

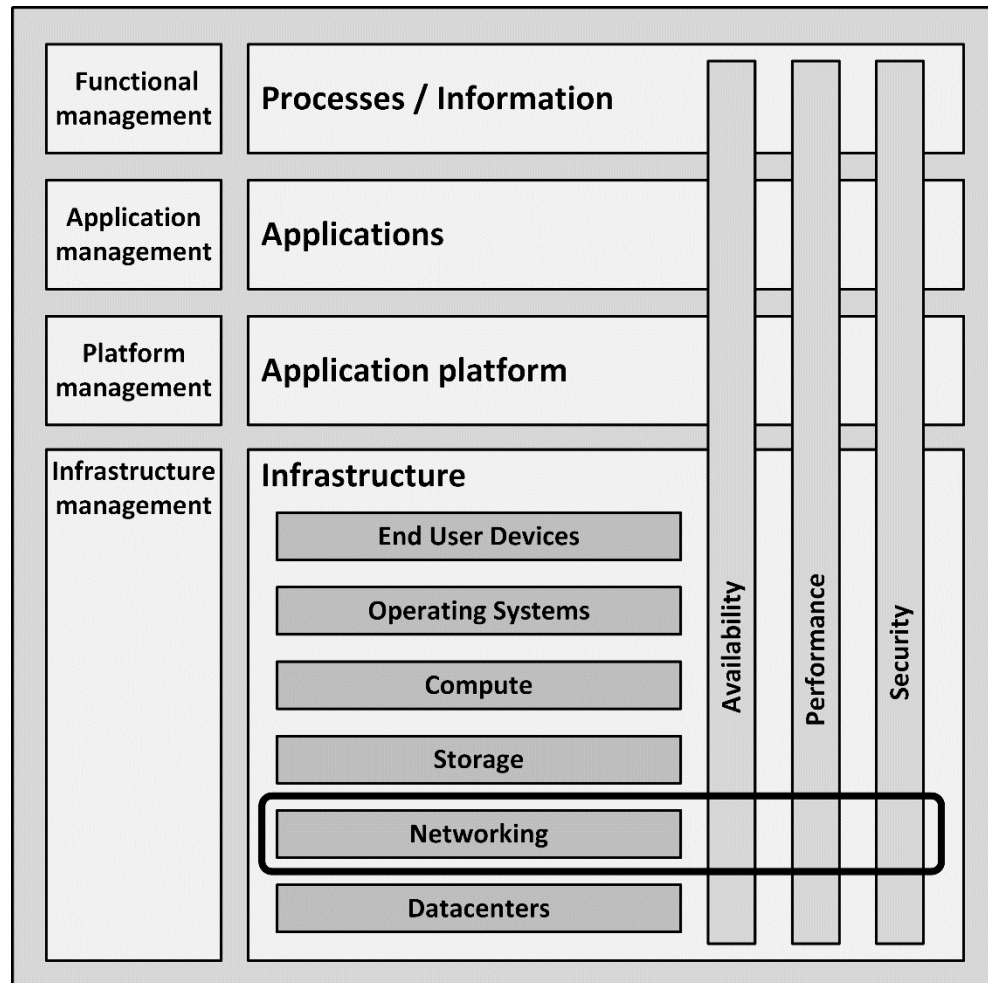
IT Infrastructure Architecture

Infrastructure Building Blocks
and Concepts

Networking

Introduction

- Mainframe computers in the 1960s were stand-alone machines
- In the late 1960s, a number of computers were connected by means of the ARPANET – the predecessor of the internet
- With PCs in the 1980s, local Area Networks (LANs) were introduced
 - They allowed PCs to connect to each other and to shared resources like a file server, a printer or a router to the internet



Networking building blocks

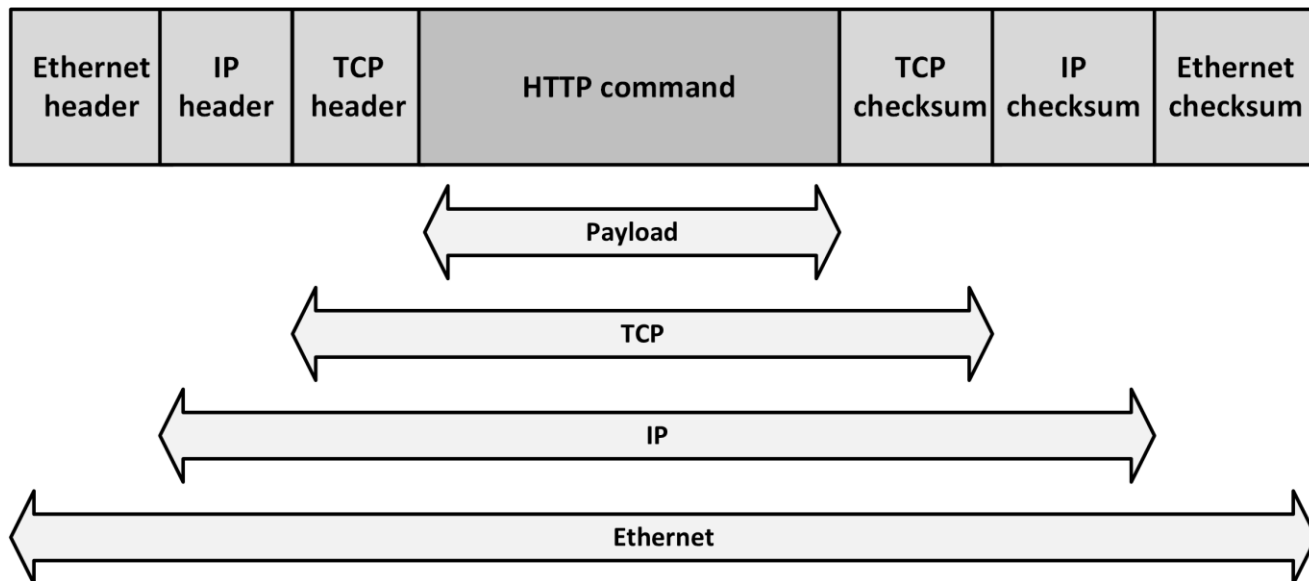
OSI Reference Model

- The OSI Reference Model (OSI-RM) was developed in 1984 by the International Organization for Standardization (ISO)
- Seven layers define the different stages that data must go through to travel from one host to another over a network

	Layer	Implementation
7	Application	BOOTP & DHCP DNS & DNS SEC NTP SNMP
6	Presentation	TLS SSL
5	Session	PPTP L2TP VPN
4	Transport	TCP UDP NAT
3	Network	IP (v4, v6, sec) MPLS ICMP OSPF IGMP
2	Data link	Ethernet Wi-Fi X25, ATM Frame relay WAN GPRS, 3G
1	Physical	Cabling & patching UTP Dark fiber SONET/SDH DSL T and E-carrier

OSI Reference Model

- The OSI stack allows:
 - Implementing network components independently of each other
 - Ensuring all components work together
- Provides freedom to implement the network stack in an optimal way for a certain usage
- Each layer's payload contains the protocol for the next layer



Physical layer

Cables

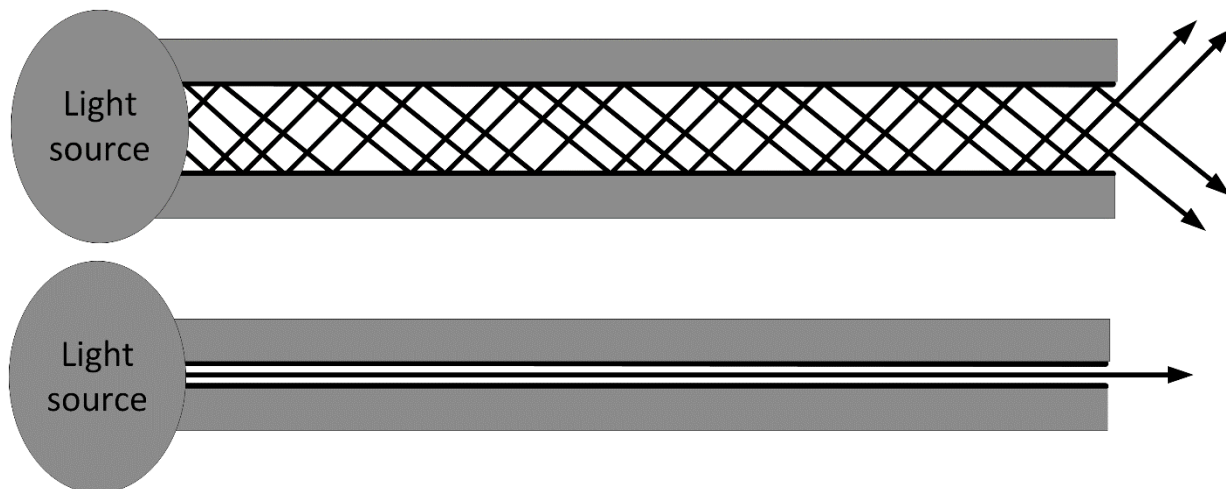
- At the most elementary level, networking is about cables
- Copper based cables:
 - Coax
 - Twisted pair
- UTP comes in several quality ratings called categories



Category	Maximum bandwidth
5 or 5e	1 Gbit/s
6	10 Gbit/s
7	10 Gbit/s
8	40 Gbit/s

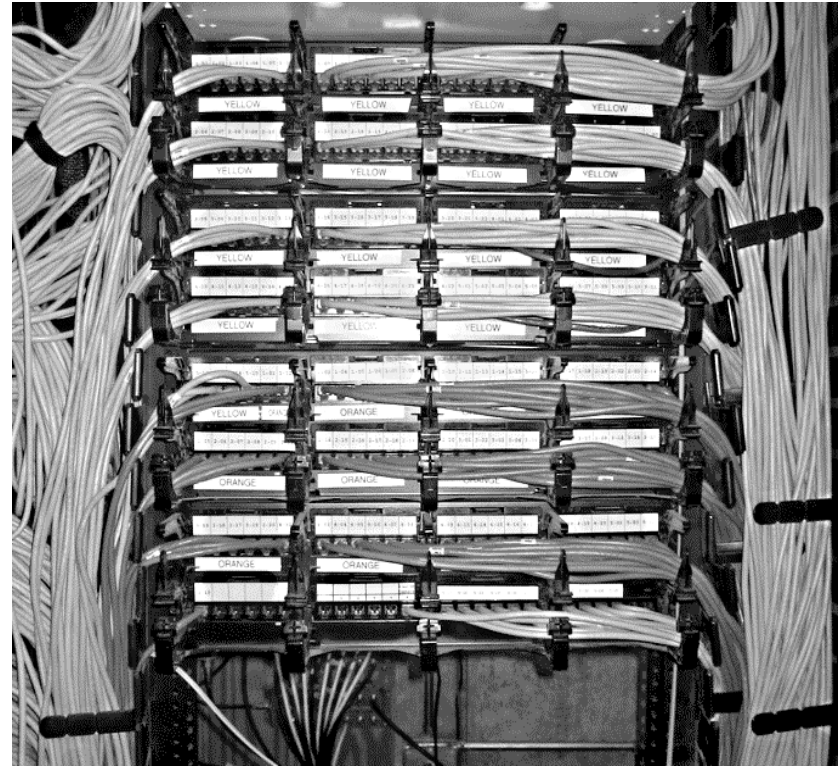
Fiber optic cabling

- A fiber optic cable contains multiple strands of fiber glass or plastic
 - Each provide an optical path for light pulses
- Light source:
 - Light-emitting diode (LED)
 - Laser
- Two types of fiber optic cable are most common:
 - Multi-Mode Fiber (MMF)
 - Single Mode Fiber (SMF)



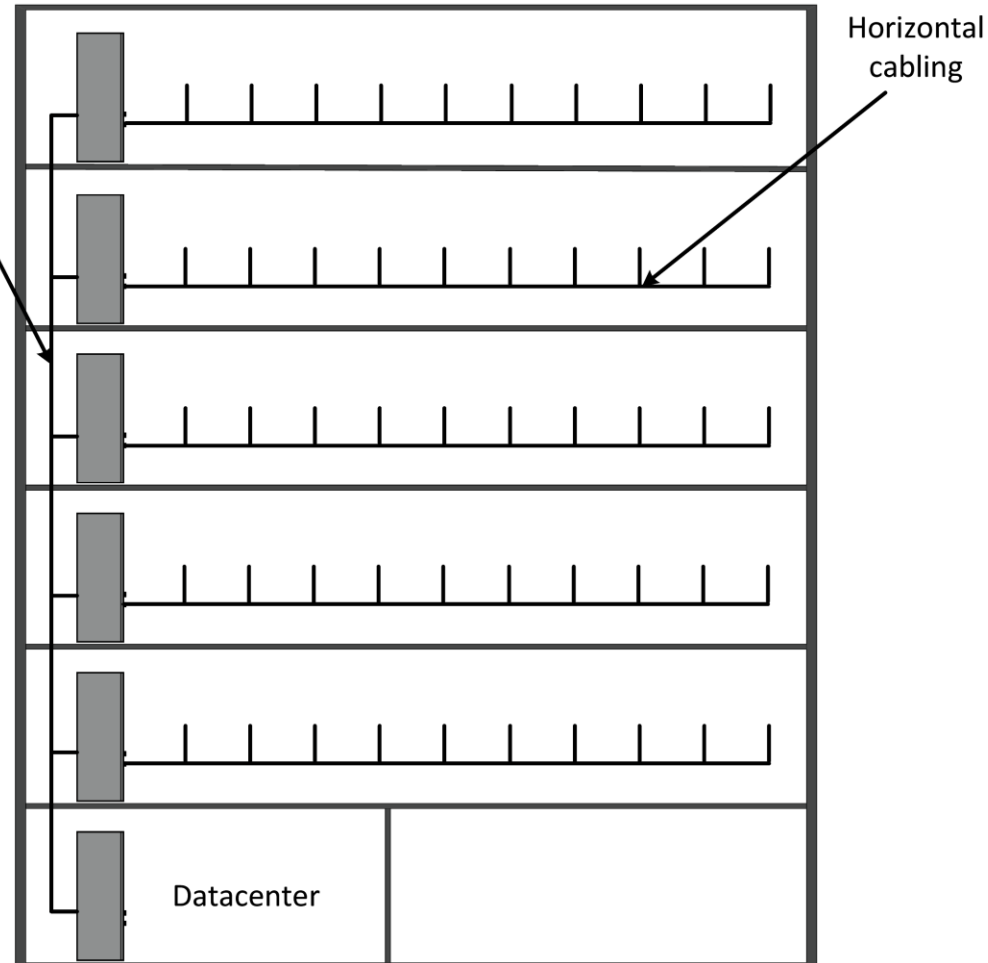
Patch panels

- Cables in buildings are most visible in patch panels
 - In racks in the datacenter
 - In patch closets in various locations in (office) buildings
- They connect systems in a flexible way, without having to change the installed cabling in the building
- Patch panels are passive connecting devices
- Connecting systems is done using patch cables



Vertical and horizontal cabling

- The main distribution cabling in buildings connects the patch panels on the floors to the datacentre (vertical cabling)
- Endpoints in the walls are connected to the patch panels (horizontal cabling)



Leased lines

- Leased lines are dedicated data connections between two locations, provided by a telecom provider
- Leased lines are based on:
 - T or E carrier lines
 - SONET
 - SDH
 - Dark fiber

Internet access

- Three ways to connect to the internet:
 - Leased line
 - Cable internet access
 - Uses cable television infrastructure
 - Digital Subscriber Line (DSL)
 - Asymmetric DSL (ADSL)
 - Symmetric DSL (SDSL)
 - Very High DSL (VDSL)

Network Interface Controllers (NICs)

- Hardware component that connects a server or end user device to a physical network cable
- The NIC is actually both a physical layer and data link layer device
 - Provides physical access to a networking cable and an implementation of a datalink protocol like Ethernet
- A NIC has a fixed MAC address that is uniquely assigned to its network interface

Datalink layer

Ethernet

- Developed at Xerox PARC between 1973 and 1975
- Originally employed a shared medium topology, based on coax cable
- Later Ethernet used twisted pair cabling with hubs and switches
 - Decreased the vulnerability of the network caused by broken cables or bad connectors
- An Ethernet packet contains:
 - Source and destination MAC addresses
 - Data that needs to be transported (payload)
 - Cyclic redundancy check

Preamble	Frame delimiter	Destination MAC address	Source MAC address	Length	Payload	CRC checksum
----------	--------------------	-------------------------------	--------------------------	--------	---------	-----------------

Ethernet CSMA/CD

- Carrier Sense Multiple Access with Collision Detection
- Any machine can start transmitting packets when the shared carrier is not in use
 - Coax cable, twisted-pair hub or Wi-Fi radio signal spectrum
- Carrier sensing circuitry checks the activity on the carrier
- When two machines start to transmit a packet at the same time, a packet collision occurs
 - This is detected by all sending machines
 - They will stop the transmission immediately
 - After a short waiting time, they will retransmit their packet when the carrier is not in use anymore

WLAN (Wi-Fi)

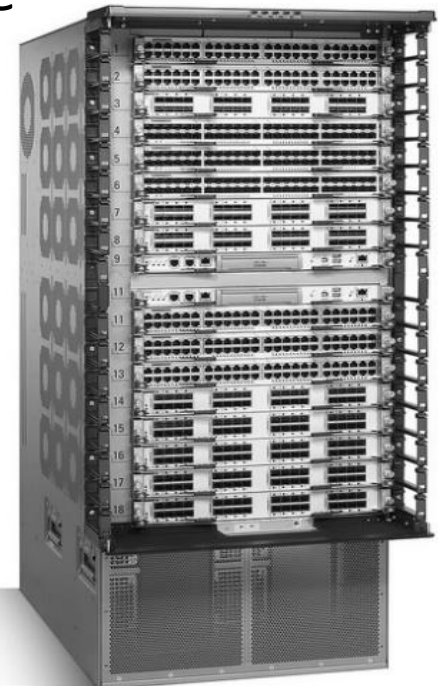
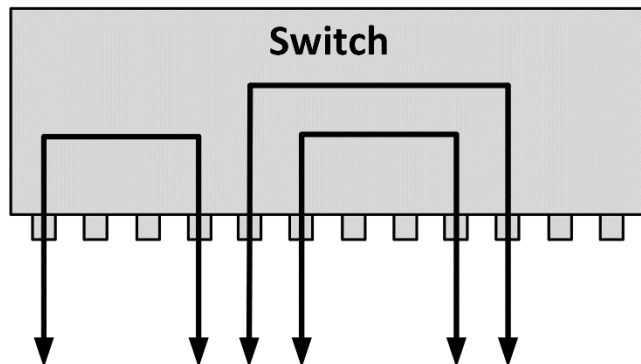
- A wireless local area network (WLAN) links two or more devices using radio transmissions
- Wi-Fi: WLANs that are based on the IEEE 802.11 protocol family
- Wi-Fi is a special implementation of Ethernet
 - The radio spectrum is the shared medium

WLAN (Wi-Fi)

- Wi-Fi range is about 30 m
- Access points are base stations for a wireless network
- Data encryption: Wi-Fi Protected Access (WPA)
 - WPA dynamically generates a new key for each packet
 - WPA includes a Message Integrity Check
 - Prevents an attacker from capturing, altering and/or resending data packets

Switching

- Switches split a single network segment into multiple segments
 - Each segment has one device
- Switches learn which MAC address is connected to which port
- Data sent to a certain MAC address will only be forwarded to the switch port that has that MAC address connected
- On a switched network, many simultaneous data transfers can take place, in full-duplex



WAN

- Wide Area Networks (WANs) started to appear in the 1980s
- Most WAN connections today are based on packet switching technologies
 - Devices transport packets via a virtual point-to-point link across a carrier network
- Packet switched networks are very reliable
- Most WAN connections have been migrated to VPNs running on one of the following technologies:
 - The MPLS network of a network provider
 - The internet using IPsec or SSL
 - Dark fiber

Public wireless networks

- Public wireless (mobile) networks are getting more popular every day
- Public wireless networks are much less reliable than private wireless networks and have lower bandwidth
- Technologies:
 - 1G and 2G: GSM, CDMA, GPRS and EDGE
 - 3G: UMTS and HSDPA
 - 4G: LTE

Network layer

The IP protocol

- IP, in combination with TCP, was invented by Robert Kahn and Vinton Cerf in 1973
- The IP protocol is by far the most used layer 3 protocol in the world
- IPv4 is the dominant protocol on the internet today
- The IP protocol assumes that the network is inherently unreliable and that it is dynamic in terms of availability of links and nodes
- IP uses data packets that contain:
 - Source address
 - Destination address
 - Payload data (typically an Ethernet packet)

The IP protocol

- IP routing protocols dynamically define the path of IP packets from source to destination
- Routing issues:
 - Due to network disruption, IP packets can get lost or corrupted
 - When an error is detected, the IP packet is dropped by the node that found the error
 - Since each IP packet is routed individually, IP packets can arrive at the destination out of order
- The effects of dropped IP packets and IP packets arriving out of order is handled by upper layer protocols like TCP

IPv4 addresses

- IPv4 addresses are composed of 4 bytes (32 bits), represented by 4 decimal numbers, and divided by a period (like 192.168.0.1)
- An IP address has a network prefix and a host number
- All hosts with the same network prefix can communicate directly to each other
- Hosts in other networks can only be reached using a router

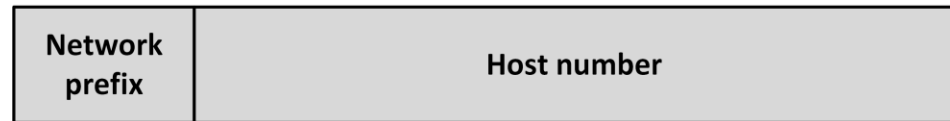
10 . 121 . 12 . 16

Network prefix	Host number
-----------------------	--------------------

IPv4 classes

- The first three bits of the first byte of an IP address define the class of the address
- Three classes of networks are defined

Class A



Class B



Class C



Class	First byte	Max number of hosts	Number of available networks
A	0-127	16,777,214	128
B	128-191	65,534	16,384
C	192-223	254	2,097,152

IPv4 subnetting

- Subnetting is used to split up the host part of an IP network in smaller subnets, each forming a new IP network

CIDR prefix	Subnet mask	Available subnets	Hosts per subnet
/24	255.255.255.0	1	254
/25	255.255.255.128	2	126
/26	255.255.255.192	4	62
/27	255.255.255.224	8	30
/28	255.255.255.240	16	14
/29	255.255.255.248	32	6
/30	255.255.255.252	64	2
/31	255.255.255.254	128	2 (only point-to-point)

Address 196 . 121 . 12 . 241

Network prefix			Sub net	Host
----------------	--	--	---------	------

Subnet mask 255 . 255 . 255 . 240

Binary 11111111 . 11111111 . 11111111 . 11110000

IPv4 - Private IP ranges

- Private IP addresses should be used for LANs
 - The number of unique IP addresses on the internet is limited
 - Hosts with public internet IP addresses can reach the internet directly
- Private IP address ranges:
 - 10.0.0.0 to 10.255.255.255 (class A address range)
 - 172.16.0.0 to 172.31.255.255 (class B address range)
 - 192.168.0.0 to 192.168.255.255 (class C address range)
- Private IP addresses:
 - Are not used on the internet
 - Are not routed by internet routers

IPv6

- IPv6 was introduced in 1998 as a successor of IPv4 to solve the problem of limited IP address space
- IPv6 uses 128-bit addresses represented in eight groups of four hexadecimal digits separated by colons
- Example:

2001:0bb8:86a2:0000:0000:8b1e:1350:7c34

IPv6

- IPv6 has the following benefits over IPv4:
 - Expanded address space
 - Better support for mobile IP
 - Fixed header length
 - Auto configuration
 - Quality of Service
 - Security
 - MTU discovery
- IPv6 is not backwards compatible with IPv4

IPv6

- Deployment models for IPv6:
 - Use IPv6 on the LAN and on dedicated WAN links
 - Protocol translation
 - Dual stack
 - IPv6 over IPv4 tunnels
- Dual stack is the simplest way to begin deploying IPv6

ICMP

- The Internet Control Message Protocol (ICMP) is an integral part of the IP protocol
- The best-known use of ICMP:
 - 'ping'
 - 'traceroute'

Routing

- A router copies IP packages between (sub)networks
- Routers compile routing tables to make IP packet forwarding decisions
- Routing and switching functionality may be combined in one device
 - A switch capable of handling routing protocols is also known as a layer 3 switch

Routing protocols

- Dynamic routing protocols automatically create routing tables
 - Based on information exchange with neighboring routers
- When a network connection experiences problems, the routing protocol automatically reconfigures the routing tables to use alternative routes
- LAN and WAN routing protocols can be divided in three classes:
 - Distance vector protocols (like RIP and IGRP)
 - Link state protocols (like OSPF and IS-IS)
 - Path vector routing (like BGP)

MPLS

- Multiprotocol Label Switching (MPLS) routes data from one network node to the next with the help of labels
- MPLS allows setting up end-to-end circuit
 - Across any type of physical transport medium
 - Using any protocol
- In practice, MPLS is mainly used to forward IP and Ethernet traffic

Transport layer

Transport layer

- The transport layer can maintain flow control, and can provide error checking and recovery of data between network devices
- The most used transport layer protocols are TCP and UDP

TCP

- Transmission Control Protocol (TCP) uses the IP protocol to create reliable transmission of so-called TCP/IP packets
 - TCP provides reliable, ordered delivery of a stream of data between applications
 - TCP introduces much overhead

UDP

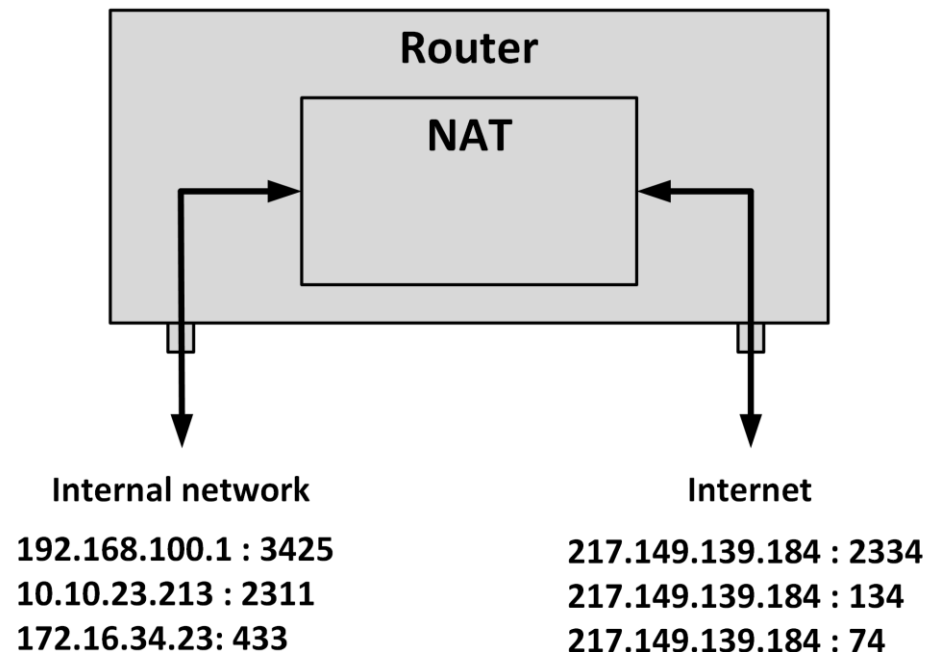
- User Datagram Protocol (UDP) emphasizes reduced latency over reliability
 - It sends data without checking if the data arrived
 - Reduces much overhead
 - UDP is typically used when some packet loss is acceptable
 - Real-time voice and video streams
 - When only small amounts of data are transmitted, that fit in one IP packet

TCP and UDP ports

- TCP and UDP use logical port numbers
- Each side of a TCP or UDP connection uses an associated port number between 0 and 65,535
- Received TCP or UDP packets are identified as belonging to a specific connection by its combination of the IP address, and the TCP or UDP port number
 - For instance: 192.168.1.2:80, the number after the colon represents the port number (80 in this case)
- Servers running a specific service listen to well-known ports:
 - FTP (port 21)
 - SSH (port 22)
 - SMTP (port 25)
 - DNS (port 53)
 - HTTP (port 80)

Network Address Translation (NAT)

- NAT allows the use of a private addressing space within an organization, while using globally unique addresses for routing data to the internet
- As a packet passes a NAT enabled router from its internal network interface to its internet interface, NAT replaces the packet's private IP address with its public IP address



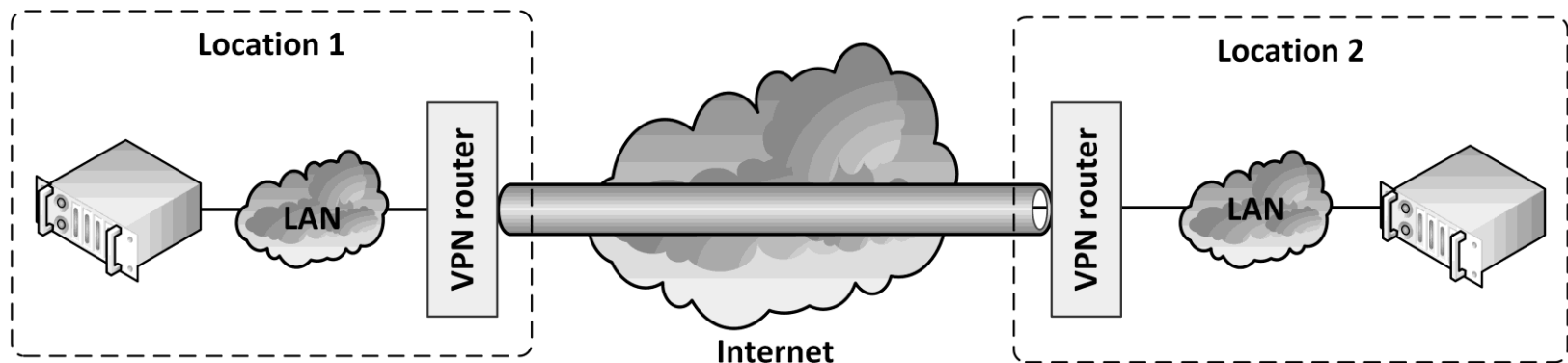
Session layer

Session layer

- The session layer provides mechanisms for opening, closing and managing a session between end-user application processes

Virtual Private Network (VPN)

- A Virtual Private Network (VPN) uses a public network to interconnect private sites in a secure way
 - Also known as a VPN tunnel
- VPN uses "virtual" connections based on IPsec/SSL
- Most network providers also offer private VPNs based on MPLS



Virtual Private Network (VPN)

- VPNs use strong encryption and strong user authentication
 - Using the internet for transmitting sensitive data is considered safe
- VPN tunnels are often used for remote access to the LAN by users outside of the organization's premises
- Most common VPN communications protocol standards:
 - Point-to-Point Tunneling Protocol (PPTP) for individual client to server connections
 - Layer 2 Tunneling Protocol (L2TP) for individual client to server connections
 - IPsec for network-to-network connectivity
- IPsec is built into IPv6 standard and is implemented as an add-on to IPv4