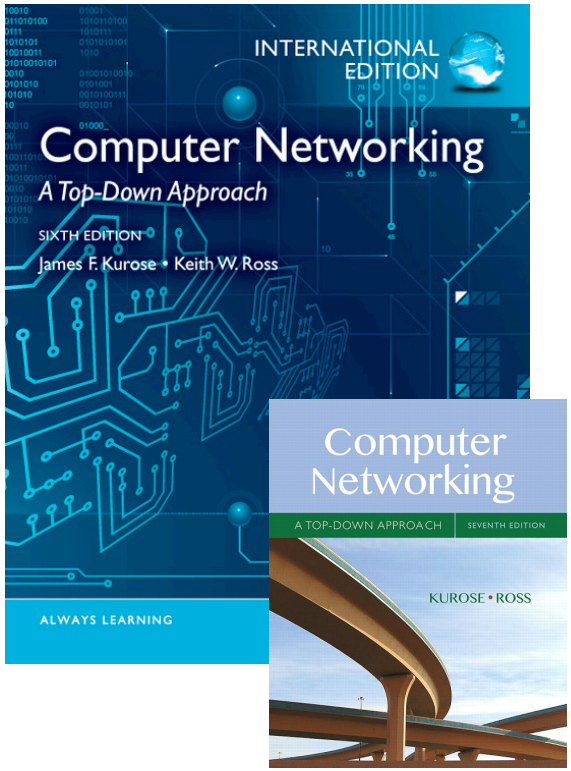
TTM4100 Summary

Computer networking bottom up

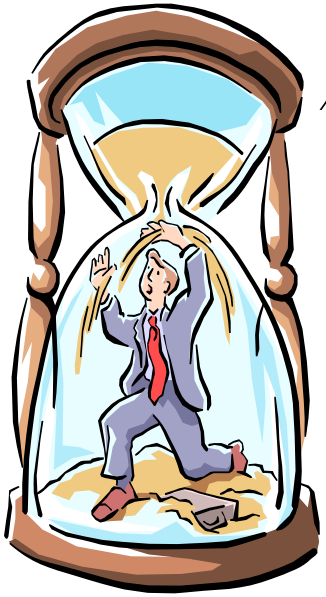
April 6. - 7, 2017

Kjersti Moldeklev, Prof II
Department of Information Security and Communication Technology
kjersti.moldeklev@ntnu.no

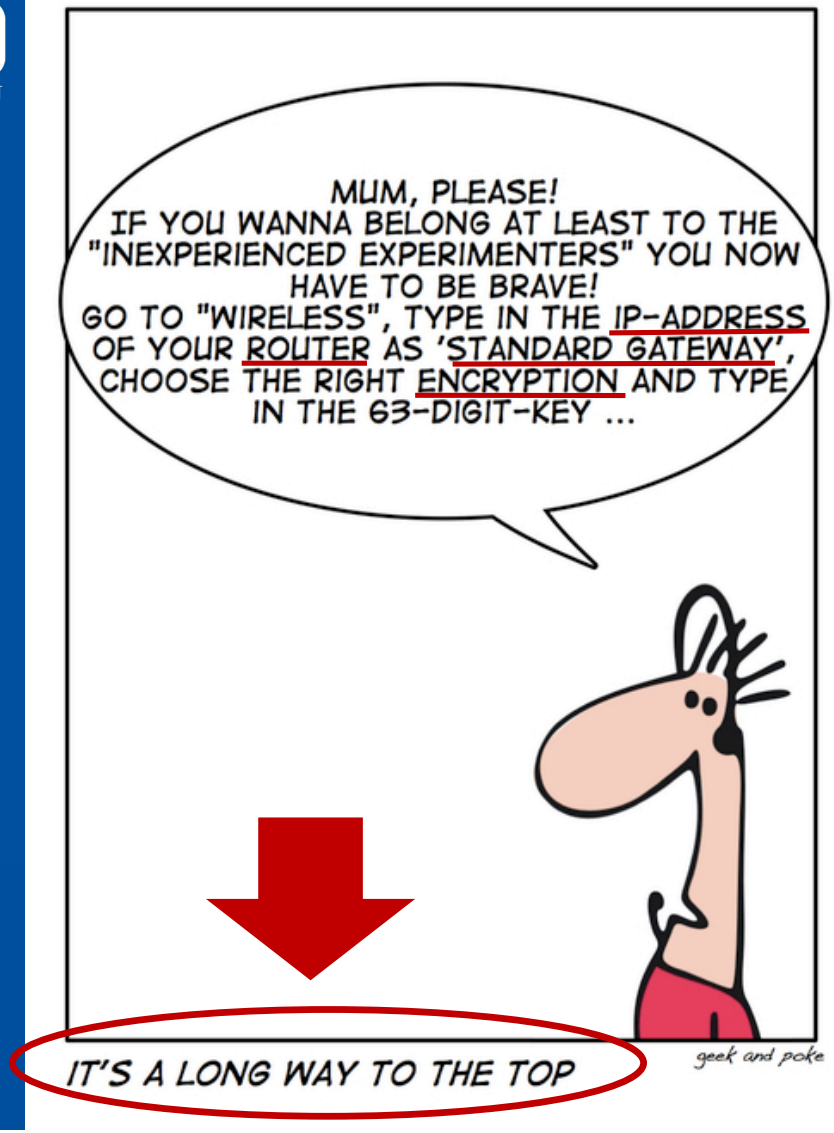


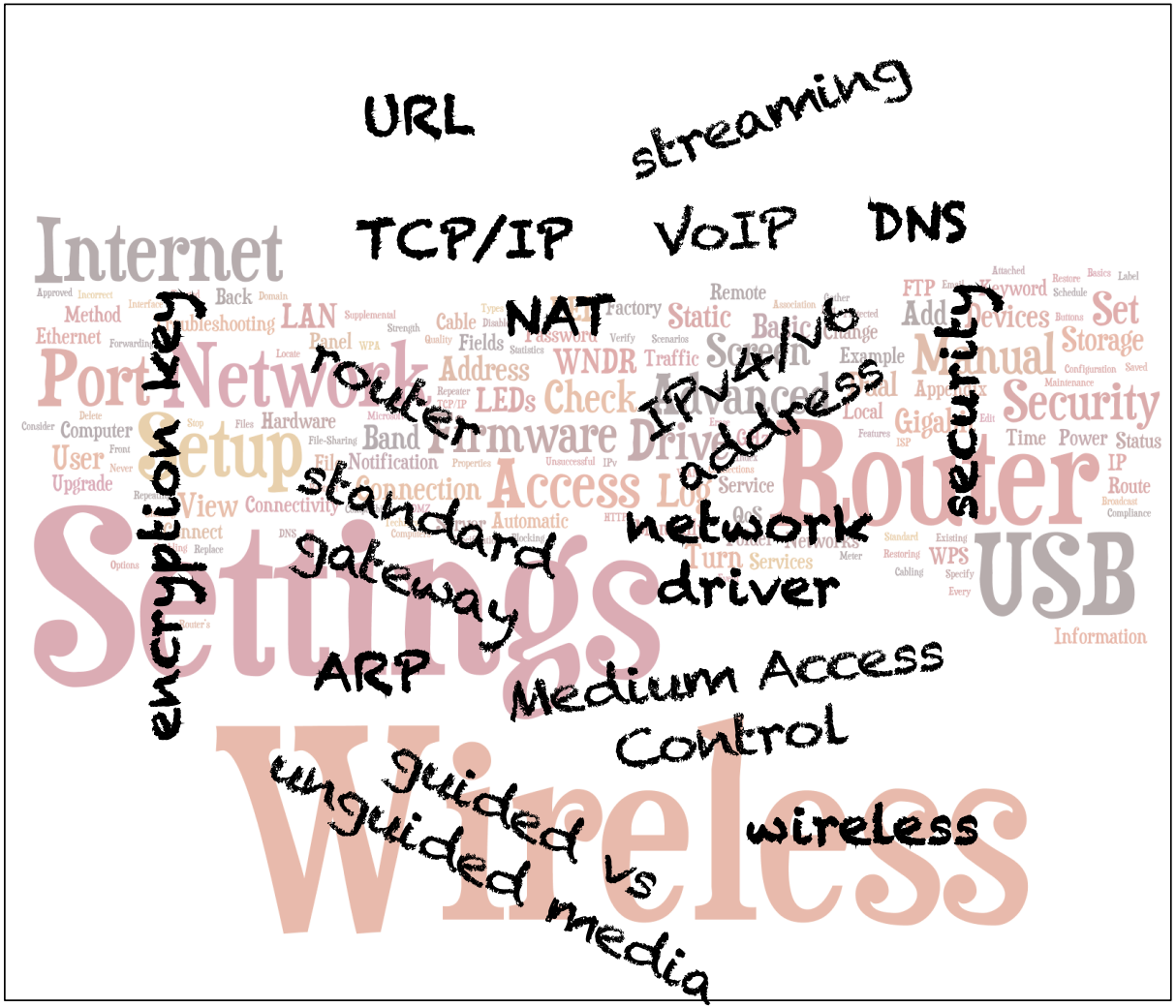
TTM4100 2017 SUMMARY – agenda

- **What is the Internet** – a small potpurri
- **Computer networking bottom up**
  - Physical + Link
  - Network
  - Transport
  - Application
- and some **security** measures along



NTNU


MUM, PLEASE!
IF YOU WANNA BELONG AT LEAST TO THE "INEXPERIENCED EXPERIMENTERS" YOU NOW HAVE TO BE BRAVE!
GO TO "WIRELESS", TYPE IN THE IP-ADDRESS OF YOUR ROUTER AS 'STANDARD GATEWAY', CHOOSE THE RIGHT ENCRYPTION AND TYPE IN THE 63-DIGIT-KEY ...
IT'S A LONG WAY TO THE TOP
geek and poke


URL
streaming
TCP/IP
VoIP
DNS
Internet
NAT
router
IPv4/v6
address
security
encryption key
standard
gateway
network
driver
ARP
Medium Access
Control
guided
unguided
vs
media
wireless
Settings
Wireless
Router
USB
Network
Port
Setup
Security
Storage
Manual
Information

Ukens medieoppslag

phishing
fraudulent emails
(distributed) denial of service
randsomware virus

DIREKTØRSVINDEL

Kripos oppfordrer flere til å anmelde datakriminalitet

Datakriminalitet øker i omfang, men de fleste sakene blir ikke anmeldt, ifølge Politidirektoratet. Kripos oppfordrer nå flere til å politianmelde slike saker.

– Vi ser en stor økning av kriminalitet begått via nett, og mot datasystemer. Angrepene er mer sofistikerte og avanserte, sier Håvard Aalmo, leder for seksjon for datakriminalitet i Kripos, til NRK. Aalmo mener flere vil bli utsatt for datakriminalitet i tiden framover, spesielt løsepengevirus, såkalt direktørsvindel og phishing. Kripos ser også en økning i tjenestenektangrep mot bedrifter. Slike angrep har til hensikt å skape ustabilitet i nettet eller å få tjenester til å bryte sammen. Mørketallsundersøkelsen for 2016 fra Næringslivets sikkerhetsråd viste imidlertid at bare én av ti bedrifter som utsettes for datakriminalitet, anmelder.

– Det er en stor underrapportering. Det er viktig at både folk og bedrifter anmelder til politiet, sier Aalmo.

Telenor ble utsatt for 3600 dataangrep i fjor, i tillegg til utallige svindelforsøk, men leverte bare inn 47 anmeldelser. Siden februar har flere hundre tusen nordmenn mottatt en svindelepost som inneholder løsepengevirus, der kriminelle oppgir utgir seg for å være Telenor.

Sikkerhetsansvarlig Caroline Lunde hos Telenor sier de blir utsatt for så mye datakriminalitet at de ikke har tid til å anmelde.

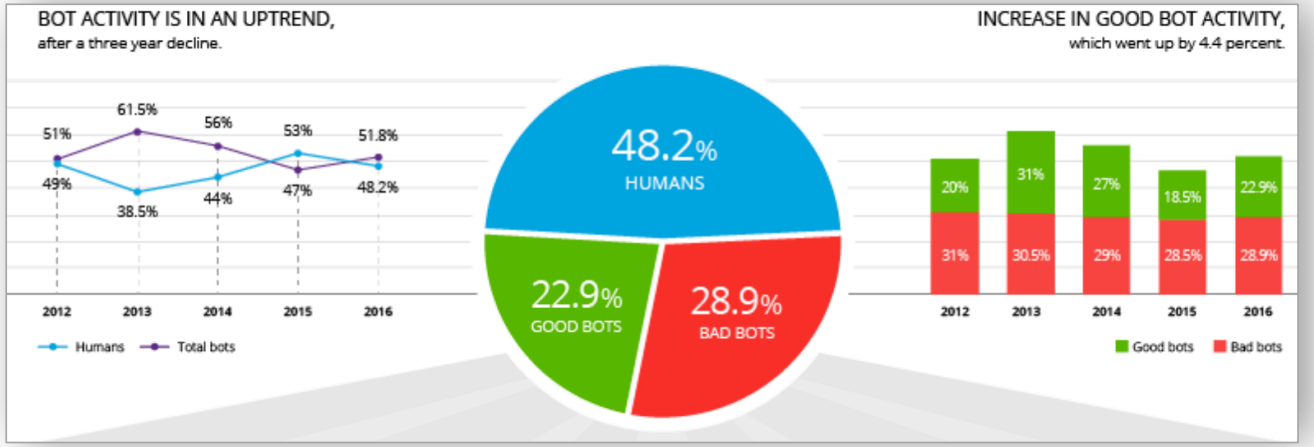
– Vi prioriterer heller ressursene våre på å sørge for at kundene våre ikke lider skade, sier Lunde. (NTB)

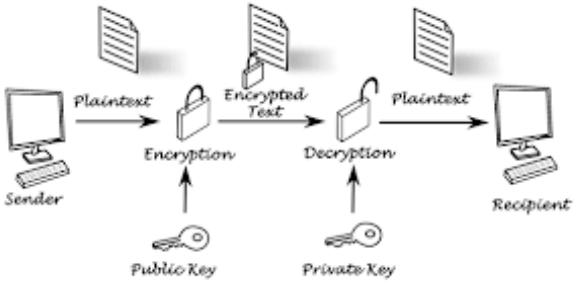
Aftenposten 4. april 2017

What is the Internet?

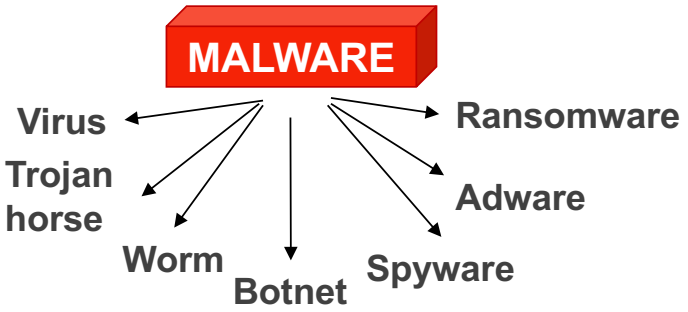
One third is related to malicious traffic

https://www.incapsula.com/blog/bot-traffic-report-2016.html



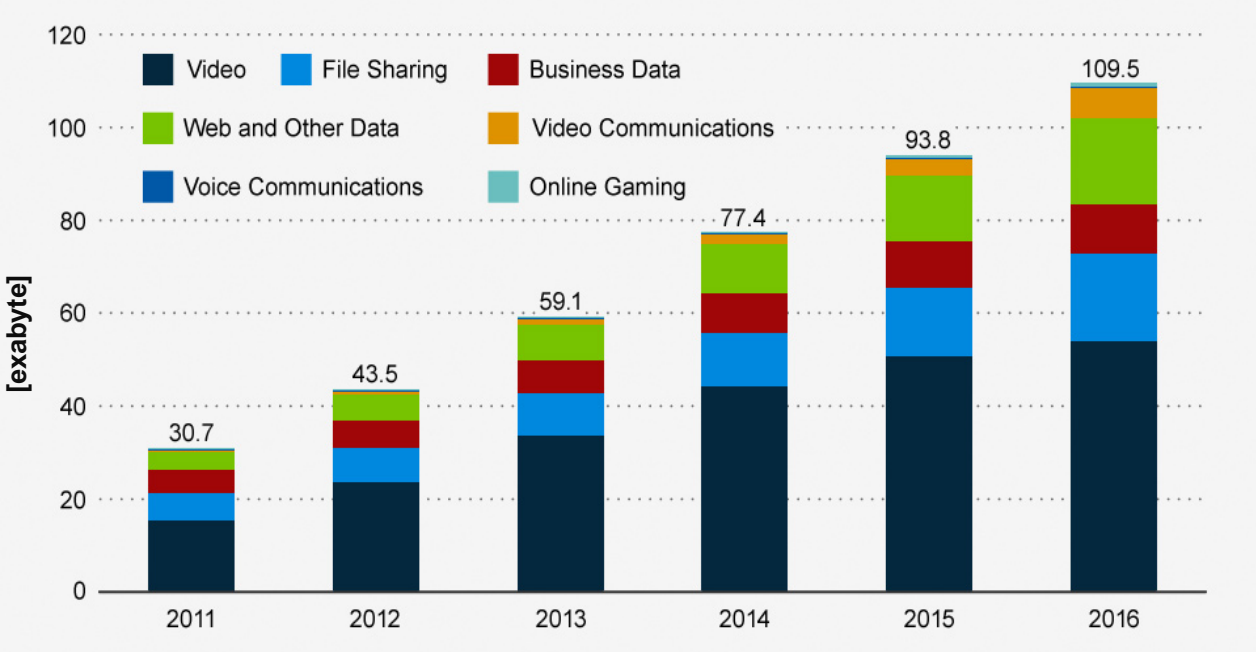


12 Top Internet security threats in 2017

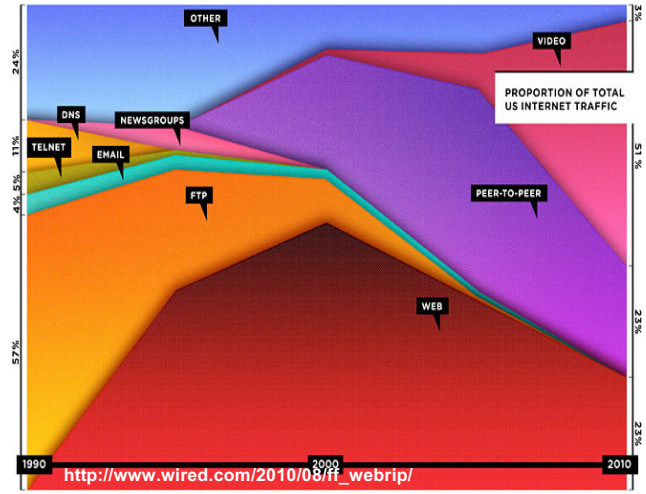


Video accounts for half of ever-growing Internet traffic

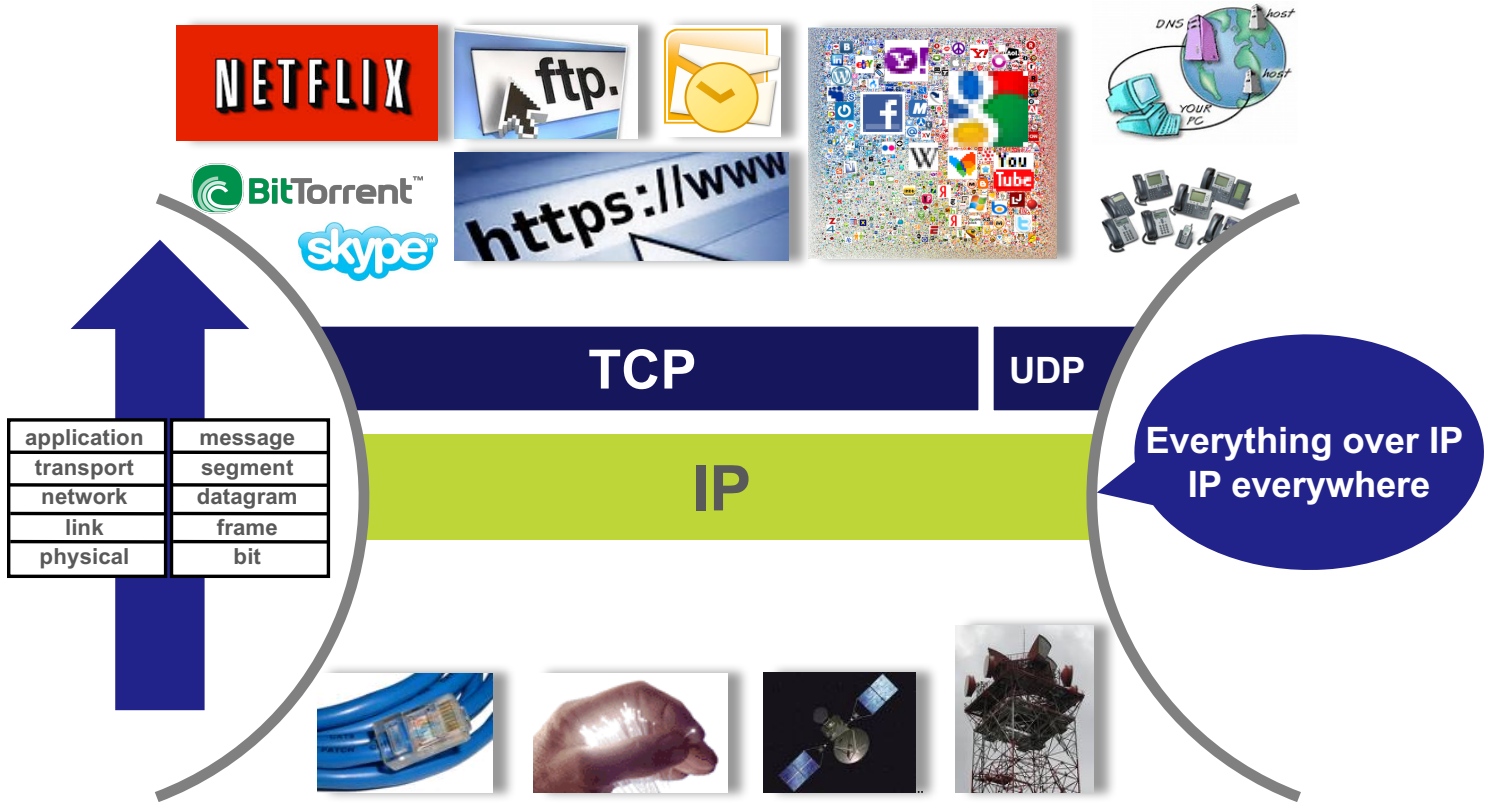
Estimated global IP traffic per month 2011-2016



Source: https://www.statista.com/chart/624/global-ip-traffic-per-month-from-2011-to-2016/

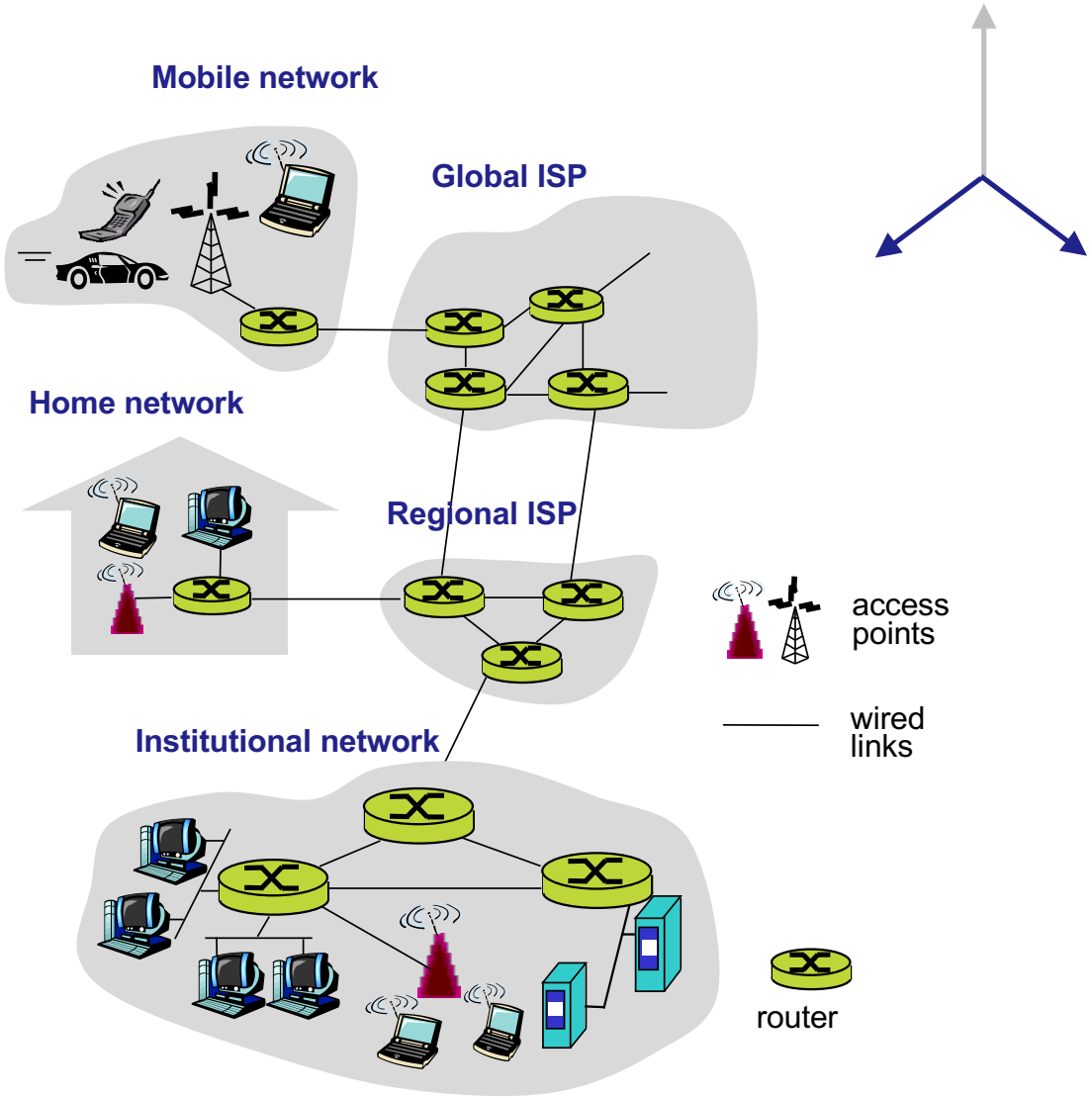


Everything over IP, IP everywhere

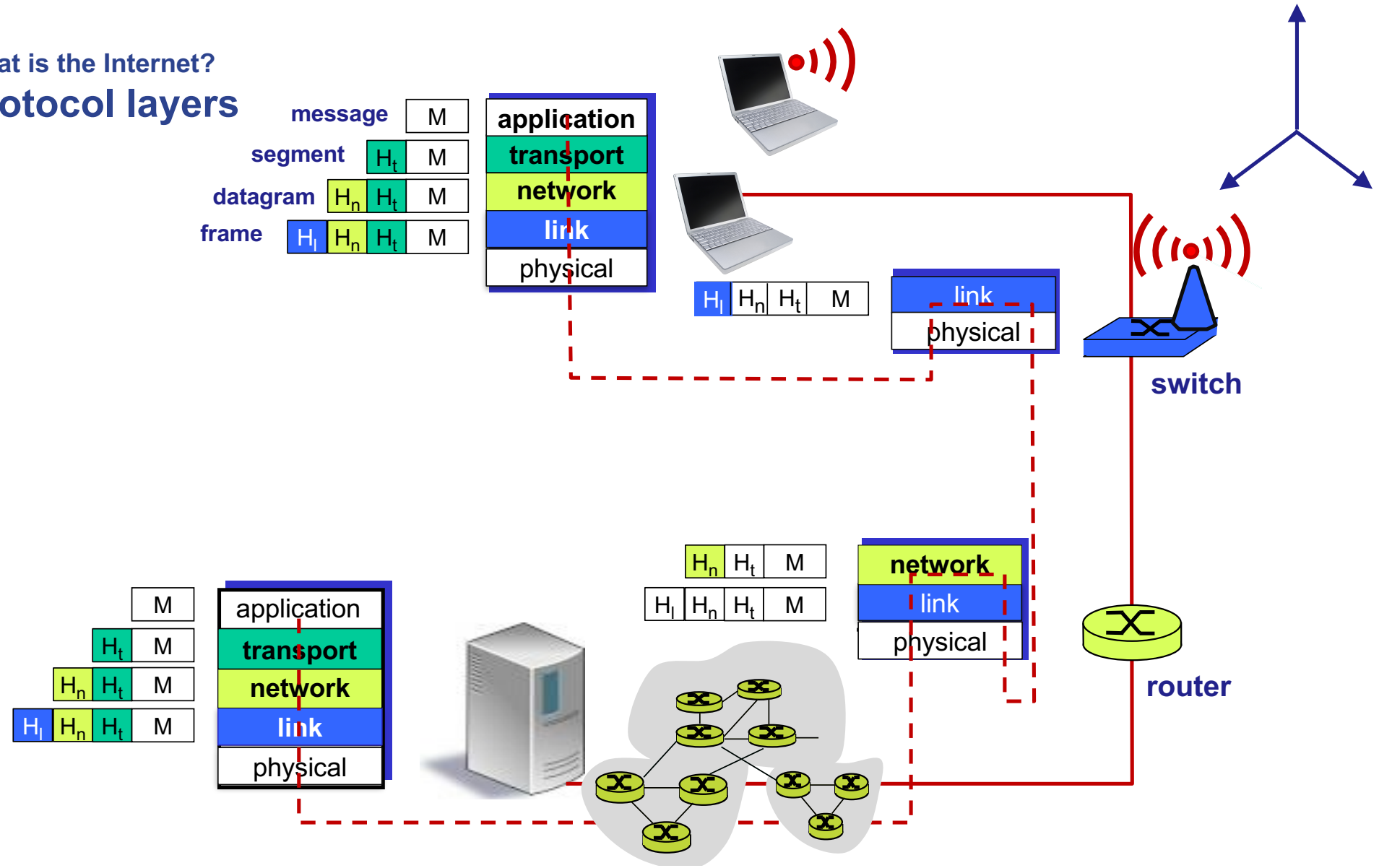


Network structure

- **Network edge**
  - applications on **end systems/hosts**
  - **Edge routers** in providers network
- **Access networks**
  - wired, wireless links
  - fiber, copper, radio, satellite
- **Network core**
  - interconnected routers
  - network of networks
- **Routers:** forward packets
- **Packets:** chunks of data



Protocol layers

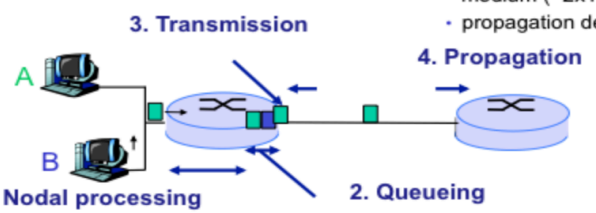


Performance parameters

Four sources of packet delay

- R=link bandwidth (bit/s)
- L=packet length (bits)
- time to send bis into link = L/R

- d = length of physical link
- s = propagation speed in medium (~$2x10^8$ m/sec)
- propagation delay = d/s

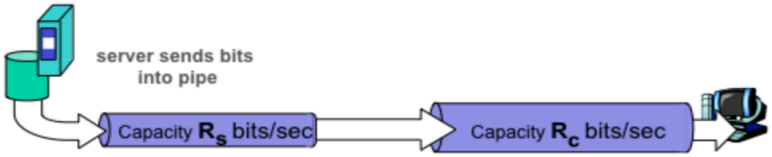


- check bit errors
- determine output link

- time waiting at output link for transmission
- depends on congestion level of router

Throughput = rate at which bits are transferred between sender/receiver

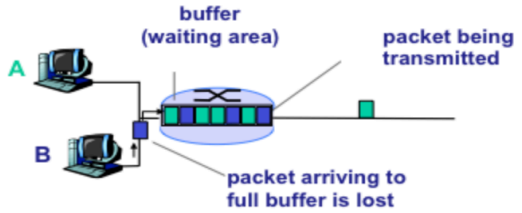
- Unit: bits per time
- Instantaneous: rate at given point in time
- Average: rate over longer period of time



End-to-end throughput cannot exceed bottleneck link

Packet arriving to full queue is dropped = packet loss

- Queue (buffer) preceding link has finite capacity
- Lost packet may be retransmitted by previous node, by source end system, or not at all

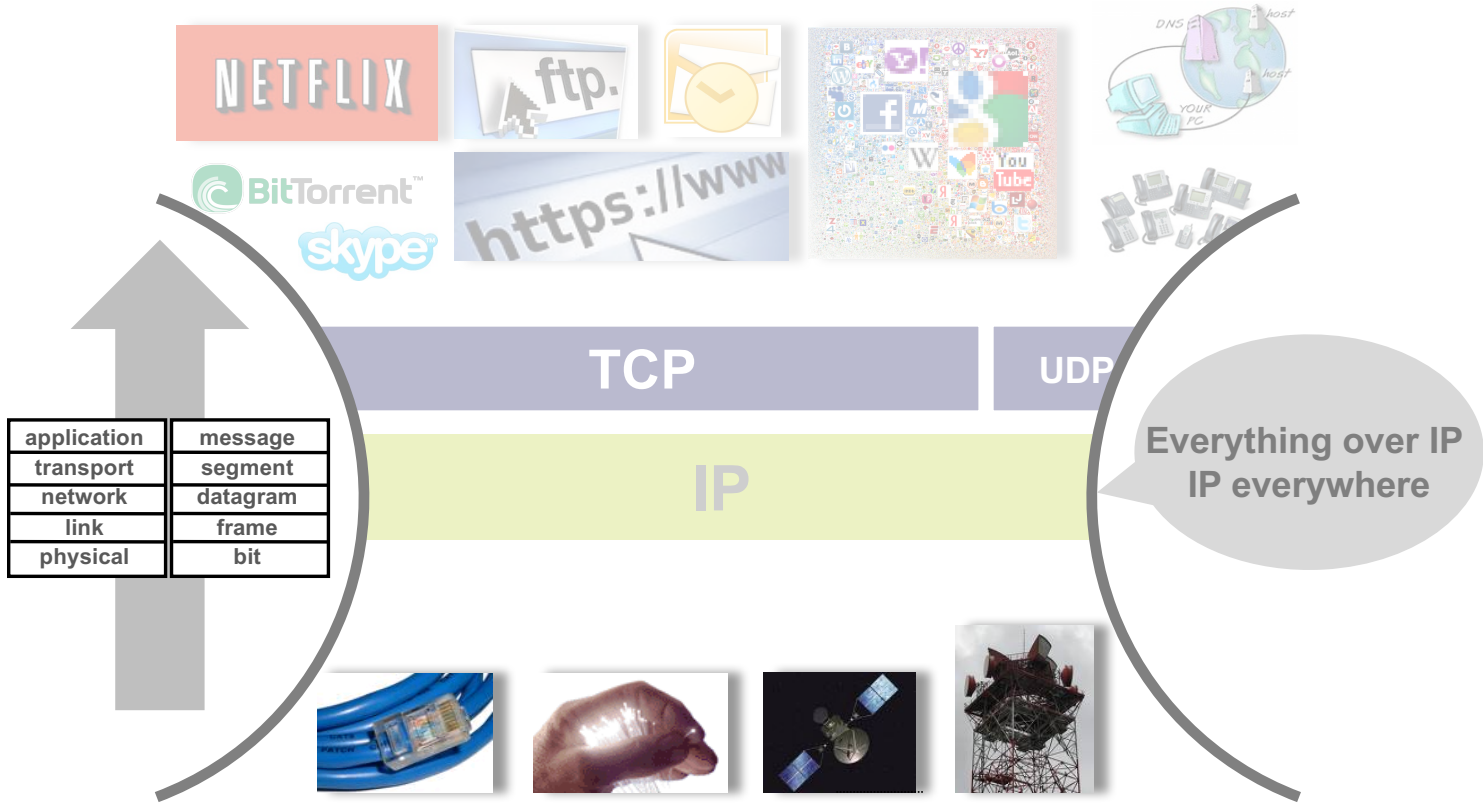


Computer networking – the Internet approach bottom up

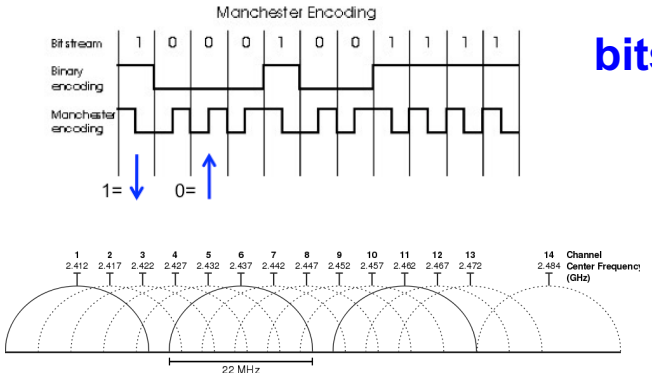
- Digital communication, transmission of **bits**, 0´s and 1´s
- The bits are **frame**d and transmitted over the link which is point-to-point or broadcast – using the **MAC address**
- The frame transports the **IP datagram** one hop towards its destination
- The IP datagram contains the **IP addresse**s (possibly changed by NAT) of the sending and receiving end system
- **Routers** forward IP datagrams **hop-by-hop**, using **forwarding tables** built by **routing protocol** information exchange
- The provided IP service is a **connectionless**, **best-effort** service without guarantees
- The **end-to-end transport layer** adds **error** and **flow control** and **congestion control**
- **Domain Name System** translates between names and IP addresses
- **Distributed applications** run only in end systems and exchange data across the network

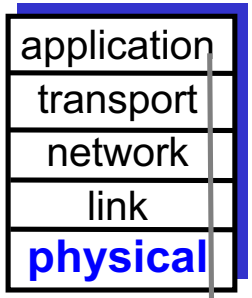
The LINK layer assembles bits to frames and brings the frames one hop towards the destination

application
transport
network
LINK
PHYSICAL

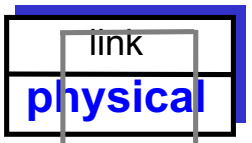


Digital communication, transmission of 0´s and 1´s by the physical layer

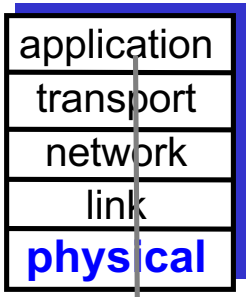


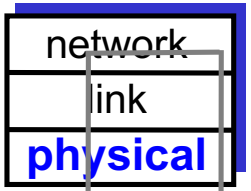


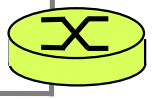
bits



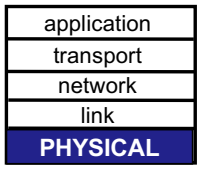
switch



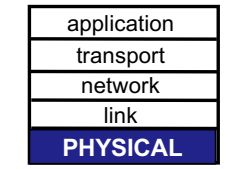




router



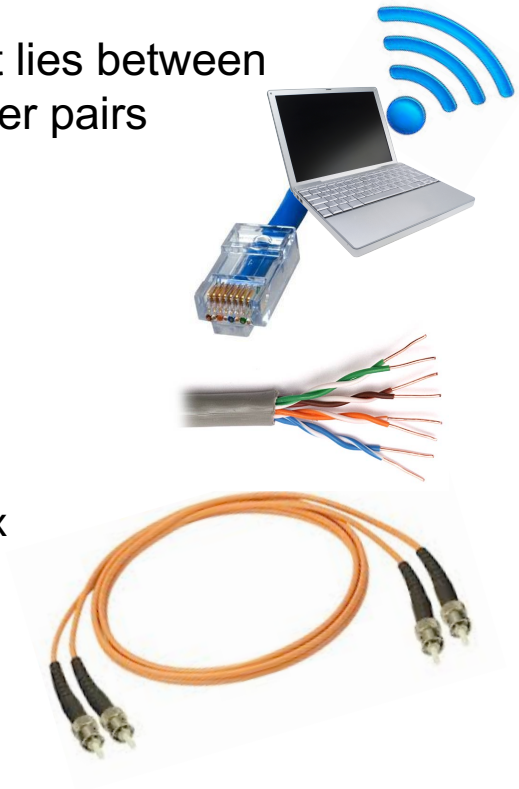
Physical media transport bits through electromagnetic waves or optical pulses



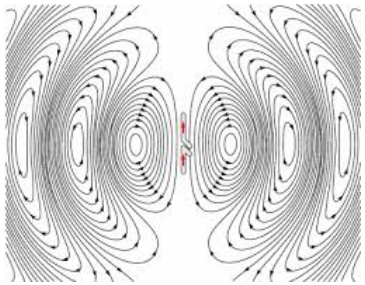
- **Bit**: propagates between transmitter/receiver pairs

- **Physical link**: what lies between transmitter/ receiver pairs
  - line coding
  - signal modulation

- **Guided media**
  - signals propagate in solid media
  - copper, fiber, coax



- **Unguided media**
  - no physical “wire”
  - signals propagate freely in electromagnetic spectrum
  - bidirectional
  - propagation environment effects



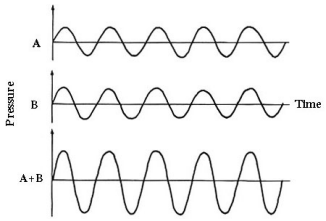
- **Bit error rate** depends on modulation and signal-to-noise ratio

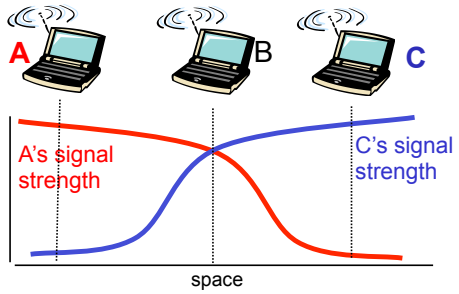
NTNU

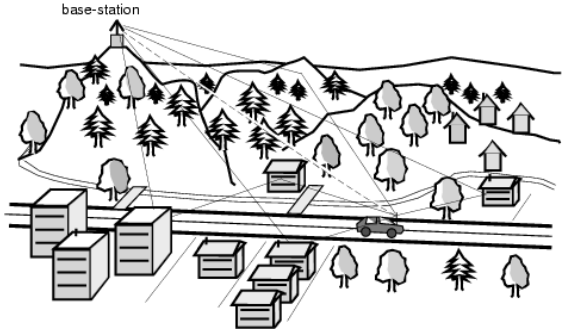
Wireless communication is more challenging than wired communication

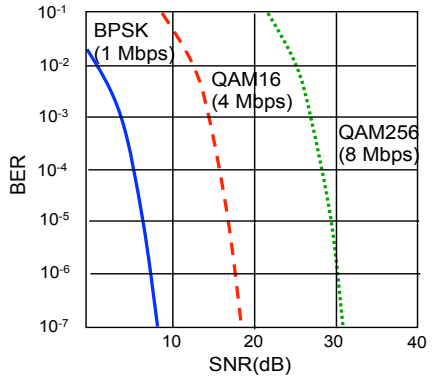
application
transport
network
link
PHYSICAL

- **Decreasing signal strength:** radio signal attenuates as it propagates through matter (path loss)
- **Interference** from other sources
- **Multipath** propagation: radio signal reflects off objects ground, arriving destination at slightly different times

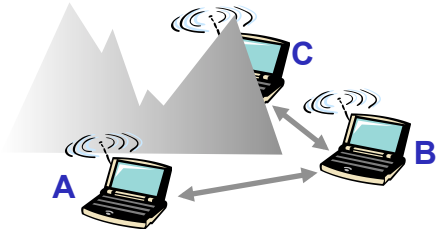






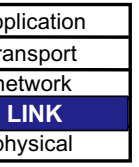


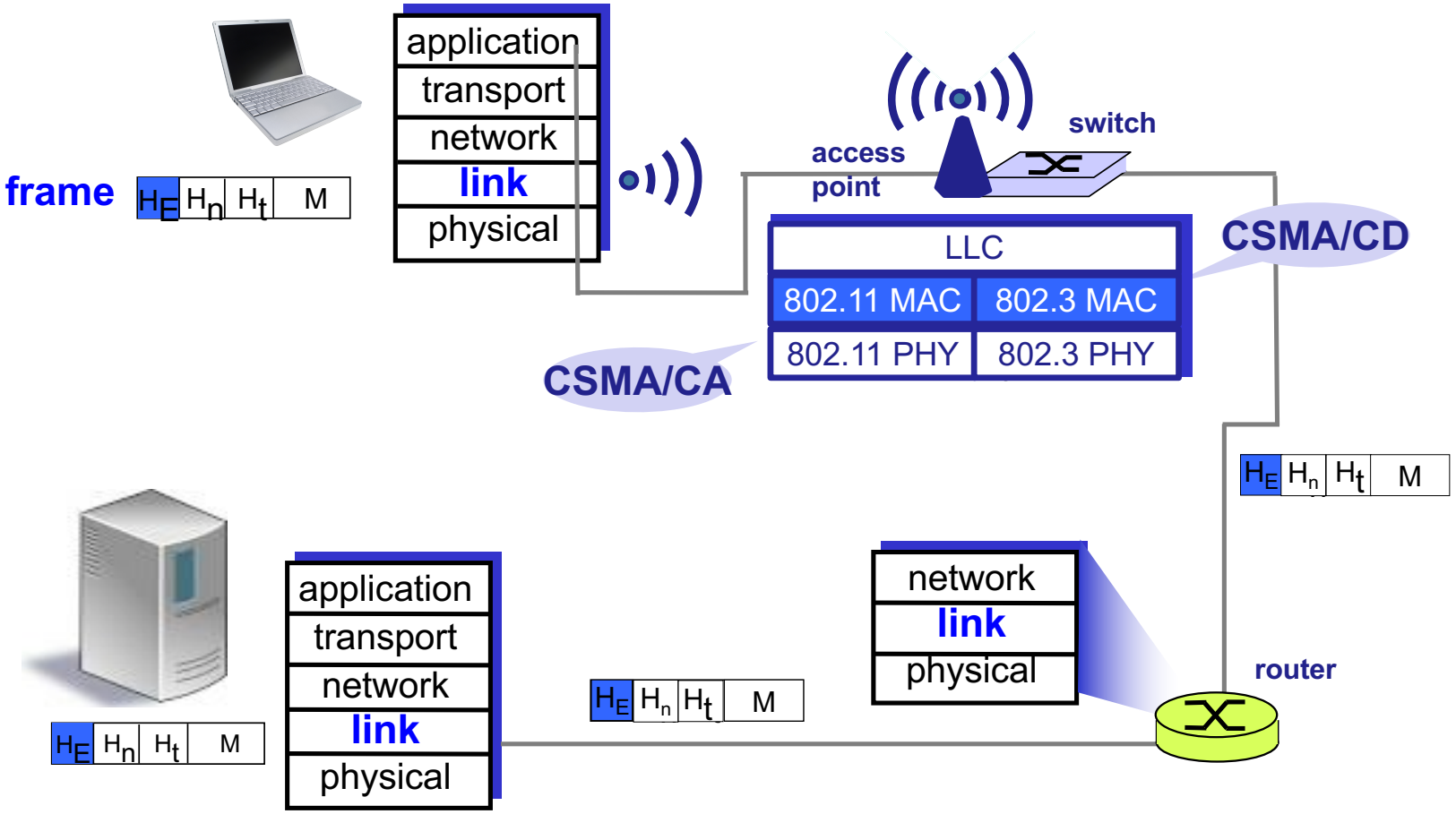
Larger **SNR signal-to-noise ratio** – easier to extract signal from noise



Hidden terminal problem

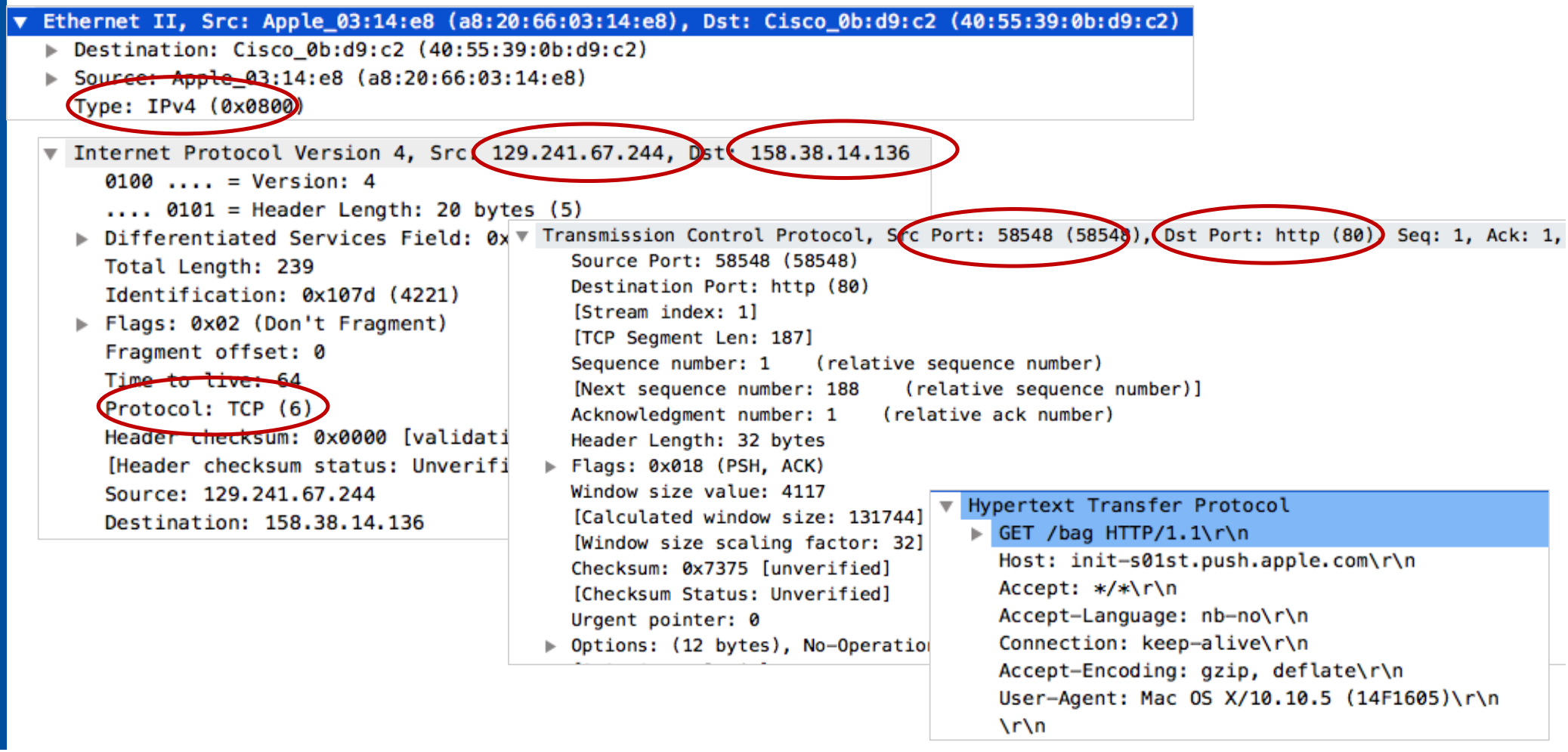
The link layer is point-to-point or broadcast and transmitter and receiver are the same





CSMA/CD Carrier Sense Multiple Access/Collision Detect
CSMA/CA Carrier Sense Multiple Access/Collision Avoidance

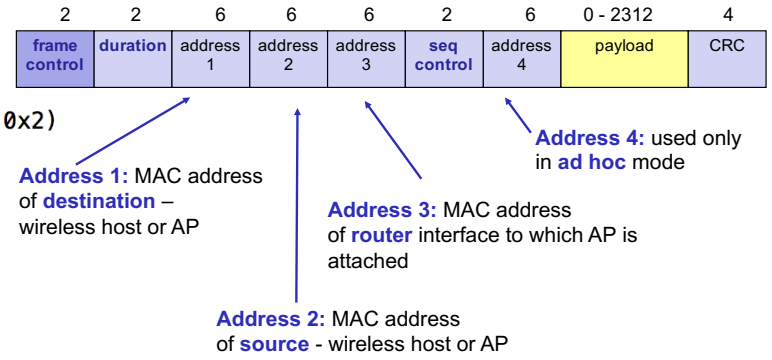
Ethernet 802.3 encapsulating IP/TCP/HTTP



Ethernet 802.11 encapsulating IP/UDP/DNS response

```
▼ IEEE 802.11 QoS Data, Flags: .p....F..
    Type/Subtype: QoS Data (0x0028)
  ▼ Frame Control Field: 0x8842
      .... ..00 = Version: 0
      .... 10.. = Type: Data frame (2)
      1000 .... = Subtype: 8
    ▼ Flags: 0x42
        .... ..10 = DS status: Frame from DS to a STA via AP(To DS: 0 From DS: 1) (0x2)
        .... .0.. = More Fragments: This is the last fragment
        .... 0... = Retry: Frame is not being retransmitted
        ...0 .... = PWR MGT: STA will stay up
        ..0. .... = More Data: No data buffered
        .1.. .... = Protected flag: Data is protected
        0... .... = Order flag: Not strictly ordered
    .000 0000 0010 1100 = Duration: 44 microseconds
    Receiver address: Apple_98:a8:e0 (60:03:08:98:a8:e0)      Address 1
    Destination address: Apple_98:a8:e0 (60:03:08:98:a8:e0)
    Transmitter address: Cisco_77:46:bf (fc:5b:39:77:46:bf)   Address 2
    Source address: Cisco_0a:75:44 (d8:67:d9:0a:75:44)        Address 3
```

802.11 frame format – multiple addresses




```
▼ Logical-Link Control
  ▶ DSAP: SNAP (0xaa)
  ▶ SSAP: SNAP (0xaa)
  ▶ Control field: U, func=UI (0x03)
    Organization Code: Encapsulated Ethernet (0x000000)
    Type: IPv4 (0x0800)
```

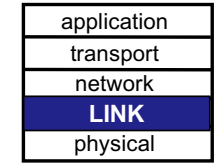
```
▼ Internet Protocol Version 4, Src: 129.241.0.201, Dst: 10.24.3.206
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 77
    Identification: 0x969f (38559)
  ▶ Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 62
    Protocol: UDP (17)
    Header checksum: 0x1561 [validation
    [Header checksum status: Unverified
    Source: 129.241.0.201
    Destination: 10.24.3.206
```

```
▼ User Datagram Protocol, Src Port: domain (53), Dst Port: 64674 (64674)
    Source Port: domain (53)
    Destination Port: 64674 (64674)
    Length: 57
    Checksum: 0xb241 [unverified]
```

```
▼ Domain Name System (response)
    Transaction ID: 0x9ed4
  ▶ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  ▼ Queries
    ▶ sslvpn2.ntnu.no: type A, class IN
  ▼ Answers
    ▶ sslvpn2.ntnu.no: type A, class IN, addr 129.241.77.152
```

NTNU

A medium access protocol regulates the transmission into a shared broadcast channel



1. Channel partitioning

- divide channel into smaller “pieces” (time slots, frequency, code)
- allocate piece to node for exclusive use

TDMA; FDMA; CDMA

2. Random access

- channel not divided, allow collisions
- “recover” from collisions

slotted ALOHA; ALOHA; CSMA, CSMA/CD; CSMA/CA

3. Taking turns

- nodes take turns, but nodes with more to send can take longer turns

Polling; token passing

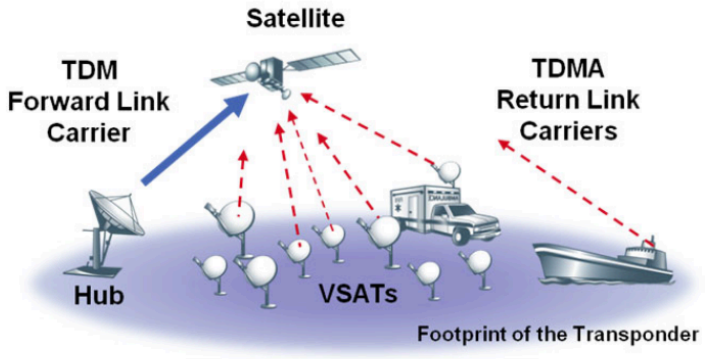
Networks without Barriers

SatLink

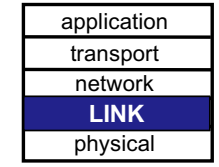
- SatLink is a leading provider of satellite networks systems and services, serving the needs for basic and broadband access into remote regions and seas of the world. We have more than twenty-five years of track record installing and operating satellite and telecom ground facilities in the remotest parts of the world, both directly and working through partners. SatLink is wholly owned by Trio Connect, LLC, a US based company majority owned and backed by Abry Partners. SatLink includes subsidiaries in the United Arab Emirates and Norway and remote offices in Indonesia and Denmark. With these n
serve markets in Latin America, Africa, the Middle East, and parts
product portfolio includes industry leading satellite broadband access

TDM/TDMA: THE SATELLITE TECHNOLOGY FOR IP NETWORKS

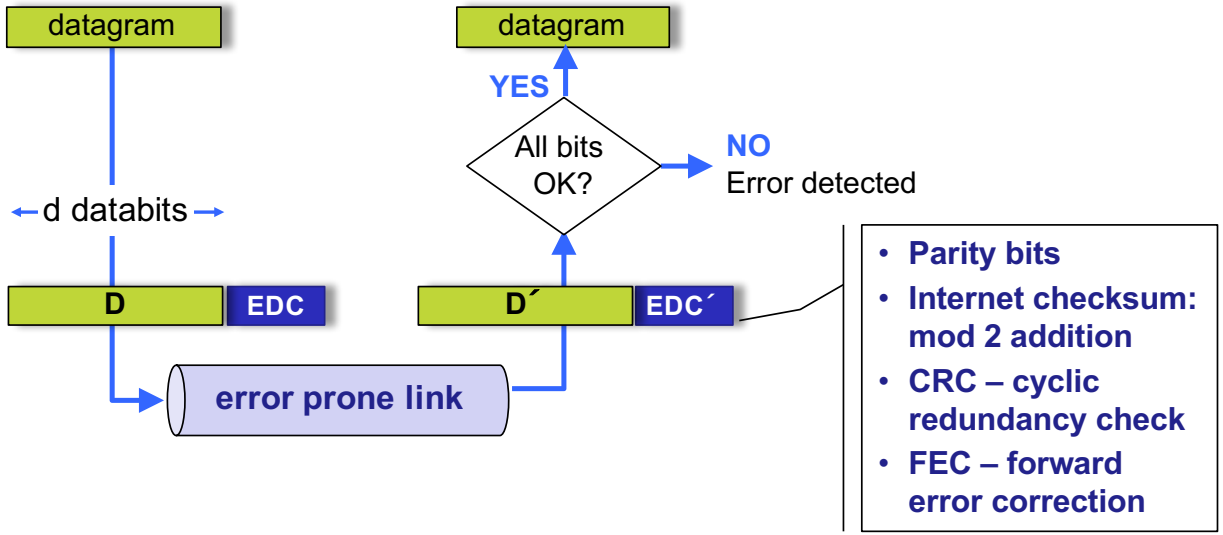
Of particular importance is SatLink Communications' 20+ year record of foresight and leadership in the R&D and commercialization of satellite technologies for TDM/TDMA networks. This is the use of **TDM** (Time Division Multiplexing) in combination with **TDMA** (Time Division Multiple Access) for interactive (i.e., two-way) communications via satellite to almost any location on or near the earth. The figure below illustrates the basic elements of a TDM/TDMA network.

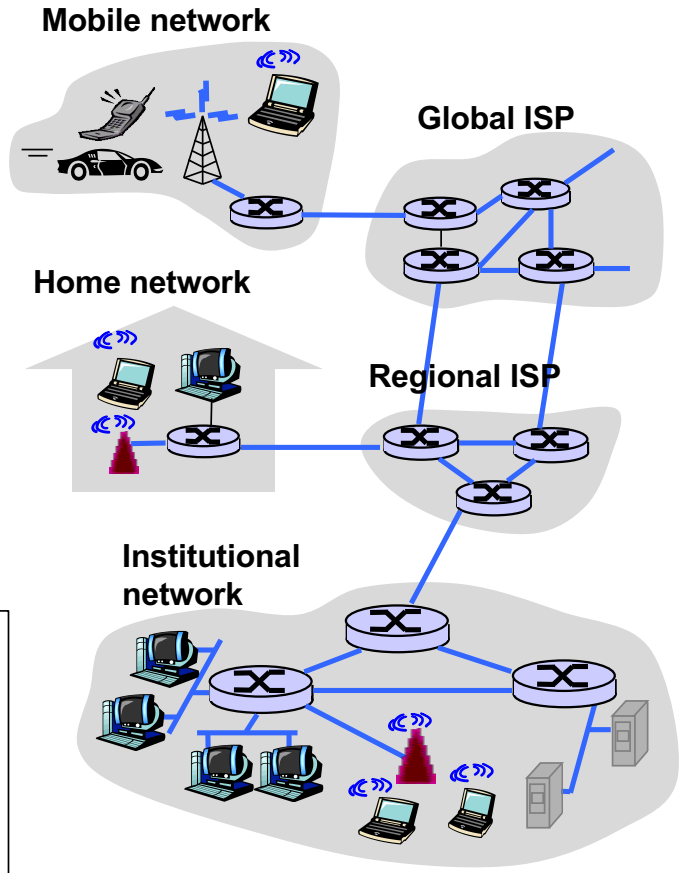


The link layer detects errors hop-by-hop

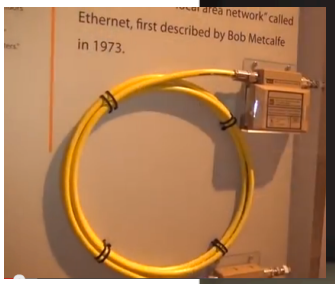


- Point-to-point vs broadcast
- Medium Access Control (MAC) if shared medium
- Half- or full-duplex
- **Error detection** (and **correction**) EDC through redundancy bits



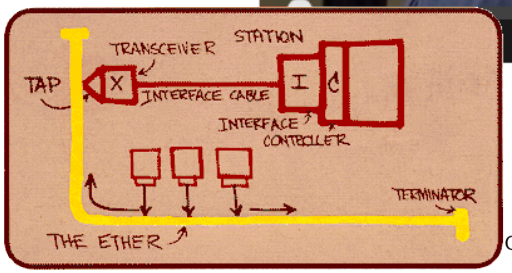


On the first Ethernet LAN



Ethernet is going UP (speed), through (WAN), over (wireless), down (embedded microcontrollers being networked), across (metro ethernet bridging LAN and WAN)

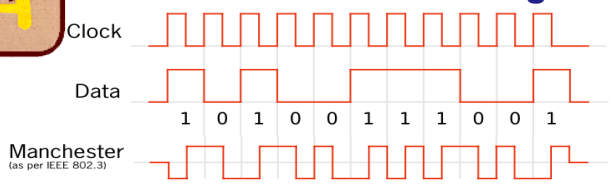
"Efficiency depends on the diameter of the network (in bits) , and as you go faster and faster the efficiency goes down"



"Diameter of network in bits" t_{prop}

A ⟷ **B**

Manchester encoding

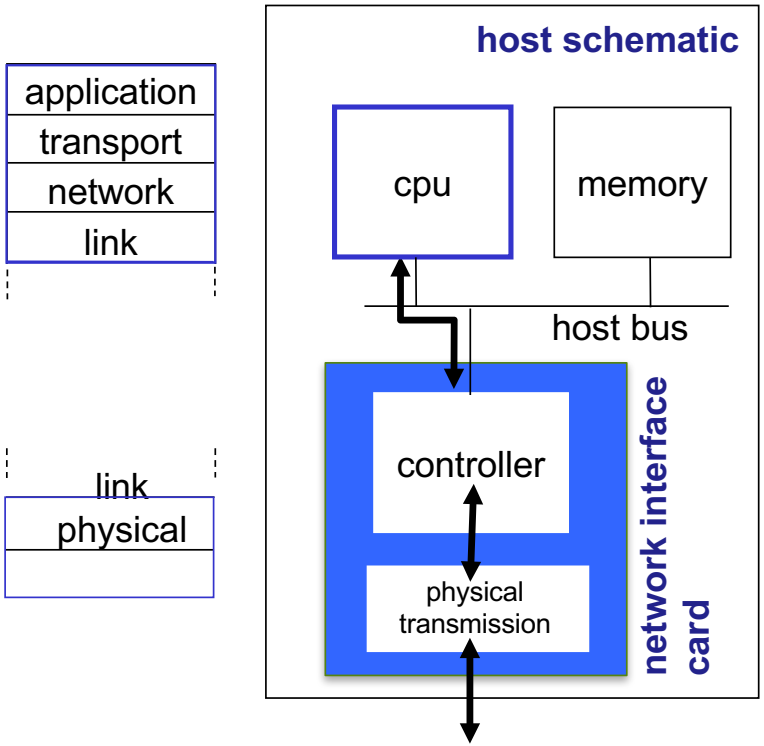


$$efficiency = \frac{1}{1 + 5t_{prop}/t_{trans}}$$

NTNU

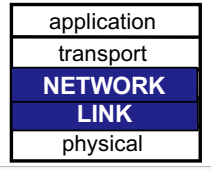
The link layer is implemented in each and every host/node

- Network interface card – NIC, implements link + physical layer
- Combination of hardware, firmware and software (network driver)

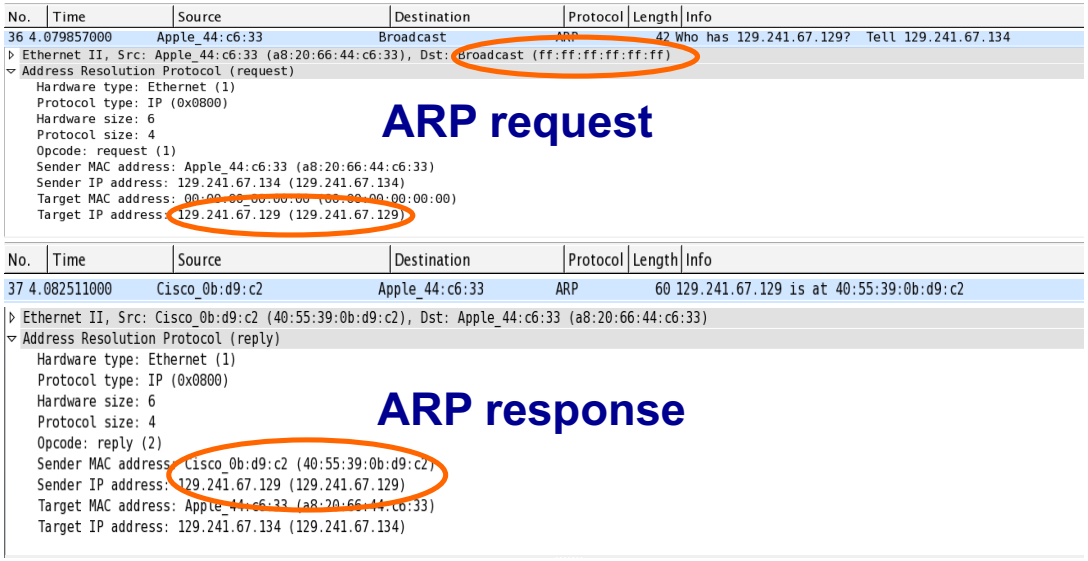


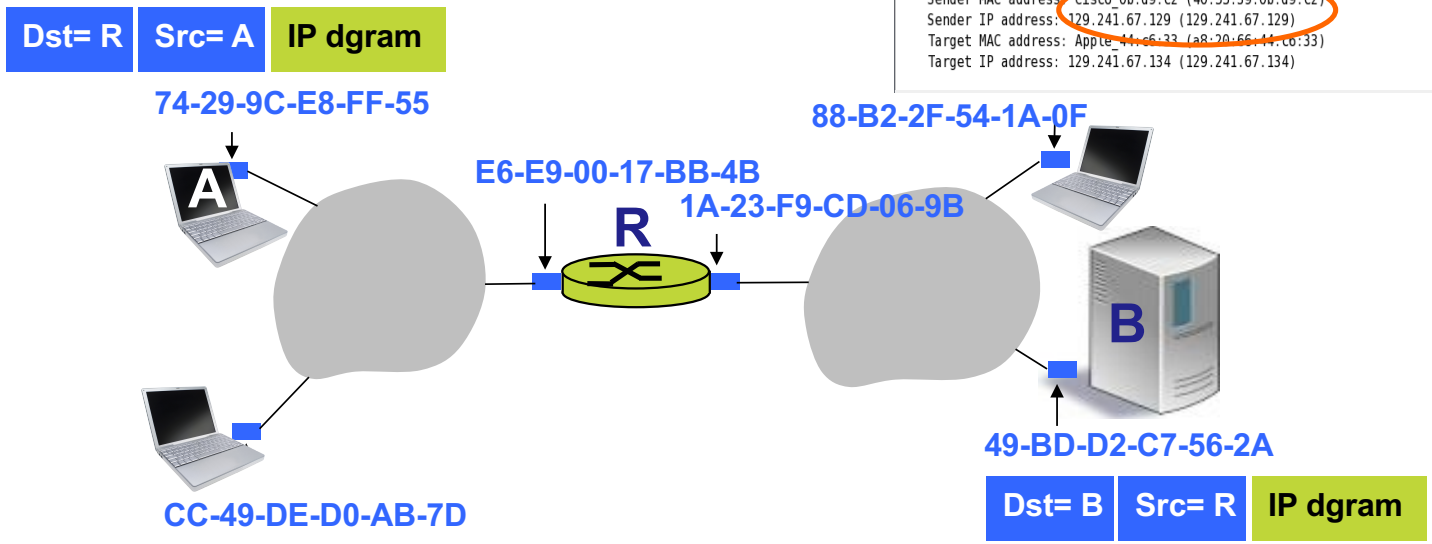
The link layer (ethernet) forwards frames hop-by-hop using the MAC address

Who
has this IP address?

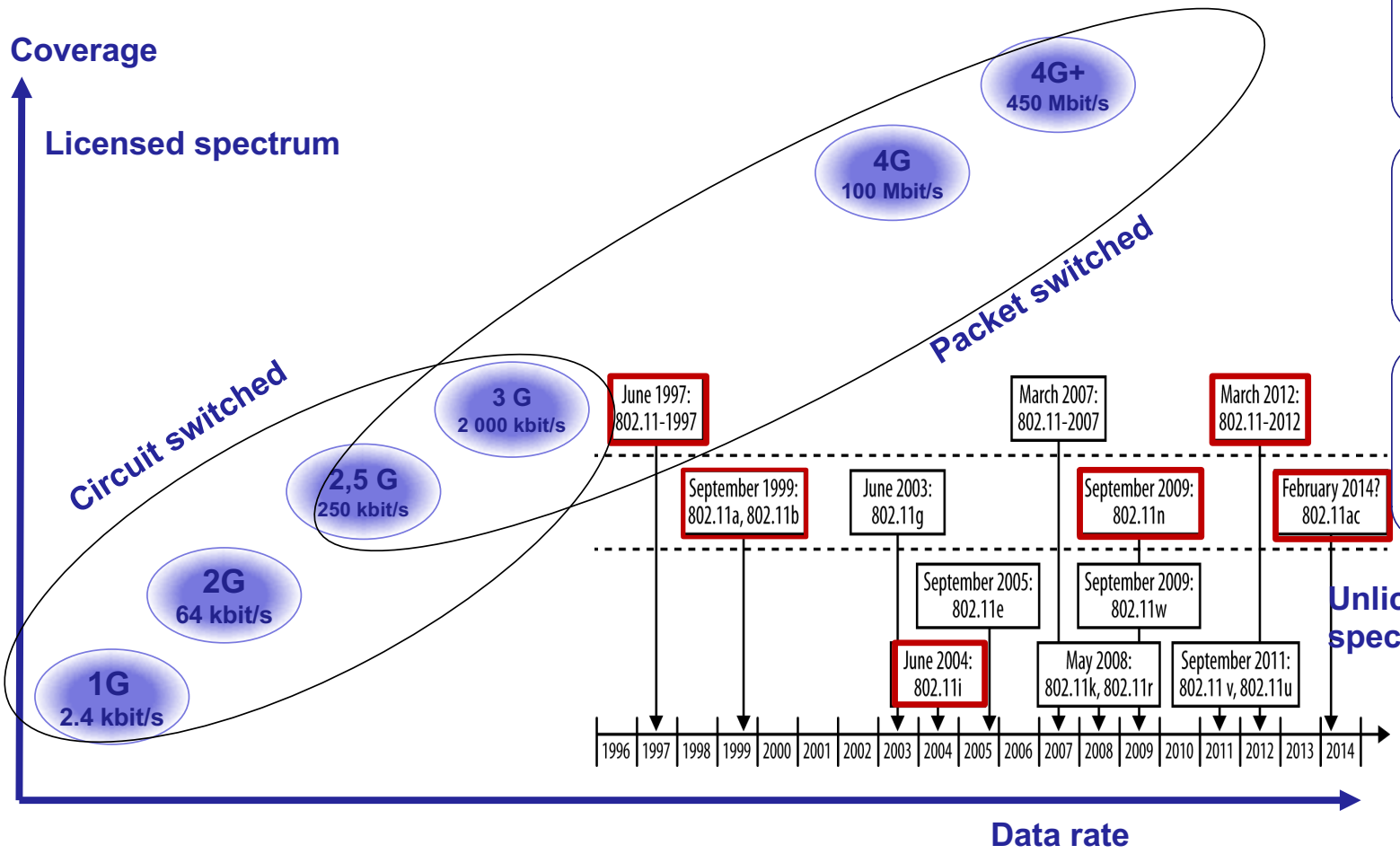


- **ARP** (address resolution protocol) translates **IPv4** address of next hop (next router or end system) to **MAC** (Medium Access Control) address of next hop
- Broadcast - runs within a subnet





Summary wireless and mobile: significant improvements in radio link bandwidth and efficiency -> Internet access networks



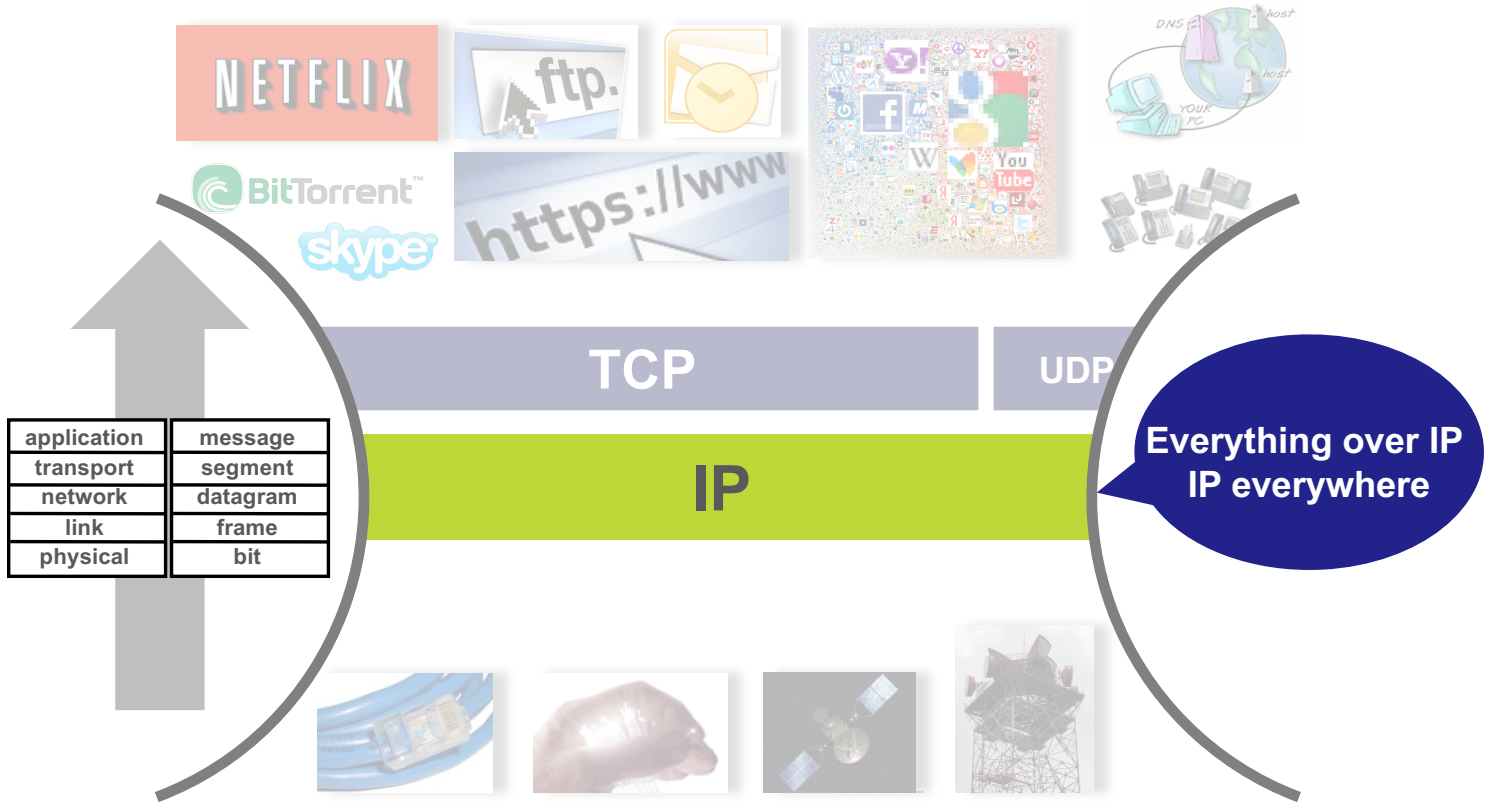
WEP has been outdated for years. Easily hacked due to 24-bit IV and weak authentication. Risky choice!

WPA addressed WEP flaws. Two modes: personal & enterprise. Use only if WPA2 not available. TKIP no longer considered secure.

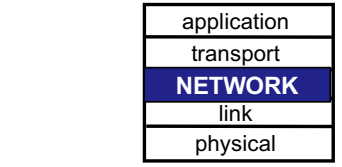
”Bruk **WPA2**-kryptering og skru ned sendestyrken på basestasjonen. Det er ingen grunn til å kringkaste signalet til halve nabolaget.”

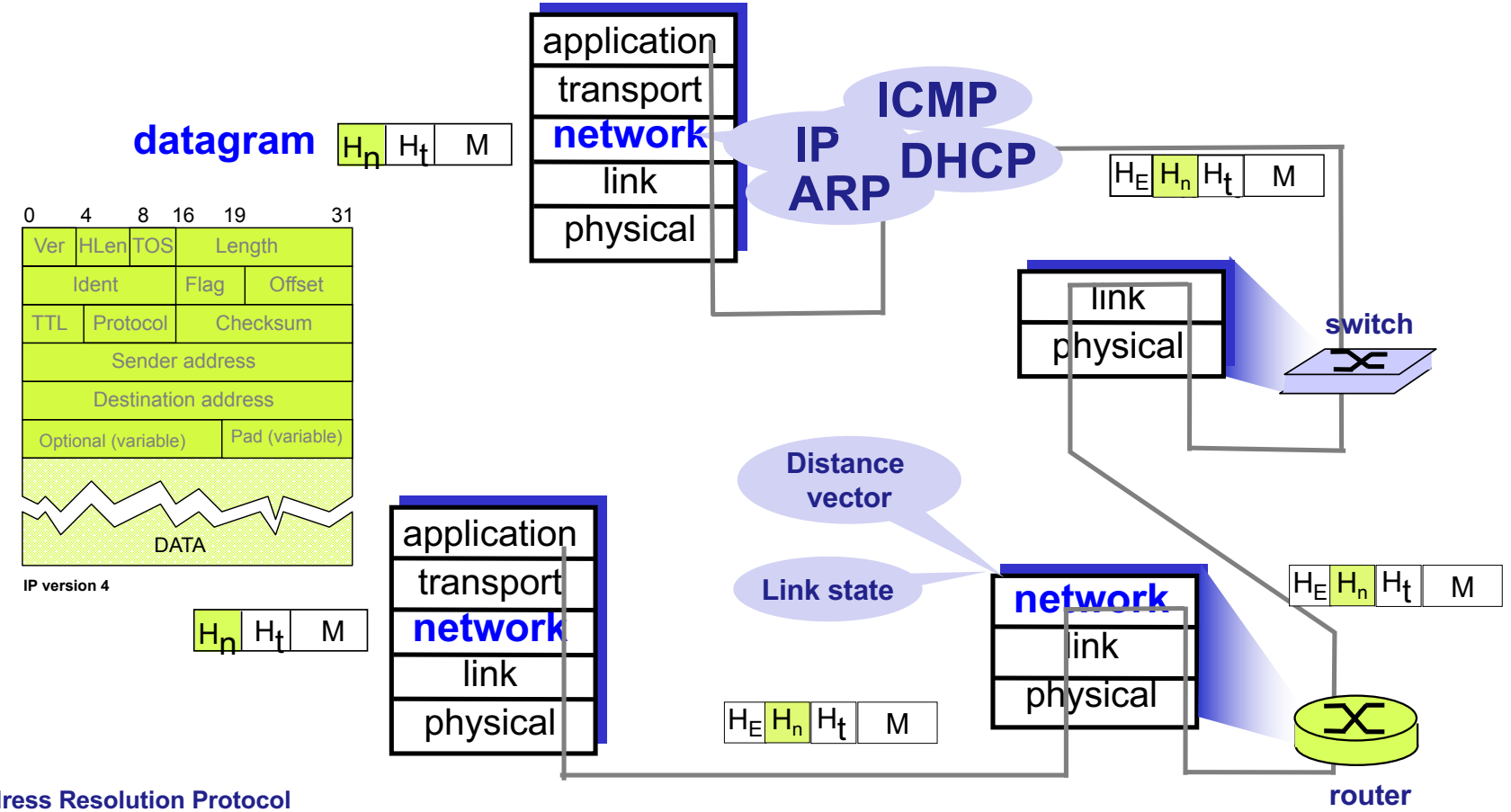
The NETWORK layer interconnects physical networks to transfer datagrams from source to destination

application
transport
NETWORK
link
physical



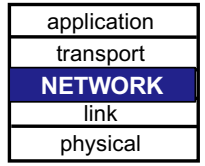
The Internet network layer is in every router and every host



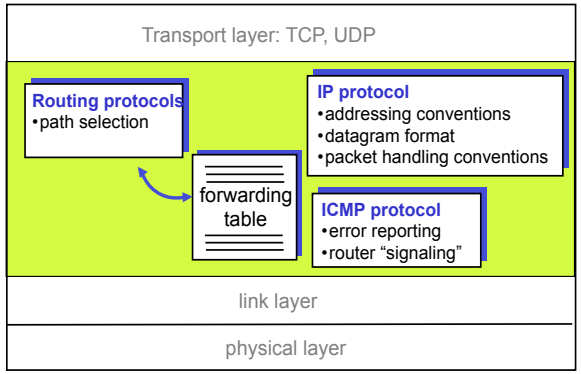


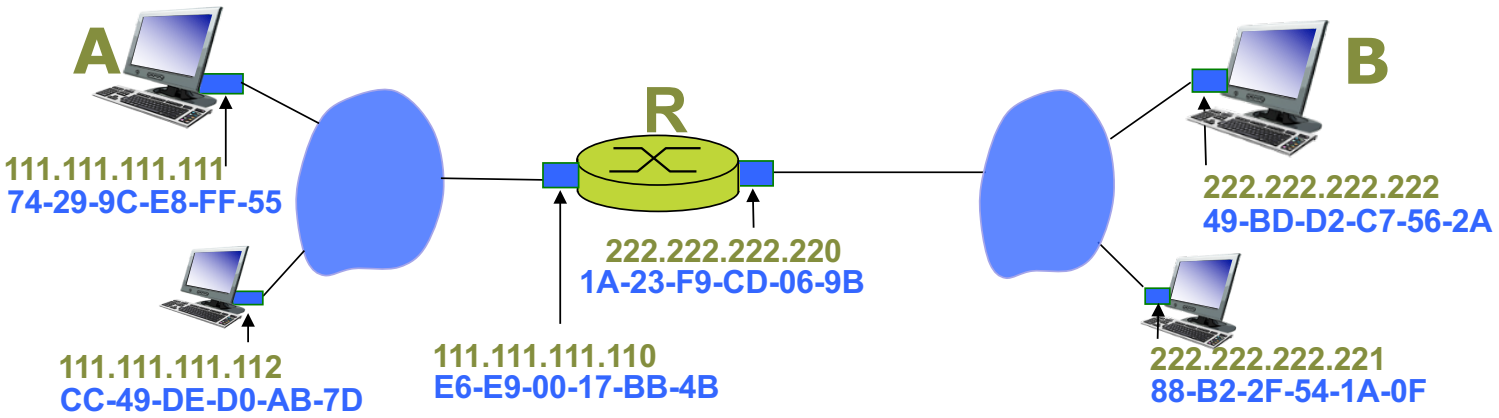
ARP Address Resolution Protocol
DHCP Dynamic Host Configuration Protocol
ICMP Internet Control Message Protocol

Internet network service is a best effort service



- The Internet datagram model is **connectionless**
- Each packet is forwarded independent of other packets
- Routing protocols build routing/forwarding tables
- Routers use the destination IP-address (possibly changed by NAT) to forward the datagram on the appropriate outbound link
- Underlying link networks have different **Maximum Transfer Units**: fragmentation and reassembly

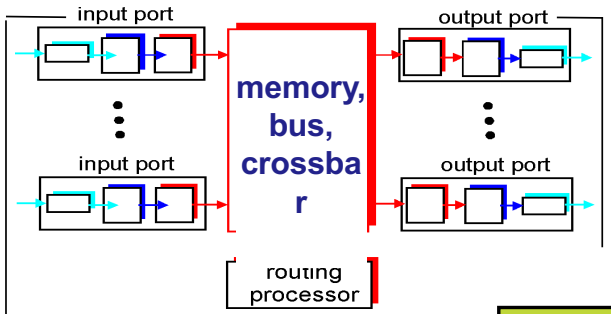




The first two packets on the Internet – LO

Routers forward IP datagrams, using forwarding tables built by routing protocols

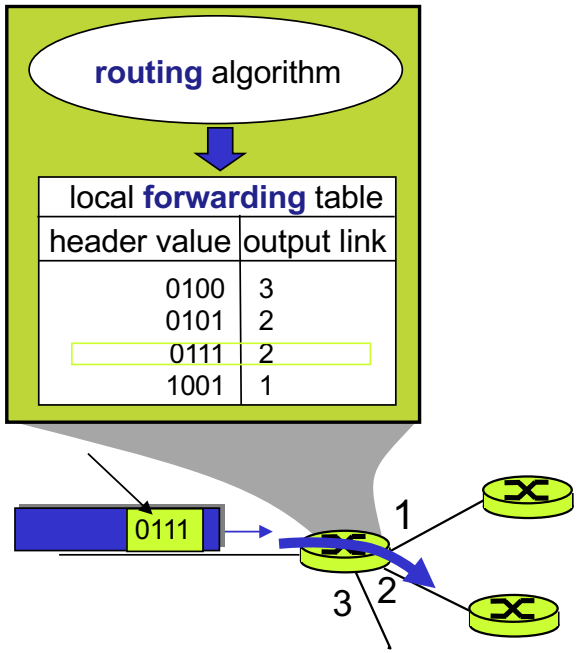
Queuing if datagrams arrive faster than forwarding rate into switch fabric, possibly **head-of-line blocking**



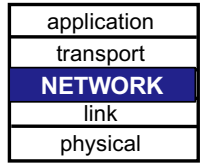
Queuing and **loss** if packets arrive from fabric faster than output line speed

Routing: determine route taken by packets from source to destination

Forwarding: move packets from router's input to appropriate router output - Longest prefix matching on destination address of each datagram



IPv4 technical challenges motivate for IPv6



- IPv4 **limited number** and types of **addresses**
- IPv4 **address structure** gives **large routing tables**
  - Bad address hierarchy
- IPv4 **missed support** for **new services** (but has been added)
  - QoS, mobility, multicast, security
- Additional IPv6 motivation
  - Header format helps speed in processing/forwarding

```
▶ Frame 284: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface 0
▶ Ethernet II, Src: Apple_ee:45:5a (c8:bc:c8:ee:45:5a), Dst: Sonicwal_10:51:f7 (00:17:c5:10:51:f7)
▼ Internet Protocol Version 4, Src: 10.0.0.103, Dst: 172.16.3.31
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 68
    Identification: 0x3595 (13
  ▶ Flags: 0x00
    Fragment offset: 0
    Time to live: 255
    Protocol: UDP (17)
    Header checksum: 0xcc7d [v
    [Header checksum status: U
    Source: 10.0.0.103
    Destination: 172.16.3.31
```

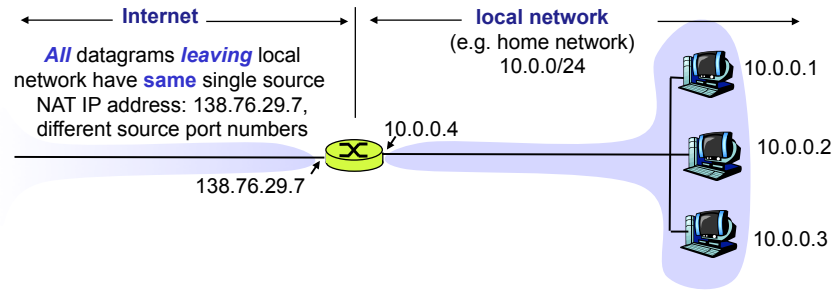
```
▶ Frame 7: 104 bytes on wire (832 bits), 104 bytes captured (832 bits) on interface 0
▶ Ethernet II, Src: Apple_98:a8:e0 (60:03:08:98:a8:e0), Dst: CiscoInc_a0:00:c8 (00:05:73:a0:00:c8)
▼ Internet Protocol Version 6, Src: 2001:700:300:4108:91aa:6ca0:aff1:fa4d, Dst: 2001:948:7:1::d
    0110 .... = Version: 6
  ▶ .... 0000 0000 .... .... .... .... .... = Traffic class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... .... .... 1010 1101 1001 0111 0110 = Flowlabel: 0x000ad976
    Payload length: 50
    Next header: UDP (17)
    Hop limit: 64
    Source: 2001:700:300:4108:91aa:6ca0:aff1:fa4d
    Destination: 2001:948:7:1::d
```

But the life time for the IP address space has been extended because of

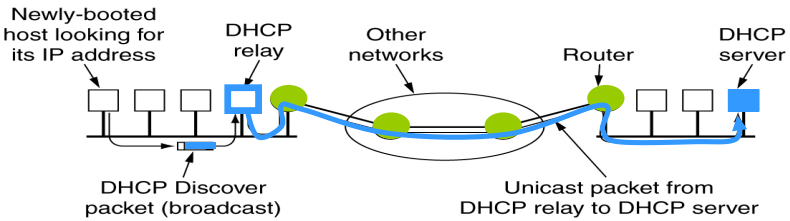
- **CIDR (Classless InterDomain Routing)**
  - Address format: **a.b.c.d/x**, where **x** is # bits in subnet portion of address

200.23.16.0/23 ← subnet part → ← host part →

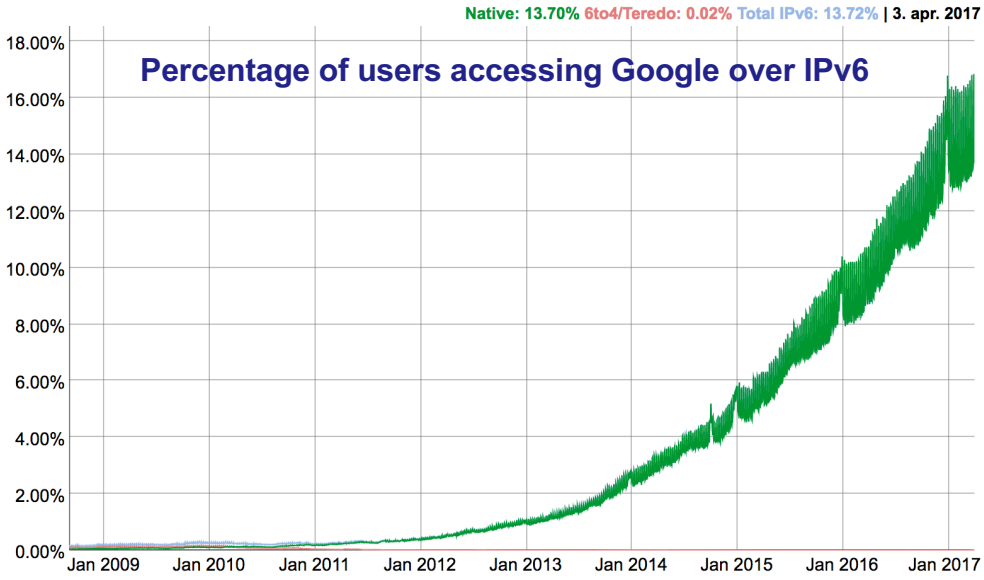
- **NAT – Network Address Translation**



- **DHCP – Dynamic Host Configuration Protocol**



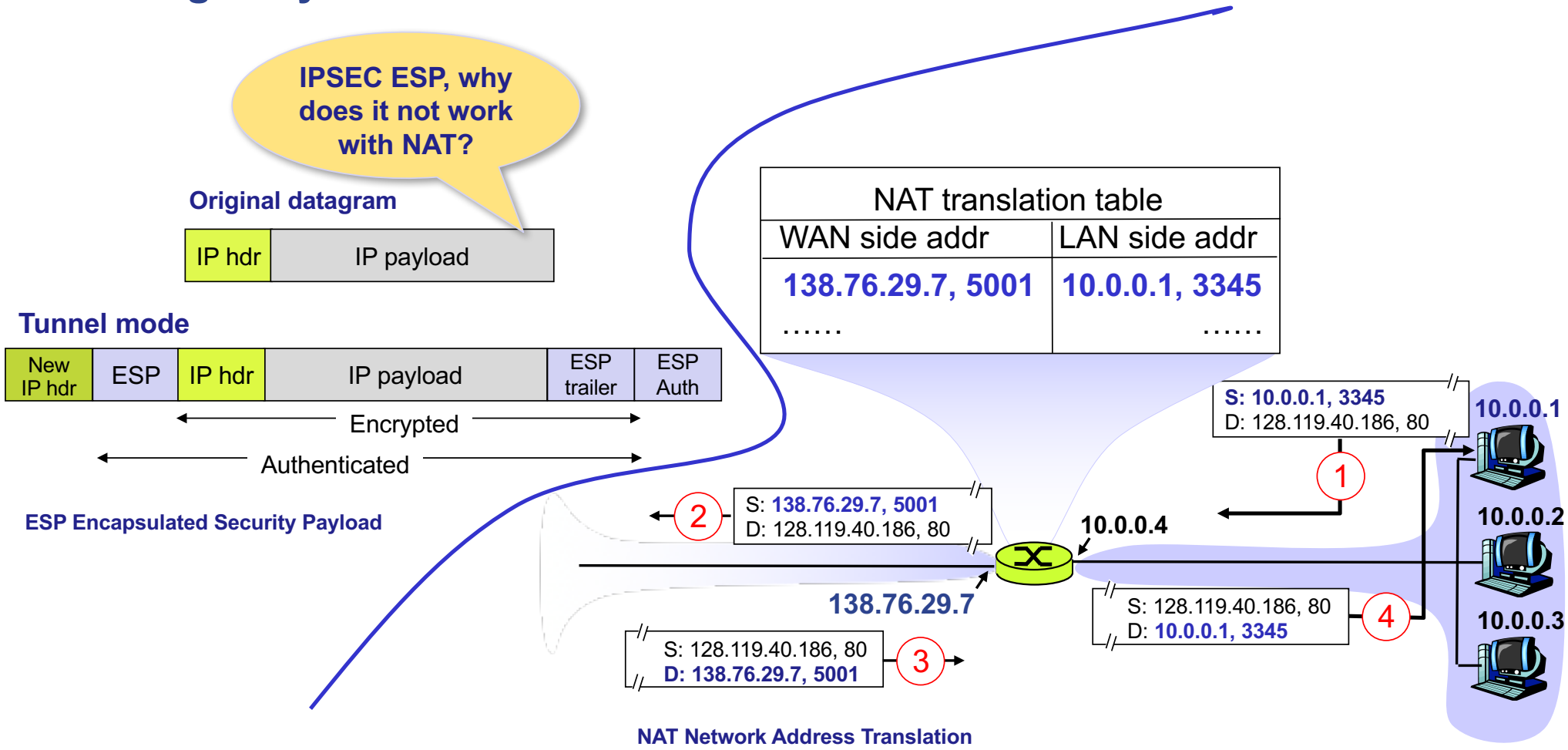
However, the use of IPv6 is now a reality



Source	Destination	Length	Info
10.24.32.226	129.241.0.201	70	Standard query 0xd4e5 A google.com
10.24.32.226	129.241.0.201	70	Standard query 0xf191 AAAA google.com
129.241.0.201	10.24.32.226	98	Standard query response 0xf191 AAAA google.com AAAA 2a00:1450:400f:804::2
129.241.0.201	10.24.32.226	86	Standard query response 0xd4e5 A google.com A 216.58.211.142

Source	Destination	Length	Info
2001:700:300:410…	2a00:1450:400f:804::200e	98	49762 → http(80) [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=32 TSval=851442058 …
2001:700:300:410…	2a00:1450:400f:804::200e	98	[TCP Retransmission] 49762 → http(80) [SYN] Seq=0 Win=65535 Len=0 MSS=1440 W…
2a00:1450:400f:8…	2001:700:300:4108:a949:1ccf:bd40:8046	94	http(80) → 49762 [SYN, ACK] Seq=0 Ack=1 Win=27960 Len=0 MSS=1410 SACK_PERM=1…
2001:700:300:410…	2a00:1450:400f:804::200e	86	49762 → http(80) [ACK] Seq=1 Ack=1 Win=131392 Len=0 TSval=851443075 TSecr=42…
2001:700:300:410…	2a00:1450:400f:804::200e	419	GET / HTTP/1.1
2a00:1450:400f:8…	2001:700:300:4108:a949:1ccf:bd40:8046	86	http(80) → 49762 [ACK] Seq=1 Ack=334 Win=29056 Len=0 TSval=4286655945 TSecr=…
2a00:1450:400f:8…	2001:700:300:4108:a949:1ccf:bd40:8046	557	HTTP/1.1 302 Found (text/html)
2001:700:300:410…	2a00:1450:400f:804::200e	86	49762 → http(80) [ACK] Seq=334 Ack=472 Win=130912 Len=0 TSval=851443092 TSec…

IPSEC provides authentication, confidentiality and integrity, and is challenged by NAT

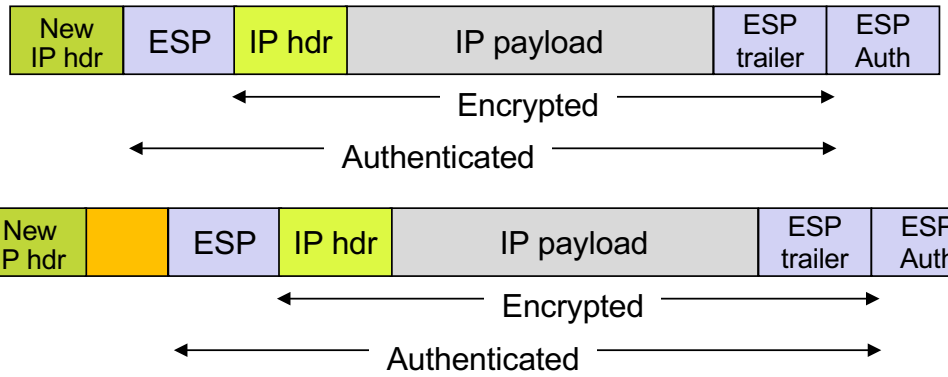


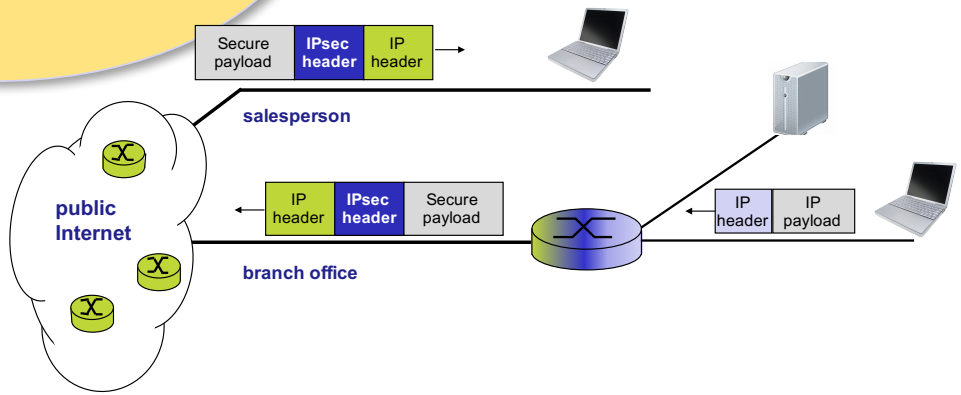
NTNU

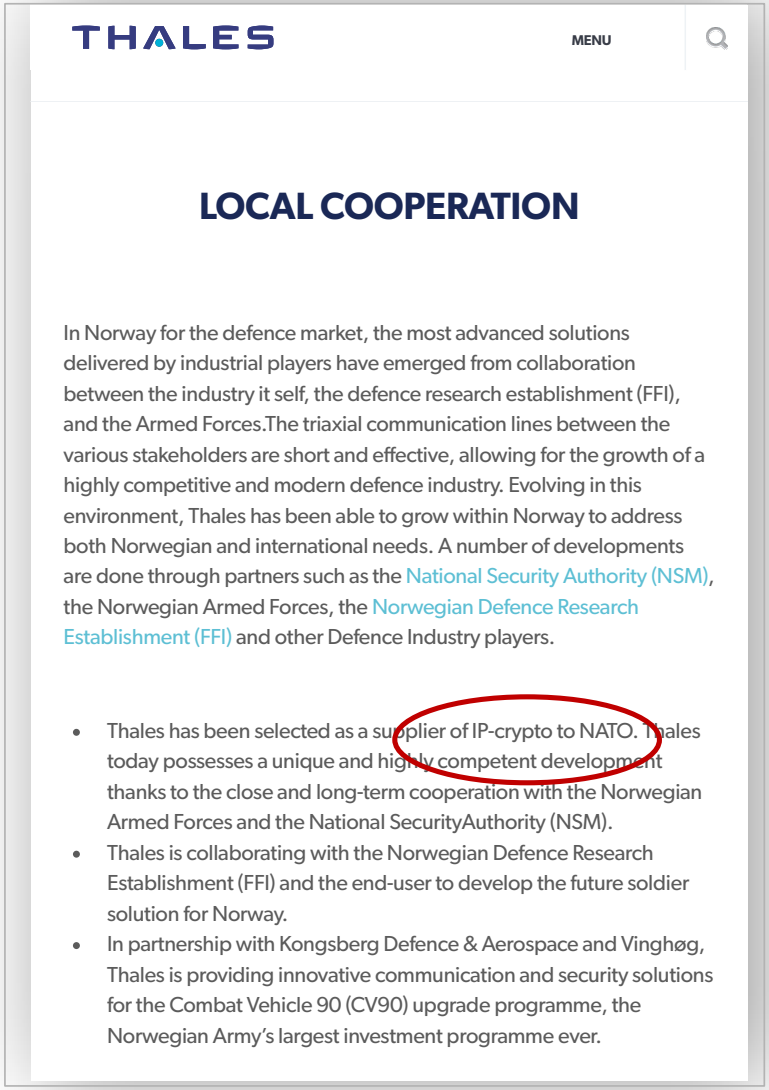
Which protocol would you add to the tunnel to allow for NAT-traversal when using IPSEC?

Original datagram

Tunnel mode





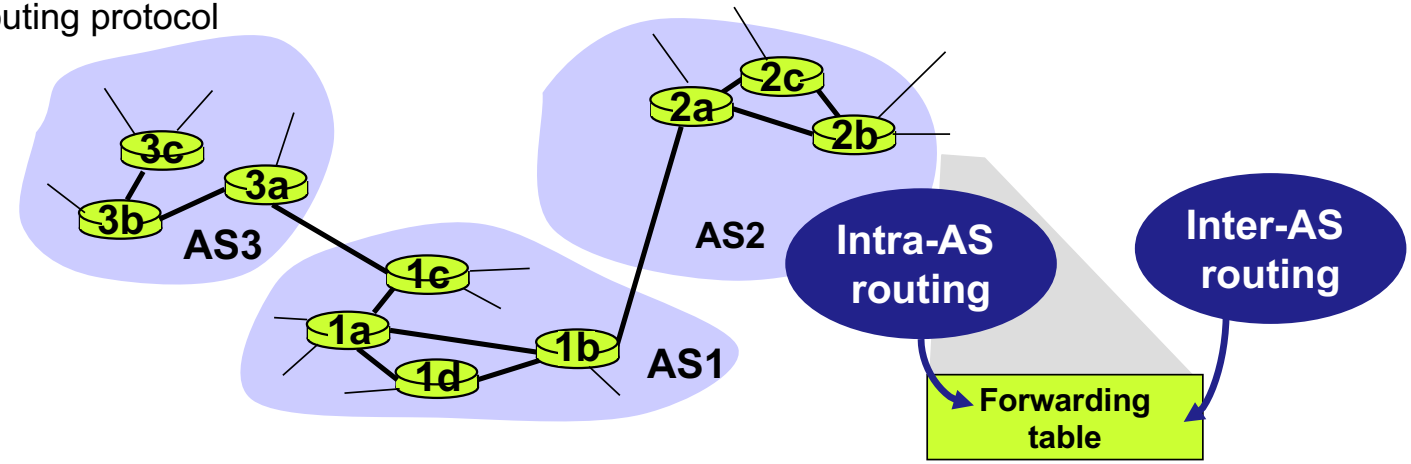

THALES
MENU
LOCAL COOPERATION
In Norway for the defence market, the most advanced solutions delivered by industrial players have emerged from collaboration between the industry it self, the defence research establishment (FFI), and the Armed Forces.The triaxial communication lines between the various stakeholders are short and effective, allowing for the growth of a highly competitive and modern defence industry. Evolving in this environment, Thales has been able to grow within Norway to address both Norwegian and international needs. A number of developments are done through partners such as the National Security Authority (NSM), the Norwegian Armed Forces, the Norwegian Defence Research Establishment (FFI) and other Defence Industry players.
Thales has been selected as a supplier of IP-crypto to NATO. Thales today possesses a unique and highly competent development thanks to the close and long-term cooperation with the Norwegian Armed Forces and the National SecurityAuthority (NSM).
Thales is collaborating with the Norwegian Defence Research Establishment (FFI) and the end-user to develop the future soldier solution for Norway.
In partnership with Kongsberg Defence & Aerospace and Vinghøg, Thales is providing innovative communication and security solutions for the Combat Vehicle 90 (CV90) upgrade programme, the Norwegian Army's largest investment programme ever.

NTNU

Hierarchical routing aggregates networks into domains = “autonomous systems” (AS)

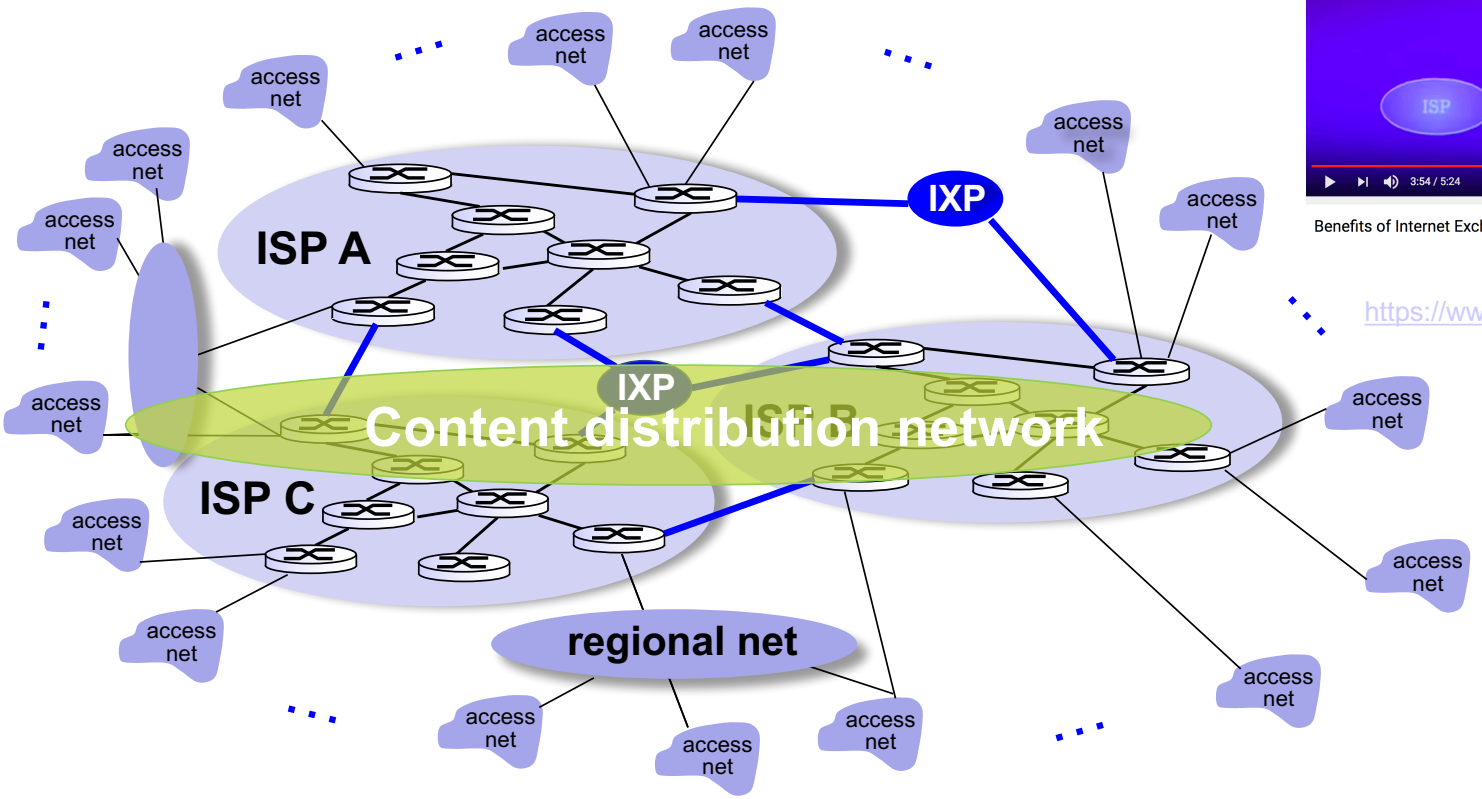
application
transport
NETWORK
link
physical

- **Routers in same AS** run same routing protocol
  - **“Intra-AS”** routing protocol
  - Routers in different AS´s can run different intra-AS routing protocols
- **Gateway router** has a direct link to router in another AS
  - **“Inter-AS”** routing protocol
- Forwarding table configured by both intra- and inter-AS routing algorithm
  - intra-AS sets entries for internal destinations
  - inter-AS & intra-AS sets entries for external destinations

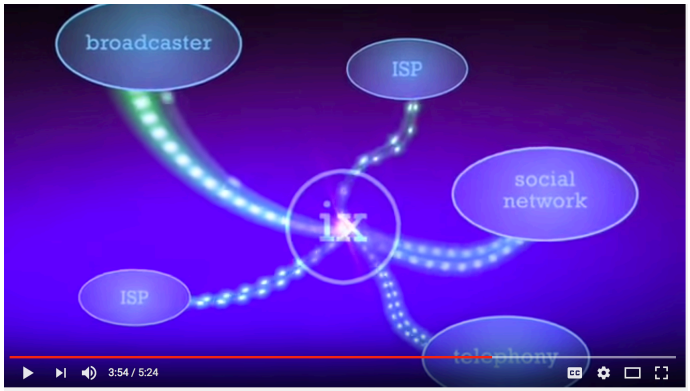


What is the Internet?

Network of networks



ISP Internet Service Provider
IXP Internet eXchange Provider



Benefits of Internet Exchange Points

YouTube

https://www.youtube.com/watch?v=TKNQ1lgguM8

Netflix challenged net neutrality, and offers now its open connect CDN to larger internet service providers

Netflix og bredbåndsleverandørene krangler om regninga for videostrømming

Amerikanske Netflix-brukere har havnet i kryssilden når de store nettaktørene kjemper om hvem som skal betale for bredere bredbånd og skarpere HD-video. Også norske aktører er uenige om regninga.

”…mer enn 50 prosent av veksten økt bruk av amerikanske strømmetjenester, med Netflix i spissen. Våren 2013 fikk Netflix utplassert servere i kjernenettet til Altibox, noe som bidrar til høyere kvalitet og stabilitet under avspillingene.”

Altibox fortsetter den tunge satsingen på fiber til privatboliger. Økt bruk av Netflix og andre strømmetjenester er blant det som bidrar sterkest til økningen trafikken p
Harald Brombach

Altibox doblet trafikken

Kundene flokker særlig til én nettjeneste.

Av Harald Brombach - Marius Jørgenrud

Publisert 19. november 2014 kl. 13:10

UTFORDRER NETTNØYTRALITETEN?: Netflix' inntog i Norge har bydd på utfordringer for Telenor, som ønsker at videotjenester som tar opp mye kapasitet i nettet skal betale. Kritikerne mener imidlertid at prinsippet om nettnøytralitet står på spill når store og pengesterke aktører blir positivt diskriminert. Bildet er fra Netflix-serien «Orange is the New Black». FOTO: PROMO

Netflix inngår hemmelig avtale med Telenor

Forbrukerrådet reagerer.

JOAKIM THORKILDSEN
joakim@filtermagasin.com
FILTER

fredag 7. mars 2014, kl.08:46

(Filtermagasin.no): Forholdet mellom Telenor og Netflix har vært noe anstrengt etter at den amerikanske strømmegiganten etablerte seg i Norge høsten 2012.

Når tjenesten ble så populær på kort tid la det beslag på mye av Telenors kapasitet, og internettleverandøren ønsket at Netflix skulle betale for å leie plass til sine servere i Telenors datahaller. Dette ville garantert en bedre bildekvalitet for tjenestens kunder, og man ville unngått flaskehalser som oppstår når store trafikkmengder blir overført fra Netflix' servere i utlandet.

Men Netflix nektet, og skeptikerne mente det ville utfordret prinsippet om nettnøytralitet hvis pengesterke aktører kunne kjøpe seg forrang.

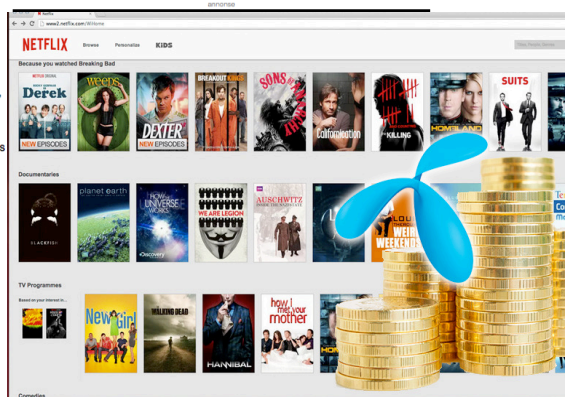
Nå har Netflix likevel krøpet til korset og inngått en avtale med Telenor, ifølge Dagens Næringsliv.

- Demonterer internett

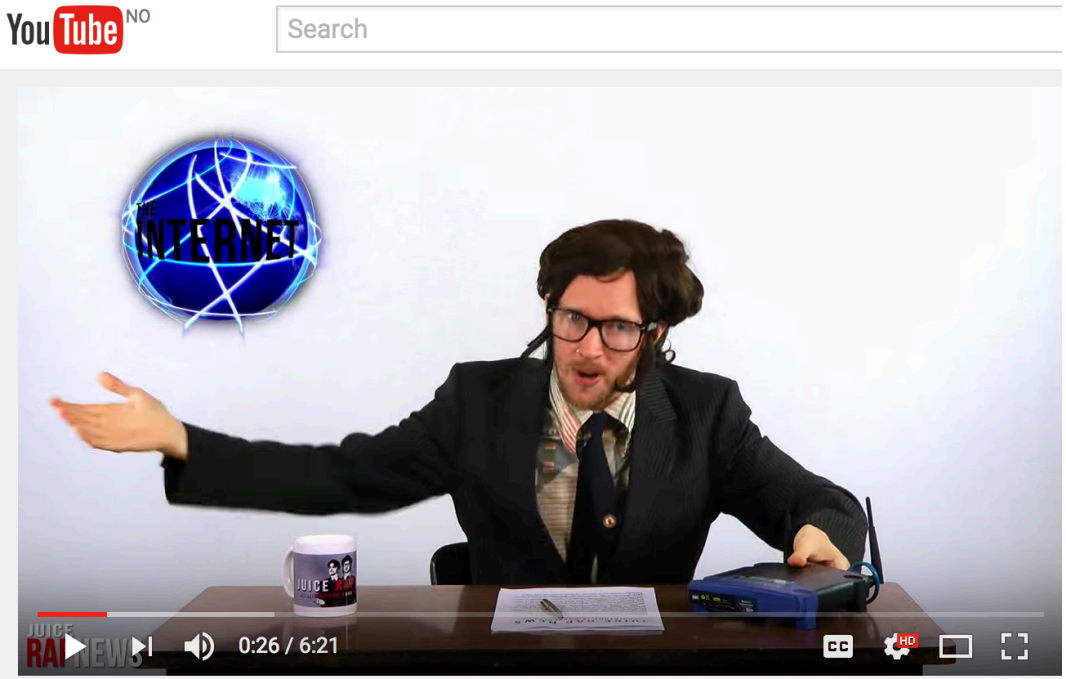
Innholdet i avtalen er imidlertid hemmelig, og Telenor ønsker ikke å kommentere overfor DN om de får betalt av Netflix.

- Men det er klart at det er en kommersiell avtale. Partene har forretningsmessige grunner til ikke å gå ut med detaljer som kan påvirke forhandlinger med andre aktører, sier Jørn Bremtun, senior kommunikasjonsrådgiver i Telenor, til Filter.

Netflix inngikk også en avtale med den amerikanske nettleverandøren Comcast for to uker siden, en avtale som ifølge New York Times innebar en «milepæl i internetthistorien».

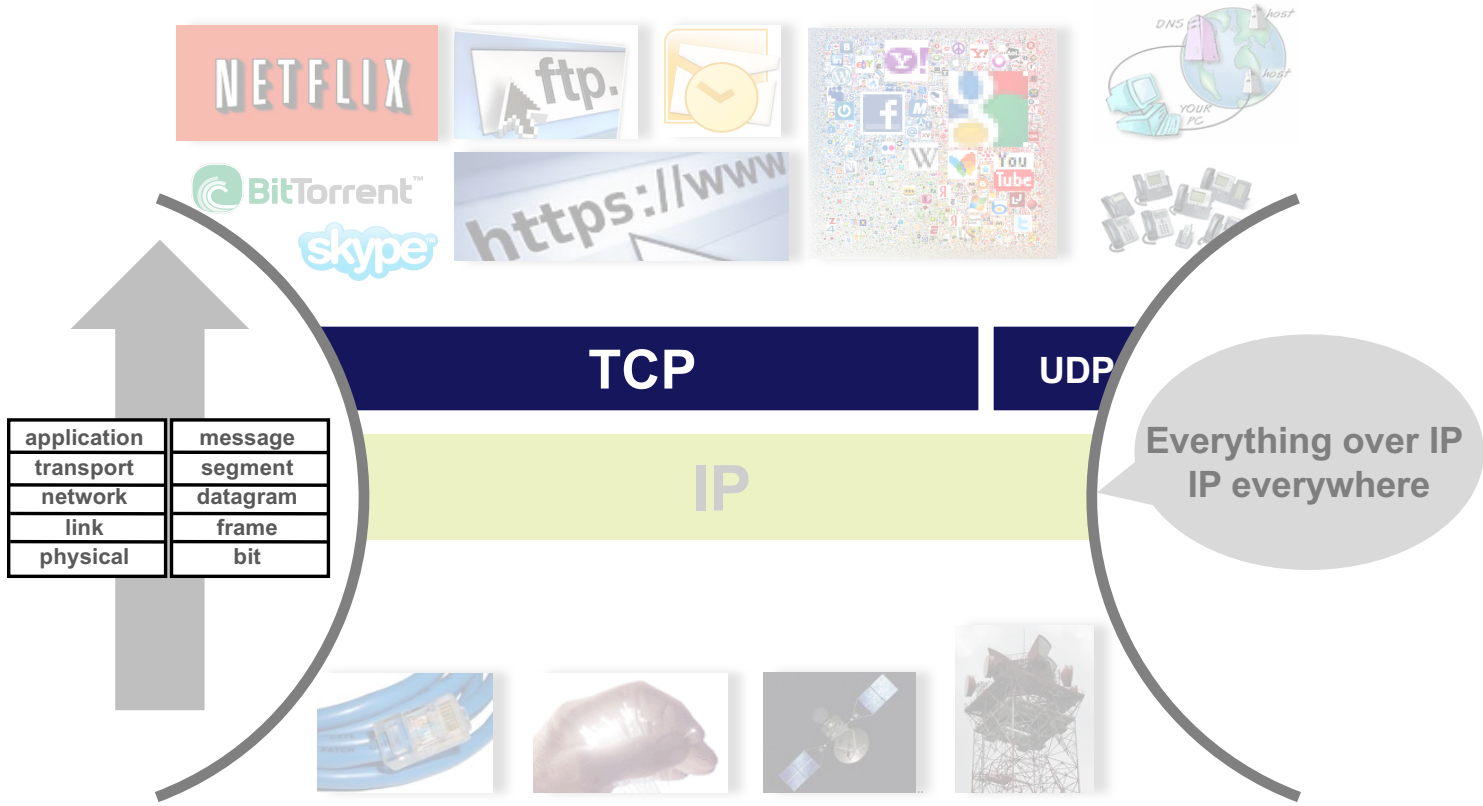


Internet network providers did not embrace net neutrality



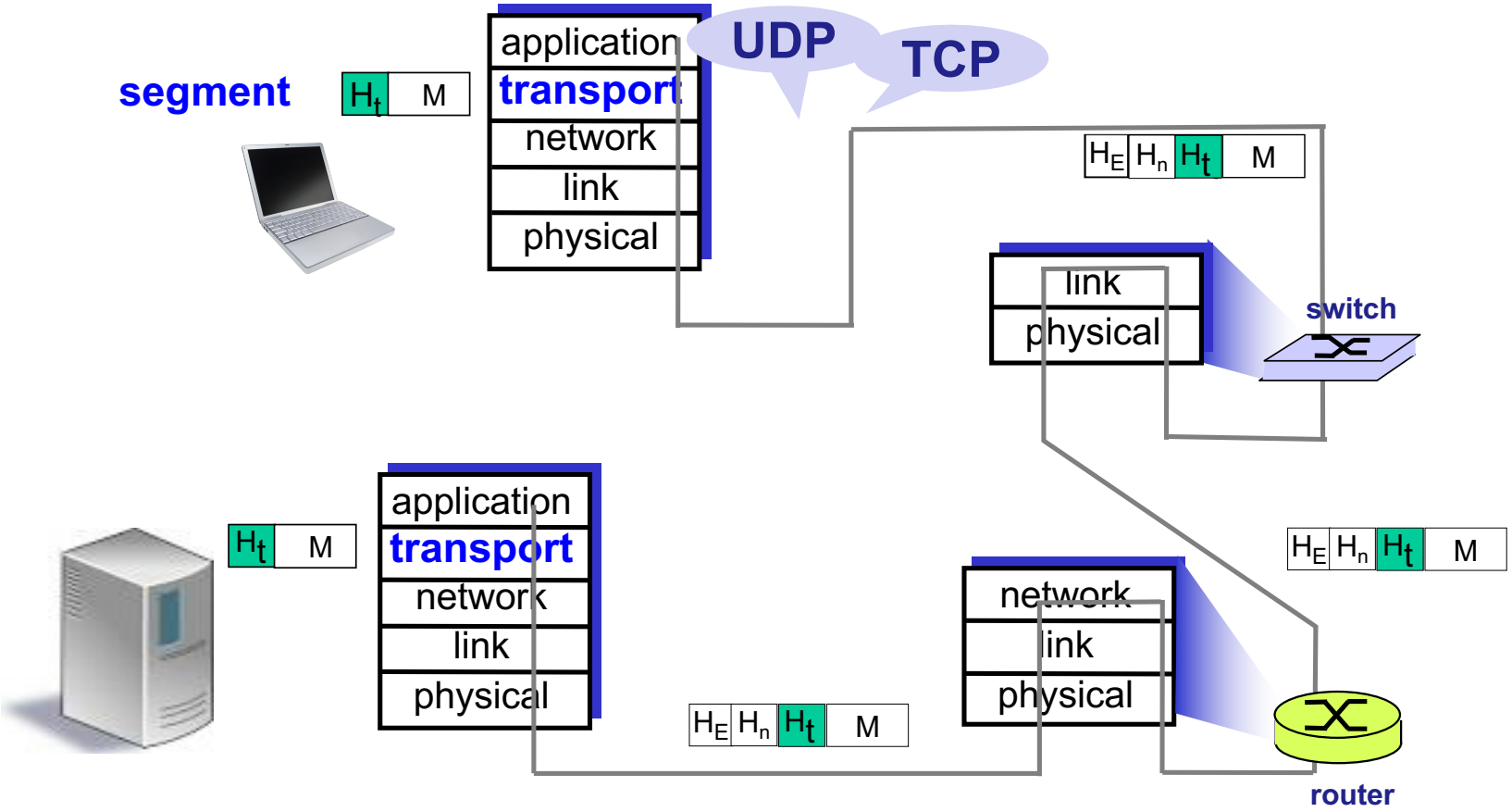
The TRANSPORT layer transports segments end-to-end

application
TRANSPORT
network
link
physical



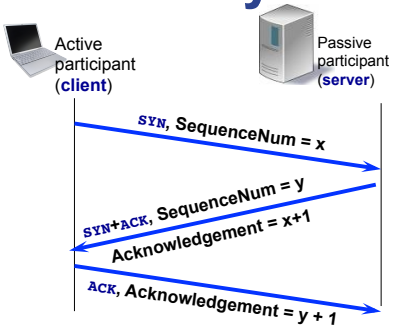
application	message
transport	segment
network	datagram
link	frame
physical	bit

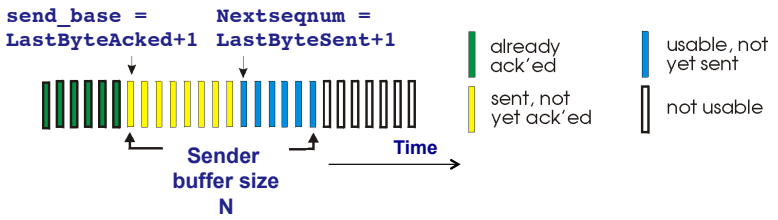
The end-to-end transport layer bridges the gap between the best-effort network service and the application requirements

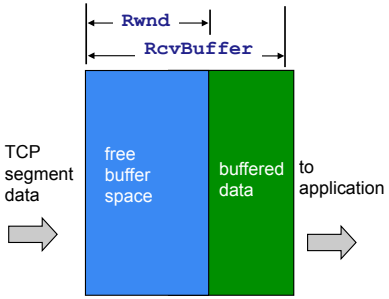


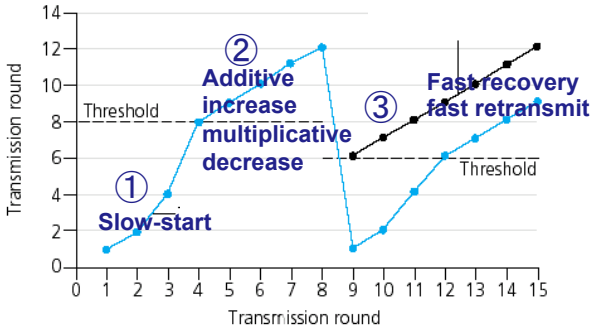
TCP – Transmission Control Protocol delivers a reliable byte stream

- **Point-to-point full duplex**
  - one sender, one receiver
- **Connection-oriented**
  - handshaking
    initiates sender and receiver state before data exchange
- **Error control**
  - bit error, segment error
- **Flow control**
  - sender will not overwhelm receiver
- **Congestion control**
  - sender adjust transmission dependent on network load



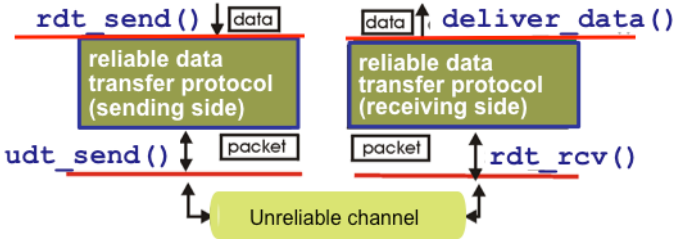






NTNU

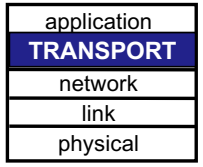
A reliable data transfer (rdt) service over an unreliable network channel must handle bit errors and packet loss



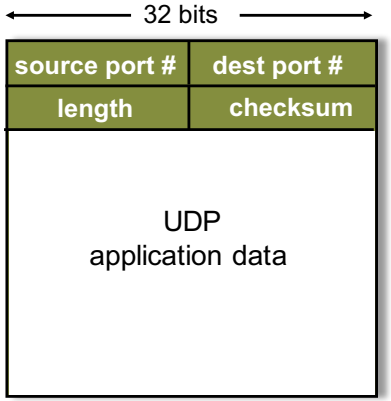
Protocol	Channel characteristic	Protocol functions added
Rdt 1.0	Error free	
Rdt 2.0	Bit error S-> R; only data corrupt	**Checksum**, receiver feedbak (**ACK**, **NAK**), **retransmission** on NAK
Rdt 2.1	Bit error S <-> R; ACK NACK may also be corrupt	**Sequence number** on data packets, **checksum** on ACK/NAK
Rdt 2.2	Bit error S <-> R	**no NACK,** **seq#** also **in ACKS,** **retransmission on duplicate ACK**
Rdt 3.0	**Bit error S <-> R, packet loss**	**Countdown timer**, retransmission on timeout

Window: for pipelined transmission

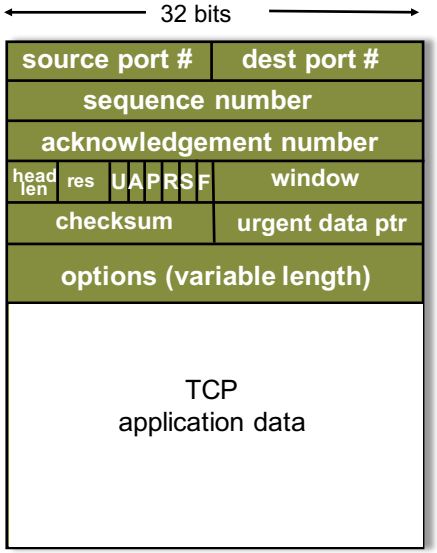
Transport protocol port numbers are used for demultiplexing to relevant application process



- **UDP – User Datagram Protocol**
  - unreliable, unordered delivery
  - no-frills extension of “best-effort” IP



- **TCP – Transmission control protocol**
  - reliable, in-order delivery
  - connection setup
  - flow control
  - congestion control
  - full duplex byte stream



➔**Port numbers** (source and destination) of transport protocol header &
IP addresses (source and destination) of network protocol header direct segment to appropriate socket

NTNU

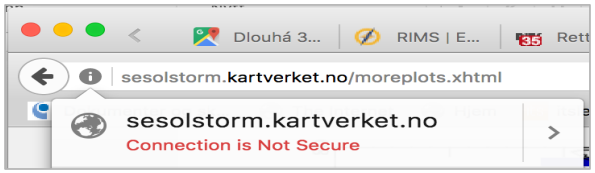
The transport protocol is chosen by the application choosing stream or datagram socket

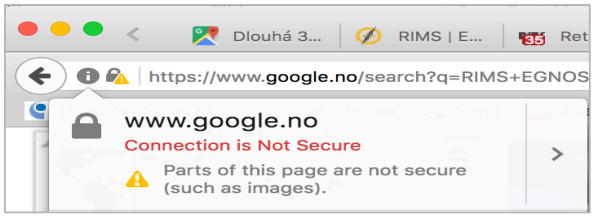
application
TRANSPORT
network
link
physical

Application	Application layer protocol (port)	Underlying transport protocol
e-mail	SMTP (25)	TCP
remote terminal access	Telnet (23)	TCP
web	HTTP (80)	TCP
file transfer	FTP (20,21)	TCP
streaming multimedia	HTTP e.g. Netflix, Youtube	TCP or UDP
Internet telephony	SIP, RTP, e.g. Skype	typically UDP, but TCP for firewall traversal

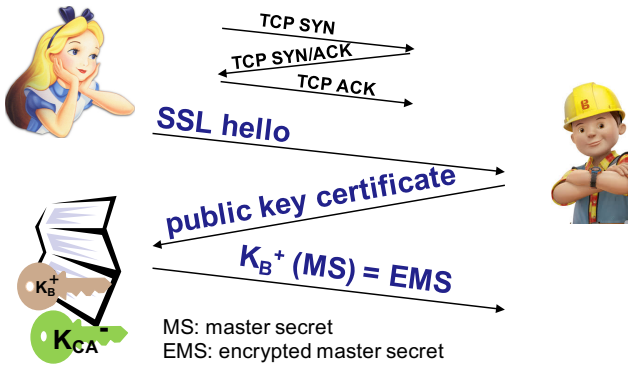
Securing the data end-to-end

SSL/TSL provides authentication, confidentiality, and integrity

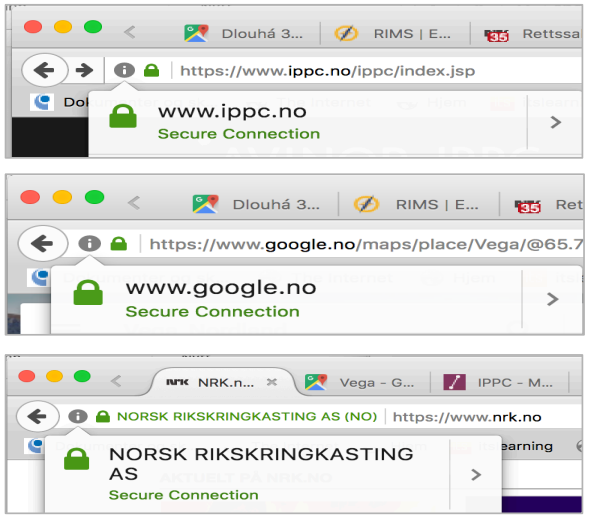


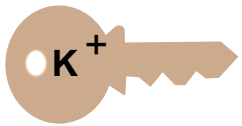


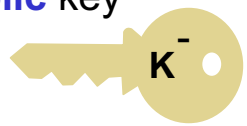
- **Handshake**: Alice and Bob use their certificates, private keys to **authenticate** each other and **exchange shared secret**
- **Key derivation**: Alice and Bob use **shared secret** to derive set of keys
- **Data transfer**: data to be transferred is broken up into series of **records**
- **Connection closure**: special messages to **securely** close connection



- Agree on cryptographic algorithms at the beginning of the SSL session,



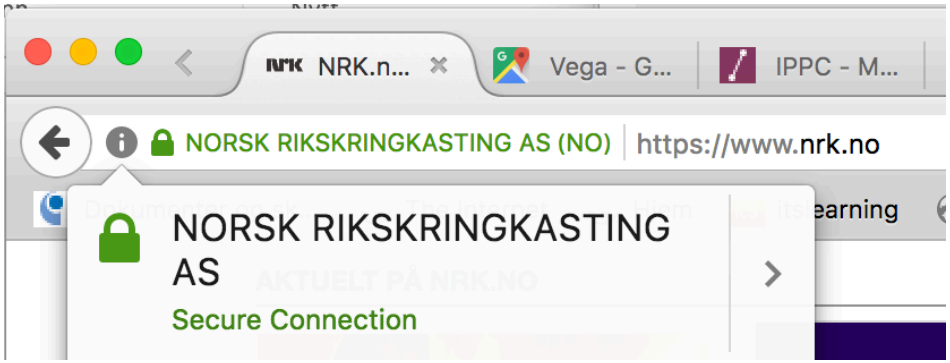


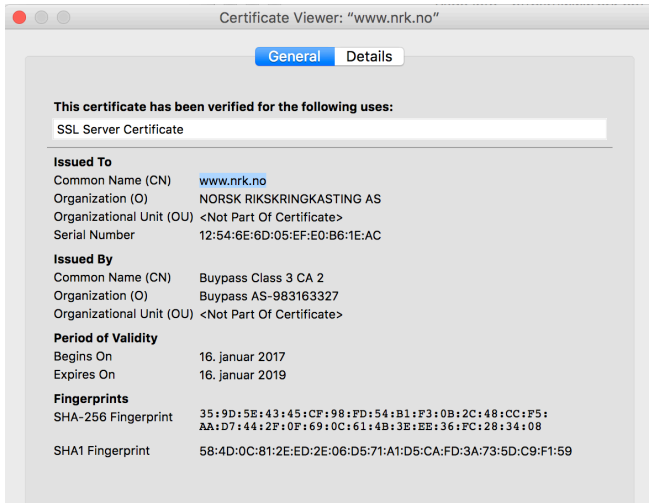


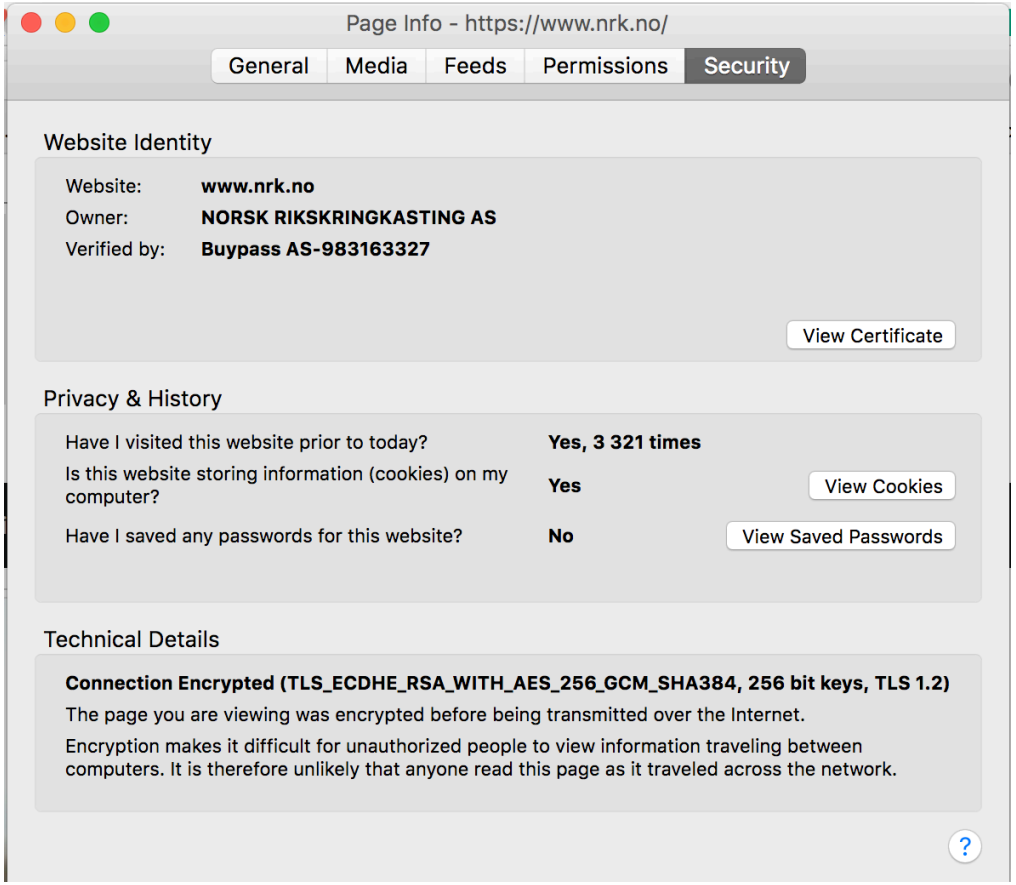
How to distribute the public key?

plaintext message, m → **encryption algorithm** → ciphertext $K^-(m)$ → **decryption algorithm** → plaintext $m = K^-(K^+(m))$

Certificate: a digital signature of the public key of an entity (e.g. NRK) by a certification authority (e.g. Buypass)







Selskapsinformasjon

Buypass AS er en ledende leverandør av brukervennlige og sikre løsninger for elektronisk identifikasjon, elektronisk signatur og betaling. Vi tilbyr en komplett portefølje av tjenester for identifisering og kryptering av informasjon gjennom hele den elektroniske verdikjeden. Buypass er også Norges eneste utsteder av internasjonalt godkjente SSL-sertifikater.

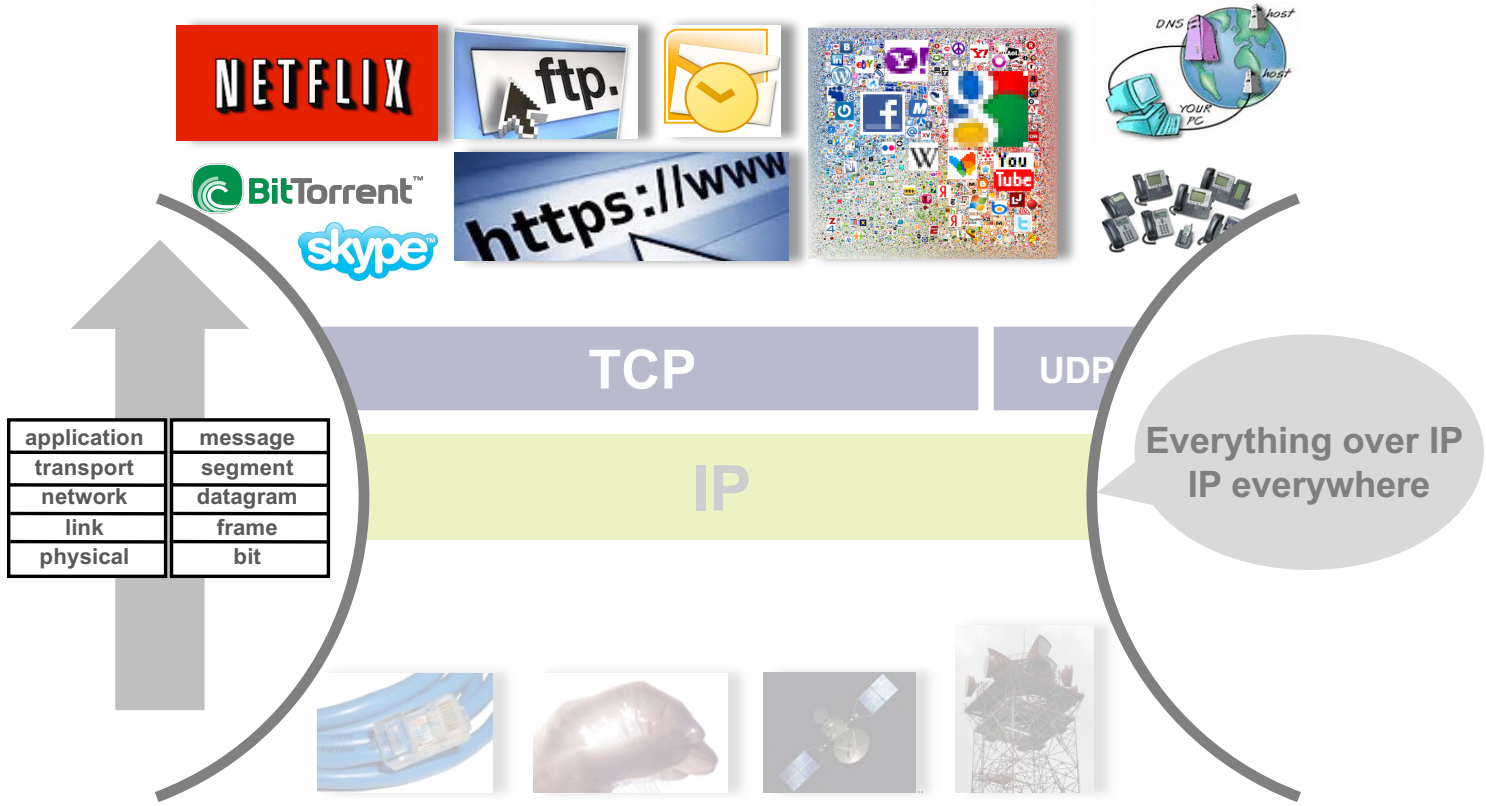
Buypass ble etablert i 2001, og har siden starten satset tungt på å bygge opp et unikt kompetansemiljø for utvikling av brukervennlige sikkerhetsløsninger som tilfredstiller markedet og myndighetenes strengeste sikkerhetskrav. Buypass leverer løsninger til bruk både i forbrukermarkedet, private bedrifter og offentlige virksomheter.

Pr. oktober 2016 er vi 78 fast ansatte, samt et varierende antall innleide/engasjerte fordelt på vårt hovedkontor i Oslo og avdelingskontor på Gjøvik.

Buypass er registrert hos Nasjonal kommunikasjonsmyndighet (Nkom) (tidligere Post og teletilsynet) som utsteder av kvalifisert ID i henhold til Lov om elektronisk signatur og er deklarert i henhold til Selvdeklarasjonsforskriften og Kravspesifikasjon for PKI i offentlig sektor. Selskapet har også konsesjon fra Finansdepartementet som e-pengeforetak i henhold til Finansieringsvirksomhetsloven.

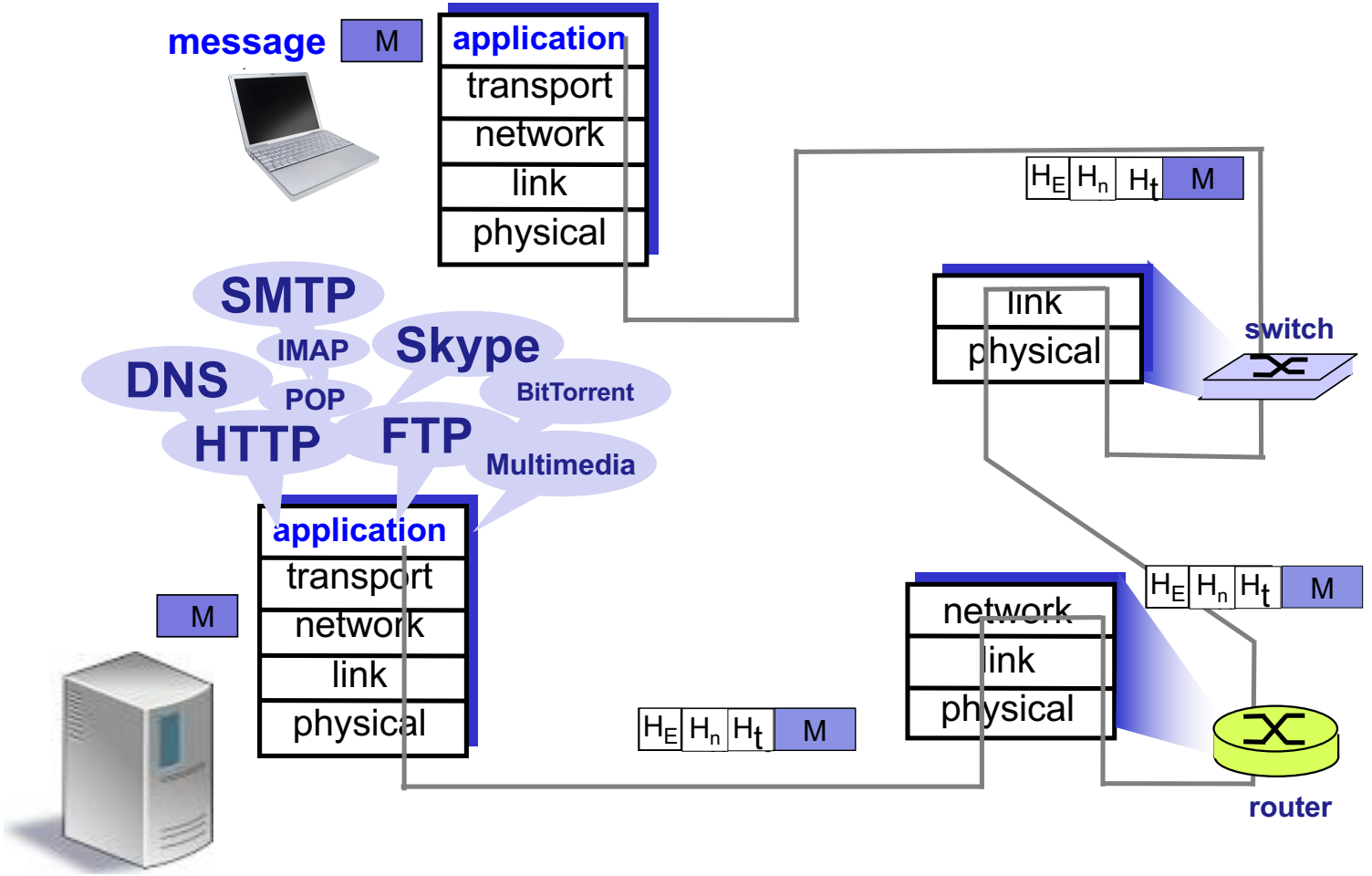
The APPLICATION layer handles application- and user-specific data

APPLICATION
transport
network
link
physical

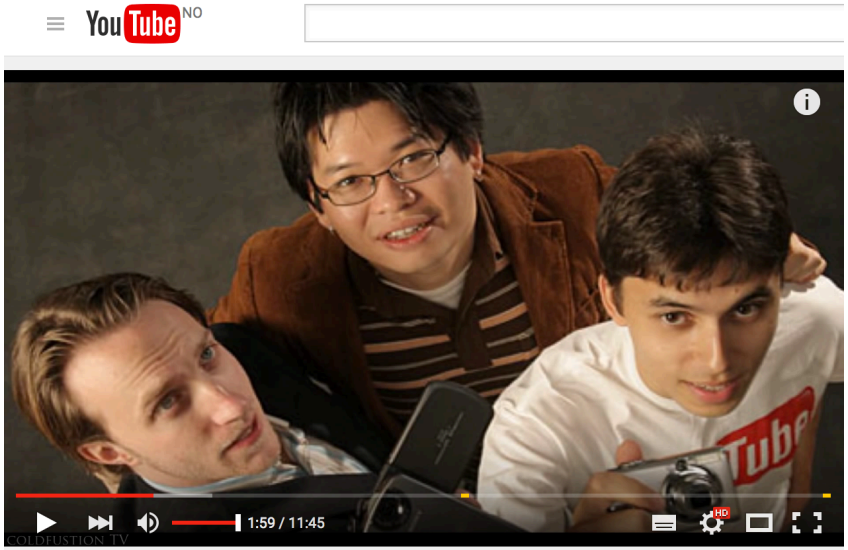


application	message
transport	segment
network	datagram
link	frame
physical	bit

The application layer runs distributed applications



“25 years ago streaming internet over the internet was pretty much science fiction”



https://www.youtube.com/watch?v=P4dT-IW9260

The Surprising History of YouTube!

ColdFusion

Abonner 606 964

276 156

Legg til Del Mer 7 957 87

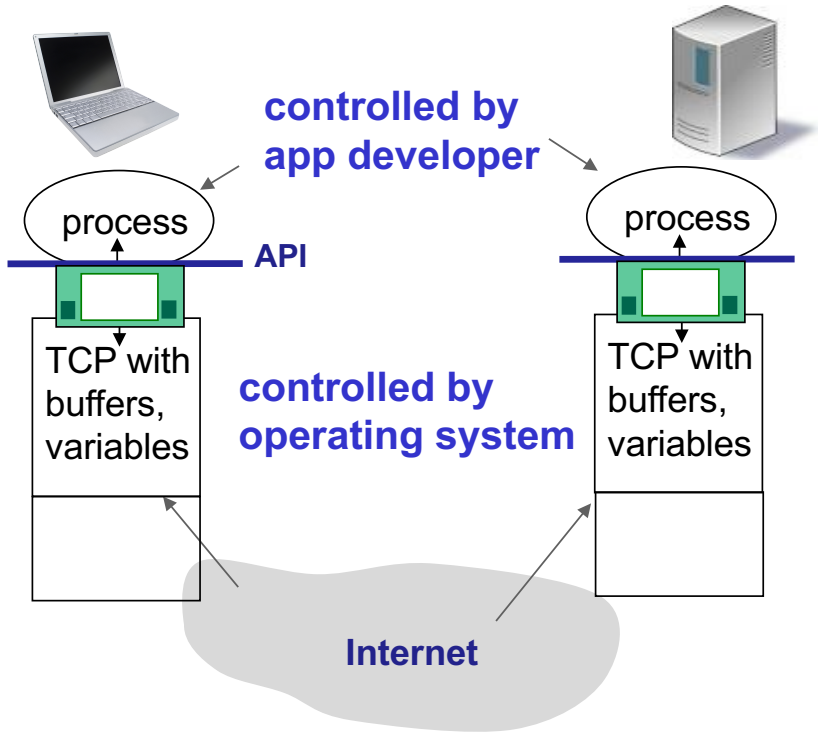
Publisert 4. feb. 2015

Except for the Google plus integration and the generally angry comment section, YouTube is a vibrant, thriving community that has taken over a lot of the internet's video sector. In this video we'll take a look at how large the website really is and how it started.

Application processes send and receive messages to/from their sockets

APPLICATION
transport
network
link
physical

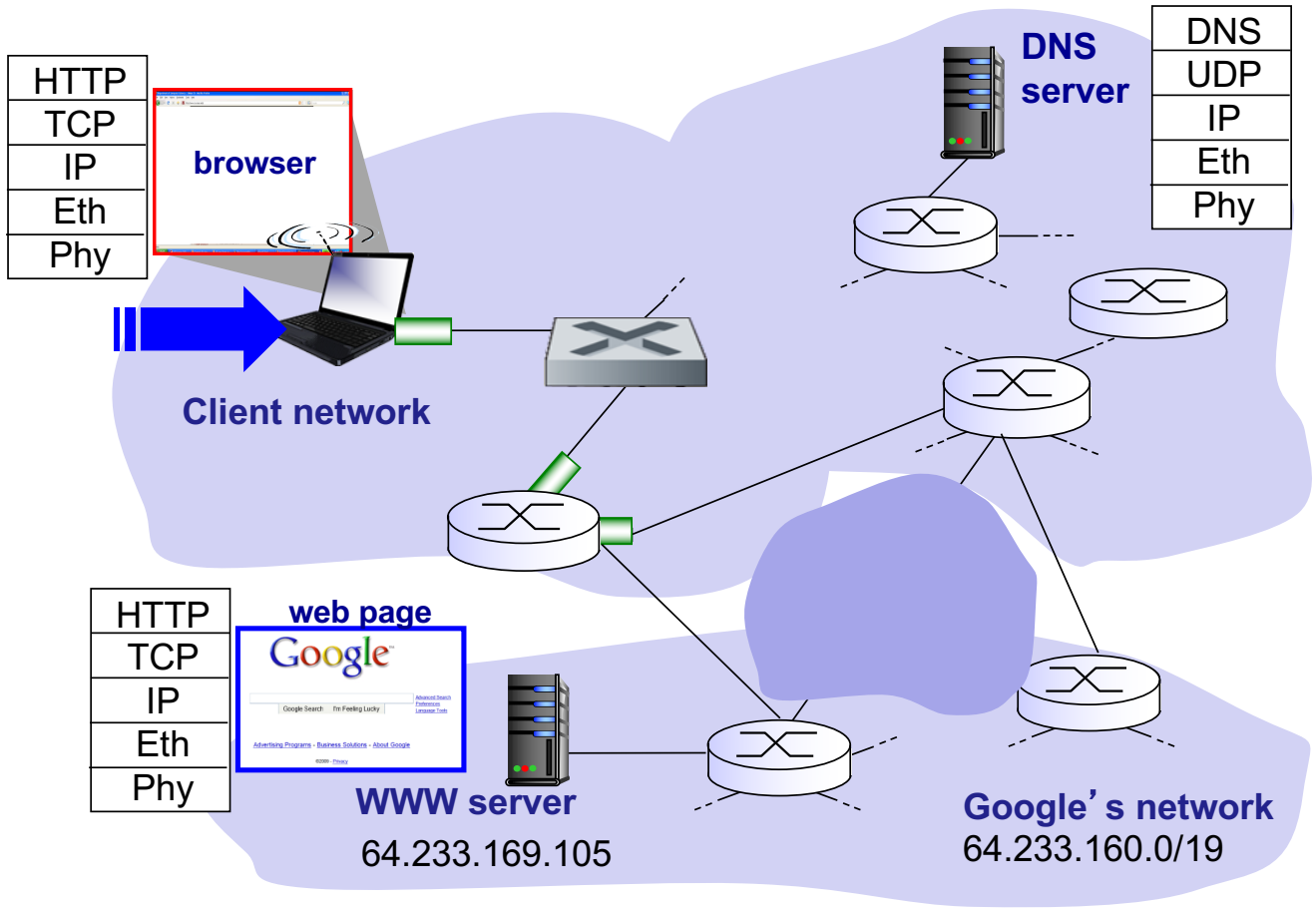
- Communication protocols accessed through **API**
  (application programming interface)
  - choice of transport protocol
  - ability to fix a few parameters
- Transport layer
  brings message to socket at receiving process



Processes are addressed through (source and destination) IP addresses and transport ports

“A day in the life” scenario – loading web page from www.google.com

APPLICATION
transport
network
link
physical



A day in a life of a simple web page request

	Frame len	IP len	UDP or TCP data	Src MAC	Dst MAC	Src IP	Dst IP	Trans-port proto-col	TP proto-col flags	Highest protocol and msg type	Comments
1	342	328	308	00:1f:f3:5a:12:33	ff:ff:ff:ff:ff:ff	0.0.0.0	255.255.255.255	**UDP**	**----**	**DHCP req**	Only IP broadcas
2	342	328	308	00:0c:cf:32:48:00	00:1f:f3:5a:12:33	129.241.66.1	129.241.67.145	**UDP**	**----**	**DHCP ACK**	Only from 66.1
3	42	---	---	00:1f:f3:5a:12:33	ff:ff:ff:ff:ff:ff	---	---	**---**	**----**	**ARP req**	Ethernet broadcast without IP
4	60	---	---	00:0c:cf:32:48:00	00:1f:f3:5a:12:33	---	---	**---**	**----**	**ARP rsp**	
5	74	60	40	00:1f:f3:5a:12:33	00:0c:cf:32:48:00	129.241.67.145	129.241.0.200	**UDP**	**----**	**DNS query**	Only communication to
6	142	128	108	00:0c:cf:32:48:00	00:1f:f3:5a:12:33	129.241.0.200	129.241.67.145	**UDP**	**----**	**DNS resp**	this server
7	78	64	0	00:1f:f3:5a:12:33	00:0c:cf:32:48:00	129.241.67.145	74.125.79.147	**TCP**	**SYN**	**--**	TCP connection set-up
8	74	60	0	00:0c:cf:32:48:00	00:1f:f3:5a:12:33	74.125.79.147	129.241.67.145	**TCP**	**SYN ACK**	**--**	
9	66	52	0	00:1f:f3:5a:12:33	00:0c:cf:32:48:00	129.241.67.145	74.125.79.147	**TCP**	**ACK**	**--**	
10	946	932	880	00:1f:f3:5a:12:33	00:0c:cf:32:48:00	129.241.67.145	74.125.79.147	**TCP**	**ACK**	**HTTP REQ**	HTTP GET over TCP
11	1484	1470	1418	00:0c:cf:32:48:00	00:1f:f3:5a:12:33	74.125.79.147	129.241.67.145	**TCP**	**ACK**	**HTTP RSP**	HTTP response over TCP
12	79	52	13	00:0c:cf:32:48:00	00:1f:f3:5a:12:33	74.125.79.147	129.241.67.145	**TCP**	**ACK**	**HTTP RSP**	"
13	66	52	0	00:1f:f3:5a:12:33	00:0c:cf:32:48:00	129.241.67.145	74.125.79.147	**TCP**	**ACK**	**----**	
30 sec traffic pause											
14	66	52	0	00:1f:f3:5a:12:33	00:0c:cf:32:48:00	129.241.67.145	74.125.79.147	**TCP**	**FIN**	----	TCP connectio
15	66	52	0	00:0c:cf:32:48:00	00:1f:f3:5a:12:33	74.125.79.147	129.241.67.145	**TCP**	**ACK**	----	
16	66	52	0	00:0c:cf:32:48:00	00:1f:f3:5a:12:33	74.125.79.147	129.241.67.145	**TCP**	**FIN**	----	
17	66	52	0	00:1f:f3:5a:12:33	00:0c:cf:32:48:00	129.241.67.145	74.125.79.147	**TCP**	**ACK**	----	

DHCP

ARP

DNS/UDP

TCP

HTTP/TCP

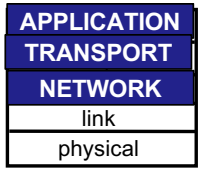
TCP

The Ethernet protocol header is 14 bytes, the IP 20 bytes, and the TCP including options is 32 bytes.

APPLICATION
TRANSPORT
NETWORK
link
physical

NTNU

A day in the life … loading page www.google.com



- Laptop connecting to network needs IP address, address of first-hop router, address of DNS server – **DHCP**
- Before sending HTTP request, need IP address of www.google.com: DNS
- To send frame containing DNS request to first hop router, need MAC address of router interface: **ARP**
  - Router replies on ARP broadcast giving MAC address of router interface
- Client now knows MAC address of first hop router, so can send frame containing **DNS** query
- Router forwards IP datagram to DNS server (routing tables created by routing protocols)
- DNS reply from server with IP address of www.google.com
- **TCP** connection set up (3 way handshake) needed to send **HTTP** request
- HTTP response returns default web page at www.google.com
- TCP connection closed

A hierarchy of Domain Name Servers translates between names and IP addresses

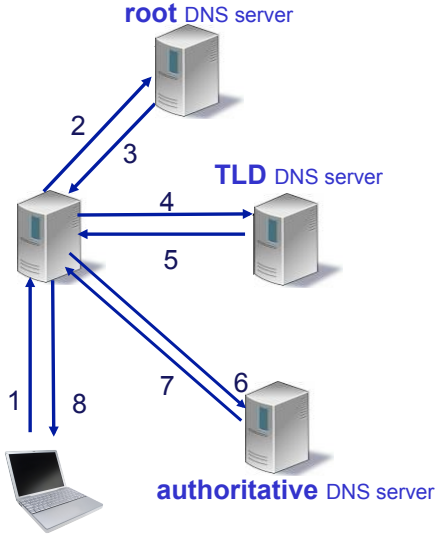
No.	Time	Source	Destination	Protocol	Length	Info
4862	11.519100000	129.241.67.134	129.241.0.200	DNS	74	Standard query 0x4d2e A www.google.com
4863	11.519571000	129.241.0.200	129.241.67.134	DNS	90	Standard query response 0x4d2e A 216.58.209.10

```
▷ Ethernet II, Src: Apple_44:c6:33 (a8:20:66:44:c6:33), Dst: Cisco_0b:d9:c2 (40:55:39:0b:d9:c2)
▷ Internet Protocol Version 4, Src: 129.241.67.134 (129.241.67.134), Dst: 129.241.0.200 (129.241.0.200)
▷ User Datagram Protocol, Src Port: 61220 (61220), Dst Port: domain (53)
▽ Domain Name System (query)
    [Response In: 4863]
    Transaction ID: 0x4d2e
  ▷ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▽ Queries
    ▷ www.google.com: type A, class IN
```

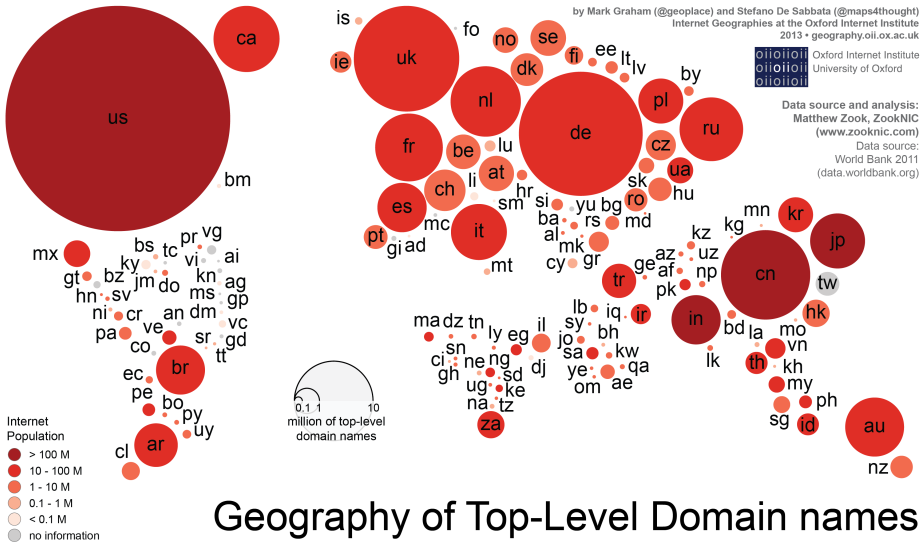
DNS request

```
▷ Ethernet II, Src: Cisco_0b:d9:c2 (40:55:39:0b:d9:c2), Dst: Apple_44:c6:33 (a8:20:66:44:c6:33)
▷ Internet Protocol Version 4, Src: 129.241.0.200 (129.241.0.200), Dst: 129.241.67.134 (129.241.67.134)
▷ User Datagram Protocol, Src Port: domain (53), Dst Port: 61220 (61220)
▽ Domain Name System (response)
    [Request In: 4862]
    [Time: 0.000471000 seconds]
    Transaction ID: 0x4d2e
  ▷ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  ▽ Queries
    ▷ www.google.com: type A, class IN
  ▽ Answers
    ▷ www.google.com: type A, class IN, addr 216.58.209.100
```

DNS response



APPLICATION
transport
network
link
physical

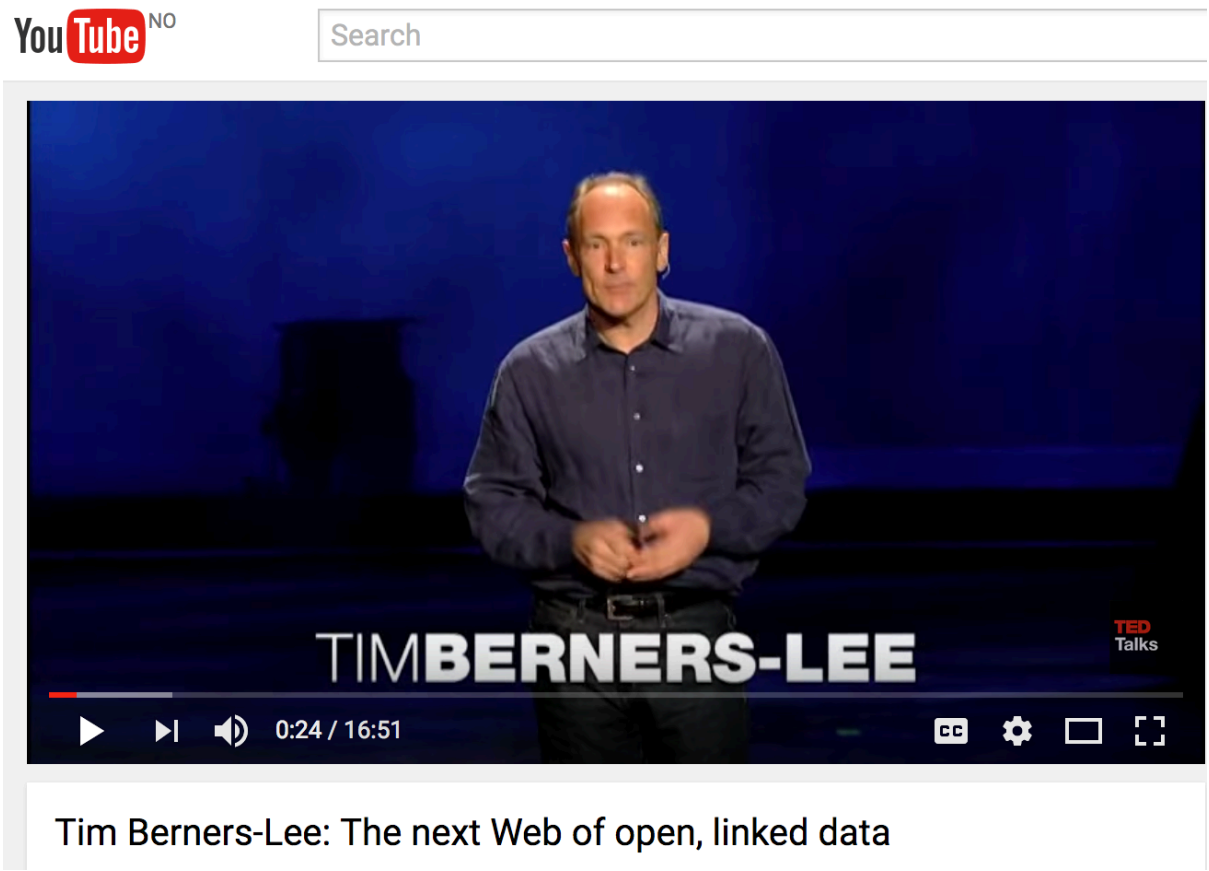


Geography of Top-Level Domain names

NTNU

The World Wide Web

APPLICATION
transport
network
link
physical



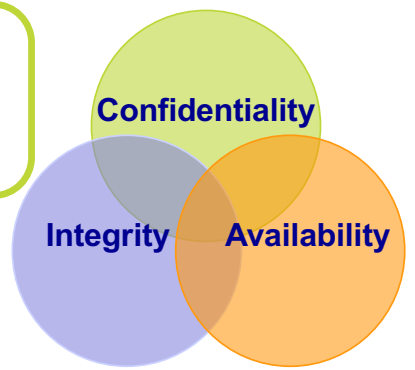
http://www.youtube.com/watch?v=OM6XIICm_qo

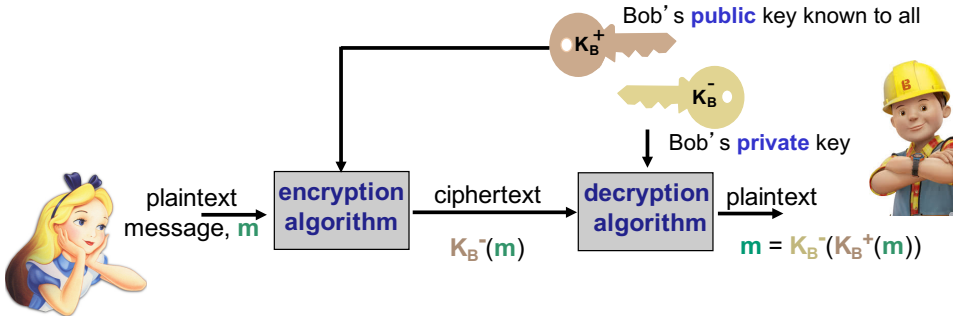
Summary

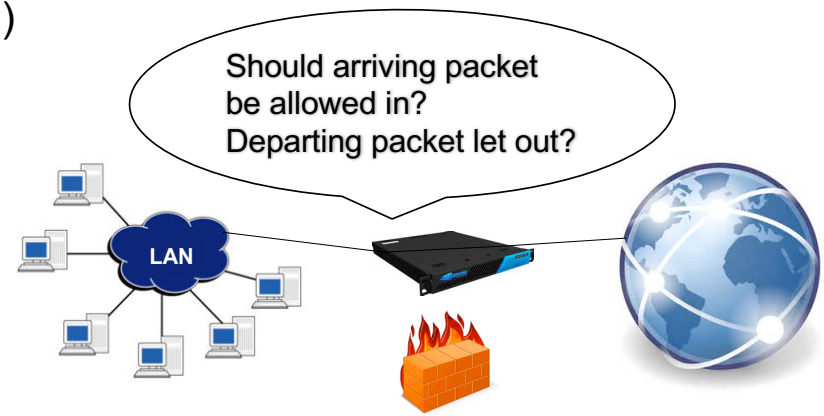
Security

- basic techniques……
  - cryptography (symmetric and public)
  - cryptographic hash
  - end-point authentication
- …. used in many different security scenarios
  - secure email
  - secure data transport (SSL/TLS)
  - IPSEC
  - IEEE 802.11 WLAN
- operational security
  - firewalls
  - intrusion detection system

Authentication: sender and receiver want to confirm identity of each other







Summary

The InterNET: A protocol view