.
□ Document in *final* the **hostname, ifconfig, route –n, iptables -nL** output for Kate, Jin, Jack and Sun
□ Record in *final* output from **iptables –nL**
□ Demonstrate your results to the instructor
- Instructor's initials: __________

Task 2

□ Install a DHCP server on Jin to service the 192.168.2.0/24 and 10.10.10.0/24 networks using a DHCP relay on Sun

The final is available now on the web site

Final - 60 points



CIS 192 - Final Exam – Spring 2009 (60 points) Name ____________________

Resources: Open book and Internet. Note, during the test you may not ask for or get assistance from others.

Demonstrate skills (60 points*)

- Do Task 1 and any other two tasks (20 points each*)
- Do additional tasks for extra credit (6 points each*)
- Document your results in a file called *final* that you will submit at the end
- Make sure your tasks will still be working aster a system restart
- When you finish a task, have the instructor sign off that the task completed satisfactorily.

Task 1

- ☐ Configure the systems as shown in the diagram above
- ☐ Kate and Jack are Ubuntu systems, Jin and Sun are CentOS systems, William is an Windows XP system
- ☐ Kate and Jin should have Internet access
- ☐ Setup forwarding and static routes so that all VMs can ping each other
- ☐ Modify the default firewalls on Jin and Sun to allow unlimited packet forwarding.
- ☐ Reboot your system to make sure the configuration is persistent.
- ☐ Document in *final* the **hostname, ifconfig, route –n, iptables -nL** output for Kate, Jin, Jack and Sun
- ☐ Record in *final* output from **iptables –nL**
- ☐ Demonstrate your results to the instructor
  - Instructor's initials: __________

Task 2

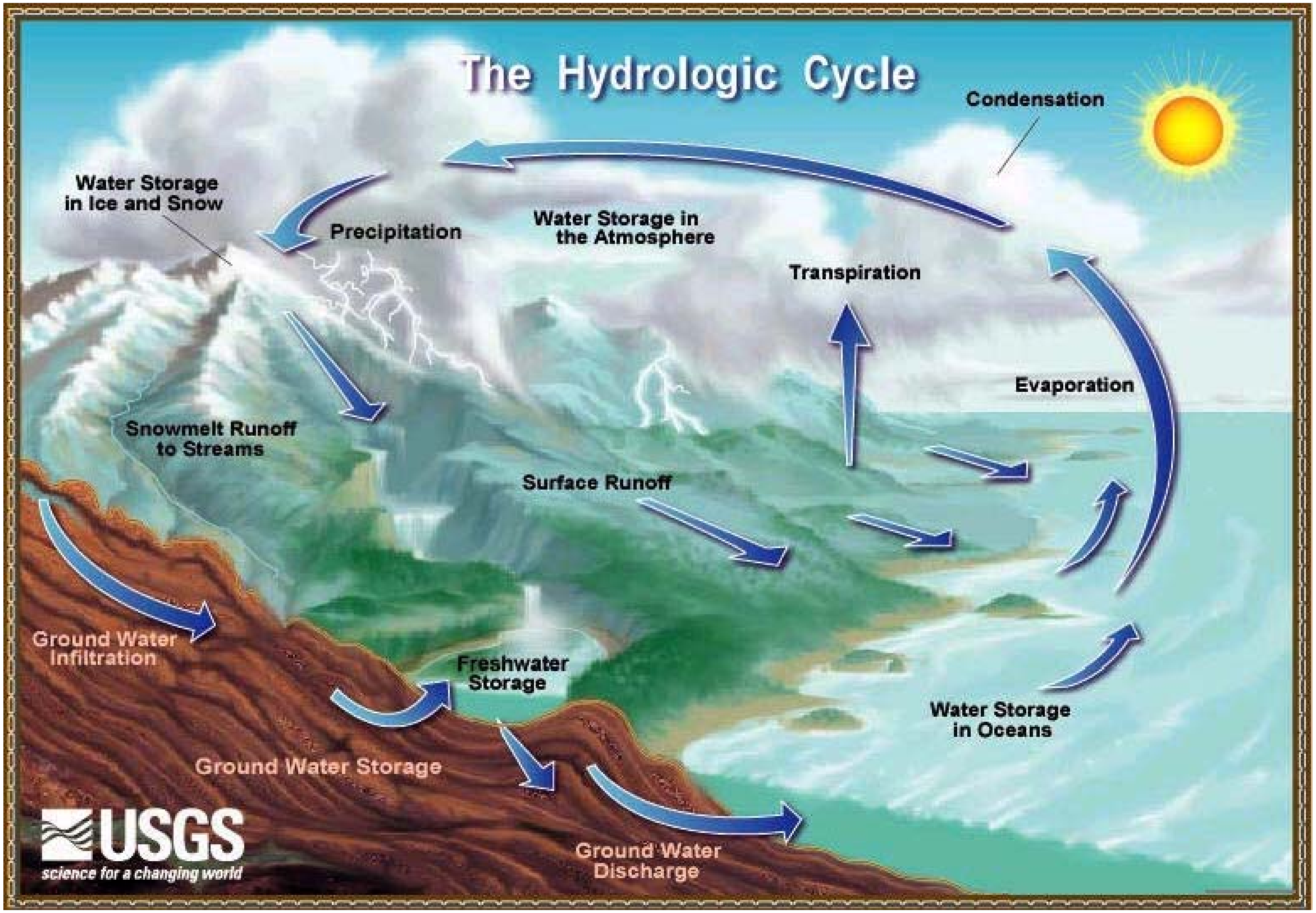
- ☐ Install a DHCP server on Jin to service the 192.168.2.0/24 and 10.10.10.0/24 networks using a DHCP relay on Sun

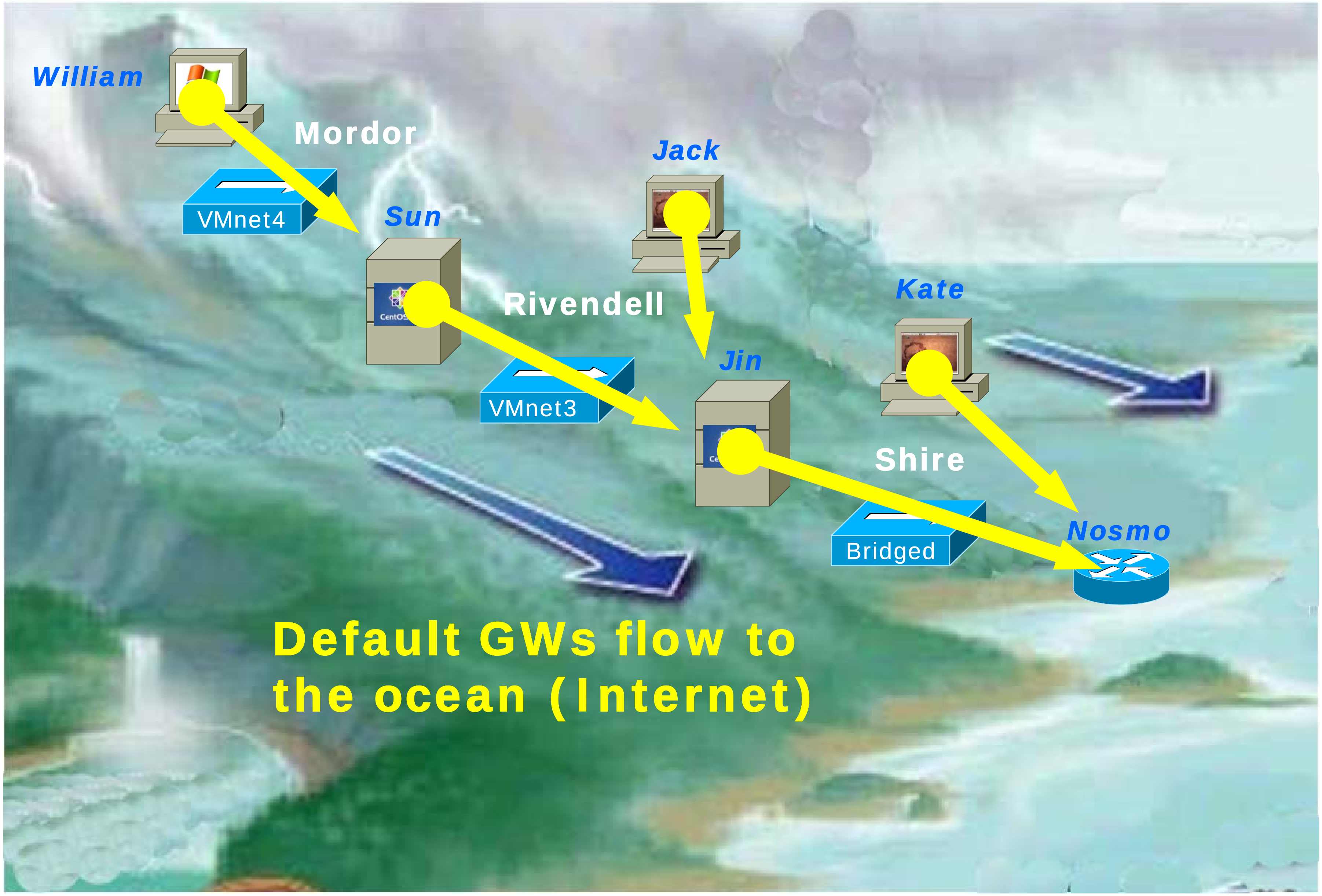
The final is available now on the web site

Tips

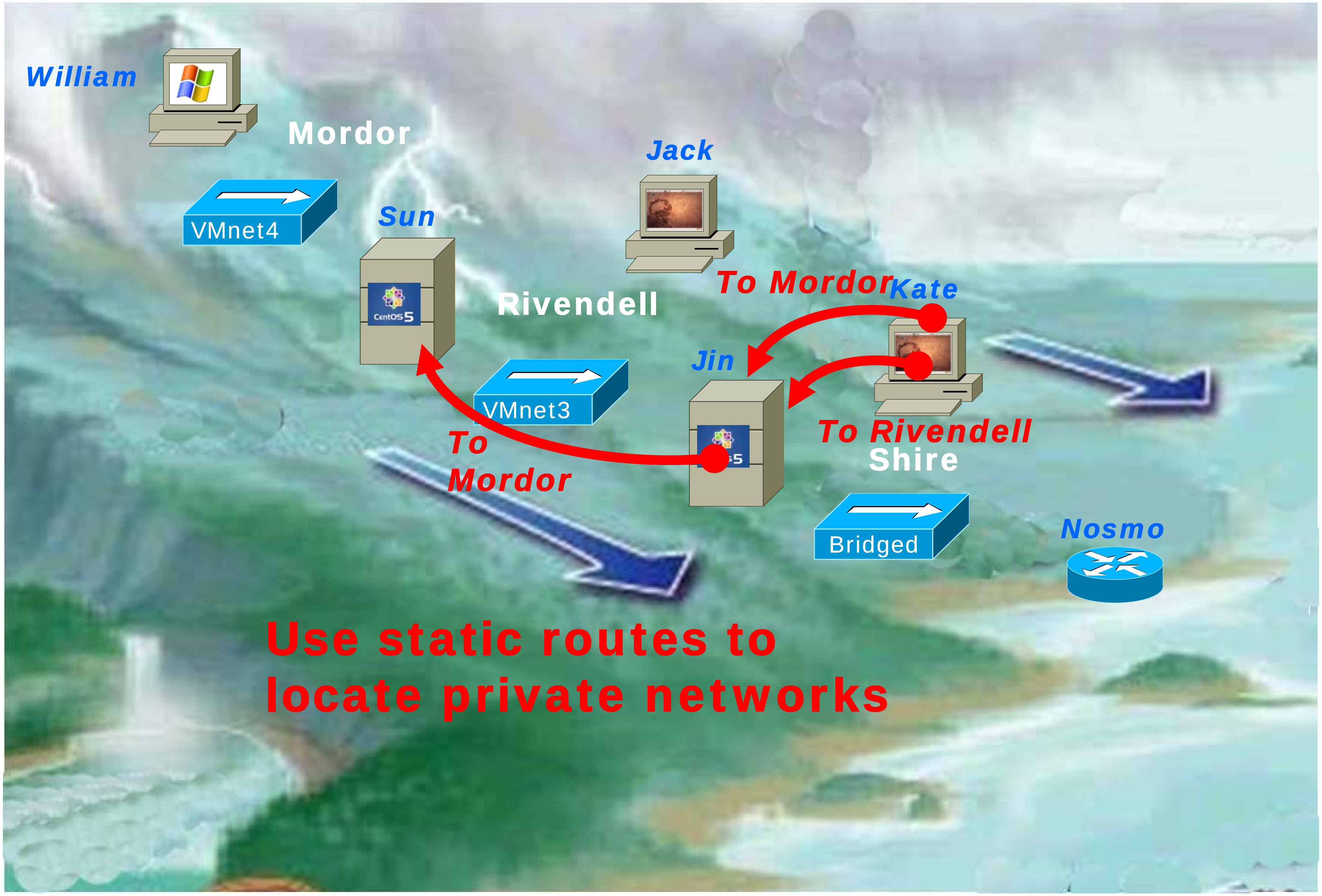
- Prior to the final, select the tasks you plan to do and practice implementing them over and over till you can do them in your sleep.
- Take note of any implementation problems that come up and record the troubleshooting solutions you discovered to fix them.
- Make yourself some personal checklists with the steps, command examples, and references to help things go smoothly during the exam.

More Tips


The Hydrologic Cycle
Condensation
Water Storage in Ice and Snow
Precipitation
Water Storage in the Atmosphere
Transpiration
Evaporation
Snowmelt Runoff to Streams
Surface Runoff
Ground Water Infiltration
Freshwater Storage
Water Storage in Oceans
Ground Water Storage
Ground Water Discharge
USGS
science for a changing world

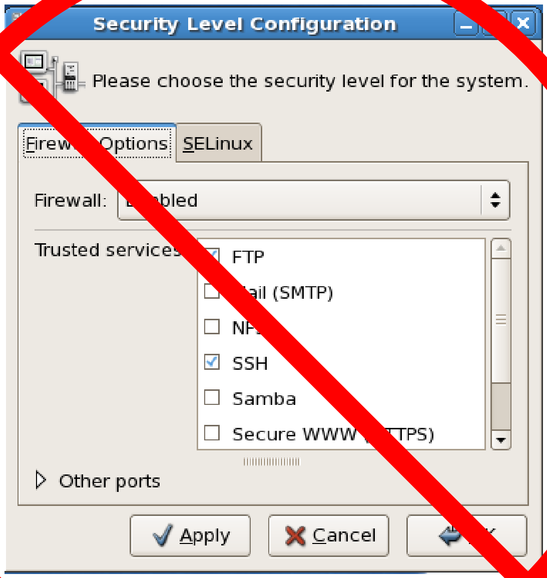


Default GWs flow to the ocean (Internet)



Use static routes to locate private networks

*If you use **iptables** commands (recommended) to configure the firewall then DON'T use the Security Level Configuration tool or the **lokkit** command!*



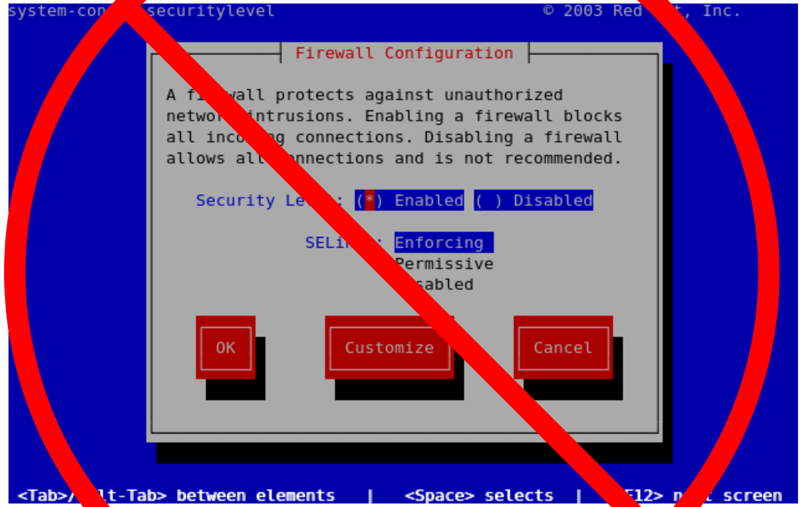
Security Level Configuration

Please choose the security level for the system.

Firewall: E bled

Trusted services ☑ FTP
☐ ail (SMTP)
☐ NF
☑ SSH
☐ Samba
☐ Secure WWW (TTPS)

Security Level Configuration



```
system-con   securitylevel                                  © 2003 Red    t, Inc.

                    Firewall Configuration

   A fi    wall protects against unauthorized
   networ  intrusions. Enabling a firewall blocks
   all inco   ng connections. Disabling a firewall
   allows all   nnections and is not recommended.

       Security Le    : (*) Enabled  ( ) Disabled

                SELi    : Enforcing
                          Permissive
                           sabled

        OK            Customize            Cancel

<Tab>/ lt-Tab> between elements   |  <Space> selects  |    F12> n   screen
```

lokkit

*The Security Level Configuration tool and the **lokkit** command will clobber any changes you have made with **iptables** commands!*

The Final is Tuesday June 3
Room 2501 - Starts at 5:30 PM

- Extra credit labs are due midnight June 3
- Five forum posts are due midnight June 3
- The final will be open book open notes, open computer

Workshop

Open Lab Workshop

Lab 10 - Internet Services

Extra Credit Labs

Final preparation

Wrap

Backup

Classroom Static IP addresses for VM's

Station	IP	Static 1
Instructor	172.30.1.100	172.30.1.125
Station-01	172.30.1.101	172.30.1.126
Station-02	172.30.1.102	172.30.1.127
Station-03	172.30.1.103	172.30.1.128
Station-04	172.30.1.104	172.30.1.129
Station-05	172.30.1.105	172.30.1.130
Station-06	172.30.1.106	172.30.1.131
Station-07	172.30.1.107	172.30.1.132
Station-08	172.30.1.108	172.30.1.133
Station-09	172.30.1.109	172.30.1.134
Station-10	172.30.1.110	172.30.1.135
Station-11	172.30.1.111	172.30.1.136
Station-12	172.30.1.112	172.30.1.137

Station	IP	Static 1
Station-13	172.30.1.113	172.30.1.138
Station-14	172.30.1.114	172.30.1.139
Station-15	172.30.1.115	172.30.1.140
Station-16	172.30.1.116	172.30.1.141
Station-17	172.30.1.117	172.30.1.142
Station-18	172.30.1.118	172.30.1.143
Station-19	172.30.1.119	172.30.1.144
Station-20	172.30.1.120	172.30.1.145
Station-21	172.30.1.121	172.30.1.146
Station-22	172.30.1.122	172.30.1.147
Station-23	172.30.1.123	172.30.1.148
Station-24	172.30.1.124	172.30.1.149

Note the static IP address for your station to use in the next class exercise

Classroom DHCP IP allocation pools table by station number

Station	IP	Start	End
01	172.30.1.101	172.30.1.50	172.30.1.54
02	172.30.1.102	172.30.1.55	172.30.1.59
03	172.30.1.103	172.30.1.60	172.30.1.64
04	172.30.1.104	172.30.1.65	172.30.1.69
05	172.30.1.105	172.30.1.70	172.30.1.74
06	172.30.1.106	172.30.1.75	172.30.1.79
07	172.30.1.107	172.30.1.80	172.30.1.84
08	172.30.1.108	172.30.1.85	172.30.1.89
09	172.30.1.109	172.30.1.90	172.30.1.94
10	172.30.1.110	172.30.1.95	172.30.1.99
11	172.30.1.111	172.30.1.200	172.30.1.204
12	172.30.1.112	172.30.1.205	172.30.1.209

Station	IP	Start	End
13	172.30.1.101	172.30.1.210	172.30.1.214
14	172.30.1.102	172.30.1.215	172.30.1.219
15	172.30.1.103	172.30.1.220	172.30.1.224
16	172.30.1.104	172.30.1.225	172.30.1.229
17	172.30.1.105	172.30.1.230	172.30.1.234
18	172.30.1.106	172.30.1.235	172.30.1.239
19	172.30.1.107	172.30.1.240	172.30.1.244
20	172.30.1.108	172.30.1.245	172.30.1.249
21	172.30.1.109	172.30.1.250	172.30.1.254
22	172.30.1.110	172.30.1.30	172.30.1.34
23	172.30.1.111	172.30.1.35	172.30.1.39
24	172.30.1.112	172.30.1.20	172.30.1.44
Instruct	172.30.1.100	172.30.1.45	172.30.1.49

Station-09

Use these pools of addresses based on your station number to avoid conflicts on the classroom network

Q11. What MUA is installed on Hershey?

/bin/mail and /or evolution

```
[rich@hershey rich]$ type mail
mail is /bin/mail
[rich@hershey rich]$ rpm -qa | grep evolution
evolution-1.2.2-4
[rich@hershey rich]$
[rich@hershey rich]$ mail
Mail version 8.1 6/6/93.  Type ? for help.
"/var/spool/mail/rich": 1 message
>   1 rich@middelearth.net  Tue May 12 11:50  22/664   "Almost"
& x
[rich@hershey rich]$
```