CS443 - Networks

Note Title 1/30/2013

- Lab wcs due yesterday
- Next HW posted over crypto
  due Tuesday

Networking Basics: The OSI Model

Application	user application interaction
Presentation	structure representation
Session	session checkpointing and recovery
Transport	reliability
Network	logical addressing, routing
Data Link	physical addressing, 802.11
Physical	media, signal, binary transmission

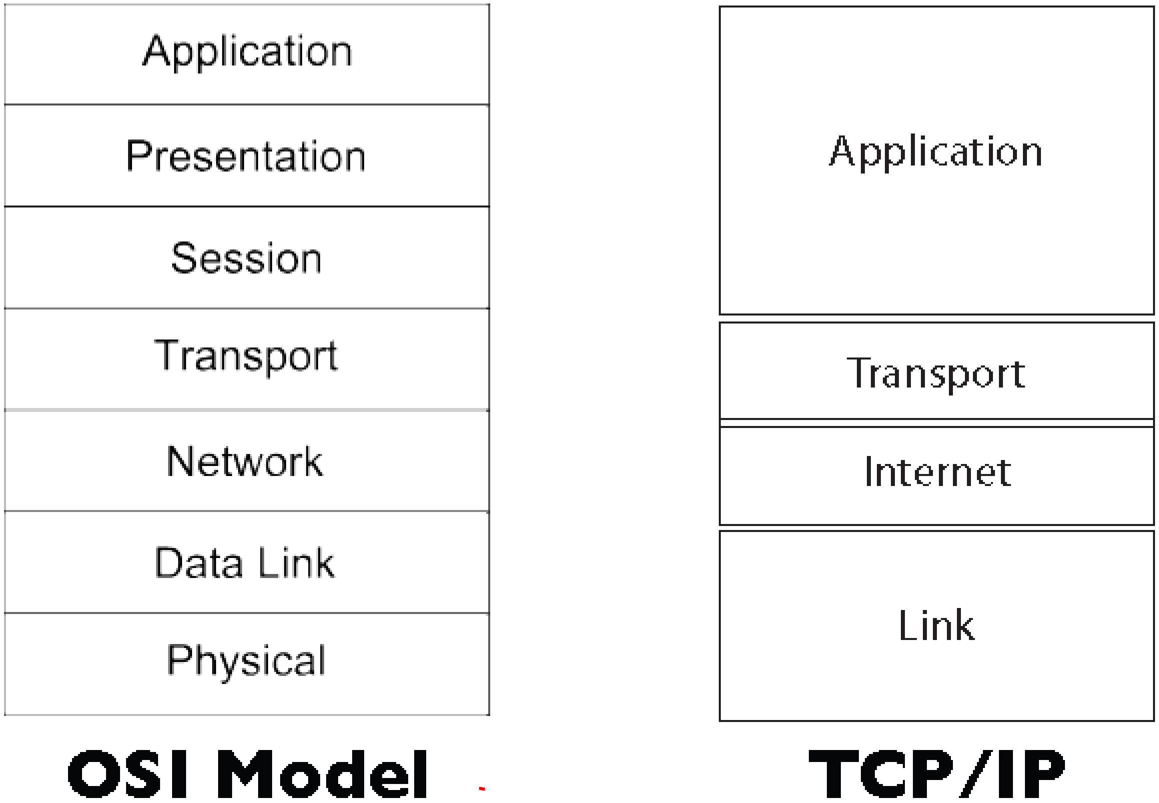
TCP/IP

There are different layes + implementations in OSI Model.

The internet protocol suite (TCP/IP) is an implementation of the OSI.

It doesn't use as fine of granularity, but it also has different "levels".

TCP/IP Layers



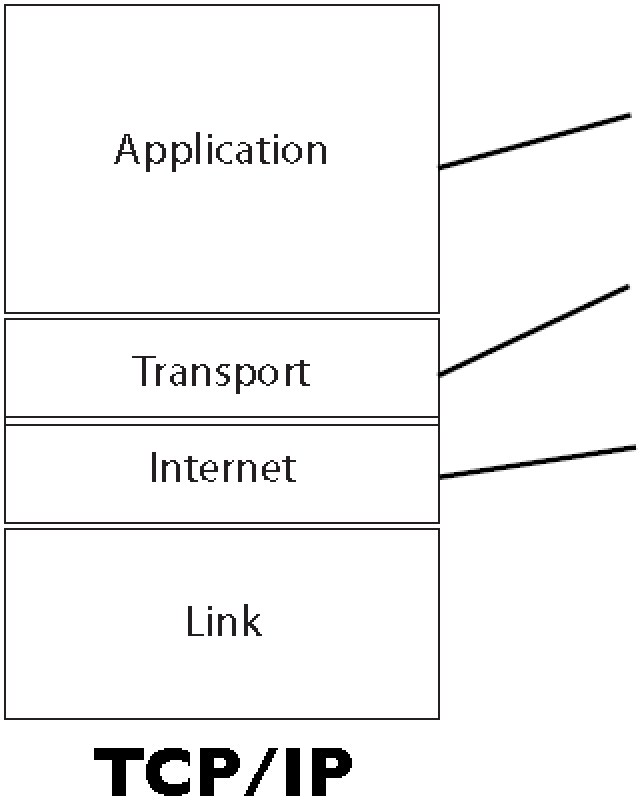
Application
Presentation
Session
Transport
Network
Data Link
Physical

OSI Model

Application
Transport
Internet
Link

TCP/IP

TCP/IP Layers



Application

Transport

Internet

Link

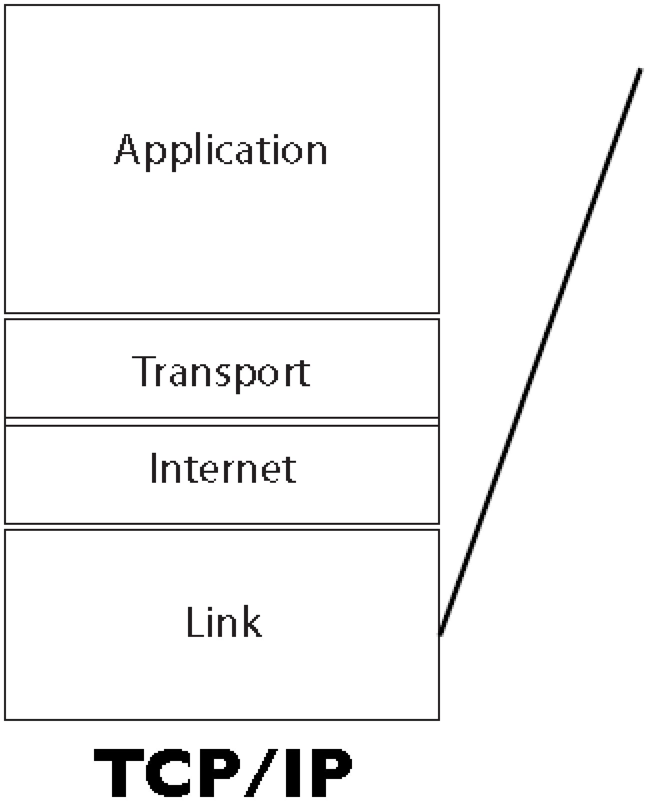
TCP/IP

Determines how an application should use the network.

Handles details of data transmission at the end-points of communication.

Expresses how packets should be forwarded and how packets should be addressed (also called **Network Layer**)

TCP/IP Layers



Sometimes divided into Link Layer and Physical Layer.

Link Layer: Provides for synchronization and transfer of information. Defines how physical machines address each other.

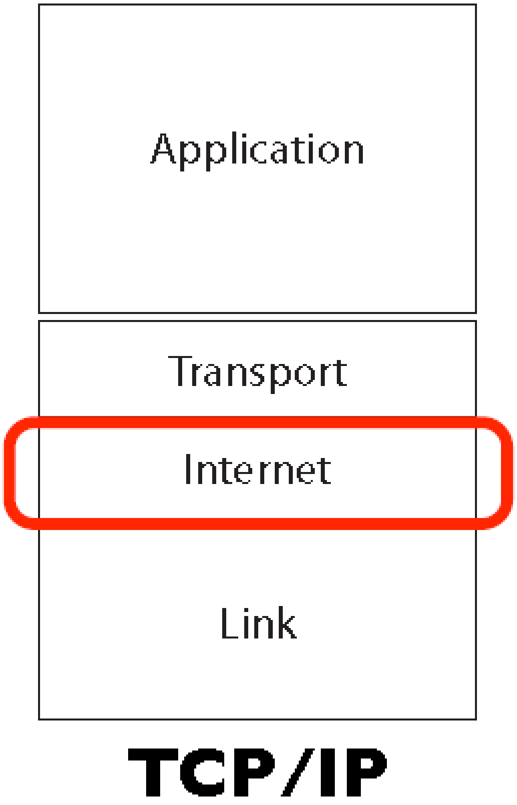
Physical Layer: Defines electrical aspects of sending signals along a wire or wirelessly. Also addresses switch and router hardware.

TCP/IP:

We'll focus on the Internet layer –

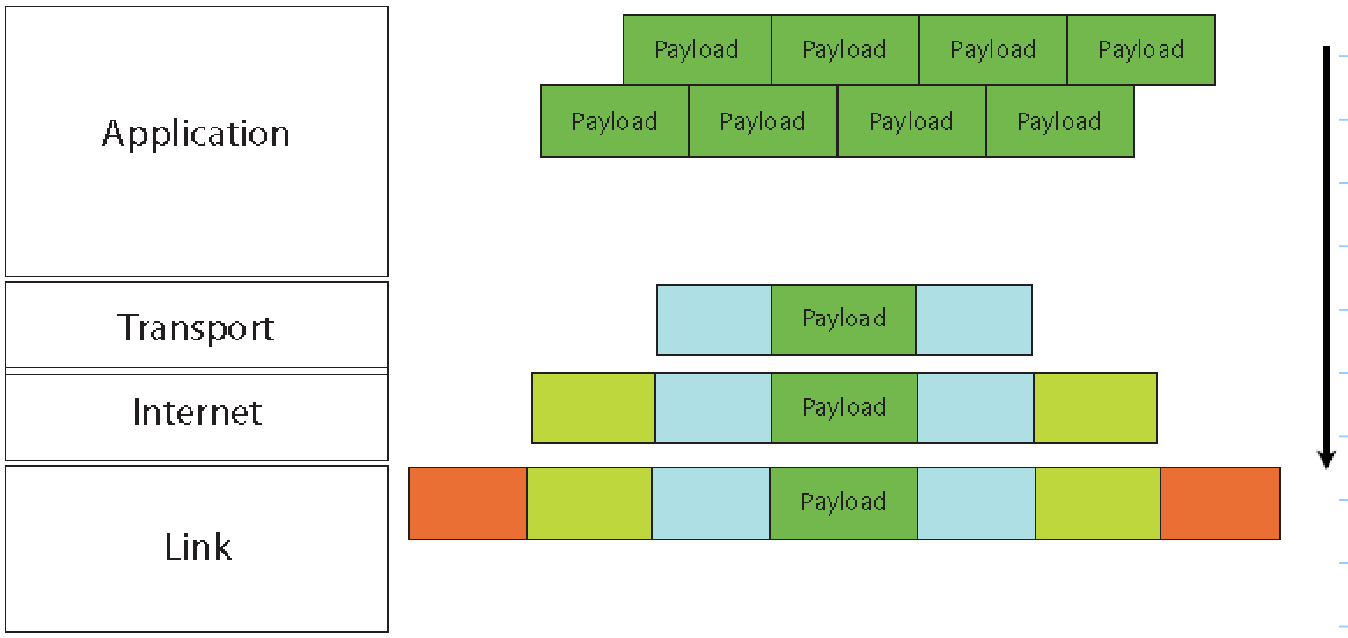
how packets are addressed and forwarded over the network.

(Also called Network layer)



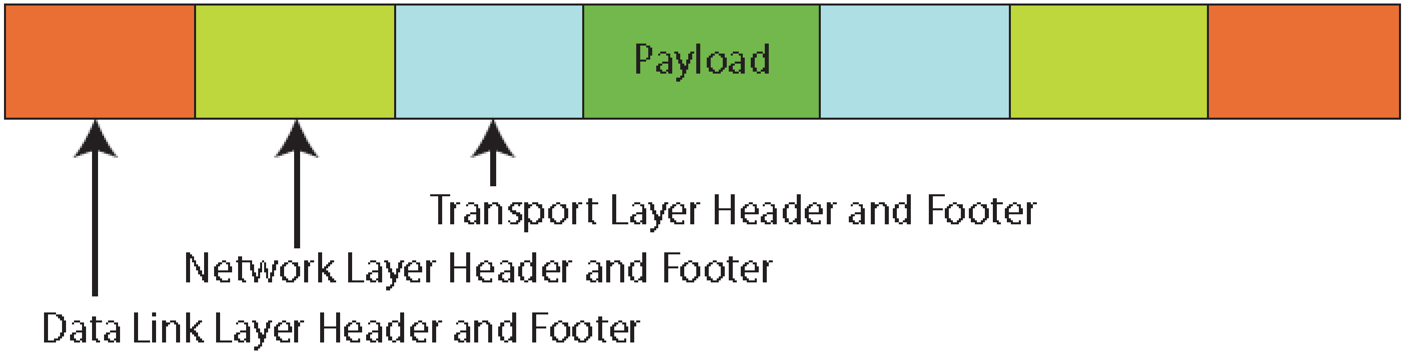
Transmitting Data :

Data is divided in packets, and each layer adds headers.



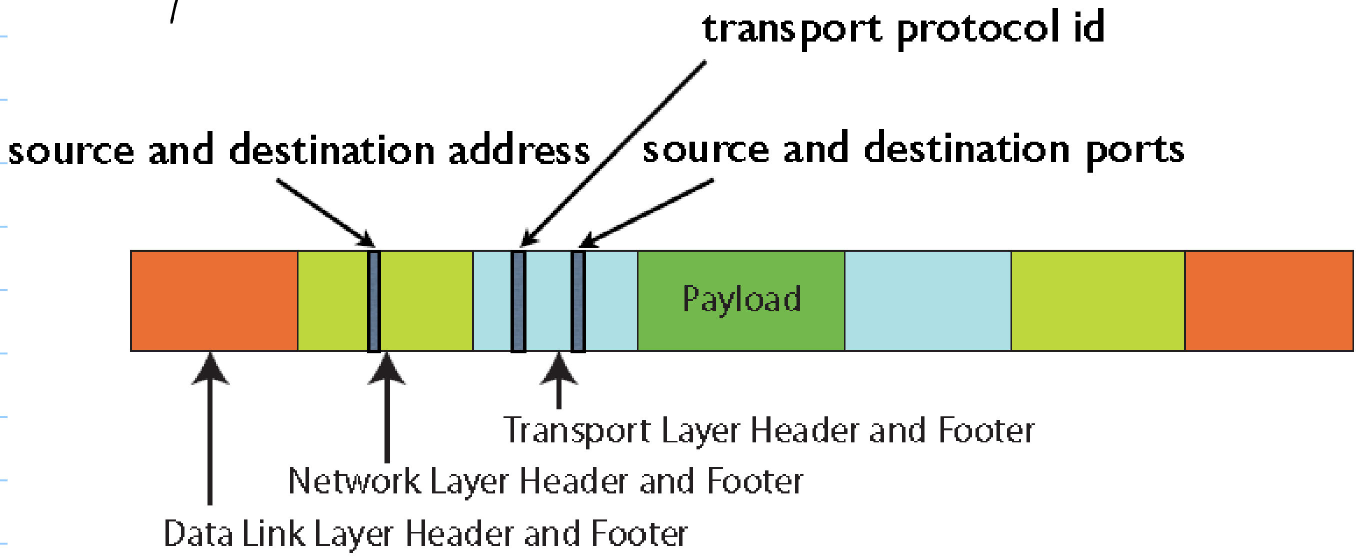
Security View

Certain areas of these headers & footers are very interesting from a security point of view.


Payload
Transport Layer Header and Footer
Network Layer Header and Footer
Data Link Layer Header and Footer

In particular, much information which details possible vulnerabilities is available!

Note: This data can't really be hidden! (Why?)


transport protocol id
source and destination address
source and destination ports
Payload
Transport Layer Header and Footer
Network Layer Header and Footer
Data Link Layer Header and Footer

Relevant Data in Headers

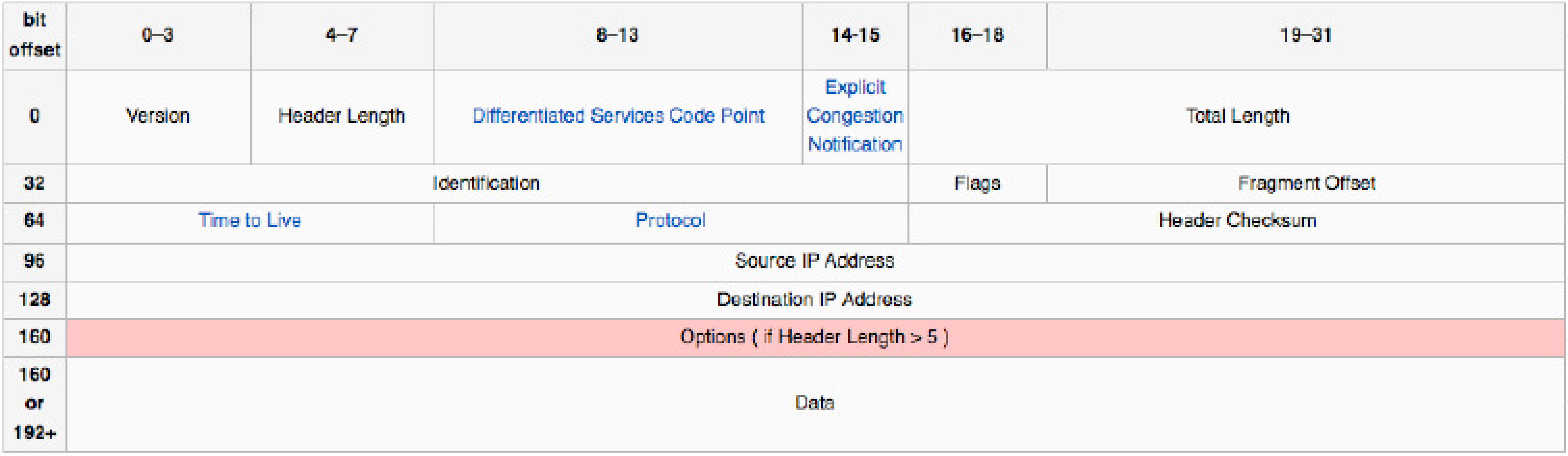
- IP-address : $\underbrace{192}_{0-255}.168.53.1$
- MAC address : 5C:68:AB: . . .

  hard coded to card
- Port number : 0-65535

  80 : webbrowser
- Protocol id : identifies type of traffic

Headers in IPv4:

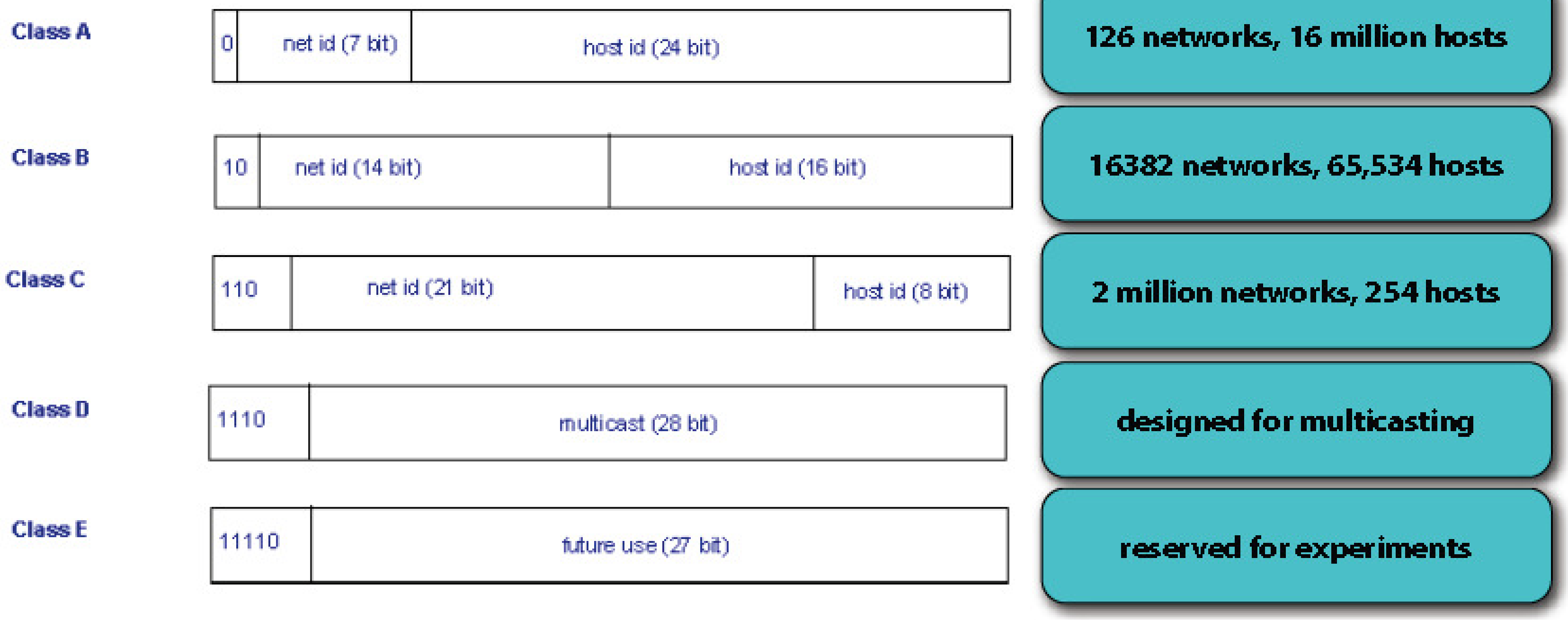
- Divided into 32-bit segments
- Headers are 5 segments long (usually), with data at the end



bit offset	0–3	4–7	8–13	14-15	16–18	19–31
0	Version	Header Length	Differentiated Services Code Point	Explicit Congestion Notification	Total Length	
32	Identification				Flags	Fragment Offset
64	Time to Live		Protocol		Header Checksum	
96	Source IP Address					
128	Destination IP Address					
160	Options (if Header Length > 5)					
160 or 192+	Data					

IPv4

126.255.0.1



Class A	0	net id (7 bit)	host id (24 bit)	126 networks, 16 million hosts
Class B	10	net id (14 bit)	host id (16 bit)	16382 networks, 65,534 hosts
Class C	110	net id (21 bit)	host id (8 bit)	2 million networks, 254 hosts
Class D	1110	multicast (28 bit)		designed for multicasting
Class E	11110	future use (27 bit)		reserved for experiments

Example: Consider the address:

10001000 11100101 11001001 0001000

128+64+32+ 4+1 128+64+8+1 8 4 2 1

Class? B: 136.229.201.8

What IP?

Problem:

IPv4 was designed in 1981.

Classes A-C allow for under 4.3 billion address total.
(Reality - much smaller!)

Conclusion: out of space

Solutions

1. IPv6
2. NAT
3. Subnetting

None is a perfect cure but all have been used to offset issues.

① IPv6

- Invented in 1998
- Allows for 128-bit addresses (versus 32-bit) 2^{27} vs. 2^{128}
- Transition has been slower than expected: as of Nov. 2012, reported to be ~1% of total traffic.

IPv6 details:

- Packet headers are twice as long.
- However, processing is actually simpler + faster at routers.
- Privacy extensions exist to "hide" identity: OS generates random host identifier.

② Network Address Translation

A router stands between a private network & outside world.

Every internal IP address maps to a single IP/port which is all outside sees.

(Combines well with firewall functionality.)

Pros of NAT:

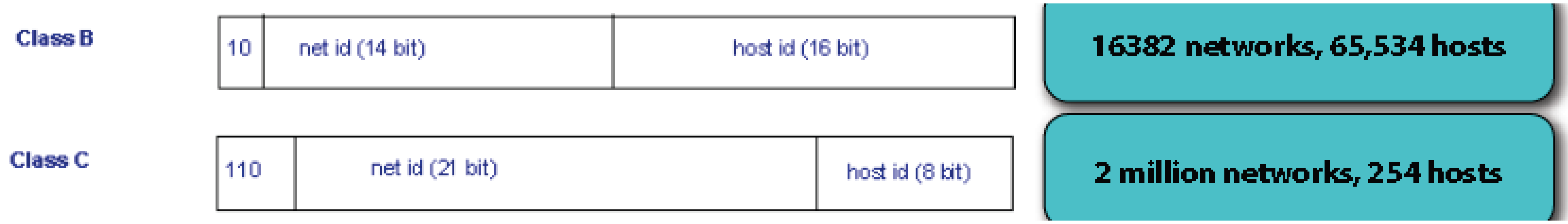
- more secure
- bandwidth saver
- cheaper

Cons:

- point of failure
- slower

3 Subnetting

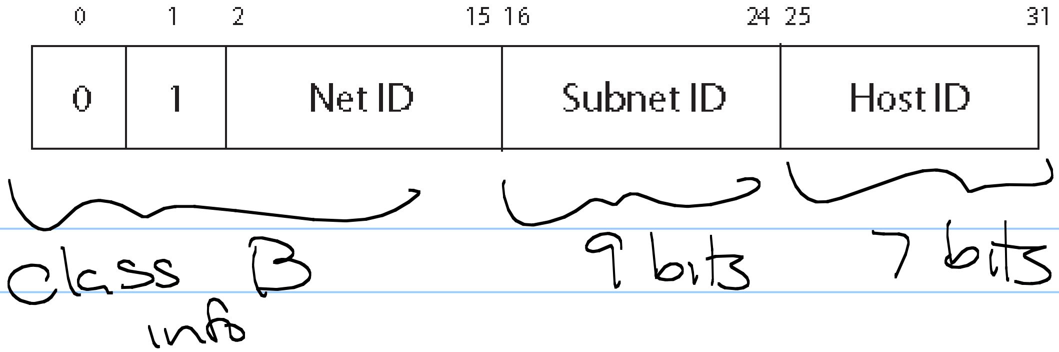
There is a jump between class B and C sizes.



Class B	10	net id (14 bit)	host id (16 bit)	16382 networks, 65,534 hosts
Class C	110	net id (21 bit)	host id (8 bit)	2 million networks, 254 hosts

Many larger networks actually subdivide them further.

Example:



subnets : 2^9

hosts in each : 2^7 machines

Subnets cont:

Every computer gets a subnet mask,
eg 255.255.255.128

11111111 11111111 11111111 10000000

As well as an IP: 128.96.34.15

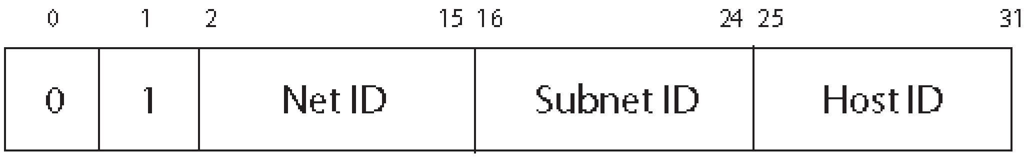
10000000 01100000 00100010 00001111

Take the bitwise AND to get the subnet versus host id:

$$\underbrace{11111111 \quad 11111111 \quad 11111111 \quad 10000000}$$

↓

$$\overbrace{10000000 \quad 01100000 \quad 00100010 \quad 00001111}$$



0	1	2 … 15	16 … 24	25 … 31
0	1	Net ID	Subnet ID	Host ID

Local Area Networks

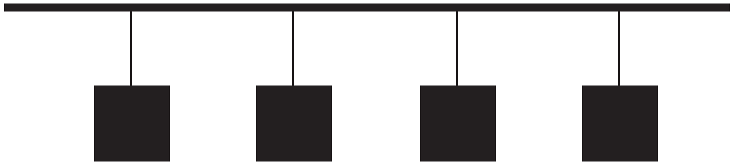
A LAN is a "small interconnection infrastructure that typically uses a shared transmission medium".

From Computer and Communication Networks by N. Mir

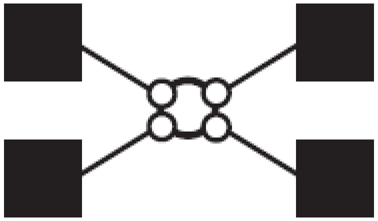
Note: A single LAN may actually be huge.

"Local" is relative, but generally these all connect to same router or switch.

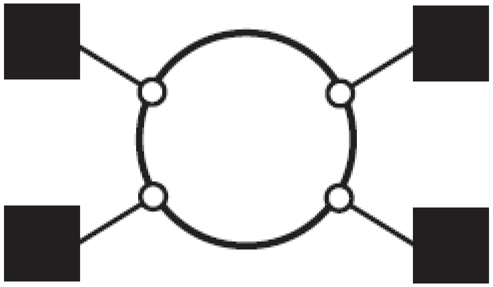
LAN Topologies



Bus Configuration

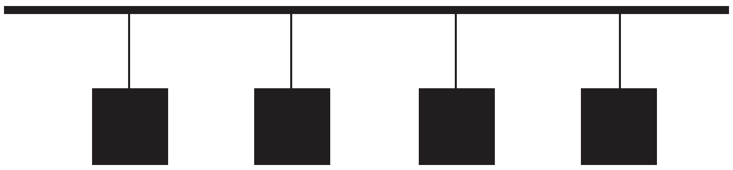


Star Configuration



Ring Configuration

Bus Configuration



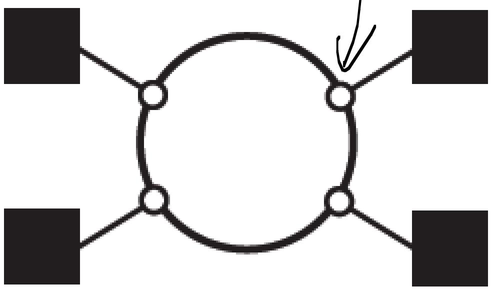
Bus Configuration

Transmissions are propagated on the bus in both directions.

All users (locally) will recieve all packets.

Ring Configuration

repeaters



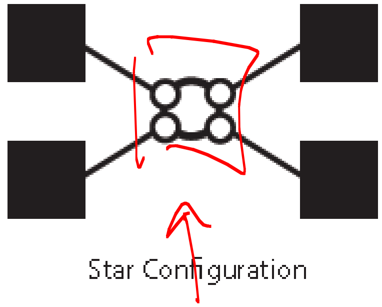
Ring Configuration

Sender gives packet to repeater.

Repeater forwards until reaches destination.

If reaches original source, not forwarded any further.

Star configuration



Star Configuration

Center of "star" is a multi-port hub or switch.

Frames are sent to center, which either broadcasts or sends to targeted destination.

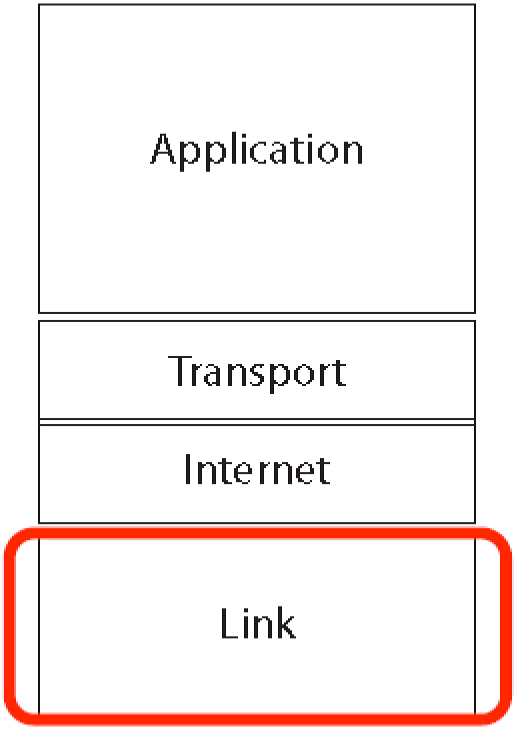
Note:

None of these have much security!

All are vulnerable to attack and to eavesdropping.

Adding Security

To address this, we'll dive down a level to the Link layer.



TCP/IP

Two major issues:

1. System protection:

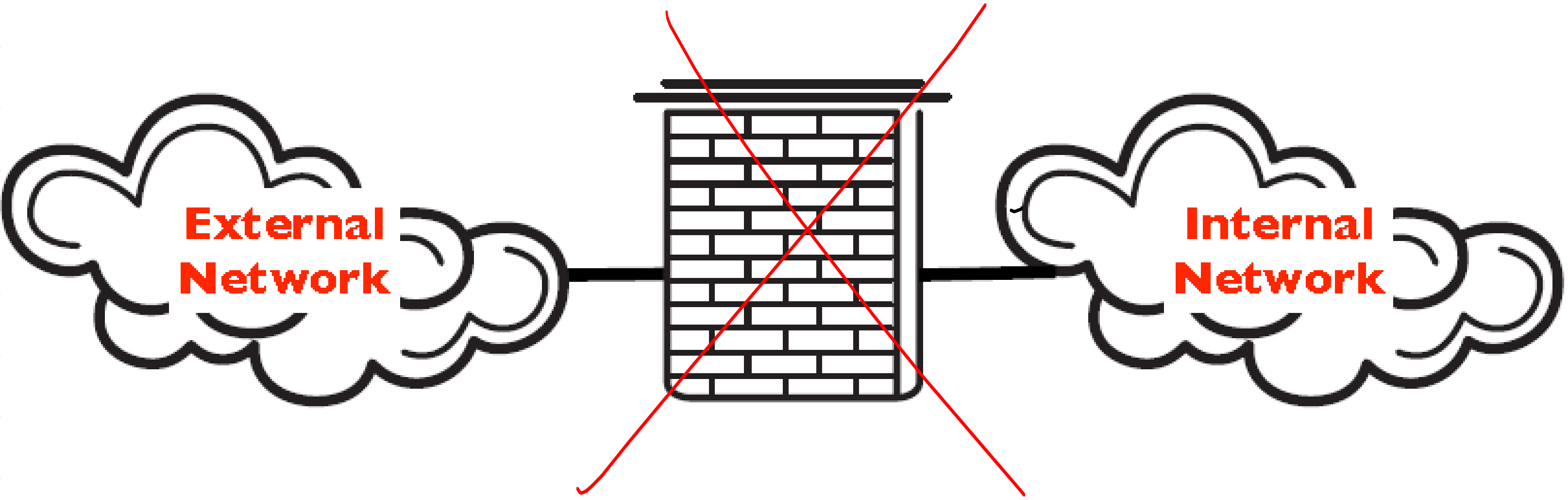
   Machines must read packets, but info in them could be dangerous.

2. Hiding information:

   Nothing in IP prevents intermediaries from reading payloads of packets.

Firewalls : System Protection

All traffic from the inside network to the outside (or vice versa) must pass through the firewall.



Different Systems

large infrastructure

- Firewalls can be dedicated systems, or pieces of local Software.

resource hogs, local & customizable

- Many different types, with different levels of saftey depending of the amount of checking or monitoring.

(Generally, as always, faster means less. secure.)

Packet Filtering Firewalls - fast

Rules are based on the packet headers.

Sometimes called a "stateless firewall", since has no memory of previous connections or more complex monitoring.

Generally, packets are simply authorized based on source or destination IPs and ports, as well as particular protocol ids.

Proxies

A proxy computer is an intermediate agent or server that acts between two endpoints without allowing direct communications.

Ex: HTTP proxy:

- track webpage connection
- create local copies of data
- block certain communications
- single place for updates, filters, etc.

Proxy Firewalls : stateful monitoring

A proxy firewall bases access control on contents of packets as well as header info.

Advantages : - best security

Disadvantages :
- expensive
- single point of failure
- throttle on speed

More on stateful firewalls

In general, TCP connections fix a port number for all communication.

(Higher number ports are reallocated as needed for these connections.)

Stateful firewalls track established TCP connections & only allow traffic to specific ports for duration of one connection.

Example : IPTables

A native Linux firewall tool providing stateful monitoring.

Can be run on an individual machine, or on a server to protect larger networks.

This tool will be the focus of the next lab.

Sample: interactive use:

```
$ iptables -t filter -A INPUT -m state --state NEW -p tcp -s 192.168.0.1 --dport 23 -j REJECT
```

`iptables`

We're going to use the iptables tool to insert a new rule into netfilter.

`-t filter`

This rule is going to go in the filter table, which is the built-in packet filtering table. This rule will apply only to:

`-A INPUT`

packets that have been put into the `INPUT` *chain either by the kernel or by some previous rule and which:*

`-m state --state NEW`

represent a new connection,

`-p tcp`

are Transmission Control Protocol (TCP) packets,

`-s 192.168.0.1`

are from the host 192.168.0.1,

`--dport 23`

and are destined for port 23.

`-j REJECT`

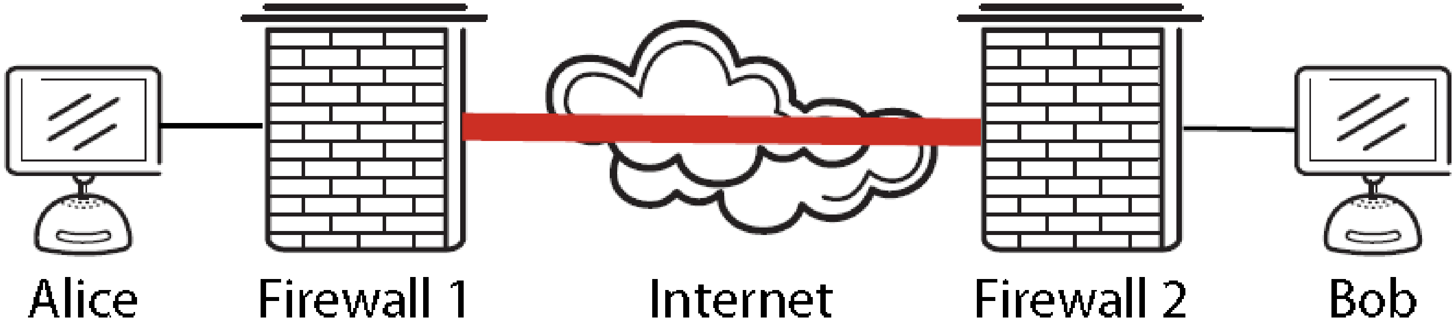
Reject any matching packet. Processing of all packets matching this rule will instantly jump to the built-in target REJECT, which means that the packet will be rejected by the kernel with some kind of network error message.

Notes on iptables:

- Can interact from command line, or (more commonly) edit the shell file controlling it.
- Requres root access!
- This is actually a user interface tool for adminstering netfiter functions in the Linux kernal.
- See assignment for full discussion and overview.

IPSec : Hiding information

Data sent over a network is inherently insecure. IPSec is a protocol that adds encryption at a low layer of TCP/IP model.

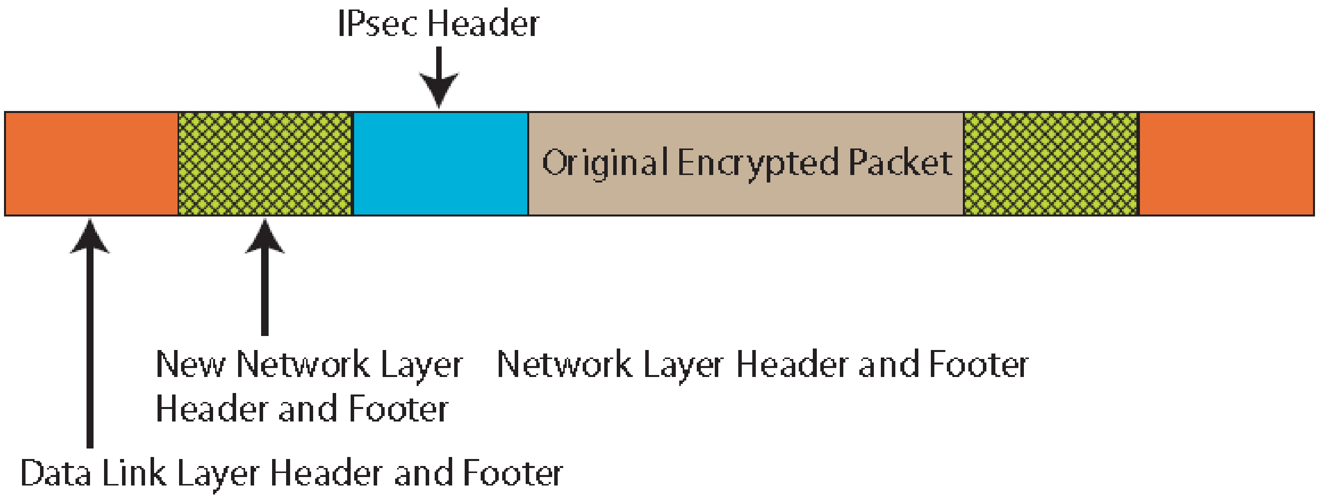


Modes

- In transport mode, only the packets are encrypted. However, authentication headers provide assurance that IP addressed can't be modified (since hash value is invalidated).
- In tunnel mode, the entire packet is encrypted, and new headers are created.

(This is how VPNs are created.)

Tunnel Mode

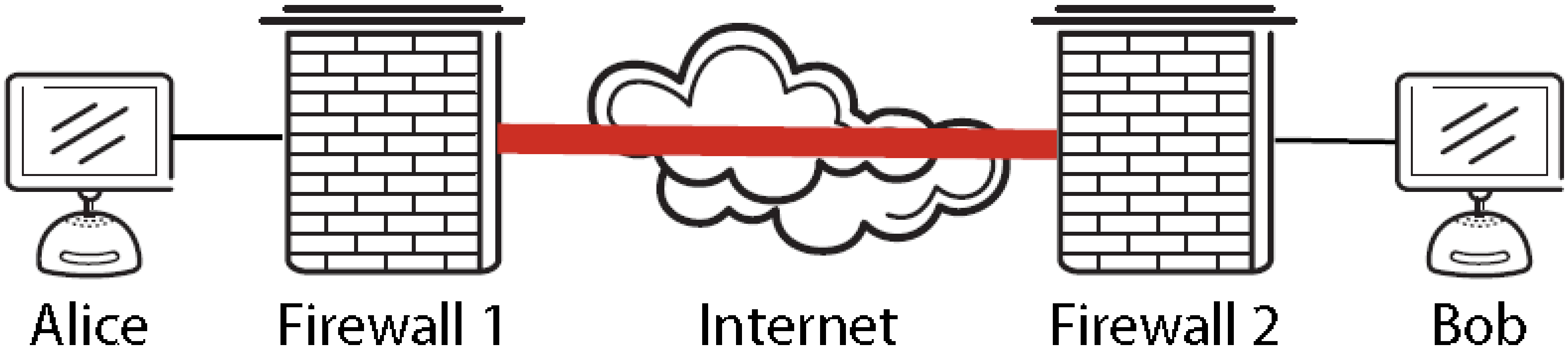

IPsec Header
Original Encrypted Packet
New Network Layer Header and Footer
Network Layer Header and Footer
Data Link Layer Header and Footer

“Refers to keeping the original IP packet intact and adding a new IP header and IPsec information outside.

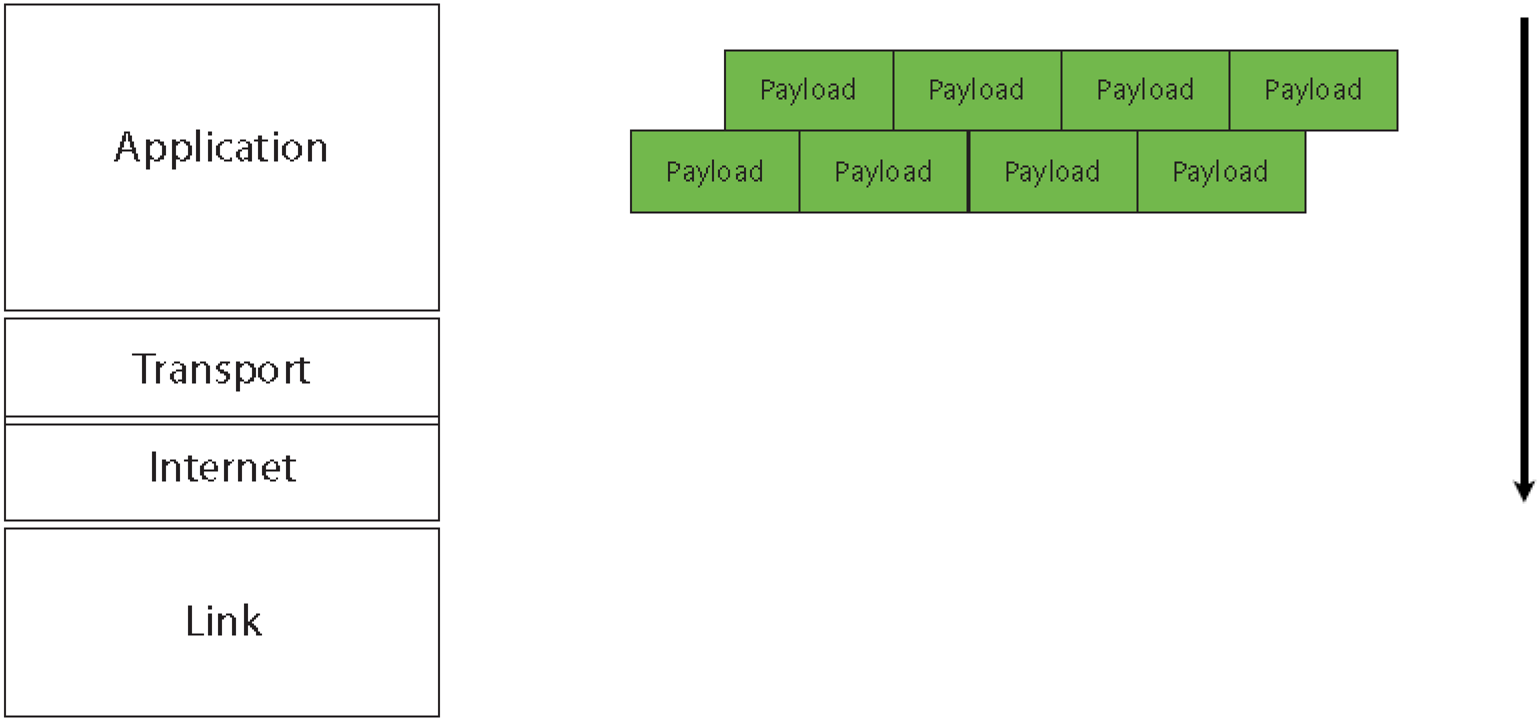
Content taken from "Network Security: Private Communication in a Public World."

An example of tunnel mode:

Alice wants to send Bob a message.



Step 1 :



Application

Transport

Internet

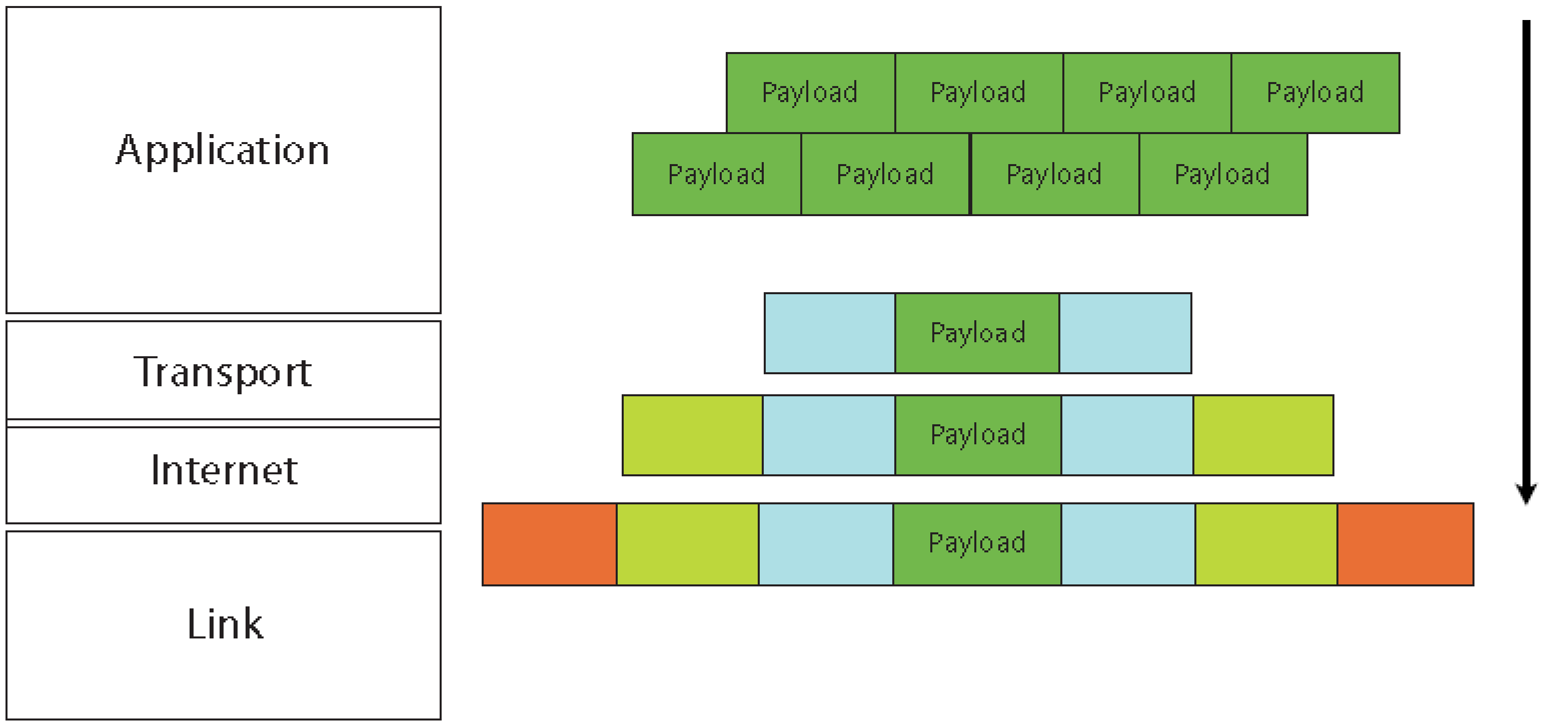
Link

Payload Payload Payload Payload

Payload Payload Payload Payload

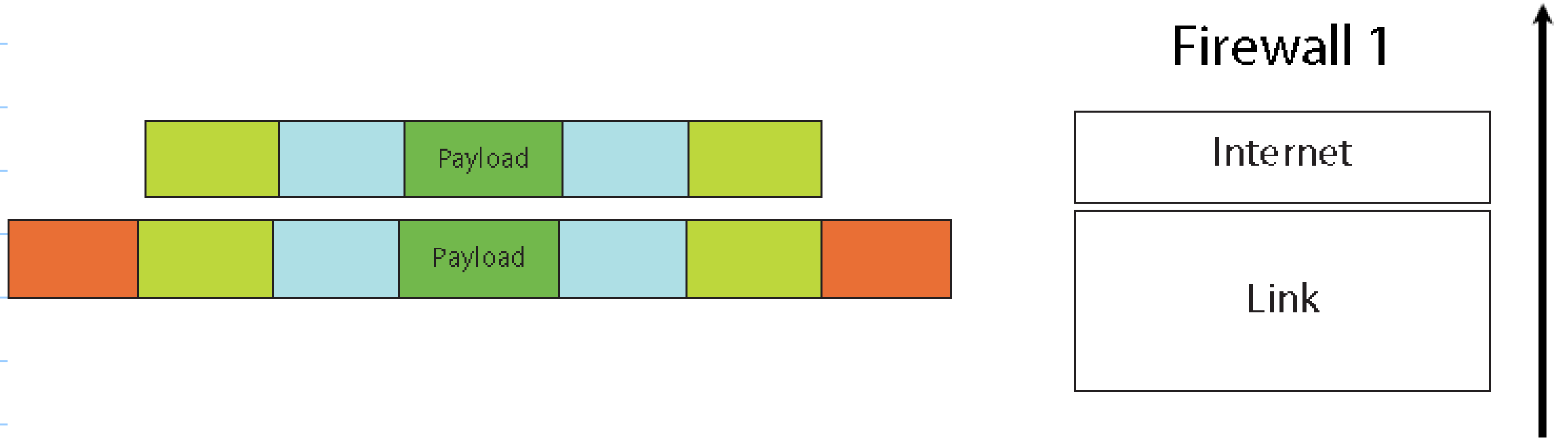
Alice sends an e-mail as usual.

Step 2 :



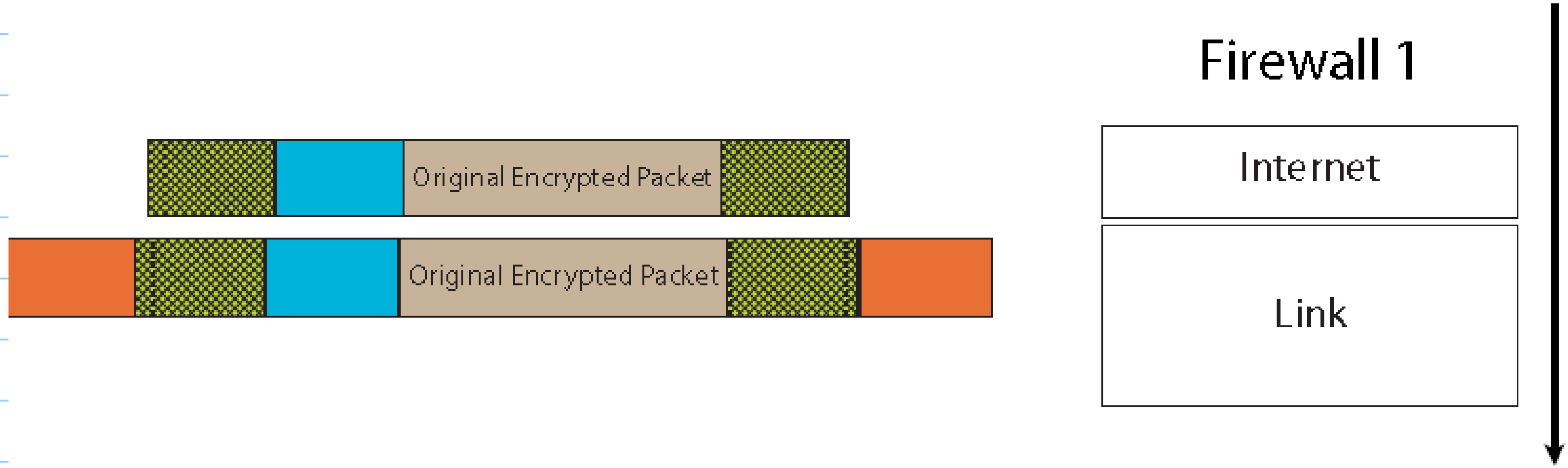
The e-mail is divided into packets. Headers are added at each layer.

At the firewall:
(either internal or external)



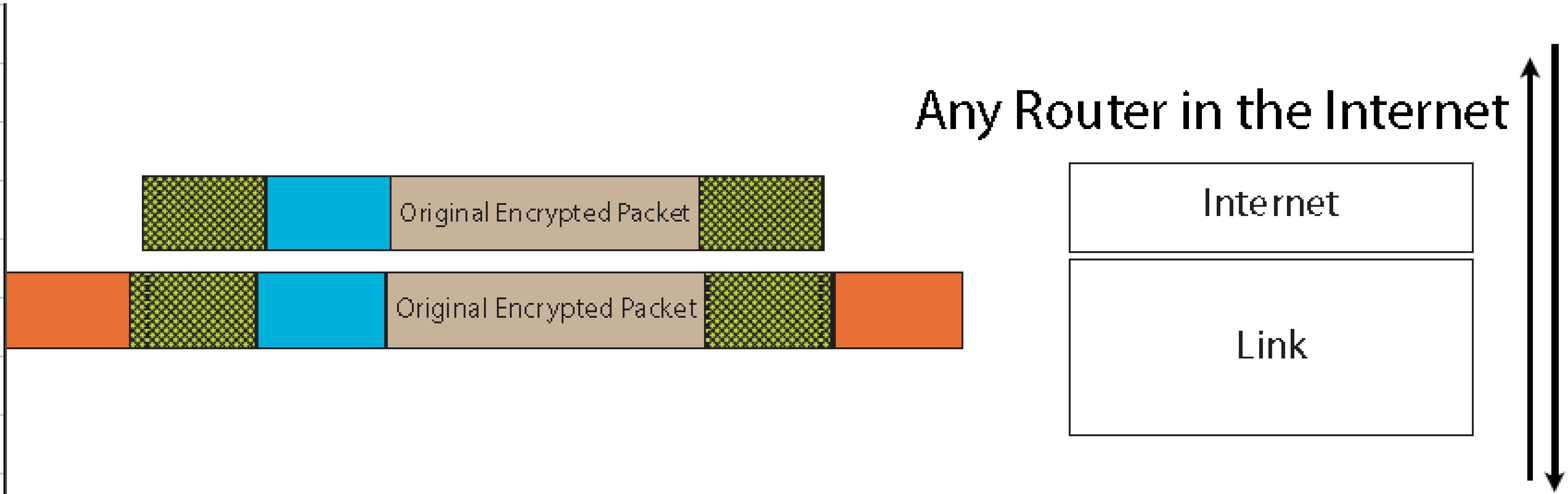
Each packet makes its way to Alice's firewall.

At the firewall (cont):



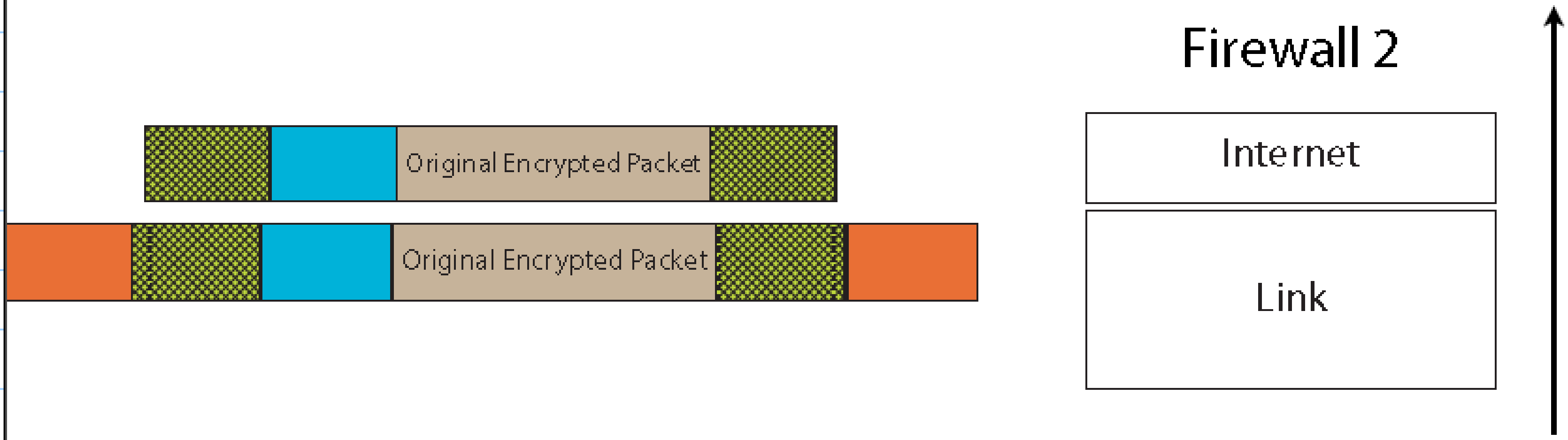
The IPsec-enabled firewall encrypts the packet, adds a IPsec header and adds a new IP header.

Intermediate Nodes


Any Router in the Internet
Original Encrypted Packet
Original Encrypted Packet
Internet
Link

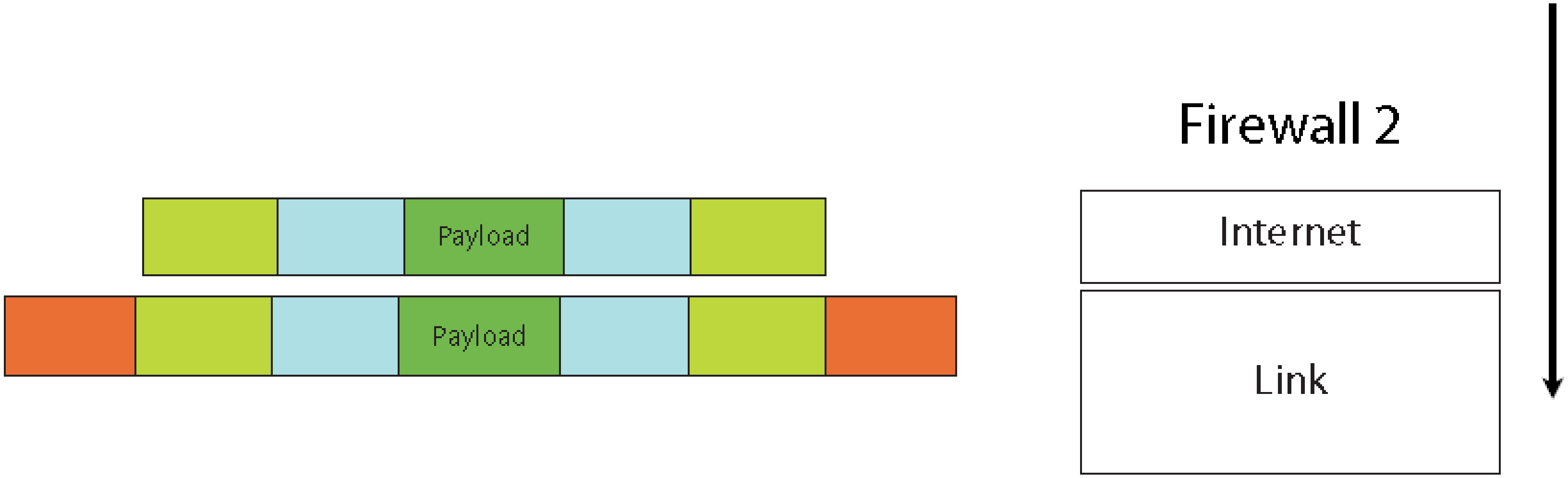
As the IPsec packet is sent through the Internet, routers will look only at the new IP header.

At the next firewall:



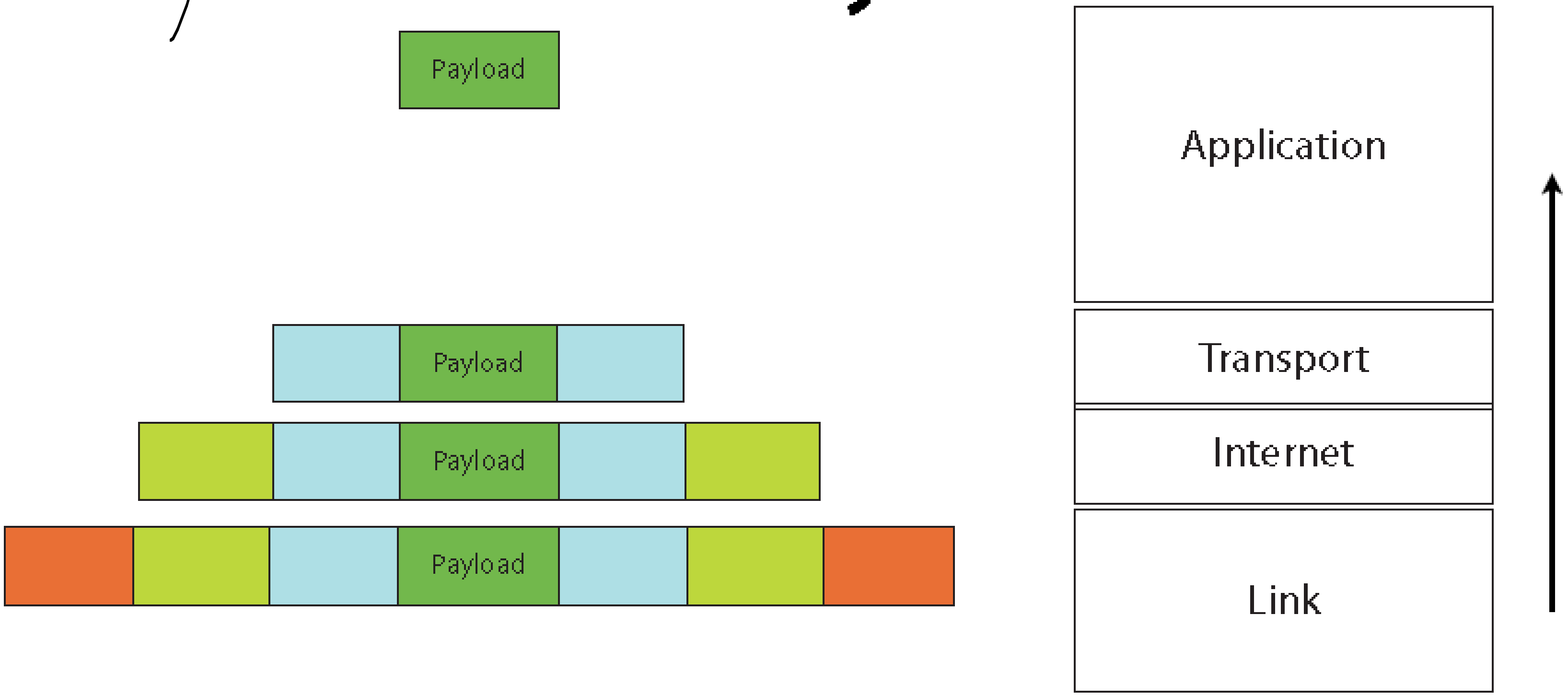
When the IPsec packet reaches Bob's firewall 2...

Firewall 2 resends:



Firewall 2 decrypts it, gets the original packet, and forwards it along to Bob.

Finally, at the destination:



At Bob's machine, all the headers are removed and the packets are assembled into Alice's e-mail.

Advantage of IPSec :

Encryption & security is at a low level.

So unlike a secure protocol (like SSH), this builds security <u>on top</u> of other protocols.

Provides authenticity, integrity, <u>and</u> confidentiality.

Next time: