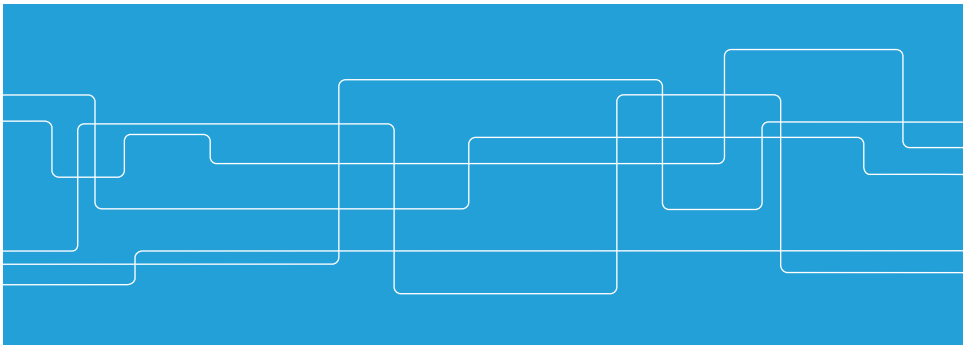
KTH ROYAL INSTITUTE
OF TECHNOLOGY

Lecture #10
Networks in more detail

Nicholas Honeth <honeth@kth.se>



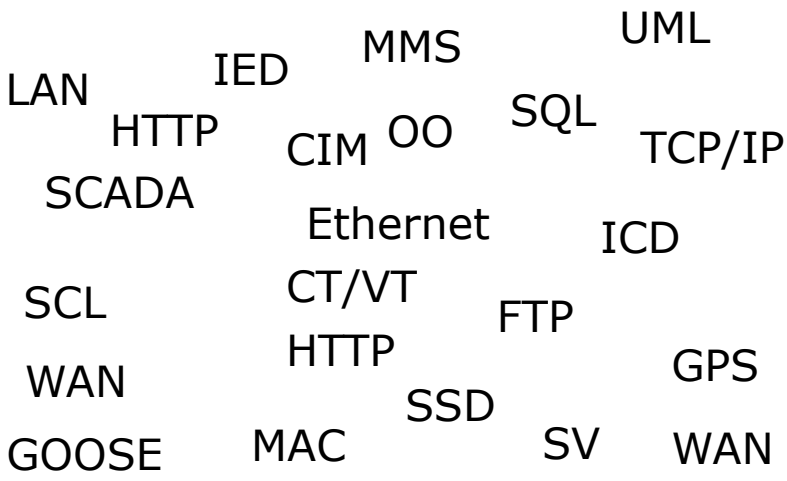
In this series…

- Lecture #9
  - Communication protocol basics
  - The OSI model
  - Relationship between OSI and SGAM
  - **Hands-on exercise**: Wireshark and HTTP
- Lecture #10
  - OSI model – physical layer
  - Topologies
  - Media Access Control
  - Routing
  - TCP/IP
  - Exercise: Ifconfig, traceroute, netstat, ping and Wireshark

In this series…

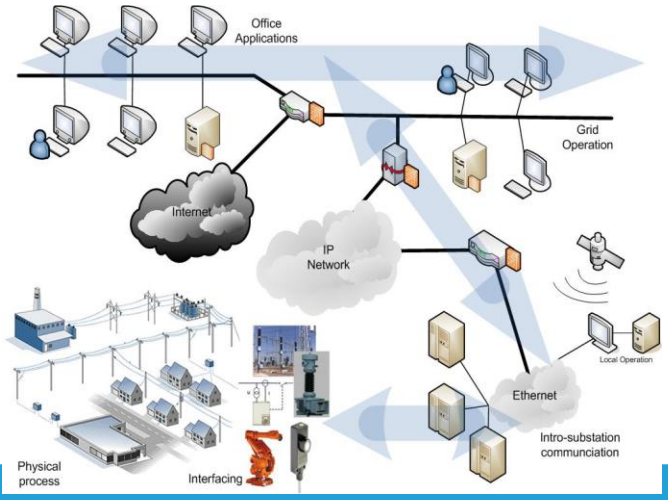
- Lecture #11
  - Power systems communication
  - Wireshark exercises
- Lecture #12
  - Delay & Jitter
  - Quality-of-Service
  - Loss and Throughput
  - Time synchronization
  - Project assignment Q&A

Some terms and acronyms…



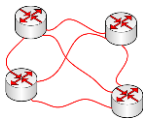
Recap

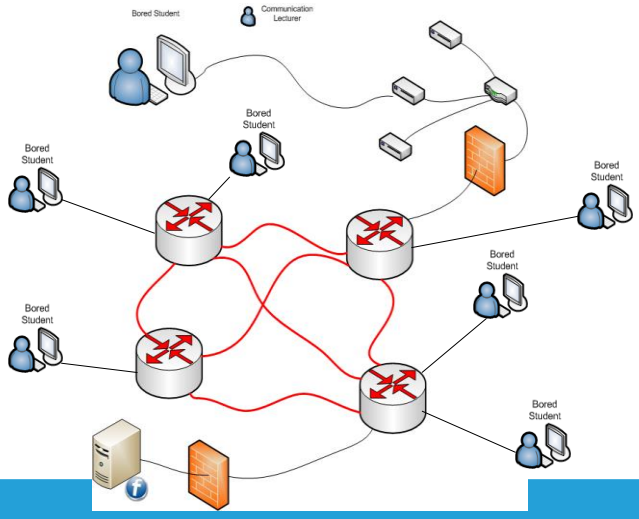
Computers and Networks in Power Systems



Recap

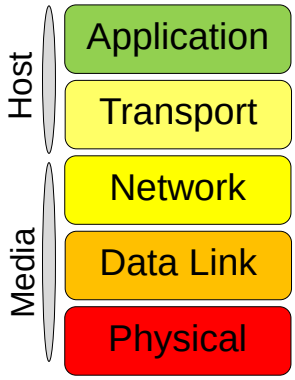
Protocol basics





Recap

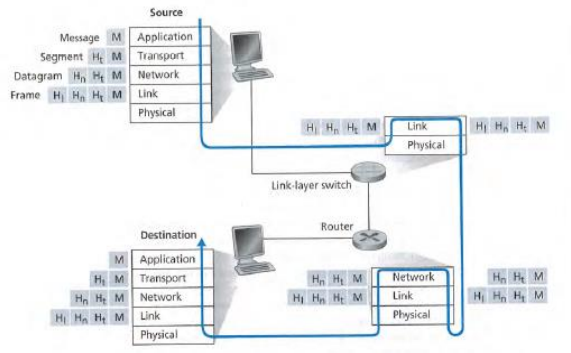
The OSI model



Recap

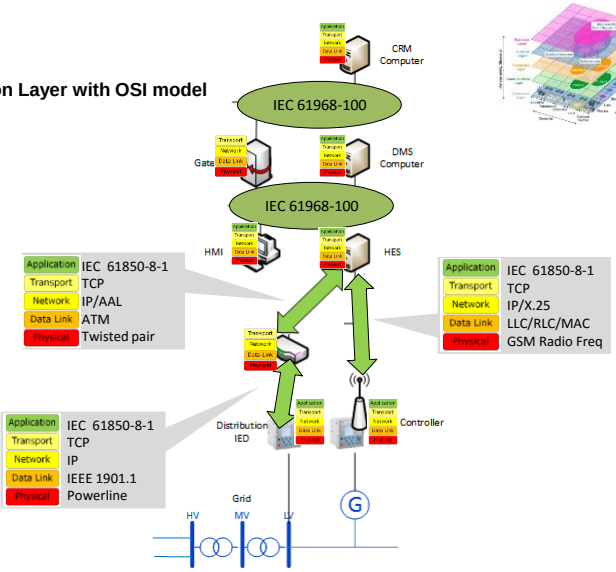
Transition between layers

Application
Transport
Network
Data Link
Physical



Recap

SGAM Communication Layer with OSI model



Physical media and devices

Mapped to the component level in SGAM

What does the physical media used to communicate actually look like?

Physical

Physical media and devices

Twisted-Pair Copper wire

Coaxial Cable

Fiber Optics

Terrestrial Radio

Satellite Radio

Communication devices

Physical

Physical media

Twisted-pair copper wire

Used in 99% of ofiice Ethernet

10*BASE-T Ethernet standard
- Uses RJ45 connector

Cat 5 - 6 Unshielded twisted pair
- Speeds up to 1Gbps

Digital Subscriber Line (DSL)
- Speeds around 10Mbps

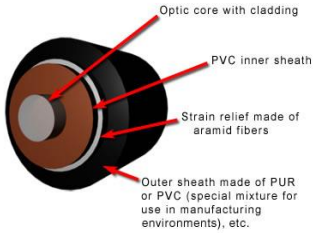
Physical media

Fiber optics

Often many cores in a single cable

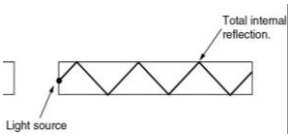
Very low attenuation up to 100km

Used for undersea cables



Very high speeds
- 100GBASE-ER4 (100Gbps 40km)

Good for applications where EMI can be a problem



Physical media

Terrestrial radio

Two main variants
- Local-area unidirectional
- Long-distance point-to-point

- Wireless LAN
  - IEEE 802.11*x*

- Point-to-point microwave

Physical media

Satellite radio

Usually used in
- Telephone networks
- Internet backbone links

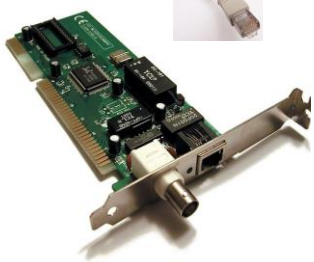
- Long propagation delay
  - 36,000 km trip one-way
  - 280 ms delay

- Used for high-speed internet where no infrastructure exists

Geostationary
Low-earth orbit

Physical media

Communication devices

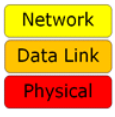


Network Interface Controller (NIC)

- Physical and data link layer
- Sometimes even network layer

- Ethernet cards have unique MAC address

- Interface to host computer
  - Polling
  - Interrupt-driven
  - Direct Memory Access



Physical media

Communication devices

Hub/Repeater

- Physical layer only
- Usually with UTP or fiber
- Extend range – point-to-point
- Create multi-point segment

Physical

Physical media

Communication devices

Switch

- Physical and data link layers (bridge)
- Managed switches exist
  - Security
  - Performance

- Learns the MAC address of each connected device
- "Switch" methods
  - Store-and-forward
  - Cut-through
  - Fragment-free – first 64 bytes
  - Adaptive – choose between the 3 above

Data Link

Physical

Physical media

Communication devices

Router

- Operates at the network layer
- Traffic directing
- Routing table – example “route PRINT”
  - Directs packet to next network
- SoHo devices – cheap, simple
- Core routers
  - High-speed connections
  - Performance management/tuning tools

Network
Data Link
Physical

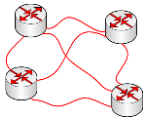
Physical media

Communication devices

Modem

- Modulator/Demodulator
- Modulates digital bitstream with analog carrier signal
- Most commonly used for phone line internet
- Radio
  - 3G, GPRS
  - Satellite
- Cable TV broaband service

Network topology

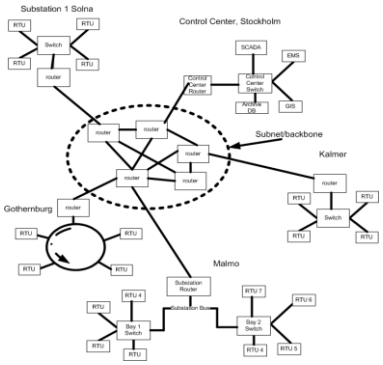


Common topologies
- Point-to-point
- Bus
- Star
- Ring
- Mesh

Mixed topologies

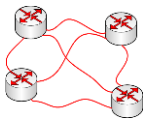
Physical and logical topologies

Duplex



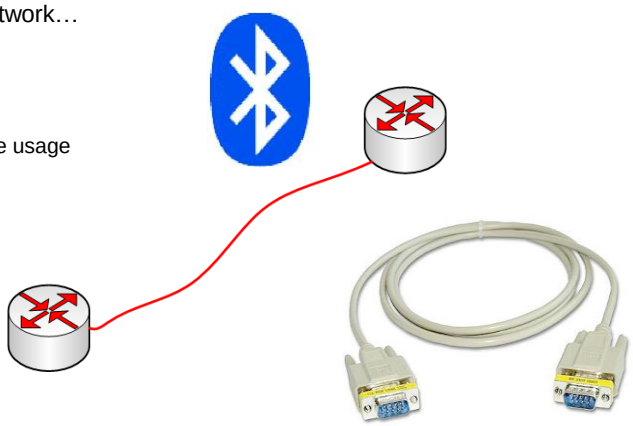
Topology

Point-to-point



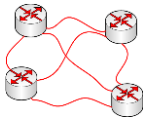
Simplest type of network…

Examples
- ”Null modem”
- Bluetooth – simple usage



Topology

Bus



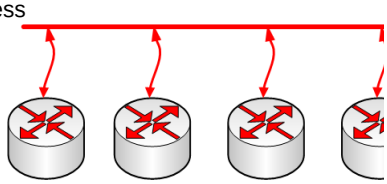
Advantages

- Bus not dependent on a single machine
- High flexibility in configuration, easy to add and remove
- Direct node to node communincation

Disadvantages

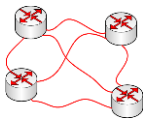
- Heavy traffic slows down network
- All nodes recieve packet, security
- Hard troubleshouting and fault isolation
- Limitation of the number of nodes

Roots of the Carrier Sense Multiple Access method come from this topology



Topology

Star

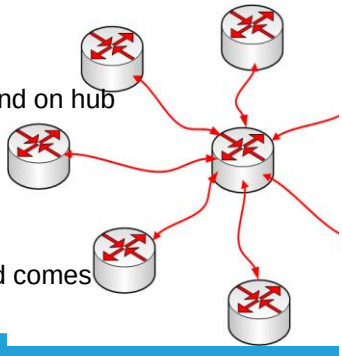


Advantages

- Simple
- Easy to add and remove nodes
- Easy managment and monitoring
- Node breakdown does not affect rest

Disadvantages

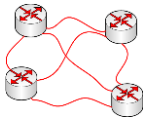
- Single point of failure, entire network depend on hub
- No node to node communication
- Cabling will increase as network increases



The Roots of the Conventional Polling Method comes from this topology

Topology

Ring

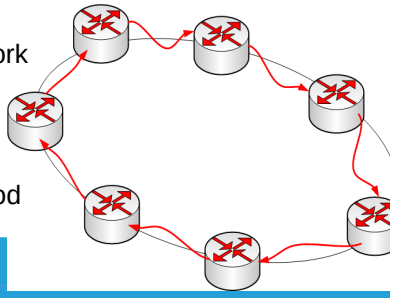


Advantages

- Generally All computer have equal access to the network
- Node to node communication
- Performance remain even with increase of load

Disadvantages

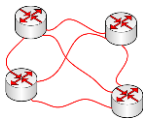
- Single node failure impacts network
- Sometimes hard to isolate faults
- Adding removing nodes disrupts network



Related to the Token Media Access Method

Topology

Mesh

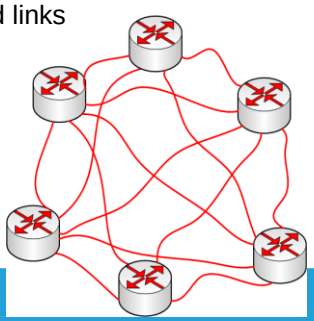


Advantages

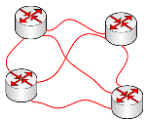
- High fault tolerance
- Redundant

Disadvantages

- Expensive
- Too many Network Interface Controllers and links

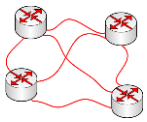


Topology
Mesh

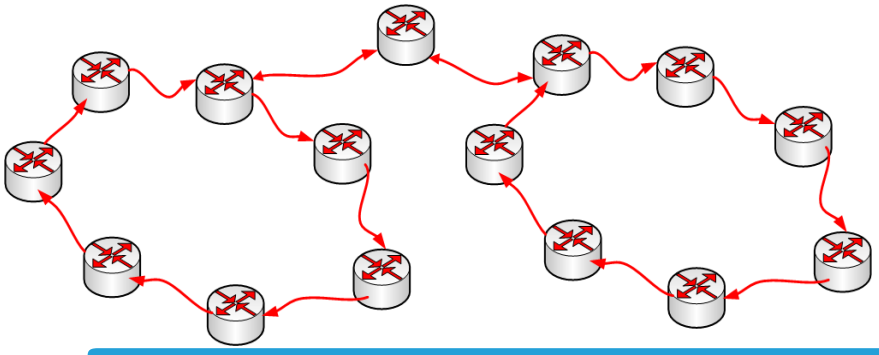


Topology

Mixed topologies – Star Ring

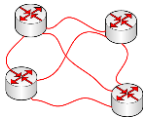


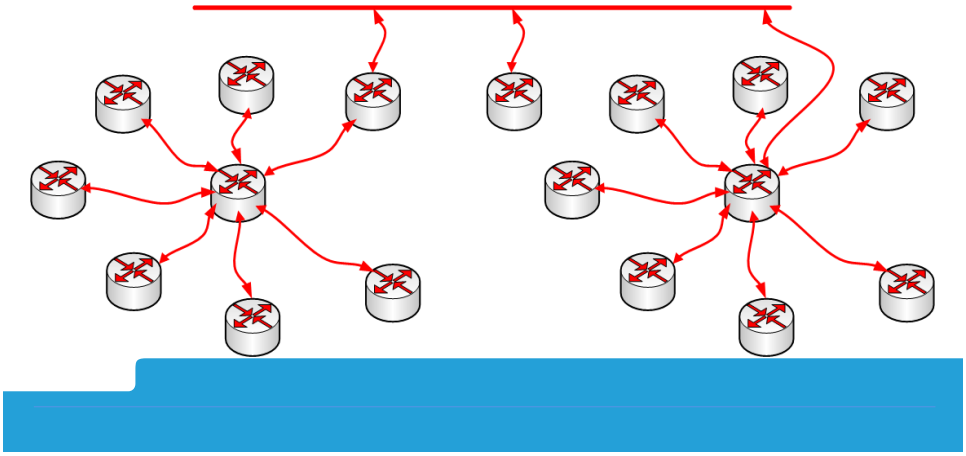
Star, Ring and Bus, are basic topologies, and can be combined e.g Star Ring or star star Bus topologies



Topology

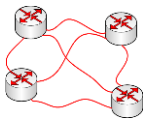
Mixed topologies – Star Bus



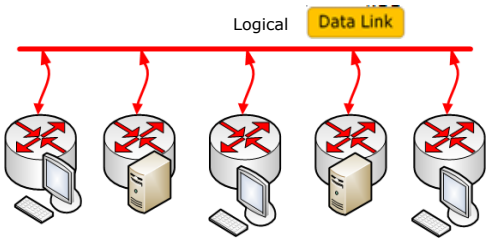


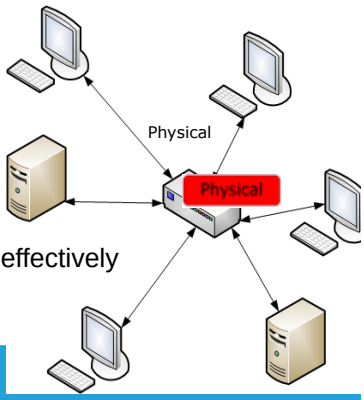
Topology

Physical and logical topologies



Example: Ethernet was originally based on bus topology but with the use of a hub it is phyiscally a star

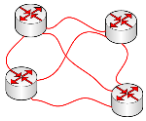




Hub retransmits the signal to all ports. Thus effectively making it bus network.

Topology

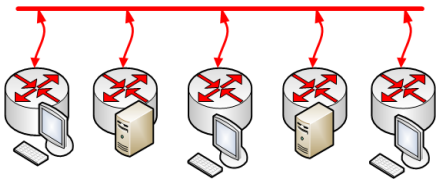
Physical and logical topologies

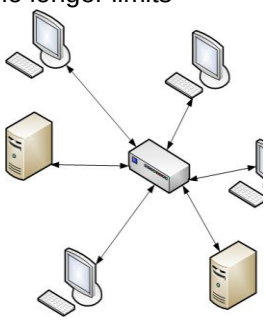


Topologies determine the characteristics of the network, for example:

- Layout of the network and wiring
- Number of Nodes and size of the network
- Message Reliability

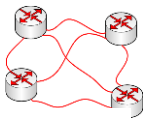
In modern networking the physical topology no longer limits the media access method used.

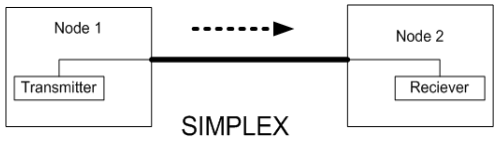


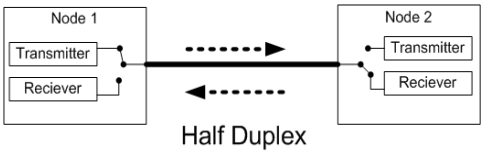


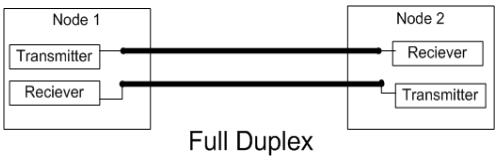
Topology

Duplex



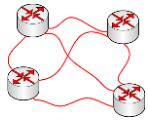


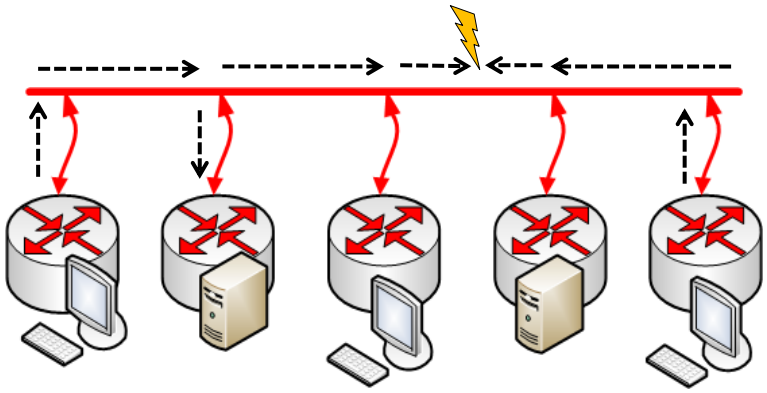




Media Access Control

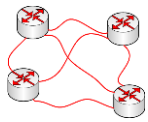
Carrier-sense multiple access (CSMA) / Collision Detection (CD)

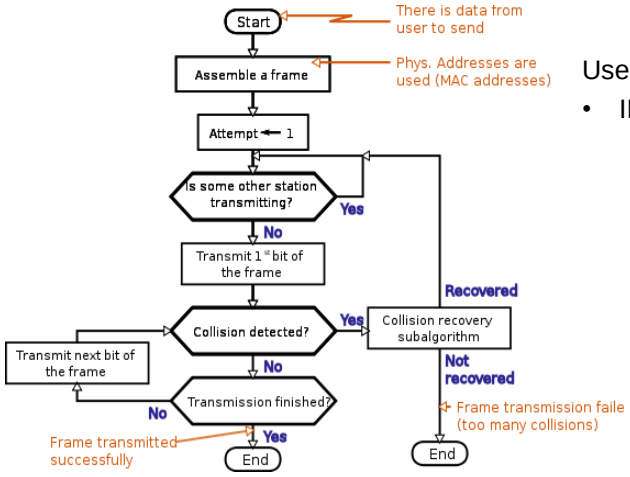




Media Access Control

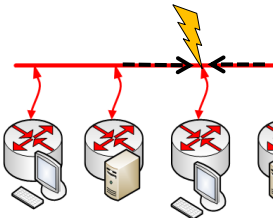
Carrier-sense multiple access (CSMA) / Collision Detection (CD)





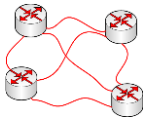
Used in

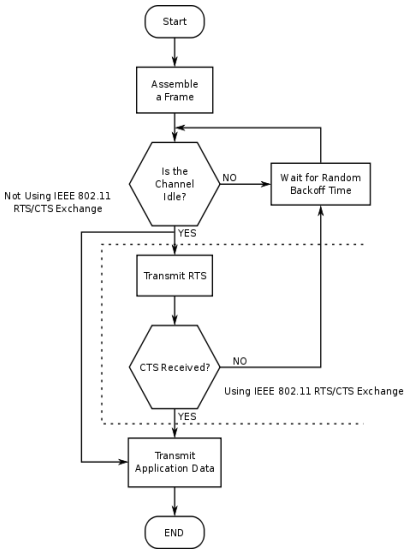
- IEEE 802.3 wired Ethernet



Media Access Control

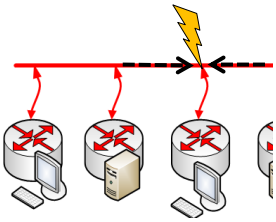
Carrier-sense mutliple access (CSMA) / Collision Avoidance (CA)





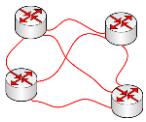
Used in

- IEEE 802.11
- IEEE 802.15



Media Access Control

Carrier-sense mutliple access (CSMA) / Collision Detection (CD)

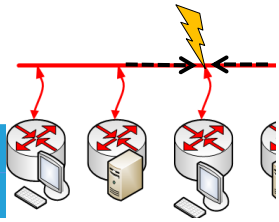


Advantages

- Peer to Peer Communication
- Efficient under a range of loading conditions
- Variations in data transfer requirements handled
- Urgent request can be handled instantly
- No centralized bus controller is required

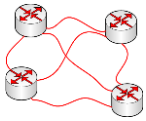
Disadvantages

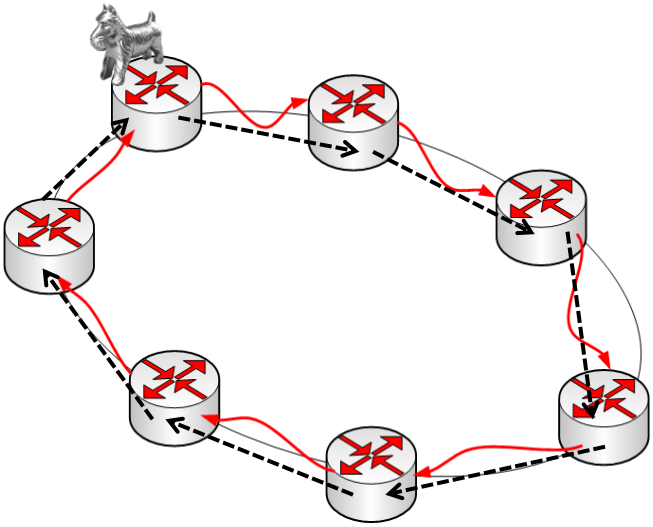
- Communication failure to a specific device will only response requested and none given
- Network configuration is complex
- Non deterministic response times
- Data collision is inherent
- Medium capture effect



Media Access Control

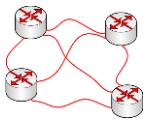
Token Passing – Token Ring





Media Access Control

Token Passing – Token Ring

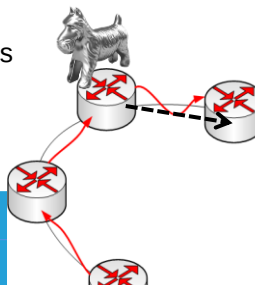


Advantages

- No Data Collisions
- Peer to peer communication
- Efficient under lightly loaded systems
- Variations in data transfer requirements can be handled by the system

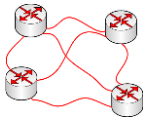
Disadvantages

- Hard to detect communication or node failure
- Network still dependent on central communications controller
- Semi deterministic response times obtained
- Unnecessary waiting times still inherent



Media Access Control

Other types

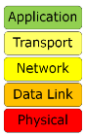


Mainly for wireless networks:

- Slotted ALOHA
- Dynamic TDMA
- CDMA
- OFDMA

Not so relevant for our overview, but good to recognise.

Routing and Addressing

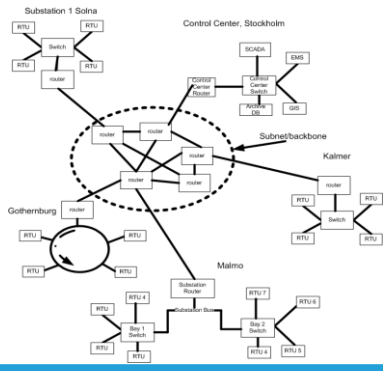


Network layer

- IP addresses
- Broadcast and multicast
- Routing tables

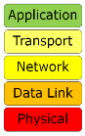
Data link layer

- MAC addresses
- ARP
- Switching

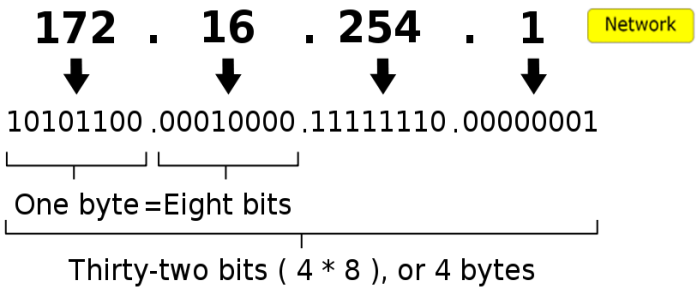


Routing and Addressing

Network layer – IP addresses



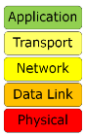
An IPv4 address (dotted-decimal notation)



32 bits are able to address only 4 294 967 296 unique nodes

Routing and Addressing

Network layer – IP addresses

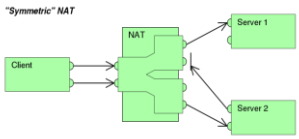


Address assignment:

- Manual static assignment
- Dynamic Host Configuration Protocol (DHCP)

Private networks can be separated from the internet using Name Address Translation (NAT)

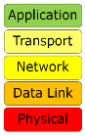
- Only one external IP address needed
- Translation using a table of **port numbers**



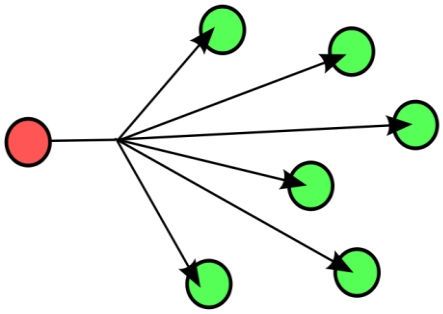
IPv6 addresses aim to mitigate the address exhaustion problem by using 128-bit addresses

Routing and Addressing

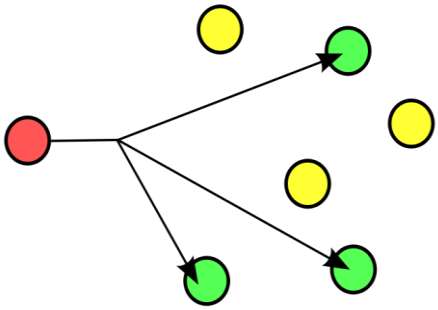
Network layer – Broadcast and multicast



Broadcast

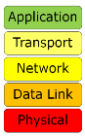


Multicast



Routing and Addressing

Network layer – Broadcast and multicast

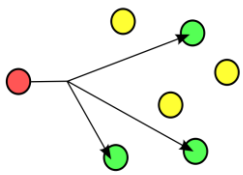


Broadcast

- Just send to everyone
- Broadcast address -> `(255.255.255.255)`

Multicast

- IP multicast group address
  - Receivers inform the network infrastructure that they are interested
    - Internet Group Management Protocol (IGMP)
- Multicast distribution tree
  - Receiver-driven tree creation



Really useful for ex. live TV broadcast over IP

- Synchrophasor data in the ”smart grid”?

Routing and Addressing

Network layer – Routing table

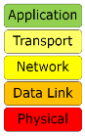


Table maintained on network-layer devices;

- Hosts
- Routers

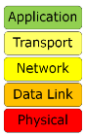
Host id	Cost	Next hop
.....	.....	.....
.....	.....	.....

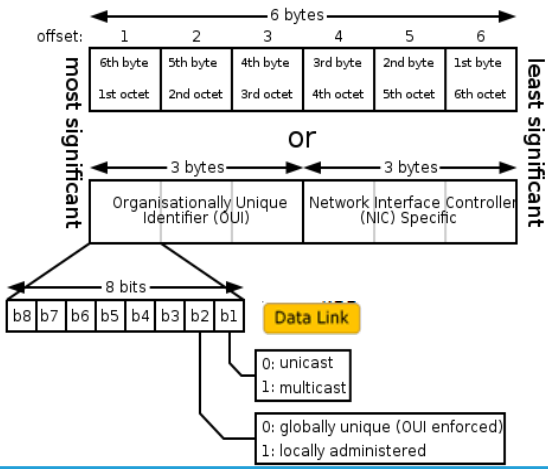
Three main fields:

- Host id – destination network ID (IP address/range)
- Cost – or metric of the path
- Next-hop – the specific address of the device to forward to

Routing and Addressing

Data link layer – MAC addresses





Routing and Addressing

Data link layer – MAC addresses

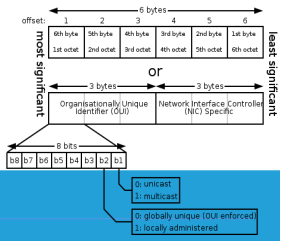
Application
Transport
Network
Data Link
Physical

Burned into H/W of NIC

Can be “spoofed”

Used in:

- Ethernet
- 802.11 wireless networks
- Bluetooth
- IEEE 802.5 token ring
- most other IEEE 802 networks
- Fiber Distributed Data Interface (FDDI)
- ATM
- The ITU-T G.hn standard – home power line



Routing and Addressing

Data link layer – Address Resolution Protocol

Application
Transport
Network
Data Link
Physical

ARP links IP address to MAC address

Replaced by Neighbour Discovery Protocol (NDP) in IPv6

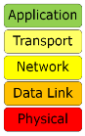
Ubiquitous among IPv4 devices

Vulnerable to local attack

- ARP poisoning

Internet Protocol (IPv4) over Ethernet ARP packet		
bit offset	0 – 7	8 – 15
0	Hardware type (HTYPE)	
16	Protocol type (PTYPE)	
32	Hardware address length (HLEN)	Protocol address length (PLEN)
48	Operation (OPER)	
64	Sender hardware address (SHA) (first 16 bits)	
80	(next 16 bits)	
96	(last 16 bits)	
112	Sender protocol address (SPA) (first 16 bits)	
128	(last 16 bits)	
144	Target hardware address (THA) (first 16 bits)	
160	(next 16 bits)	
176	(last 16 bits)	
192	Target protocol address (TPA) (first 16 bits)	
208	(last 16 bits)	

The TCP/IP stack



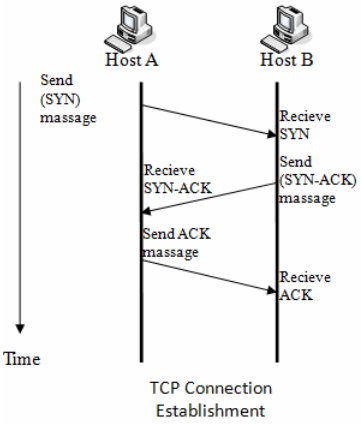
Also called the Internet Protocol Suite

Forms the core building-block of the Internet

Is just TCP at the **Transport** layer

..and IP at the **Network** layer

Provides reliable end-to-end virtual connection



Some useful tools

ifconfig/ipconfig

Show information about your local NICs

Windows> ipconfig
OSX/Linux> ifconfig

```
Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : ics.kth.se
   Link-local IPv6 Address . . . . . : fe80::79f5:2a2e:13d8:d930%22
   IPv4 Address. . . . . . . . . . . : 130.237.44. xxx
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 130.237.44.1
```

Some useful tools
Ping

Measures end-to-end delay

ping <address>

```
Pinging www.kth.se [130.237.28.40] with 32 bytes of data:
Reply from 130.237.28.40: bytes=32 time<1ms TTL=254
Reply from 130.237.28.40: bytes=32 time<1ms TTL=254
Reply from 130.237.28.40: bytes=32 time<1ms TTL=254
Reply from 130.237.28.40: bytes=32 time<1ms TTL=254

Ping statistics for 130.237.28.40:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Some useful tools
Routing Table

Shows the interface (link) to use for the next hop

Windows> route PRINT
OSX/Linux> netstat –nr

```
IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0    130.237.44.1   130.237.44. XXX   10
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    306
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    306
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    306
      130.237.44.0    255.255.255.0         On-link    130.237.44.160    266
    130.237.44.160  255.255.255.255         On-link    130.237.44. XXX   266
    130.237.44.255  255.255.255.255         On-link    130.237.44.160    266
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    306
        224.0.0.0        240.0.0.0         On-link    130.237.44. XXX   266
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    306
  255.255.255.255  255.255.255.255         On-link    130.237.44. XXX   266
===========================================================================
Persistent Routes:
  None
```

Some useful tools
Traceroute

Shows the router at each hop in the network

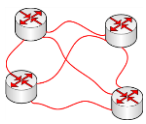
Windows> tracert <address>
OSX/Linux> traceroute <address>

```
Tracing route to www.google.se [216.58.209.131]
over a maximum of 30 hops:

  1     1 ms    <1 ms    <1 ms  130.237.44.2
  2    <1 ms    <1 ms    <1 ms  vss3-vss2-p2p.gw.kth.se [130.237.211.123]
  3    <1 ms    <1 ms    <1 ms  cn6-vss3-p2p.gw.kth.se [130.237.211.118]
  4    <1 ms    <1 ms    <1 ms  br1g-cn6-p2p.gw.kth.se [130.237.0.1]
  5    <1 ms    <1 ms    <1 ms  kth-br2.sunet.se [193.11.0.197]
  6    <1 ms    <1 ms    <1 ms  m1tug-ae4.sunet.se [130.242.85.209]
  7    <1 ms    <1 ms    <1 ms  se-tug.nordu.net [109.105.102.17]
  8    <1 ms    <1 ms    <1 ms  google-gw.nordu.net [109.105.98.6]
  9    13 ms     1 ms     1 ms  216.239.43.122
 10     1 ms     1 ms     1 ms  216.239.49.217
 11     1 ms     1 ms     1 ms  arn09s05-in-f131.1e100.net [216.58.209.131]

Trace complete.
```

Communication Networks II
Conclusion



We've looked at some **phyical media** and **devices**
Important to understand:
- Ethernet switch
- Internet Protocol router

Topologies for interconnection of network devices.

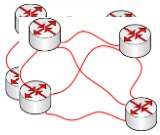
Media Access Control techniques for shared media

Addressing in in the data link and network layers

How Internet Protocol **routing** works (very briefly)

What to expect next…

Protocols used in SCADA and SAS



Which protocols are used?

…and how do they work?