



# Communication Networks

Nicholas Honeth (nicholash@ics.kth.se)



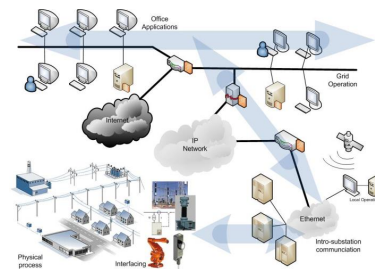
## Contents of the series

- **Lecture 10**
    - Recap of the networks we've seen so far
    - OSI model
    - Circuit and packet switching
    - Physical media
  - **Lecture 11**
    - Topologies
    - Media access techniques
    - Addressing and routing
    - Protocols in power systems applications
  - **Workshop 2**
    - Short recap of lectures 10 and 11
    - Delay, loss and throughput
    - Wireshark demo
-



## Contents of lecture 11

- Recap of the last lecture
- Topologies
- Media access techniques
- Protocols in power systems applications



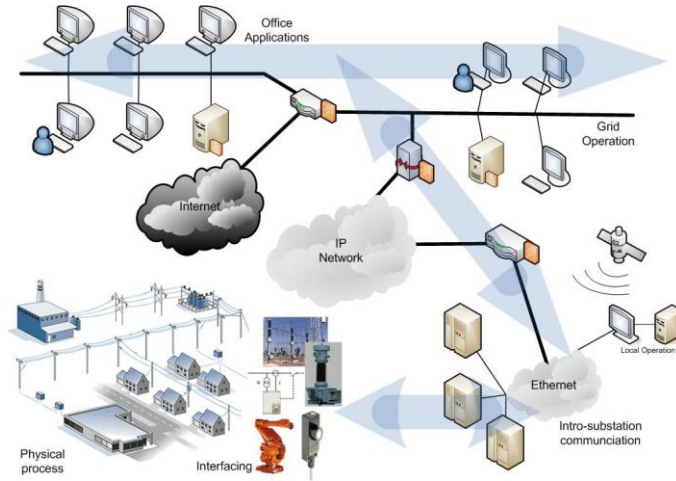
## Some terms and acronyms...

LAN IED MMS UML  
 HTTP CIM OO SQL TCP/IP  
 SCADA Ethernet ICD  
 SCL CT/VT FTP  
 WAN HTTP GPS  
 GOOSE MAC SSD SV WAN



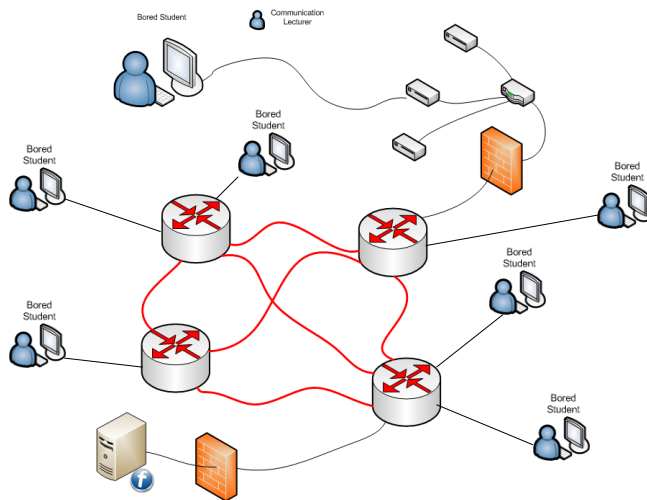
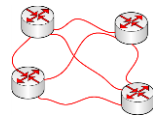
# Recap

Computers and Networks in Power Systems



# Recap

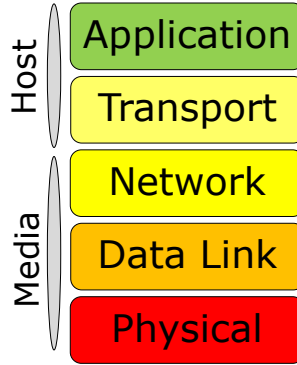
Protocol basics





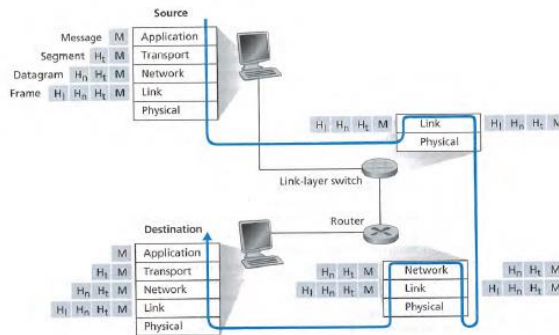
# Recap

The OSI model



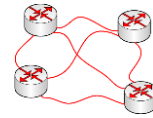
# Recap

Transition between layers

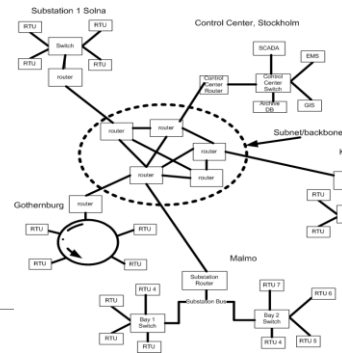




# Network topology

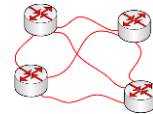


- Common topologies
  - Point-to-point
  - Bus
  - Star
  - Ring
  - Mesh
- Mixed topologies
- Physical and logical topologies
- Duplex

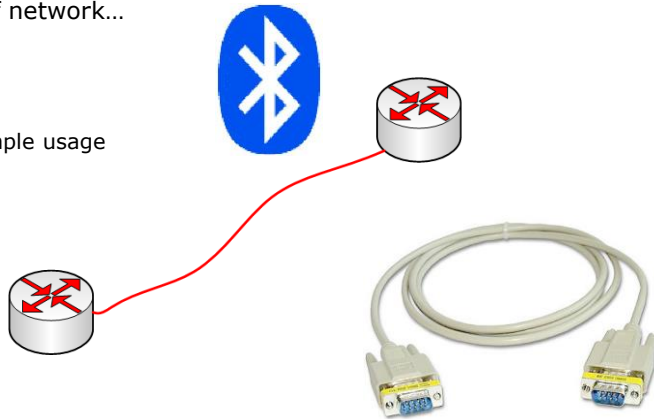


# Topology

Point-to-point



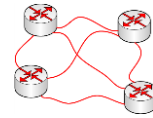
- Simplest type of network...
- Examples
  - "Null modem"
  - Bluetooth – simple usage





## Topology

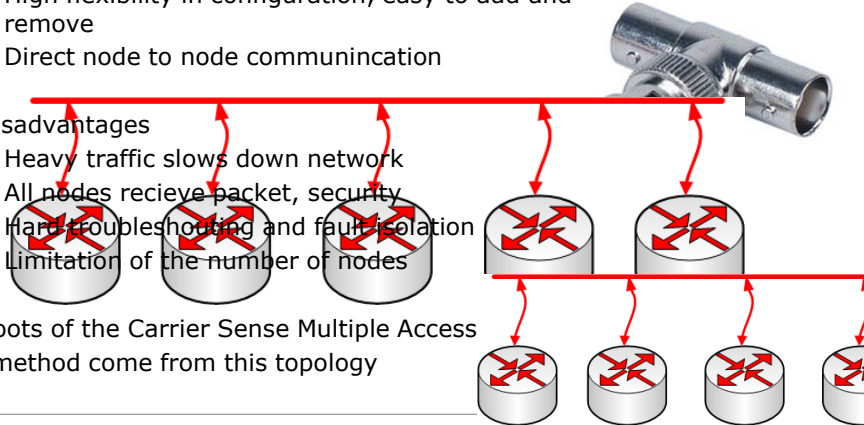
### Bus



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

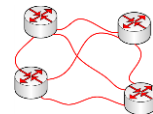
- Disadvantages
  - Heavy traffic slows down network
  - All nodes receive packet, security
  - Hard troubleshooting and fault isolation
  - Limitation of the number of nodes

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



## Topology

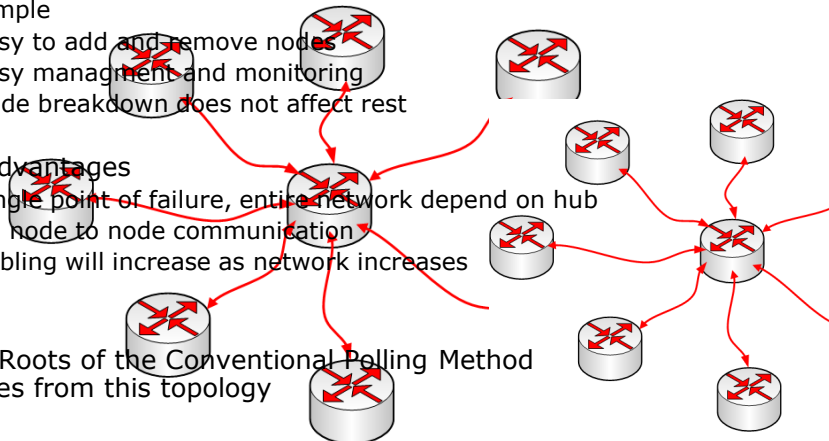
### Star



- Advantages
  - Simple
  - Easy to add and remove nodes
  - Easy management 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

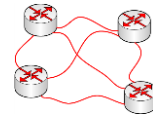
- The Roots of the Conventional Polling Method comes from this topology



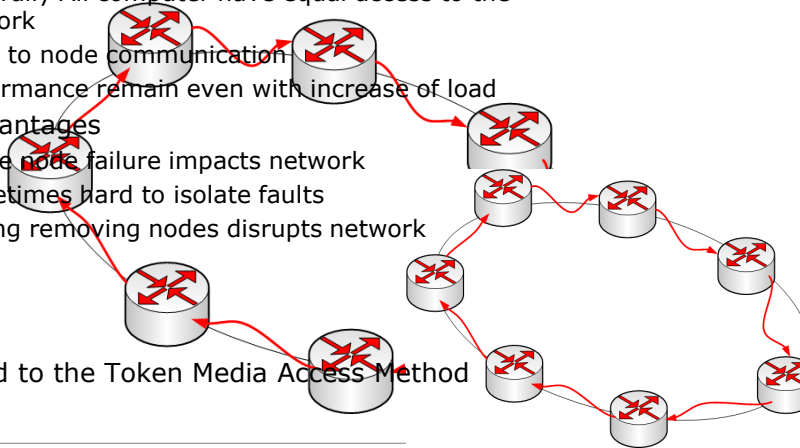


## Topology

### Ring

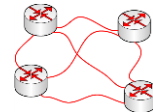


- Advantages
  - Generally All computer have equal access to the network
  - Node to node communication
  - Performance remain even with increase of load
- Disadvantages
  - Single node failure impacts network
  - Sometimes hard to isolate faults
  - Adding removing nodes disrupts network
- Related to the Token Media Access Method

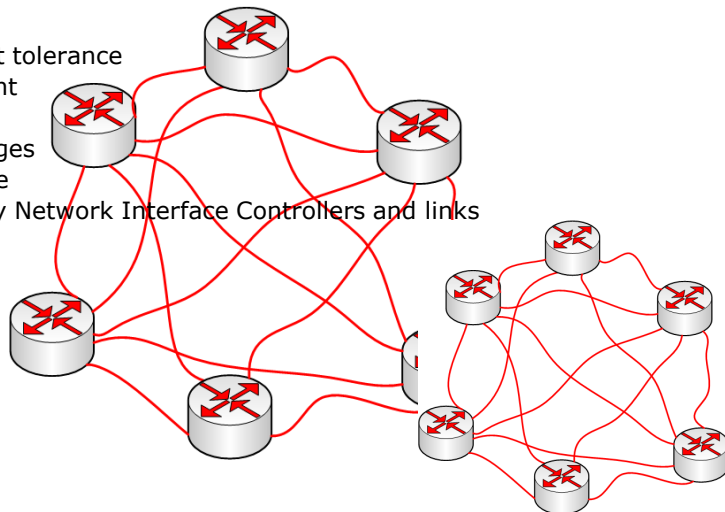


## Topology

### Mesh



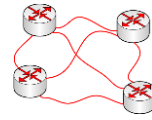
- Advantages
  - High fault tolerance
  - Redundant
- Disadvantages
  - Expensive
  - Too many Network Interface Controllers and links





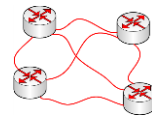
# Topology

Mesh

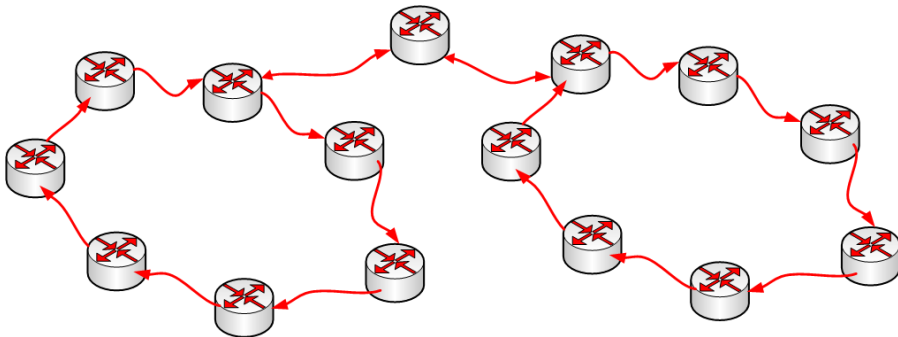


# Topology

Mixed topologies - Star Ring



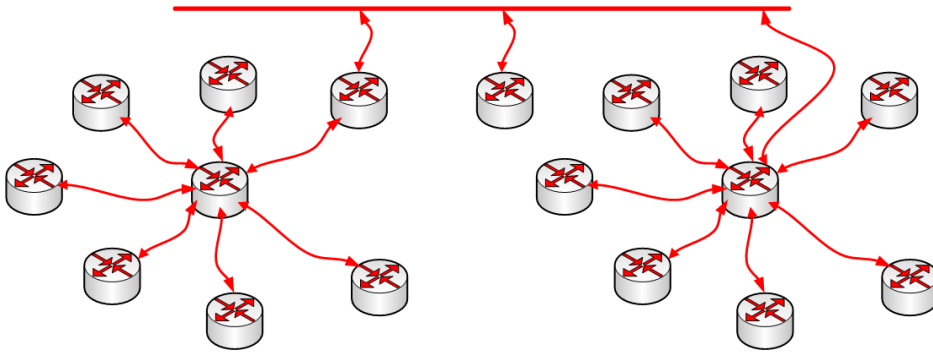
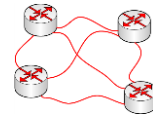
Star, Ring and Bus, are basic topologies, and can be combined e.g Star Ring or star star Bus topologies





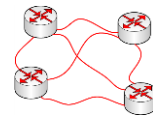
# Topology

Mixed topologies - Star Bus

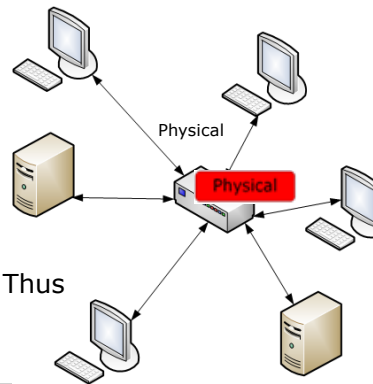
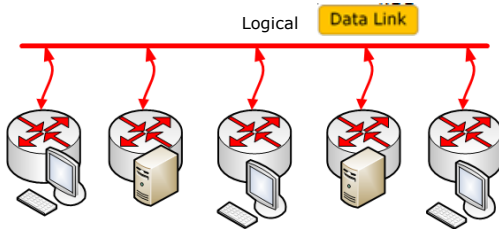


# Topology

Physical and logical topologies



- Example ethernet traditionally was based on bus topology but with the use of a hub it is physically a star

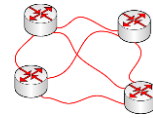


- Hub retransmits the signal to all ports. Thus effectively making it bus network.

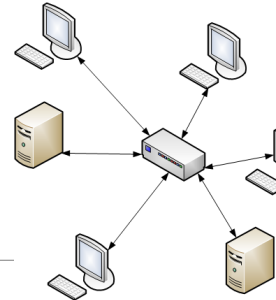
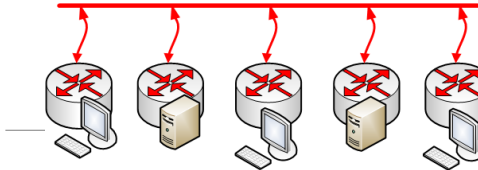


# Topology

Physical and logical topologies

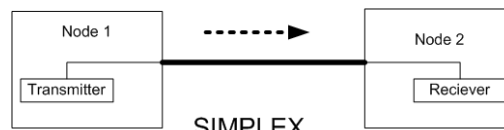
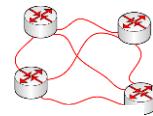


- Topologies determine the characteristics of the network, for example:
  - Layout of the network and wiring
  - Number of Nodes and size of the network
  - Message Reliability
- In modern networking the physical topology no longer limits the media access method used.

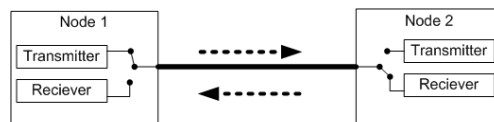


# Topology

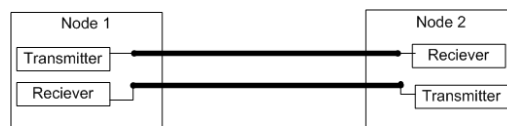
Duplex



SIMPLEX



Half Duplex



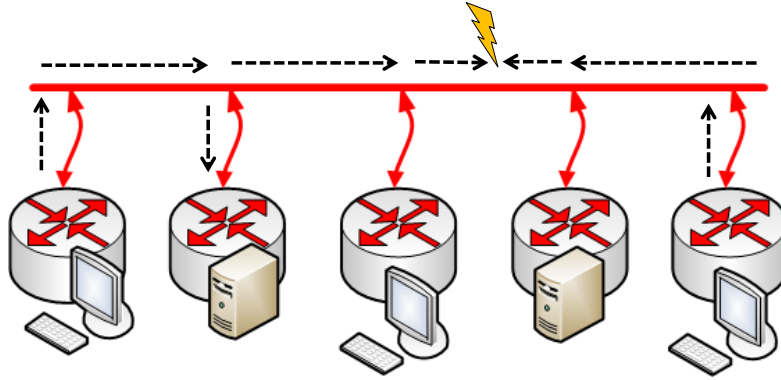
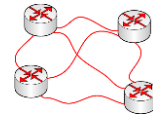
Full Duplex





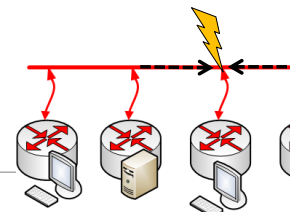
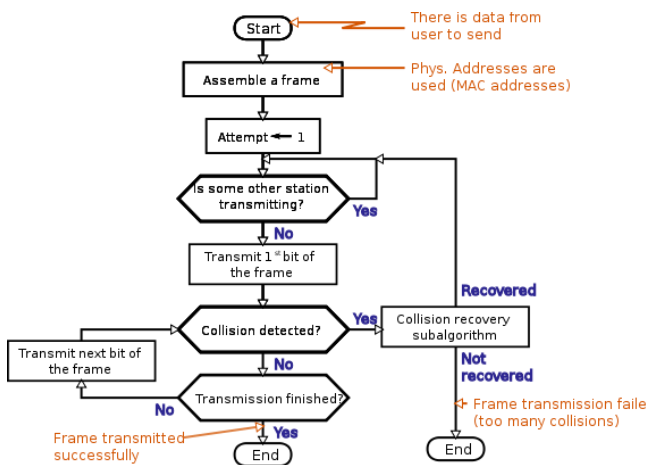
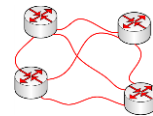
# Media Access Control

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



# Media Access Control

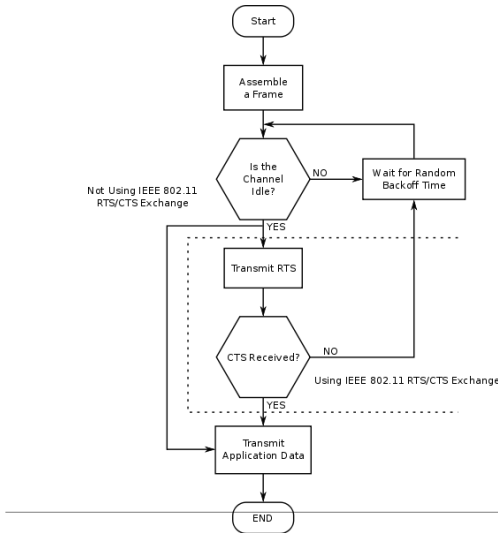
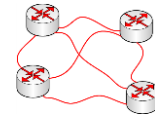
Carrier-sense multiple access (CSMA) / Collision Detection (CD)





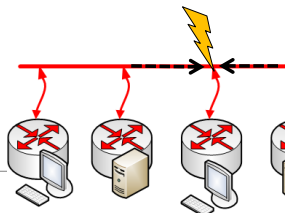
## Media Access Control

Carrier-sense multiple access (CSMA) / **Collision Avoidance (CA)**



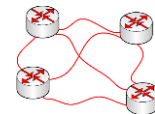
- Used in

- IEEE 802.11
- IEEE 802.15



## Media Access Control

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

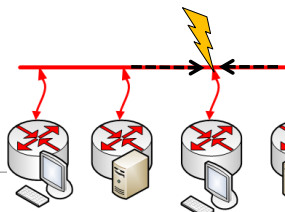


- Advantages

- Peer to Peer Communication
- Efficient under light and heavy loads
- Variations in data transfer requirements handled
- Urgent request can be handled instantly
- No centralized bus controller is required

- Disadvantages

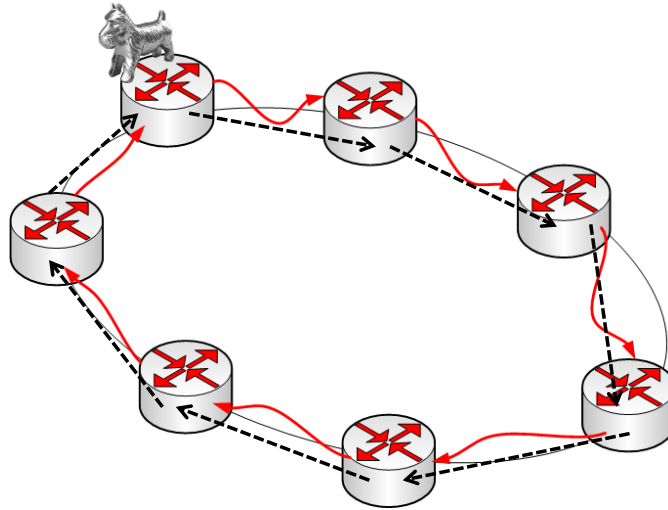
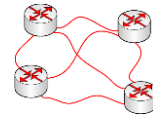
- Communication failure to a specific device will only response requested and none given
- Network configuration is complex
- Non deterministic response times
- Data collision is inherent
- Medium capture effect





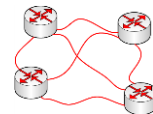
## Media Access Control

Token Passing – Token Ring



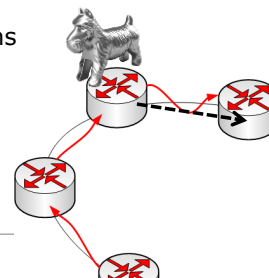
## Media Access Control

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

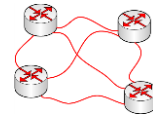
- Disadvantages
  - Hard to detect communication or node failure
  - Network still dependent on central communications controller
  - Semi deterministic response times obtained
  - Unnecessary waiting times still inherent





## Media Access Control

Other types



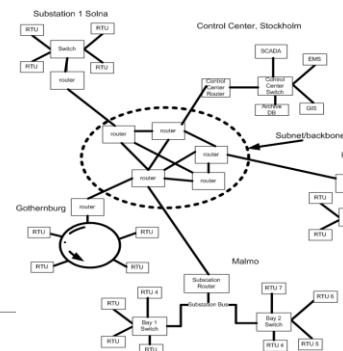
- Mainly for wireless networks:
  - Slotted ALOHA
  - Dynamic TDMA
  - CDMA
  - OFDMA
  
- Not so relevant for our overview, but good to recognise.



## Routing and Addressing



- Network layer
  - IP addresses
  - Broadcast and multicast
  - Routing tables
  
- Data link layer
  - MAC addresses
  - ARP
  - Switching





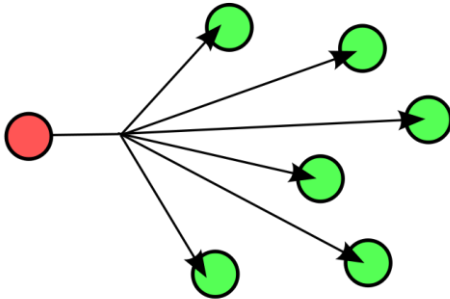


## Routing and Addressing

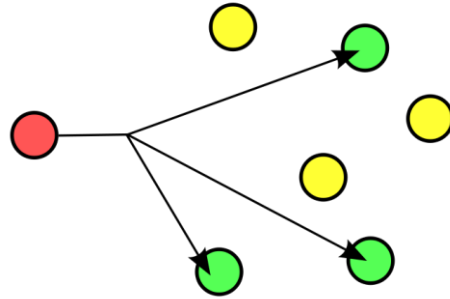
Network layer – Broadcast and multicast



Broadcast



Multicast

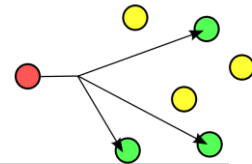


## Routing and Addressing

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
  - Phasor data in the "smart grid"?





# Routing and Addressing

Network layer – Routing table

- Application
- Transport
- Network
- Data Link
- Physical

- Table maintained on network-layer devices;
  - Hosts
  - Routers

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

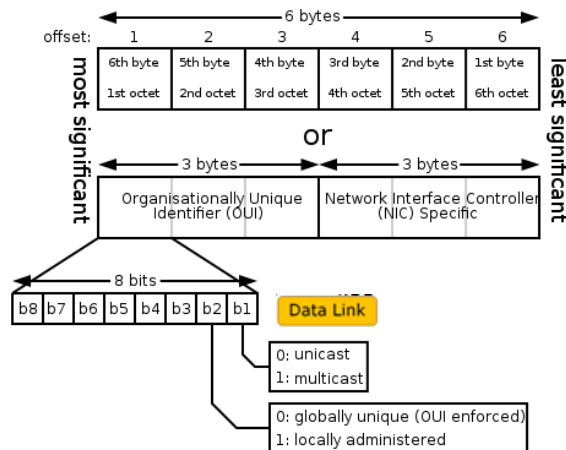
- Three main fields:
  - Host id – destination network ID (IP address/range)
  - Cost – or metric of the path
  - Next-hop – the specific address of the device to forward to



# Routing and Addressing

Data link layer – MAC addresses

- Application
- Transport
- Network
- Data Link
- Physical



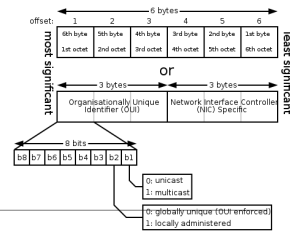


# Routing and Addressing

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)	



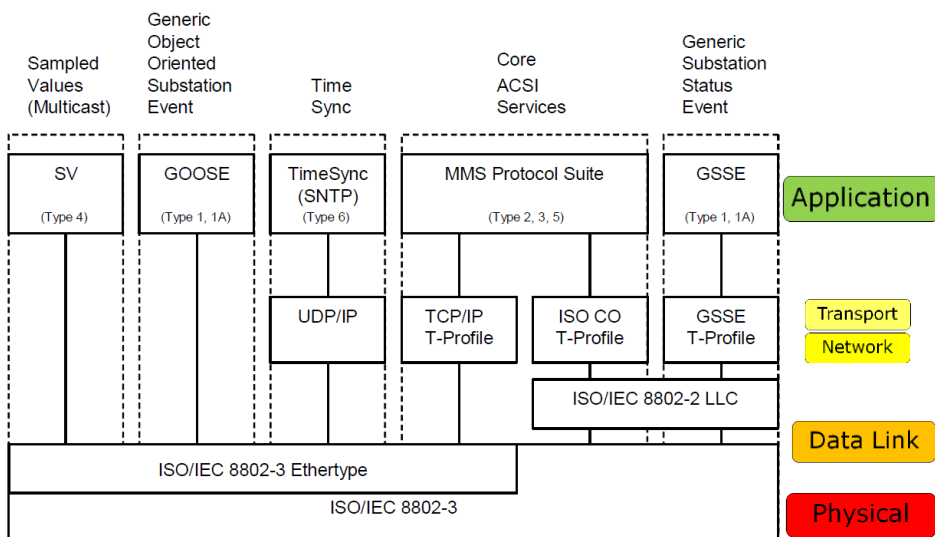
## Protocols used in power systems

- IEC 61850
  - GOOSE
  - SV
  - MMS
- IEC 60870-5-10x
- Modbus
- DNP3
- ICCP



## Protocols used in power systems

IEC 61850-8-1





## Protocols used in power systems

### GOOSE

- Generic Object Oriented Substation Event

- Specified in IEC 61850-8-1
- Status and values
- Grouped into dataset
- Transmitted within a time of 4ms

```

gocbRef: RET670LD0/LLN0$GO$ABB_GOOSE
timeAllowedtoLive: 1100
datSet: RET670LD0/LLN0$ABB_G_TRIP
goID: ABB_G_TRIP
t: Feb 19, 2011 01:34:27.690000057 UTC
stNum: 53
sqNum: 4
test: False
confRev: 1
ndsCom: False
numDatSetEntries: 5
allData: 5 items
  
```



## Protocols used in power systems

### GOOSE

IEC 61850-7-2 parameter	Parameter name
Argument	Argument
	Destination address
DatSet	datSet
GoID <sup>a)</sup>	goID
GoCBRef	gocbRef
T	t
StNum	stNum
SqNum	sqNum
timeAllowedtoLive	timeAllowedtoLive
Test	test
ConfRev	confRev
NdsCom	ndsCom
GOOSEData	numDatSetEnries
	allData
	timeAllowedToLive

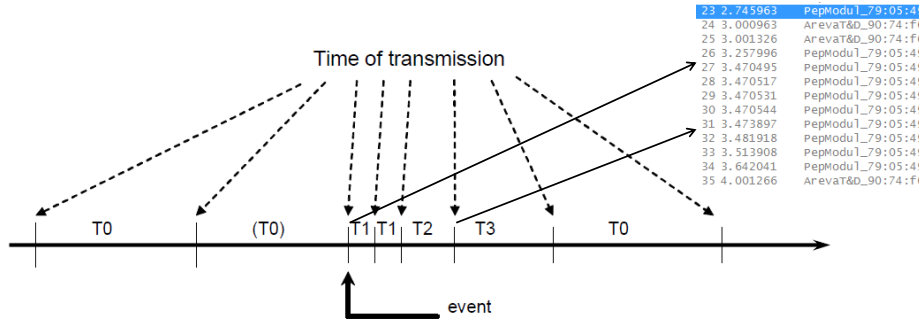
```

gocbRef: RET670LD0/LLN0$GO$ABB_GOOSE
timeAllowedtoLive: 1100
datSet: RET670LD0/LLN0$ABB_G_TRIP
goID: ABB_G_TRIP
t: Feb 19, 2011 01:34:27.690000057 UTC
stNum: 53
sqNum: 4
test: False
confRev: 1
ndsCom: False
numDatSetEntries: 5
allData: 5 items
  
```



# Protocols used in power systems

## GOOSE – retransmission strategy



- T0 retransmission in stable conditions (no event for a long time).
- (T0) retransmission in stable conditions may be shortened by an event.
- T1 shortest retransmission time after the event.
- T2, T3 retransmission times until achieving the stable conditions time.



# Protocols used in power systems

## MMS

- Open standard
- Transferring real-time process data
- Provides standard messages
- Encoding rules

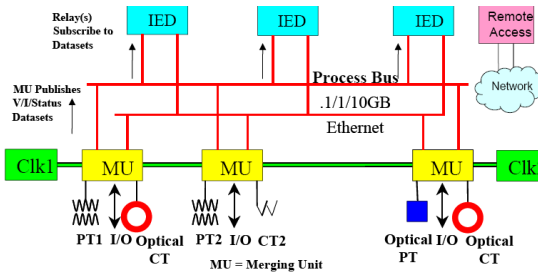
Application	Association Control Service Element (ACSE) - ISO 8649/8650
Presentation	Connection Oriented Presentation - ISO 8822/8823 Abstract Syntax Notation (ASN) - ISO 8824/8825
Session	Connection Oriented Session - ISO 8326/8327
Transport	ISO transport over TCP - RFC 1006 <a href="#">↗</a> Transmission Control Protocol (TCP) - RFC 793 <a href="#">↗</a>
Network	Internet Control Message Protocol (ICMP) - RFC 792 <a href="#">↗</a> Internet Protocol (IP) - RFC 791 <a href="#">↗</a> Address Resolution Protocol (ARP) - RFC 826 <a href="#">↗</a>
Link	IP datagrams over Ethernet - RFC 894 <a href="#">↗</a> MAC - ISO 8802-3 [Ethernet]
Physical	Ethernet



# Protocols used in power systems

## IEC 61850-9-2 Sampled Values (SV)

- Used on the process bus
- Transmits 3-phase CT/VT measurements
- Sampling rate of 4kHz
- Need time synchronization



# Protocols used in power systems

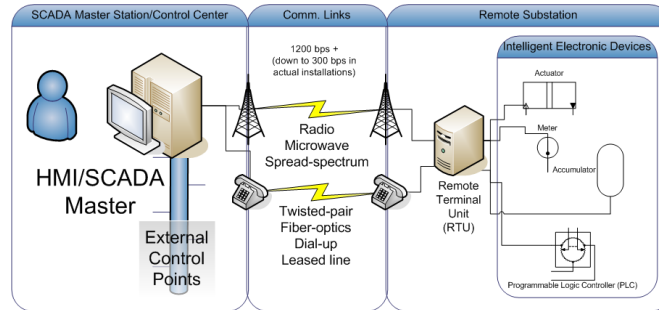
## IEC 61850-9-2 Sampled Values (SV)



## Protocols used in power systems

IEC 60870-5-10x

- A suite of "RTU protocols"...



## Protocols used in power systems

IEC 60870-5-10x

- Standard by TC57 (same as IEC 61850)

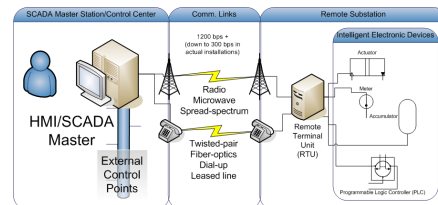
- Specifically for power systems

- Monitoring
- Control
- Teleprotection

- A few difference flavors exist:

- 101 – Serial RTU protocol
- 103 – interoperability between protection/substation devices
- 104 – Variant of 101 carried over TCP/IP

- Still very commonly used.





## Protocols used in power systems

IEC 60870-5-10x

IEC 101 Frame Format, Variable length		
Data unit	Name	Function
Start Frame	Start Character	Indicates start of Frame
	Length Field (*2)	Total length of Frame
	Start Character (repeat)	Repeat provided for reliability
	Control Field	Indicates control functions like message direction
	Link Address (0, 1 or 2)	Normally used as the device / station address
Data Unit Identifier	Type Identifier	Defines the data type which contains specific format of information objects
	Variable Structure Qualifier	Indicates whether type contains multiple information objects or not
	COT (1 or 2)	Indicates causes of data transmissions like spontaneous or cyclic
	ASDU Address (1 or 2)	Denotes separate segments and its address inside a device
Information Object	Information Object Address (1 or 2 or 3)	Provides address of the information object element
	Information Elements (n)	Contains details of the information element depending on the type
Information Object-2	-----	
Information Object-m	-----	
Stop Frame	Checksum	Used for Error checks
	Stop Char	Indicates end of a frame



## Protocols used in power systems

Modbus

- Master/slave RTU protocol mainly for PLC interfacing
  - Address up to 240 devices
  - *Coils* and *contacts* – old names for status and command points
- Many versions (“flavours”)
  - Serial RTU, ACSII
  - TCP/IP
  - UDP

Modbus TCP Frame Format		
Name	Length	Function
Transaction Identifier	2 bytes	For synchronization between messages of server & client
Protocol Identifier	2 bytes	Zero for MODBUS/TCP
Length Field	2 bytes	Number of remaining bytes in this frame
Unit Identifier	1 byte	Slave Address (255 if not used)
Function code	1 byte	Function codes as in other variants
Data bytes	n bytes	Data as response or commands

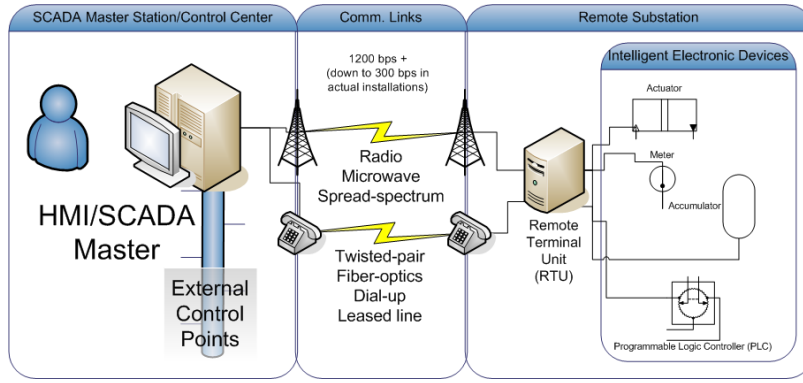
Modbus RTU Frame Format		
Name	Length	Function
Start	3.5c idle	at least 3-1/2 character times of silence (MARK condition)
Address	8 bits	Station Address
Function	8 bits	Indicates the function codes like read coils / inputs
Data	n * 8 bits	Data + length will be filled depending on the message type
CRC Check	16 bits	Error checks
End	3.5c idle	at least 3-1/2 character times of silence between frames



# Protocols used in power systems

DNP3

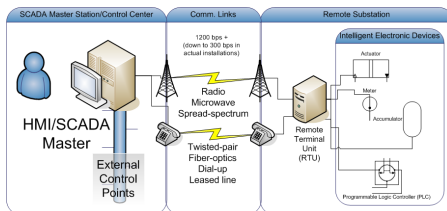
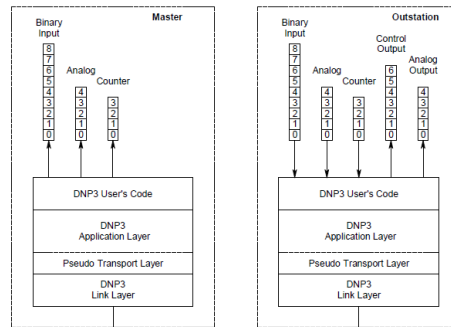
Also an "RTU protocol"...



# Protocols used in power systems

DNP3

- Distributed Network Protocol
  - SCADA master
  - Remote Terminal Units (RTU)
  - Intelligent Electronic Devices (IED)
- Mainly for SCADA->RTU/IED
- Polling and spontaneous access



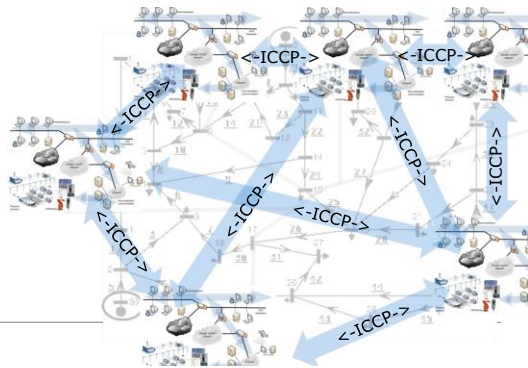
Physical Media  
 //  
 User Requests  
 ← User Responses



## Protocols used in power systems

### ICCP

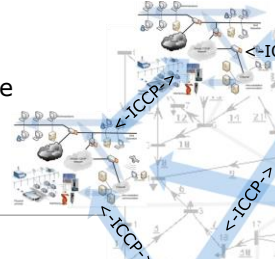
- Inter-Control Center Communications Protocol (IEC 60870-6/TASE.2)
  - Communication between SCADA systems
  - Client/server model
  - Carried over TCP/IP
  - No authentication or encryption



## Protocols used in power systems

### ICCP - Functionality

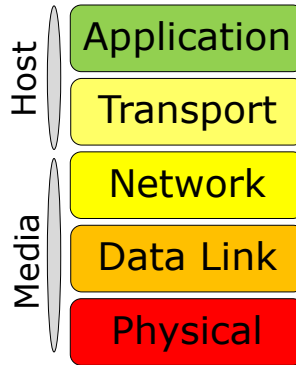
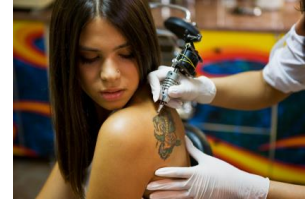
- Functions such as:
  - Periodic System Data
    - Status points, analogue points, quality flags, time stamp, counters, protection events
  - Device Control
    - on/off, trip/close, raise/lower etc and digital setpoints.
  - Program Control
    - Allows an ICCP client to remote control programs executing on an ICCP server.
  - Scheduling, accounting, outage and plant information
  - Historical time series data between a start and end date



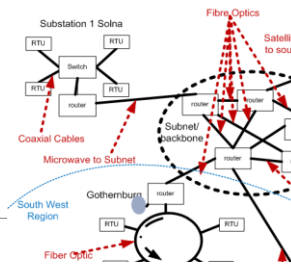


## Conclusions

Thinking of getting a tattoo?

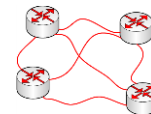


The OSI model will always be fashionable!



## Communication Networks

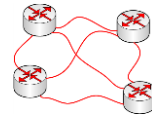
Conclusion



- A language to categorise and understand the many protocols, media and devices that exists
  - The OSI model
- Looked at the architectures, protocols and network infrastructure used in power systems control (SCADA & SAS)
- Routing and switching in more detail
- Protocols used in power systems applications



What's next..



### Workshop 2:

- Recap of the series
  - Brief discussion of metrics on networks
  - GOOSE/Wireshark example
  - Workshop time for project
-