PATTERNS IN NETWORK ARCHITECTURE:

VERTICAL COMPOSITION

OR

LAYERING
**PURPOSE:**

**TO BUILD A NETWORK WITH A LARGER SPAN OUT OF SMALLER, HETEROGENEOUS NETWORKS**

The Internet has its own name space, protocols, headers, routing, etc.

Each underlay network has its own name space, protocols, headers, routing, etc.
OTHER PURPOSES

TO BUILD A NETWORK WITH BETTER PERFORMANCE OR RELIABILITY ON TOP OF AN EXISTING NETWORK
for example, Resilient Overlay Networks

to share the resources of an existing network in a disciplined way
for example, Virtual LANs

to build a network with links that offer a superior communication service
for example, Virtual Private Networks

during the semester, be on the lookout for other purposes!
ATTACHED NODES AND LOCATIONS

A could have locations in multiple networks (gateway, multihoming)

at A, location[U] = A'

B' could be the node in U where nodes from multiple networks are attached (sharing)

at B', attached[O] = B

it is strange for a machine to have multiple members in one network, but that is how IP works

different IP interfaces of one machine, with distinct IP addresses

what are the consequences?
THE DETAILS OF LAYERING 1

A sends packet in session s encapsulating it in header H

1

A sends packet in session s encapsulating it in header H

2

at A, forwarding[H, Self] = k1

3

B acquires packet on link with local linkIdent k2

4

B acquires packet on link with local linkIdent k2

5

at B, forwarding[H,k2] = k3

6

C acquires packet on link with local linkIdent k4

7

C acquires packet on link with local linkIdent k4

8

H.destination = C, so C receives packet in session s, decapsulating it from header H

8
THE DETAILS OF LAYERING 2

3 A transmits packet on link with local linkIdent k1

4 B acquires packet on link with local linkIdent k2

A B C

header H'

3 0' at A, uses[k1] = (U,s') and location[U] = A'

9' at B', implements[s'] = (O,k2) and attached[O] = B

A' B'

1' A tells A' to send packet in session s', encapsulating it in header H'

8' B' receives packet in session s', decapsulating it from header H'

header H'

source = A' destination = B' sessionIdent = s'
THE DETAILS OF LAYERING 3

3. A transmits packet on link with local linkIdent k1

4. B acquires packet on link with local linkIdent k2

header $H'$

$source = A'$

$destination = B'$

$sessionIdent = s'$

$overlay = O$

$Network O$

$Network U$

$store$ uses$[k1] = (U,s')$

$store$ implements$[s'] = (O,k2)$

at A, location$[U] = A'$

A asks A' for an implementation $s'$ of $k1$ to B;

location$[B,U] = B'$

STORE

B' receives packet in session $s'$, decapsulating it from header $H'$ and seeing overlay = $O$

B' asks B for a linkIdent $k2$ implemented by $s'$

STORE

1'. A tells A' to send packet in session $s'$, encapsulating it in header $H'$

8'. B' receives packet in session $s'$, decapsulating it from header $H'$ and seeing overlay = $O$

at B', attached$[O] = B$

Network state can be set up dynamically
A transmits packet on link with local linkIdent k1

B acquires packet on link with local linkIdent k2

there is a direct, dynamic link from any node to any other attached to the same LAN—no forwarding needed

A' gets the location of B by broadcasting an ARP request

B' receives packet, decapsulating it from header H'

H' does not need s' and O because they are constants

source = A'
destination = B'
sessionIdent = s'
overlay = O
OTHER PURPOSES

TO BUILD A NETWORK WITH BETTER PERFORMANCE OR RELIABILITY ON TOP OF AN EXISTING NETWORK

for example, Resilient Overlay Networks

TO SHARE THE RESOURCES OF AN EXISTING NETWORK IN A DISCIPLINED WAY

for example, Virtual LANs

TO BUILD A NETWORK WITH LINKS THAT OFFER A SUPERIOR COMMUNICATION SERVICE

for example, Virtual Private Networks

during the semester, be on the lookout for other purposes!
IP NETWORK LAYERED ON A VLAN?

3 A transmits packet on link with local linkIdent k1

4 B acquires packet on link with local linkIdent k2

0' at A, location[U] = A'; A asks A' for an implementation of k1 to B; location[B,U] = B'

9' at B', attached[O] = B; B' asks B for a linkIdent k2 from A

1' encapsulate packet in header H' and send

A' gets the location of B by broadcasting an ARP request

B' receives packet, decapsulating it from header H'

header H'

source = A'
destination = B'
sessionIdent = s'
overlay = O

this LAN is shared among VLANs, but it cannot be just an Ethernet, because it has IP links

H' does not need s', O is the VLAN tag

must only broadcast to members of VLAN
IP NETWORK LAYERED ON A VLAN

IP SUBNETWORK WITH PREFIX A
members of each subnet directly connected

A1 ------- A2 ------- A3

VLAN X
M1 ------- M2 ------- M7 ------- M3

links are a spanning tree

PHYSICAL LAN has
host members with names M1, M2, M6
switches with names M3, M7

IP BACKBONE has
routers with names A3, B4

IP SUBNETWORK WITH PREFIX B

B4 ------- B5 ------- B6

VLAN Y
M4 ------- M5 ------- M6 ------- M3

one machine does 3 completely different things (name, links, forwarding) in its roles as A3, M3 in X, M3 in Y

PHYSICAL LAN has
host members with names M5, . . .
switches with names M4
DISCUSSION OF

“A SURVEY OF VIRTUAL LAN USAGE IN CAMPUS NETWORKS”
OTHER PURPOSES

TO BUILD A NETWORK WITH BETTER PERFORMANCE OR RELIABILITY ON TOP OF AN EXISTING NETWORK
for example, Resilient Overlay Networks

TO SHARE THE RESOURCES OF AN EXISTING NETWORK IN A DISCIPLINED WAY
for example, Virtual LANs

TO BUILD A NETWORK WITH LINKS THAT OFFER A SUPERIOR COMMUNICATION SERVICE
for example, Virtual Private Networks

during the semester, be on the lookout for other purposes!
WHY A VIRTUAL PRIVATE NETWORK?

these links are not secure!

data could be read or tampered with

attackers could insert packets with false source addresses

there could be DoS attacks, replay attacks, etc.
Your home

Public Internet

Your employer's private network

E is an address in your employer's private network

TCP session

Secure (encrypted) link

IP forwarding

IPsec session

IP forwarding
**IPsec AND NAT TRAVERSAL**

P is an IP address in your home network

NAT has an IP address in your ISP’s network

the IP session must be able to traverse the NAT

the NAT is expecting to see TCP or UDP ports as the session identifier, but an IPsec packet does not have these

so the answer is some sort of ad hoc fix built into the NAT, helped by the fact that the IPsec session begins with the Internet Key Exchange (IKE) protocol using UDP port 50

an IPsec packet has Security Parameters Indices (SPIs), but they are different in each direction
PROPERTIES OF LAYERING 1

Usually, many sessions in a network share the resources of its links.

Usually, session packets must be routed over a path of multiple links to get to their destinations.

With layering, a network can create a dynamic, source-to-destination link for each session.

This is possible because an underlay will implement the link as a session, and routing in the underlay will do all the work.
PROPERTIES OF LAYERING 2

FOR A PARTICULAR Overlay AND UNDERLAY . . .

. . . WHAT ARE THE RELATIONSHIPS BETWEEN LINKS
AND THE SESSIONS THAT IMPLEMENT THEM?

one-to-one is good

one-to-many is awkward

- when a packet is transmitted on the link, requires a mechanism to choose which session to use

many-to-one is worse

- when a packet is received in the session, there is no way to know which link should acquire it

grouping of packets is done with sessions, and we have excluded this mechanism

there is no reason to do this—extra sessions are cheap
PROPERTIES OF LAYERING 3

A network can have as many virtual links as are required . . .

. . . implemented one-to-one by as many sessions as required

what is wrong with the word “tunneling”? it implies “link over path” layering

○ ignores the possibility that the underlay session protocol could provide a service

○ ignores the need (for general purposes) to send a session identifier and overlay

WHAT PROPERTIES ARE REQUIRED OR DESIRABLE?

WHAT PROPERTIES SHOULD BE VERIFIED, AND HOW?
In the underlay, session destination must be reachable from session source.

*note that this is a motivation for reachability requirements in the underlay*

Two different links in the overlay are implemented using different resources in the underlay.

Compute the load on a network, based on its overlays.

Compute the capacity of a network, based on its underlays.
The “Details of Layering” slide showed a step-by-step algorithm for packet processing, in networks that follow the model.

Imagine that we wrote a program to do this processing in any network.

Customizations:

- specific types for names, link identifiers, session identifiers
- extra, protocol specific information in headers
- functions like . . . can become . . .
  
  location \([A, U] = A'\)
  attached\([B', O] = B\)

Optimization:

- compile efficiently to run where it needs to (router, host, VM, NIC, etc.)
WHAT DOES THE COMPOSITION OF RON AND A VPN LOOK LIKE?

... RON AND A VLAN?

... A VLAN AND A VPN?

... ALL THREE?
RON LAYERED ON A VPN

- RON flow
- RON links
- IPsec sessions
- Internet paths
VPN LAYERED ON A RON

**IPsec session**

**virtual link**

**RON flow**

**RON links**

**implements**

**UDP**

**Internet paths**
A BETTER IDEA

If both IPsec and RON had “normal” or standard session identifiers rather than something quirky, there would be no problem with running IPsec as a session protocol in a RON network.
DISCUSSION OF

"RETHINKING THE DESIGN OF THE INTERNET: THE END-TO-END ARGUMENTS VS. THE BRAVE NEW WORLD"