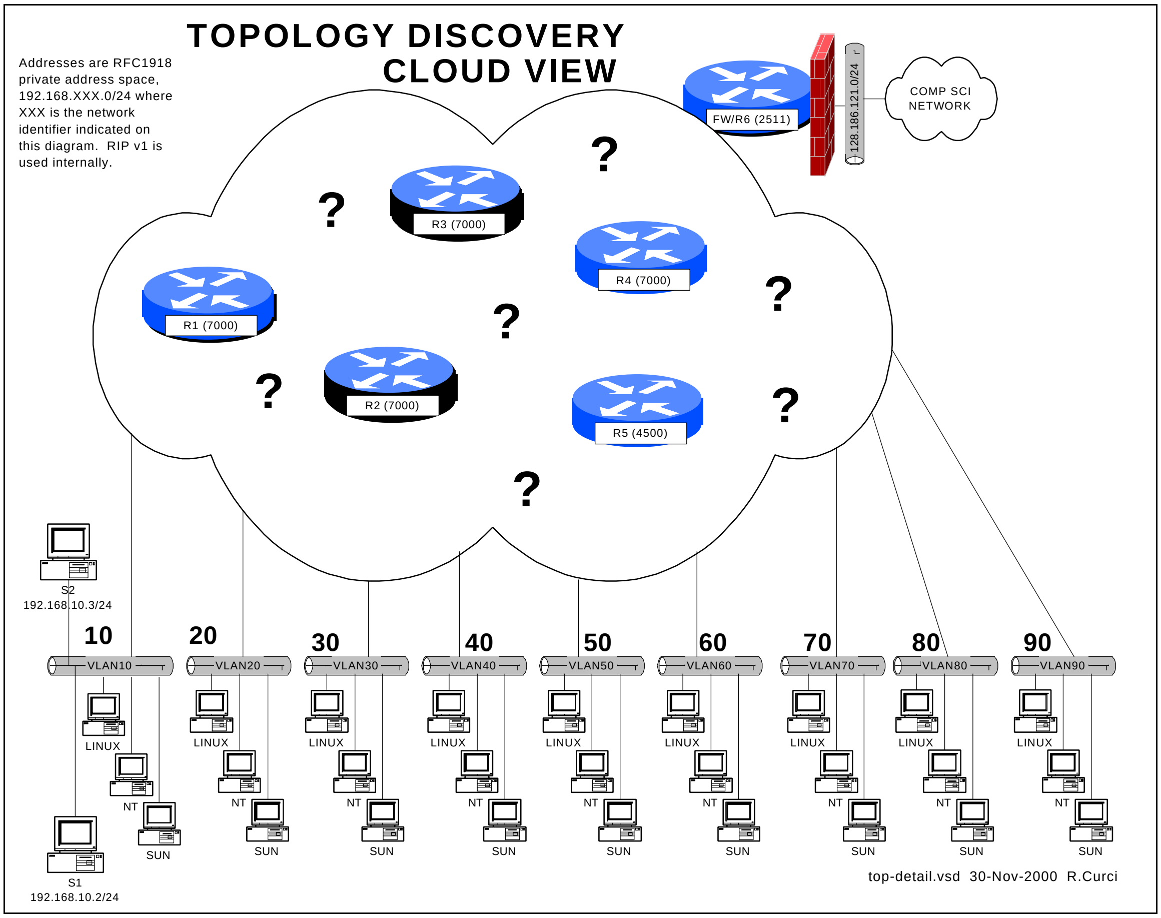
INTERNET TEACHING LAB: TOPOLOGY DISCOVERY



Addresses are RFC1918 private address space, 192.168.XXX.0/24 where XXX is the network identifier indicated on this diagram. RIP v1 is used internally.

top-detail.vsd 30-Nov-2000 R.Curci

Overview

Each team has a set of computers on its own ethernet VLAN connected to a working lab network of six Cisco routers. Your task is to configure the TCP/IP protocol on your computers and verify you can communicate between your PCs, with other team PCs, the routers, and systems outside the lab on the Internet. Once you have basic connectivity, your job is to download and use network tools to discover the IP addressing scheme and network topology of the lab network. You will be given hints but no login access to the routers for this assignment. Your journal should detail how you discovered different aspects of the addressing scheme and topology and include a detailed network diagram showing the routers, connections between routers, bandwidth of the connections, and IP addresses for all router interfaces, including where the team VLANs attach to the lab network.

Hints

For this exercise inside the lab network, we will be using RFC1918 private address space for all router and computer interfaces. The only exceptions are a single real address on router FW/R6 which is performing network address translation (NAT) to allow lab computers to access the Internet for downloading files, and a special UNIX server with two ethernet ports. The special UNIX server does not route, but you can TELNET in from outside the lab, then TELNET to your team computers, allowing indirect access.

The six Cisco routers are running the IOS operating system and intentionally have many of the security features disabled to make your job easier. The routers connect to each other through different physical network media at different bandwidths. All layer 3 networks use a 24 bit network mask. Several router features that might normally be disabled have been turned on such as “service tcp-small-servers”, “ip directed-broadcast”, and “ip source-route”. SNMP is enabled on all routers with a read-only community string “public”.

PART1 – GETTING STARTED:

Address your team computers using the following table by replacing TEAM with your integer team number:

LINUX	192.168.X.Y	X= 10 * TEAM	Y= X + 1
NT	192.168.X.Y	X= 10 * TEAM	Y= X + 2
SOLARIS	192.168.X.Y	X= 10 * TEAM	Y= X + 3

For example, team 5’s NT system should be addressed with 192.168.50.52/24.

To test basic connectivity, verify you can PING(1) each of the other teams’ local gateway IP address.

On each of your computers, install the RIP version 1 routing protocol. Under UNIX, you can use either GateD or RouteD in passive mode. Under NT 4.0, use “RIP for Internet Protocol”. Your computers should learn a list of routes including a special “default route” sometimes abbreviated “0.0.0.0”. Make sure you have removed any static default routes and are learning the default dynamically. Build a table of routes including the RIP metric. This metric indicates the number of router hops from your computer to each of the networks and will help in figuring out the topology.

Hint: The UNIX utility ripquery(1) may be helpful.

PART2 – FIND THE SIX ROUTERS:

Given the network list from part 1, PING(1) the broadcast address for each network you found above. Normally, you will hear responses from the IP address of the router interface closest to your computer connected to the destination network. If you see more than one IP address in the responses, it is an indication that there are multiple routers on the broadcast network with different paths back to your computer.

Use the TRACEROUTE(1) utility to find some of the connections between the routers. (This utility is named TROUTE.EXE under NT). For each lab network, select an IP address and trace the route to it, making a note of the IP addresses of the routers in the path. Be sure to trace the route toward the Internet by tracing to a computer science server outside the lab. You should be able to find an IP address for each of the six routers. Note that routers generally have multiple interfaces each with its own IP address, so you may find multiple IP addresses that belong to the same router.

Download install the NMAP(1) utility for UNIX. You can find it at www.insecure.org/nmap. Use this tool to scan the 192.168.0.0/16 address space to find all devices and attempt to guess their operating systems. Be careful not to scan outside the 192.168.0.0/16 lab network as most System Administrators treat scanning as an attack and will likely trigger many intrusion detection alarms. Under Florida Law, port scanning is treated as unauthorized intrusion.

PART4 – Simple Network Management Protocol (SNMP)

All of the lab routers will respond to SNMP version 1 queries. SNMP version 1 uses a simple password protection scheme called a “community”. Each router is programmed to be an SNMP “agent” and will respond to the read-only community string “public”. SNMP agents store data in a Management Information Base, or MIB. The MIB contains a lot of information including the router name, the uptime, software version, interface names, interface IP addresses, routing tables, etc. Many SNMP tools are available for Linux:

```
   snmpbulkget   snmpget      snmpset     snmptest       snmpusm
   snmpbulkwalk  snmpgetnext  snmpstatus  snmptranslate  snmpwalk
   snmpdelta     snmpnetstat  snmptable   snmptrap
```

For example, you can display individual MIB variables with SNMPGET(1):

```
   LINUX$ snmpget 192.168.10.1 public system.sysDescr.0
   system.sysDescr.0 = Cisco Internetwork Operating System Software
   IOS (tm) GS Software (GS7-J-M), Version 11.1(24), RELEASE SOFTWARE (fc1)
   Copyright (c) 1986-1999 by cisco Systems, Inc.
   Compiled Mon 04-Jan-99 21:19 by richv
   LINUX$
```

For each of your routers, look up the following MIB variables:
system.sysDescr.0
system.sysName.0
This will let you see the router names to eliminate any duplicates if you previously found more than one IP address for the same router. Using the system description, note the IOS software version of the router. You should now have enough information to draw a diagram of the six routers with the interface names, interface types (ethernet, fddi, point-to-point, loopback), how they connect to each other, and the IP addressing scheme.

PART5 – Bandwidth Measurement (IPERF/PCHAR):

IPERF(1) is a tcp performance measurement tool. It is an updated version of the Test TCP program (TTCP) written by Terry Slattery in 1985 at the US Navy Ballistic Research Lab. You can find the latest version at http://dast.nlanr.net/Projects/Iperf/. You will find both UNIX source code that complies under Linux and SUNOS, and Microsoft Windows executable files (iperf.exe and iperf-threaded.exe). Normally, you start one copy of IPERF(1) in server mode, and the other in client mode specifying the server's IP address. This utility in client mode will also work with an ordinary TCP/IP device supporting the trivial TCP DISCARD service on TCP port 9 which is enabled on all lab routers. Measure the performance from your computer to each router to help determine the bandwidth between links on your network. Note that if the packets traverse several links, the slowest link in the path will be the determining factor.

PCHAR(1) is a utility similar to TRACEROUTE(1), but tries to determine the bandwidth between adjacent hops in the path. It is an updated version of PATHCHAR(1) written by Van Jacobson at Lawrence Berkeley Labs, namesake of the IP Van Jacobson header compression. You will need to either change permissions on PCHAR(1) to be SUID root or execute it while logged in as root. It can be found at http://www.employees.org/~bmah/Software/pchar/ Be patient with this program as it can take a long time to run using the default settings.

PART6 – Windows NT Network Management / WhatsUp Gold:

Download and install the utility "WhatsUp Gold" on your NT machine. You can download a 30-day evaluation copy from www.ipswitch.com. You will find both a self-installing Win95/98/NT/2000 executable and a users guide in Adobe Acrobat PDF format. If you don't have Adobe Acrobat Reader already loaded, you can find it at www.adobe.com. As of this writing, the latest software is version 5. Test out the following tools and verify the results are consistent with your topology drawing:

- traceroute tool
- snmp tool
- scan tool
- throughput tool

How does the SCAN tool compare to the UNIX NMAP utility?

Run the throughput tool to test each router using both the ICMP and TCP/discard/port-9 modes. How do these measurements compare to each other and to tests you made earlier with the UNIX IPERF utility?

Use this software to create a live map of your network including the six routers and IP networks. Change the polling method to TCP/IP—SNMP since this provides more information than the default ICMP method. Edit the symbols on the map to abbreviate the router names such as "R1" and network names using the third octet of the IP network number. This will help give you more room to fit all the icons on the screen. Configure the system to poll the devices every 10 seconds (Make sure you are not polling any devices outside of the lab environment). If configured properly, you should be able to view the map where the icon color indicates the status (i.e. green=good) and you should also be able to right-click your mouse on the router icons to Telnet, Ping, Traceroute, etc., to the highlighted device.

Configure the system such that if any of the routers go down on weekdays between 9am and 5pm, the system will send you an automatic e-mail message.

Configure the system to implement a WWW server such that you can check the status of your network remotely with the use of a web browser.

Hint: The "discover devices/intelligently scan network devices with SNMP seed router" function may save you time to initially build your map.