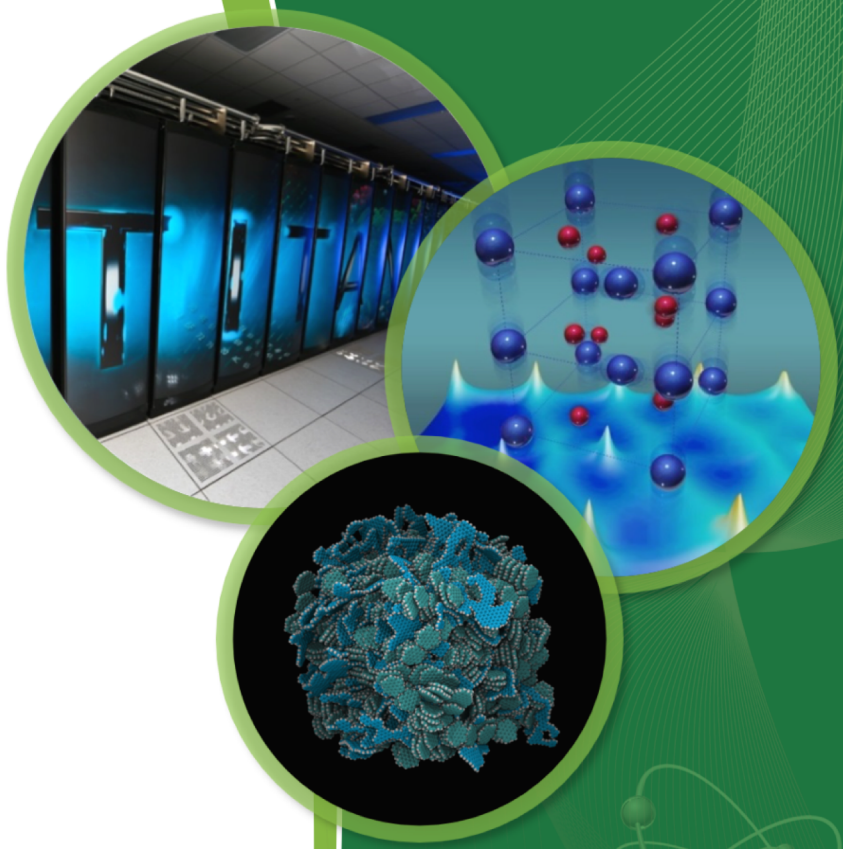
Introduction to Communication

The Network Stack

Dan King, Drew Herron, Allison Silverstein



NASPI North American SynchroPhasor Initiative

OAK RIDGE National Laboratory

Layer	DOD4 TCP/IP	Function	Synchrophasor Example
7: Application	Application Data	End User Layer – Provides the interface to the network stack for users and higher-level applications. This layer describes interface services such as Web (HTTP/S), E-Mail (POP3, SMTP, IMAP), and File Transfer (S/FTP, TFTP).	
6: Presentation		Syntax Layer – Layer that deals with formatting and translating data for the Application Layer. This includes compression and encryption services. TLS and SSL are common layer 6 protocols.	
5: Session		Port Layer – Allows the creation of sessions between networked systems. This layer is where the idea of an active connection between applications exists. Applications such as Secure Shell (SSH) and Remote Desktop (RDP, VNC) are in this layer.	Gateway Exchange Protocol – a Publish/Subscribe protocol used with openPDC to transfer data
4: Transport	Transport Data Channel	Data Channel Layer – Breaks the data that needs to be sent through the network into individual messages. This layer handles network traffic control and confirmation. The Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) are in this layer.	TCP/IP and UDP are proven technologies that are implemented not only in commercial IT and the internet as a whole, but also within industrial and scientific systems. OpenPDC uses TCP/IP for its communication needs.
3: Network	Internet	Packet Layer – This is the layer through which metadata is used to decide how to move packets containing messages through a given network. It's here that physical (MAC) and logical (IP) addresses are mapped to allow for packet routing.	
2: Data Link		Frame Layer – Describes exactly how data is formatted as it passes between network nodes. Ethernet frames are defined in this layer.	IRIG Timecode used within a PDC system for time synchronization. IEEE 1344 Extension to IRIG-B
1: Physical	Link	Physical Link Layer – This is the interface between the digital domain of computers and networking and the analog domain of the real world. Fiber, copper, cellular, and microwave technologies used for the transfer of data are described in this layer.	Cellular radios used to connect a PMU to a PDC. Copper and Fiber Wires.

7: Application
6: Presentation
5: Session
4: Transport
3: Network
2: Data Link
1: Physical

PDC

Historian | Visualization | Analytics | Operations | Configurator

7: Application
6: Presentation
5: Session
4: Transport
3: Network
2:Data Link
1: Physical

Using the data that PMUs produce involves operations that are above layer 7 of the model. These applications have nothing to due with communications per se, just the consumption of the data produced by it.

[11]

1: Physical
2:Data Link
3: Network
4: Transport
5: Session
6: Presentation
7: Application

All of the operations individual PMUs perform, such as the actual gathering of data, the computation of phasors, the generation of alarms, the handling of leap seconds; all of these occur above layer 7 of the model. Once the PMU starts the process of exporting data, this model takes hold.

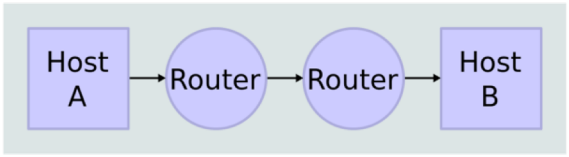
[12]

Local Storage | Alarming | Processing | Measurement | Configuration

PMU

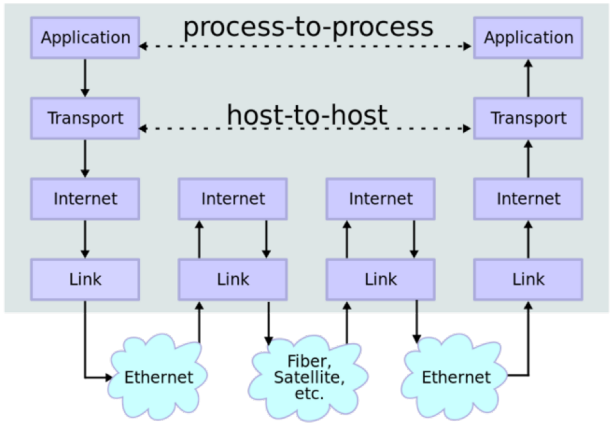
7: Application
6: Presentation
5: Session
4: Transport
3: Network
2: Data Link
1: Physical

Network Topology

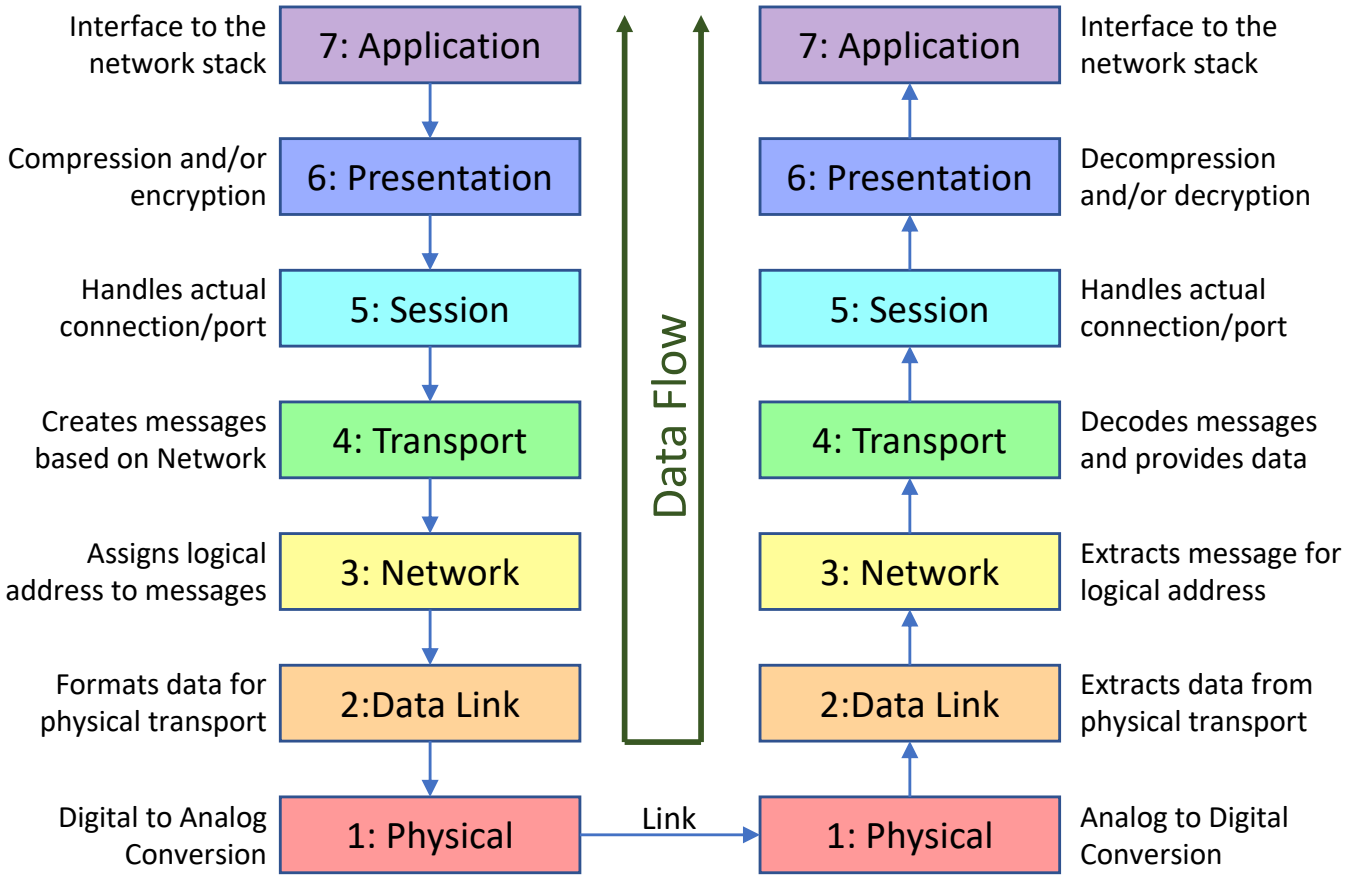


The connection between two hosts on a network can involve a large number of hops. In terms of time and physical distance data spends most of its time going between layers 1-3. It's usually only at the endpoints where it reaches layers 4-7.

Data Flow



Encapsulation and Decapsulation



Each layer of the OSI model provides for layers of encapsulation. This allow users, developers, and troubleshooters the ability to pay attention to interfaces rather than having to worry about the entire system.

For example the creation of a new Network Layer protocol requires only that the new protocol be able to interface with existing protocols on the Data Link Layer and the upgrade of Transport Layer protocols to handle the new protocol. Layer 1 and Layers 5-7 can be completely agnostic to these changes.

This allows for reuse of devices, code, and intellectual property as technology advances and changes.

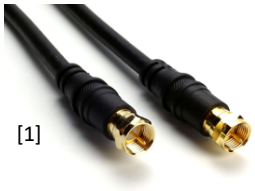
http://www.comptechdoc.org/independent/networking/protocol/protlayers.html

7: Application
6: Presentation
5: Session
4: Transport
3: Network
2: Data Link
1: Physical

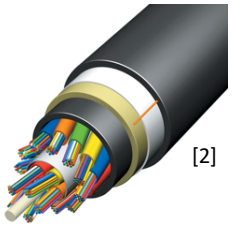
This is the interface between the digital domain of computers and networking and the analog domain of the real world. Fiber, copper, cellular, and microwave technologies used for the transfer of data are described in this layer.

Wired

Wired connections use electrical or light signals to transmit across some physical medium. In addition to the wire, both sides must have some type of electronics that convert the physical signals to zeros and ones.


[1]

Coax


[2]

Fiber


[3]

Ethernet


[4]

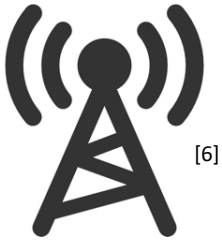
Serial

Wireless

Wireless connections use electromagnetic waves to transmit through space (usually open air). In addition to the signal, both sides must have specialized antennas and other RF equipment that convert the physical signals to zeros and ones.


[5]

802.11


[6]

Cellular


[7]

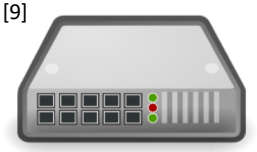
Microwave


[8]

Radio

Most wireless signals can freely talk to multiple endpoints on the same channel. For wired links, connecting multiple nodes on the same line is not as simple as splicing wires. Hubs can be used to solve this problem.

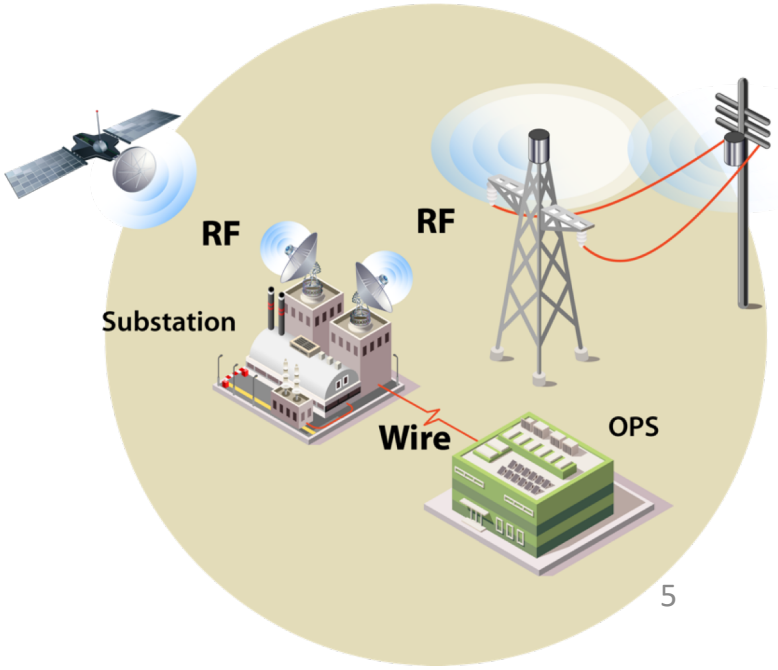
[9]



Both wired and wireless signals will be bound by limits to range. By using signal repeaters, the range can be increased. Depending on the technology, this can reduce overall bandwidth.

Multiple types of physical layers can exist within a single system. This is commonly seen when using an access point on a home network.

For a synchrophasor system this could include a wirelss signal from the PMU itself that transmits back to an aggregator that uses a wire to transfer data back to an operations center



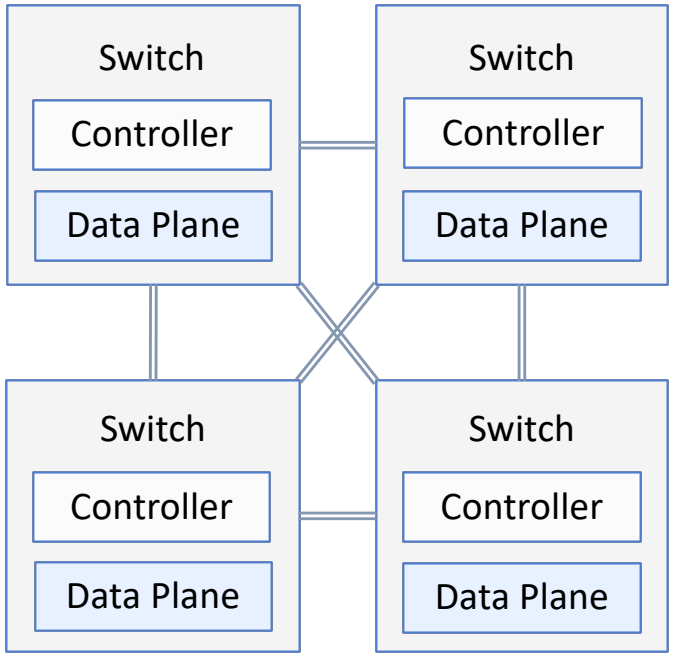
7: Application
6: Presentation
5: Session
4: Transport
3: Network
2: Data Link
1: Physical

These layers define how data moves between nodes on the network.

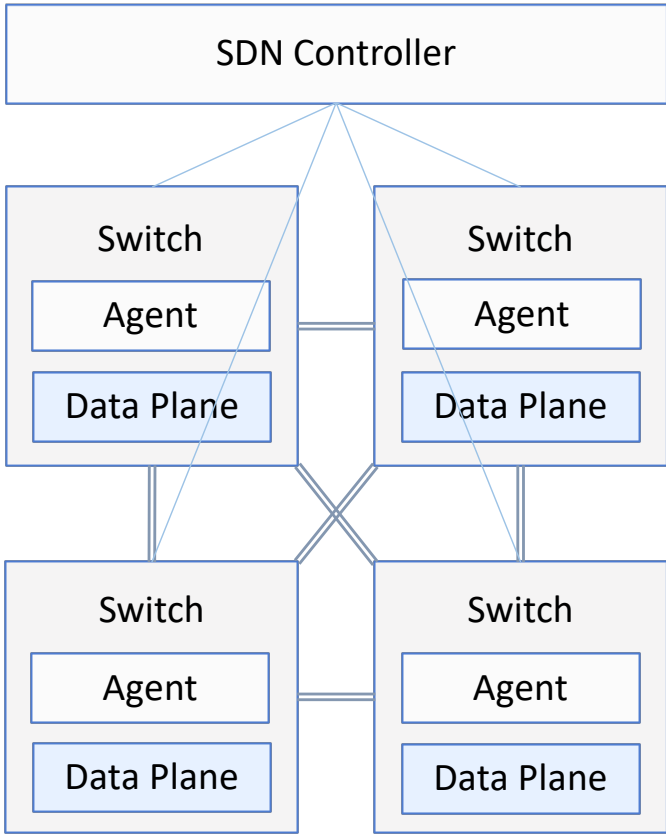
Layer 2, the Data Link Layer, defines hardware addressing and how data is structured on top of the physical layer.

Layer 3, the Network Layer, creates a layer of abstraction between addresses of physical addresses (such as a specific MAC address) and logical devices (such as an IP address).

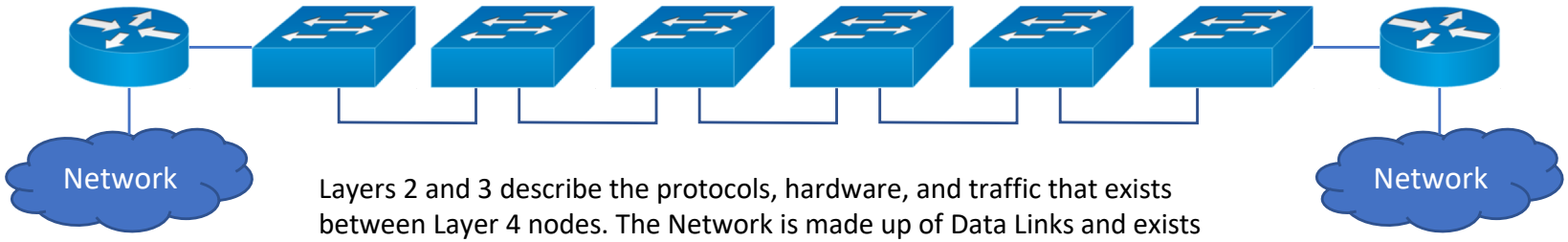
Software Defined Networking



In standard switching, each switch is configured and controlled as an independent entity.



In a software-defined network, a central controller is capable of dynamically reconfiguring switches to improve reliability and performance.



Layers 2 and 3 describe the protocols, hardware, and traffic that exists between Layer 4 nodes. The Network is made up of Data Links and exists entirely between layers 1-3. This is true whether the network is the internet as a whole or a simple home network only connecting your laptop and printer.

7: Application
6: Presentation
5: Session
4: Transport
3: Network
2: Data Link
1: Physical

[Layer 7] User interacts with web browser that sends data to switch

[Layer 3] Switch uses Layer 3 info to route data to the router

[Layer 4] Router repackages Layer 3 data with new, external IP address

[Layer 3] The internet is just another network, albeit quite a large one

[Layer 4] Router repackages Layer 3 data with new, internal IP address

[Layer 3] Switch uses Layer 3 info to route data to the web server

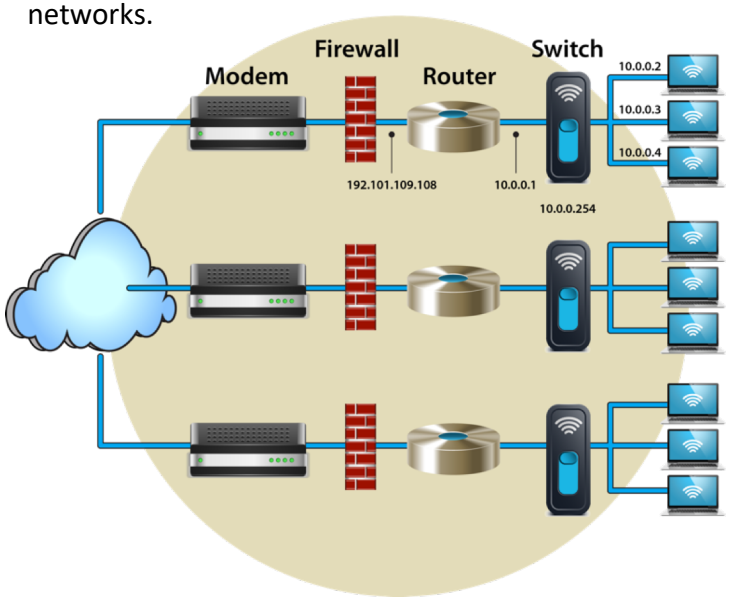
[Layer 7] Web service interacts with disk to serve data

In the figure above 3 separate networks are represented, the client network, the internet, and the server network. It is the services provided at layer 4 that provide the mechanism for stitching these networks together.

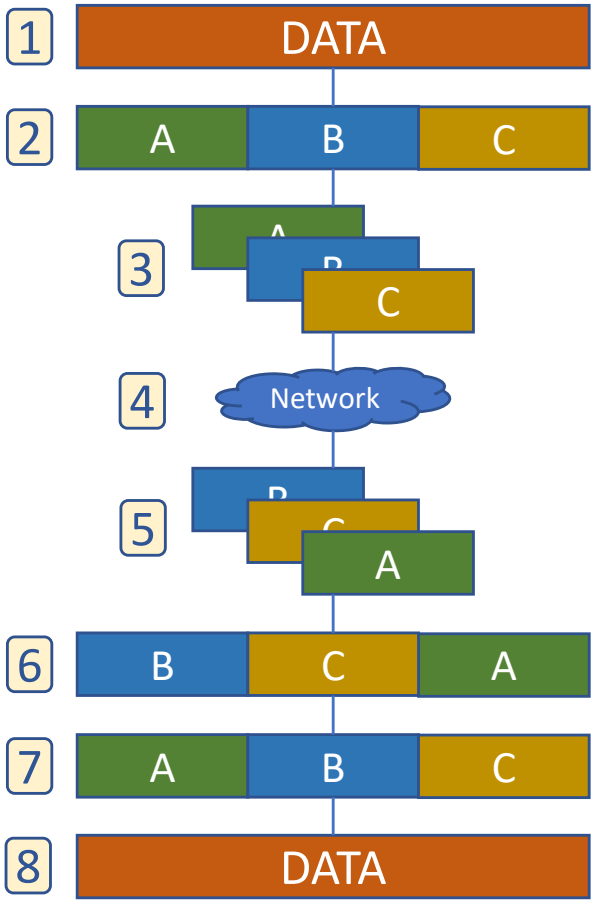
This layer acts as an interface between the Application layers above it and the Network layers below it and encompasses two main tasks.

First, this layer converts data from a compute node into messages that can be sent through a network.

Next, this layer acts as an interface between different networks.



Layer 4 protocols, such as TCP perform an important role as interface between the computing node and the network. This includes making sure that not only all of the data [1] gets to its destination [8], but that it is stitched back together [7]. Due to limits on packet size going through a network [4], it is necessary to split data blocks into smaller pieces [2]. While this data is transmitted serially [3] it does not always reach its destination in the same order [5]. This can be due to pathing or packets being dropped, requiring retransmission. In this case it needs to be reordered on the other end [6] in order to maintain data integrity.



Routers are the most representative example of layer 4 hardware. They provide the basic capability of connecting different networks. This is done for a variety of reasons, including security and IP address space.

The top three layers of the OSI model are closely related. Even though they have separate roles in the OSI model, many other models, such as The Internet Model combine them together as the Application Layer.

It is here that most development occurs when designing and building a communications application, as Layers 2-4 are well developed and consistent, and Layer 1 is encapsulated.

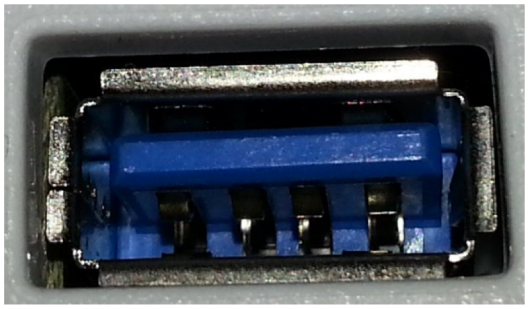
7 6 5	OpenFMB	IEC 61850	OpenPDC	DNP3	Modbus	DDS MQTT AMQP
4 3	UDP, TCP/IP					
2 1	Ethernet					

All of these communication protocols use TCP/IP and/or UDP for the basis of their communication.

7: Application
6: Presentation
5: Session
4: Transport
3: Network
2: Data Link
1: Physical

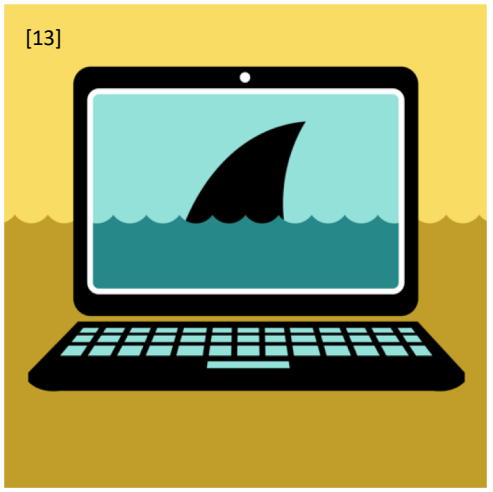
Each layer provides possible vectors for attackers to find entry into the network stack. They can be broken up into three basic categories.

1. Physical
2. Network
3. Application



[14]

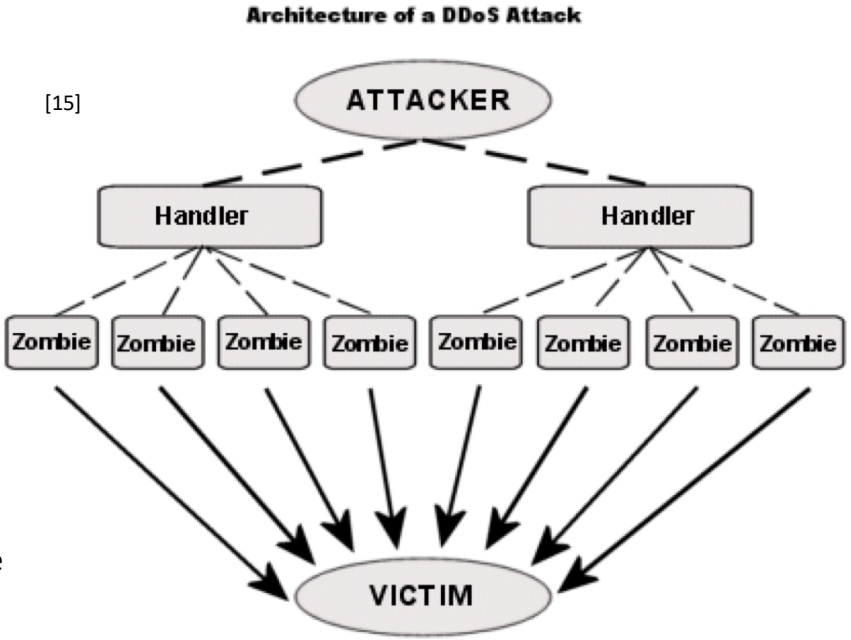
Application-level attacks can be perpetrated by using valid communications for bad purposes. This is the widest area of attack and includes such things as SQL Injection, Command Injection, Cross-Site Scripting, and many others.



[13]

Application-level attacks can also occur through mechanisms outside of the network stack, such as from users placing malicious external media into a computer (such as USB or DVD). This can even occur through using a normally innocuous peripheral such as a mouse or keyboard.

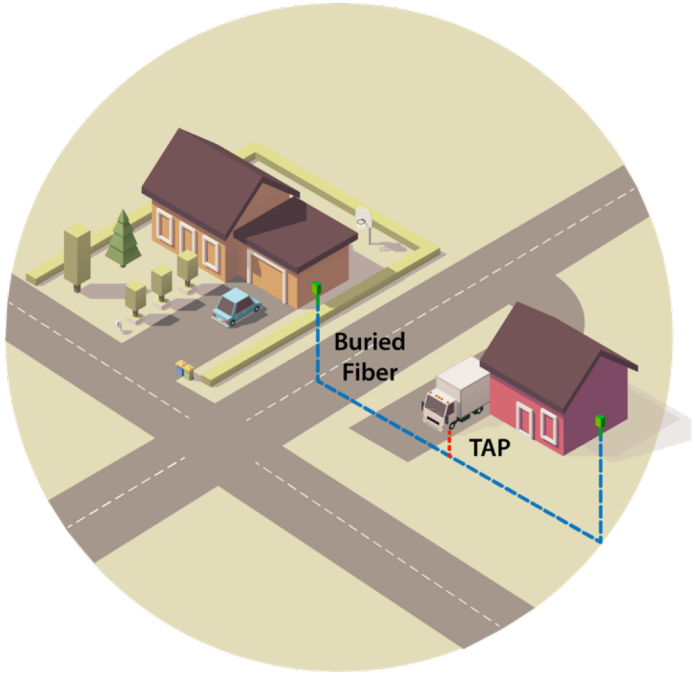
Network-level attacks are not as varied as application-level attacks, but can be incredibly sophisticated. These attacks use the nature of how layers 2-4 work in order to generate undesired outcomes. These attacks include IP Spoofing, MAC Spoofing, Denial of Service, ARP Poisoning, Replay Attacks, Malformed Packets, and others,



[15]

One Network-level attack that is relatively common is the Distributed Denial of Service Attack. This is a simple attack and very difficult to defend against, as it is simply the process of overloading a service by making multiple requests from a variety of systems.

No system is immune to DDoS attacks



Physical attacks involve malicious actors intercepting or monitoring physical signals. This can be anything from eavesdropping on transmissions to the tapping of physical lines. Information can also be gathered through power usage monitoring and unintended emanations.

7: Application
6: Presentation
5: Session
4: Transport
3: Network
2: Data Link
1: Physical

The first line of defense against security threats is the firewall. It is possible for firewalls to exist in many places through the stack, and many places through a network.

Two main types of firewalls are used today, hardware firewalls and application firewalls.

Depending on a single tool to protect your network and data is not enough. Protecting data moving between systems and data at rest with various types of open-source encryption ensures that malicious actors have a more difficult time of successfully attacking your system or gaining access to confidential information.

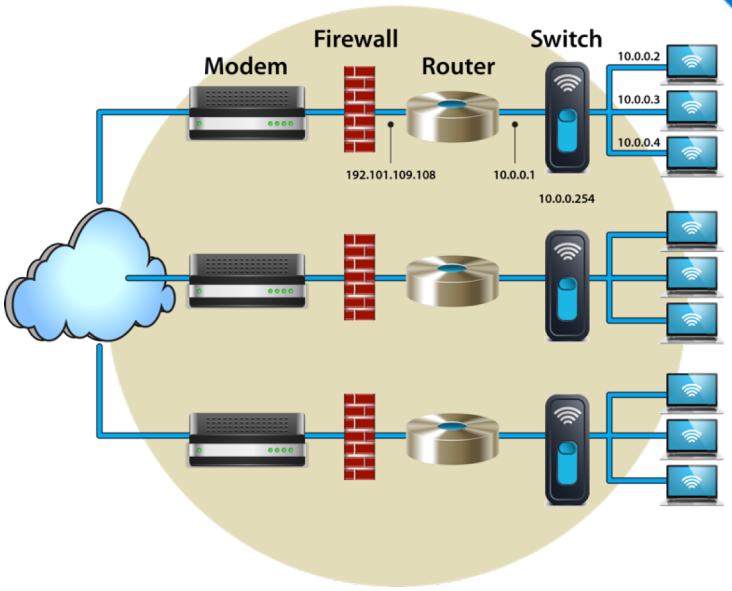
Other systems like Intrusion Prevention Systems (IPS) and Intrusion Detection Systems (IDS), along with correct and secure configuration of all network nodes (computers, routers, etc.) also help to protect your systems from attackers.

[18]

[16]

Application firewalls can be built into an operating system or provided by a third party. Generally only a single application firewall should be placed on a system, as multiple application-level firewalls can cause unintended behavior that diminishes correct functionality of a system.

[17]



Since a firewall is usually meant to protect your entire network it is advisable to place it on the main line before your router. That way all systems within your network can benefit from its protection. For more complicated networks that provide a variety of services to the outside world this may be neither possible nor recommended.

Image References

[1] https://sewelldirect.imgix.net/products/sw-33020-6/sw-33020-6.jpg
[2] https://www.aflglobal.com/productlist/Product-Lines/Fiber-Optic-Cable/Standard_ADSS_Fiber_Optic_Cable/img/ADSS-Standard.aspx
[3] https://webobjects2.cdw.com/is/image/CDW/1053158?$product-main$
[4] https://photography-909a.kxcdn.com/product-images/10480/100/10480a.jpg
[5] http://www.techiwarehouse.com/userfiles/Wireless-Router.gif
[6] http://media.idownloadblog.com/wp-content/uploads/2016/09/Cellular-Radio-Tower-Icon.jpg
[7] https://www.rosenbergerap.com/upload/201512/08/201512081424532453.jpg
[8] https://gloimg.gbtcdn.com/gb/pdm-provider-img/straight-product-img/20171020/T009174/T0091740036/goods-img/1508721954823503625.jpg
[9] By OSA [CC BY-SA 3.0 (https://creativecommons.org/licenses/by-sa/3.0)], via Wikimedia Commons
[10] https://encrypted-tbn0.gstatic.com/shopping?q=tbn:ANd9GcSA-Bktele29Tk6kpCe2_4h4m5Cs94u1qCjTG8GEy9JTUT8rjk&usqp=CAY
[11] By Victorgrigas [CC BY-SA 3.0 (https://creativecommons.org/licenses/by-sa/3.0)], from Wikimedia Commons
[12] http://powerit.utk.edu/pics/fdr-UTlogo-small.jpg
[13] By EFF-Graphics [CC BY 3.0 us (https://creativecommons.org/licenses/by/3.0/us/deed.en)], from Wikimedia Commons
[14] By RoundupResistance [CC0], from Wikimedia Commons
[15] By VicktoR (Internet) [Public domain], via Wikimedia Commons
[16] By Microsoft Windows [Public domain], from Wikimedia Commons
[17] https://www.obdev.at/Images/product-icons/littlesnitch_340@2x.png
[18] Santeri Viinamäki [CC BY-SA 4.0 (https://creativecommons.org/licenses/by-sa/4.0)], from Wikimedia Commons

NASPI North American SynchroPhasor Initiative