Networking Fundamentals: Underlay and Overlay Networks

Modern networking is commonly designed in layers.
Two important concepts are:

- Underlay
- Overlay

These terms describe the relationship between a foundational network and the services operating on top of it.
A simple way to think about it:

- The underlay provides connectivity
- The overlay uses that connectivity to create additional services or logical networks
- The overlay depends on the underlay to function.

Core Definitions

Underlay Network

The underlay is the physical or foundational network infrastructure that provides transport between devices.
The underlay is responsible for:

- Physical connectivity
- Packet forwarding
- Basic reachability
- Routing between endpoints
- Transporting frames or packets

Examples:

- Copper or Fiber cabling — basic physical connectivity
- Ethernet switching — Layer 2 forwarding
- IP routing — Layer 3 forwarding
- MPLS transport networks
- Internet connectivity

The underlay answers the question:
"How do packets physically get from point A to point B?"

Overlay Network

The overlay is a logical or virtual network built on top of another network.
The overlay adds:

- Encapsulation
- Virtualization
- Encryption
- Segmentation
- Additional services
- Logical topologies

Examples:

- VPN tunnels
- VXLAN
- GRE
- SD-WAN
- MPLS VPNs
- IPsec encryption

The overlay answers the question:

"What additional service or logical network is operating over the transport network?"

Fundamental Concept
The overlay depends on the underlay.
If the underlay fails:

- The overlay fails
- Tunnel protocols fail
- VPNs disconnect
- Virtual networks stop functioning

A common troubleshooting mistake is focusing only on the overlay while the underlay has routing or connectivity issues.

Example 1 — FM Radio
Underlay
The RF carrier signal is the underlay.
It provides the transport mechanism through the air.
Overlay
The modulated audio information is the overlay.
The music or voice is carried by modifying the carrier signal.
Important Note
This is not a traditional computer networking example, but it is an excellent analogy for understanding the concept.

Example 2 — Ethernet
Underlay
The physical infrastructure is the underlay:

- Copper cable
- Fiber cable
- Optical transceivers
- Physical signaling

Overlay
Layer 2 Ethernet frames operate over the physical infrastructure.
Examples:

- MAC addressing
- VLANs
- Ethernet switching

Clarification
Ethernet itself is usually considered part of the foundational transport system, but logically:

- Physical signaling = underlay
- Layer 2 frame forwarding = overlay

Example 3 — Layer 3 Networking
Underlay
The Layer 2 network provides transport for IP packets.
Examples:

- Ethernet
- VLANs
- Switching fabric

Overlay

IP packet forwarding operates as the overlay.
Examples:

- IPv4
- IPv6
- Routing protocols

Clarification
In enterprise networking, IP is often considered part of the primary underlay itself.
However, from a layered design perspective:

- L2 transports packets
- L3 services operate over L2

Both viewpoints are valid depending on the discussion.

Example 4 — VPN over the Internet
Underlay
The Internet or routed IP connectivity is the underlay.
It provides basic reachability between VPN peers.
Overlay
The VPN tunnel is the overlay.
Examples:

- IPsec
- SSL VPN
- OpenVPN

The overlay adds:

- Encryption
- Authentication
- Encapsulation

Policy-Based IPsec
Traditional IPsec VPNs are commonly policy-based.
In this design:

- Interesting traffic is matched by crypto ACLs
- IPsec protects matching traffic
- No routed tunnel interface exists

Example:
LAN Traffic
↓
Matched by Crypto Policy
↓
Encrypted by IPsec
↓
Internet Transport
In this model:

- Internet IP connectivity = underlay
- IPsec encryption = overlay

Route-Based VPN Using VTI
Modern VPN deployments commonly use VTIs.
A VTI (Virtual Tunnel Interface) creates a logical routed interface associated with an IPsec tunnel.
The VTI behaves similarly to a normal Layer 3 interface:

- Can have an IP address
- Can participate in routing
- Can run routing protocols
- Simplifies policy management

Example:

Routed Traffic

↓

VTI Tunnel Interface

↓

IPsec Encryption

↓

Internet Transport

In this model:

- Internet IP network = underlay
- IPsec tunnel/VTI = overlay

Example 5 — GRE over IPsec

This is a traditional enterprise design.

Underlay

The routed IP network provides connectivity.

First Overlay

The IPsec tunnel provides encryption.

Second Overlay

GRE operates over IPsec.

GRE adds:

- Tunnel interfaces
- Routing support
- Multicast transport
- Dynamic routing protocols

In this design:

- IP transport = underlay
- IPsec = overlay
- GRE = overlay over another overlay

GRE over IPsec

Original Packet

↓

GRE Encapsulation

↓

IPsec Encryption

↓

Internet

Modern Enterprise Preference

Most modern enterprise VPN designs prefer:

- Route-based VPNs
- VTIs
- Native IPsec tunnel interfaces

because they:

- Scale better
- Simplify routing
- Simplify NAT
- Simplify firewall policies
- Improve troubleshooting

GRE is still valuable for:

- Multicast transport
- DMVPN
- Legacy interoperability
- Specialized overlays

Example 6 — VXLAN Data Center Fabrics

Modern data centers commonly use overlay networking.

Underlay

The routed IP fabric is the underlay.

Usually:

- Leaf-spine architecture
- ECMP routing
- BGP underlay

Overlay

VXLAN creates logical Layer 2 segments over the routed network.

Benefits:

- Network virtualization
- Tenant isolation
- Large-scale segmentation
- VM mobility

This is one of the most important modern overlay technologies.

Example 7 — SD-WAN

Underlay

The transport circuits are the underlay.

Examples:

- MPLS
- Broadband Internet
- LTE
- 5G

Overlay

The SD-WAN fabric is the overlay.

It adds:

- Centralized policy
- Path selection
- Encryption
- Application awareness

Overlay Characteristics

Common overlay features include:

- Encapsulation
- Virtualization
- Encryption

- Segmentation
- Traffic engineering
- Abstraction

Examples of overlay protocols:

- GRE
- VXLAN
- IPsec
- MPLS VPN
- DMVPN

Underlay Characteristics

Common underlay features include:

- Physical connectivity
- Stable routing
- Low latency
- High reliability
- High bandwidth
- Deterministic forwarding

Examples of underlay technologies:

- Ethernet
- IP routing
- MPLS transport
- Optical networks
- Wireless RF transport

Troubleshooting Methodology

Always troubleshoot the underlay first.

Example sequence:

1. Verify physical connectivity
2. Verify Layer 2 forwarding
3. Verify IP reachability
4. Verify routing
5. Verify overlay services

A broken underlay causes overlay failure.

Simple Mental Model

A highway is the underlay.
The vehicles using the highway are overlays.
The highway provides transport.
The vehicles provide the service.

Summary

Underlay

Provides foundational transport and connectivity.

Examples:

- Ethernet
- IP routing
- MPLS transport
- RF carrier signals

Overlay
Provides logical services over the transport network.
Examples:

- VPNs
- VXLAN
- GRE
- SD-WAN
- Encrypted tunnels

Key Principle
The overlay depends on the underlay.
No stable underlay = no stable overlay.

Eugene Beckett
IT & Network Consultant
EPB Enterprises
https://www.linkedin.com/in/eugene-beckett