Layered Networking and Port Scanning

David Malone

22nd June 2004

IP Header

IP — a way to phrase information so it gets from one computer to another.

IPv4 Header:

Version 4 bit	Head Len 4 bit	ToS 8 bit	Total Length 16 bit	
ID 16 bit			Flags 3 bit	Frag Offset 13 bit
Time to Live 8 bit		Protocol 8 bit	Header Checksum 16 bit	
Source Address 32 bit				
Destination Address 32 bit				
Options *variable*				

An actual packet

```
4510 003c (version, len, ToS, tot len)
3fac 4000 (ID, flags, frag offset)
4006 e3f1 (TTL, protocol, hdr sum)
0a00 030a (src IP)
0a00 0005 (dst IP)
cb44 0017 ca13 4473 0000 0000
a002 ffff 1212 0000 0204 05b4
0103 0300 0101 080a 3510 12f5
```

Hard for people to read, easy for computer.

IP TCP SYN 10.0.3.10 port 52036 to 10.0.0.5 port 23.

IP over ???

IP says what the data is, and where it is to go. IP does not say how it gets there. Many other technologies may be used. Eg:

- Ethernet.
- Modem (PPP).
- ATM.

More headers must be added (and removed) as the IP packet moves from network to network. IP part stays the same, but other headers come and go.

IP over Ethernet

Ethernet is much simpler than IP and can only deliver packets to machines on the same LAN. An Ethernet header looks like:

ethernet dst, ethernet src, packet type

For example:

00:30:65:03:d9:72, 00:08:74:ba:39:f2, IP

This is the ethernet header of a packet from my laptop to the local router. This header would be followed by the IP header and then any data.

Packets within Packets

The idea of putting packets in packets is called encapsulation. It gives us a 'layered' view of networking.

Layer	Name	Description	Example
1	Physical	Physical operation of the medium	Ethernet over UTP
2	Data Link	Management of interface	Ethernet (upper level)
3	Network	How subnets interoperate	IP
4	Transport	Packetisation, retransmission, ...	TCP

There is a standard 7 layer model, but these 4 layers are enough for now.

Problems with packets

Packets may not make it to their destination:

- Lost because network is overloaded.
- Damaged by faulty hardware, stretched fiber, radio noise,
- Dropped because of firewalls, misrouting, rebooting,
- Sometimes even duplicated!

It may be that you want to retransmit, it may be that you want to resend packet to someone else, you may want to send a different packet. Layer 4 helps programs make these choices.

Layer 4 protocols

TCP The most popular IP protocol. Sends data to the other end and makes sure it gets their safely, in the right order

UDP If data gets to the far end, it is probably the data you sent. Makes no effort to ensure data gets there.

ICMP Used by IP itself for testing and diagnostics. Ping lives here.

Each of TCP, UDP and ICMP have their own headers that go after the IP header!

More about TCP

TCP is more complicated than UDP, IP or Ethernet. It begins with each side SYNchronising, so they know what data to expect. As data is sent it is ACKnowledged, so TCP knows when to retransmit lost packets. TCP is careful not to send data too fast. When the data is transfered the connection is FINished. Unexpected connections are ReSeT.

SYN →, ← SYN ACK,

ACK →,

Data is transfered and ACKed,

FIN →, ← FIN.

Ports

On any one computer multiple programs might want to use TCP and UDP at the same time. For this reason TCP and UDP headers include another address, called a port, which identifies which program you want to talk to.

Since there is a program at both ends of the network connection, there is a source and destination ports. Ports are actually numbers between 0 and 65565.

Some port numbers identify standard programs (25 = mail server, 80 = web server). Others are just used while a connection is in progress to identify the program making the connection (usually high numbers).

Official list at

`http://www.iana.org/assignments/port-numbers`

Note, there is nothing to stop someone having a program listen on a strange port. If you want to you can run your mail server on port 12345.

Encapsulation/Layering

```
[ether dst]                                  00306503d972
[ether src]                                  000874ba39f2
[type=ip]                                    0800
(version, len, ToS, tot len, ID)             4510 003c 3fac
(flags, frag off, TTL, proto, hdr sum)       4000 4006 e3f1
(src IP, dst IP)                             0a00 030a 0a00 0005
{src port, dst port}                         cb44 0017
{sequence number/ack number}                 ca13 4473 0000 0000
{hdr len, flags=SYN}                         a002
{win, csum, urgent}                          ffff 1212 0000
{tcp options}                                0204 05b4 0103 ...
```

Port Scanning

Port scanning is the equivalent of phoning extension numbers to see if you get an engaged/ringing/out-of-service tone of if you get a person or an answerphone.

With port scanning you send a packet and see what response you get (might be SYN-ACK, might be RST, might be an ICMP message, might be no response at all).

More about port scanning

Port scanning can have a few aims. Network administrators may use it to find what services are running in their networks. (Especially useful if a vulnerability in a program is discovered.)

It can be targeted at a single computer to find all the services it is running. Alternatively it might be targeted at a single service to identify computers running this service. (The latter is very common.)

Example port scan

Nmap, network mapping tool

`http://www.insecure.org/nmap/`

```
17:36:lanczos 3# nmap temp1
Starting nmap 3.50 ( http://www.insecure.org/nmap/ ) at 2004-06-20 17:37 BST
Interesting ports on temp1.maths.tcd.ie (134.226.81.110):
(The 1653 ports scanned but not shown below are in state: closed)
PORT    STATE SERVICE
7/tcp   open  echo
9/tcp   open  discard
22/tcp  open  ssh
111/tcp open  rpcbind
113/tcp open  auth
450/tcp open  tserver

Nmap run completed -- 1 IP address (1 host up) scanned in 9.584 seconds
```

Banner Collection

Some programs identify themselves when you connect.

```
17:35:scooter 11% telnet kac.cnri.dit.ie 25
Trying 147.252.67.9...
Connected to kac.cnri.dit.ie.
Escape character is '^]'.
220 kac.cnri.dit.ie ESMTP Sendmail 8.12.10/8.12.9; Sun, 20 Jun 2004 17:38:55 +0100 (IST)

17:39:scooter 13% telnet kac.cnri.dit.ie 80
Trying 147.252.67.9...
Connected to kac.cnri.dit.ie.
Escape character is '^]'.
GET / HTTP/1.0
HTTP/1.1 200 OK
Date: Sun, 20 Jun 2004 16:39:54 GMT
Server: Apache/2.0.43 (Unix) DAV/2
```

Port tricks

Other clever tricks:

- Firewalls can filter packets based on port numbers and other header information.
- If you send packets with fake source IP addresses, you may be able to hide where your port scan comes from.
- Other machines can be tricked into port scanning for you, if you fake your source address.

- Different operating systems respond to unusual packets in different ways. This allows you to 'fingerprint' the OS running on a machine.
- Sometimes viruses and Trojan programs use unusual packets as a control mechanism.
- Packet sniffers can collect packets to check if they contain unencrypted passwords.
- All traffic from one network to another can be encrypted by adding an extra header to say the packet has been encrypted. This is one way to make a VPN (virtual private network).