Virtualization Overview

Virtualization is one of the most powerful ways to manage hardware and software for an organization today. It allows a single piece of hardware to host multiple different systems thereby having the functionality of several different systems or computers working on one machine.

Virtualization is the foundation for an agile, scalable cloud and the first practical step for building cloud infrastructure. Virtualization abstracts and isolates the underlying hardware as virtual machines (VMs) operate in their own run time environment and with multiple VMs for computing, storage, and networking resources in a single hosting environment. These virtualized resources are critical for managing data, moving it into and out of the cloud, and running applications with high utilization and availability.

Virtualization is managed by a host server running a hypervisor—software, firmware, or hardware that creates and runs VMs. The VMs are referred to as guest machines. The hypervisor serves as a virtual operating platform that executes the guest operating system for an application. Host servers are designed to run multiple VMs sharing multiple instances of guest operating systems.

Virtualization also provides several key capabilities for cloud computing, including resource sharing, VM isolation, and load balancing. In a cloud environment, these capabilities enable scalability, high utilization of pooled resources, rapid provisioning, workload isolation, and increased uptime.

Hypervisor

A hypervisor or virtual machine monitor (VMM) is a piece of computer software, firmware, or hardware that creates and runs virtual machines. The hypervisor presents the guest operating systems with a virtual operating platform and manages the execution of the guest operating systems. Multiple instances of a variety of operating systems may share the virtualized hardware resources. In their 1974 article, “Formal Requirements for Virtualizable Third Generation Architectures” Gerald J. Popek and Robert P. Goldberg classified two types of hypervisor:

Type-1: native or bare-metal hypervisors.

> These hypervisors run directly on the host’s hardware to control the hardware and to manage guest operating systems. For this reason, they are sometimes called bare-metal hypervisors. A guest operating system runs as a process on the host.

Type-2: hosted hypervisors.

> These hypervisors run on a conventional operating system just as other computer programs do. Type-2 hypervisors abstract guest operating systems from the host operating system.

Types of Virtualization

There are several different types of virtualization with which you need to be familiar, including:

Server Virtualization

Server virtualization unlocks today's traditional one-to-one architecture of x86 servers by abstracting the operating system and applications from the physical hardware, enabling a more cost-efficient, agile, and simplified server environment. Using server virtualization, multiple operating systems can run on a single physical server as virtual machines, each with access to the underlying server's computing resources.

Network Virtualization

Network virtualization is the complete reproduction of a physical network in software. Virtual networks offer the same features and guarantees of a physical network, yet they deliver the operational benefits and hardware independence of virtualization—rapid provisioning, non-disruptive deployment, automated maintenance, and support for both legacy and new applications

Network virtualization presents logical networking devices and services logical ports, switches, routers, firewalls, load balancers, VPNs, and more to connected workloads.

Applications run on the virtual network exactly the same as if on a physical network. You can create a highly scalable network fabric that provides greater levels of operational efficiency and agility, faster provisioning, troubleshooting, and cloning with monitoring, QoS, and security all backed by network virtualization software.

Desktop Virtualization

Deploying desktops as a managed service gives you the opportunity to respond quicker to changing needs and opportunities. You can reduce costs and increase service by quickly and easily delivering virtualized desktops and applications to branch offices, outsourced and offshore employees, and mobile workers on iPad and Android tablets.

Application Virtualization

To maintain QoS and SLA for Tier 1 business applications in virtual environments, IT organizations must focus on the virtualization components of the project, the management and monitoring of virtualized business applications, and maintaining corporate guidelines for business continuity and disaster recovery. With a Tier 1 Application Virtualization solution, you can enhance the quality of IT services delivered, while simplifying your infrastructure, maximizing efficiency, and eliminating costly over-provisioning.

Storage Virtualization

Today, huge data volumes and real-time applications are pushing storage demands to new levels. Conventional storage systems are overwhelmed, and IT is looking for better alternatives. What’s needed is a new approach to storage, one that applies the principles of the software-defined data center to storage: it abstracts the disks and flash drives inside your servers, combines them into high-performance storage pools, and delivers these as software

Storage virtualization technology provides a fundamentally better way to manage storage resources for your virtual infrastructure, giving your organization the ability to:

- Significantly improve storage resource utilization and flexibility
- Simplify OS patching and driver requirements regardless of storage topology
- Increase application uptime and simplify day-to-day operations
- Leverage and complement your existing storage infrastructure

Security

Virtualization offers numerous advantages from a security perspective. Virtual machines are typically isolated in a sandbox environment and, if infected, can quickly be removed or shut down and replaced by another virtual machine. Virtual machines:

- Have limited access to hardware resources and, therefore help protect the host system and other virtual machines
- Do require strong configuration management control and versioning to ensure known good copies are available for restoration if needed
- Are also subject to all the typical requirements of hardware-based systems, including anti-malware software, encryption, HIDS, firewalls, and patching

Additionally, more malware and viruses are becoming virtual machine aware. They are able to detect when they are in a virtual machine and “break out” to the host system. The security architect must be aware of these tradeoffs and plan accordingly for the system and enterprise security architecture.

Virtualization and CPU Security

In addition, there is also the question of how cloud-based solutions such as Desktop as a Service (DaaS) and more broadly virtualization will impact the discussion around CPU security. It is important to be aware of these issues and take them into account when planning architectures.

For example, in June of 2012, Vulnerability VU#649219 was logged and released by the US CERT. The vulnerability report was titled: “SYSRET 64-bit operating system privilege escalation vulnerability on Intel CPU hardware.” The following is an excerpt from the Vulnerability Note:

- **Overview:** Some 64-bit operating systems and virtualization software running on Intel CPU hardware are vulnerable to a local privilege escalation attack. The vulnerability may be exploited for local privilege escalation or a guest-to-host virtual machine escape. Intel claims that this vulnerability is a software implementation issue, as their processors are functioning as per their documented specifications. However, software that fails to take the Intel-specific SYSRET behavior into account may be vulnerable.
- **Description:** A ring3 attacker may be able to specifically craft a stack frame to be executed by ring0 (kernel) after a general protection exception (#GP). The fault will be handled before the stack switch, which means the exception handler will be run at ring0 with an attacker’s chosen RSP causing a privilege escalation.
- **Impact:** A local authenticated attacker may exploit this vulnerability for operating system privilege escalation or for a guest-to-host virtual machine escape. While this vulnerability was widespread across multiple vendor platforms, it did not affect all vendors that provide virtualization solutions. Any architecture that was built upon the selection of an AMD chip as the CPU of choice would not have been exposed to this vulnerability. While the chances of this particular threat being used to attack a system may or may not have

been high at the time, the fact still remains that the security architect would bear ultimate responsibility for this threat and its impact on the systems affected.

Different Types of Virtualized Storage

Virtual storage is the pooling of physical storage from multiple network storage devices into what appears to be a single storage device managed from a central console. Storage virtualization software converts a server into a storage controller and the storage inside the server into the storage system. The benefit of virtualization is that commodity hardware, or less-expensive storage, can be used to provide enterprise-class functionality. Storage virtualization also helps the storage administrator perform the tasks of backup, archiving, and recovery more easily and in less time by disguising the actual complexity of a storage area network (SAN).

Different Types of Virtualized Storage include:

- **Host-based:** Host-based virtualization requires additional software running on the host as a privileged task or process. In some cases, volume management is built into the operating system and in other instances, it is offered as a separate product. Volumes (LUNs) presented to the host system are handled by a traditional physical device driver. However, a software layer (the volume manager) resides above the disk device driver, intercepts the I/O requests, and provides the meta-data lookup and I/O mapping. Most modern operating systems have some form of logical volume management built-in (in Linux it is called the Logical

Volume Manager or LVM; in Solaris and FreeBSD, ZFS's zpool layer; in Windows the Logical Disk Manager or LDM) that performs virtualization tasks.

- **Storage device-based:** A primary storage controller provides the virtualization services and allows the direct attachment of other storage controllers. Depending on the implementation, these may be from the same or different vendors. The primary controller will provide the pooling and meta-data management services. It may also provide replication and migration services across those controllers that it is virtualizing.
- **Network-based:** Storage virtualization operating on a network-based device (typically a standard server or smart switch) and using iSCSI or Fibre Channel (FC) networks to connect as a SAN. These types of devices are the most commonly available and implemented form of virtualization. The virtualization device sits in the SAN and provides the layer of abstraction between the hosts performing the I/O and the storage controllers providing the storage capacity.
- **Archival and Offline Storage:** Data stored in a backup or archive may need to be reloaded into the main production environment. In this case, it is not only appropriate that a suitable technical solution is in place but that there are procedures in place to ensure recovery can be done quickly and effectively.
- **Sandbox:** Sandboxing is a form of software virtualization that lets programs and processes run in their own isolated virtual environment. Typically, programs running within the sandbox have limited access to your files and system, and they can make no permanent changes. This means that whatever happens in the sandbox stays in the sandbox. Sandboxing, one alternative to traditional signature-

based malware defense, is seen as a way to spot zero-day malware and stealthy attacks in particular.

Summary

Virtualization has many benefits from both an operational and security viewpoint. The compromise of a virtual machine can usually be addressed by simply disabling the machine and then restarting it. This still requires that the VM is configured correctly and that unnecessary VMs are disabled. VMs should be tracked like other assets of the organization.

OSI and TCP/IP Models Overview

The security of a company's internal and external network and communications systems are critically important. If best practices are not applied to the actual communications systems, then valuable data can be compromised. As part of this, it is important to understand the risks, threats, and vulnerabilities associated with networks and know how to properly plan for these and other risks.

Networking technologies are typically broken down into various layers. These layers allow for segregation of function and the ability to mix different aspects of communications into a solution. The two common models are the OSI 7 layer and the TCP/IP 4 layer models.

The OSI (Open Systems Interconnect) model was defined in 1984 and is codified as an international standard ISO/IEC 7498-1. The standard has been updated several times with the most recent being 1994.

APPLICATION LAYER

Network-related application programs

PRESENTATION LAYER

Standardization of data presentation to the applications

SESSION LAYER

Management of sessions between applications

TRANSPORT LAYER

End-to-end error detection and correction

NETWORK LAYER

Management of connections across the network

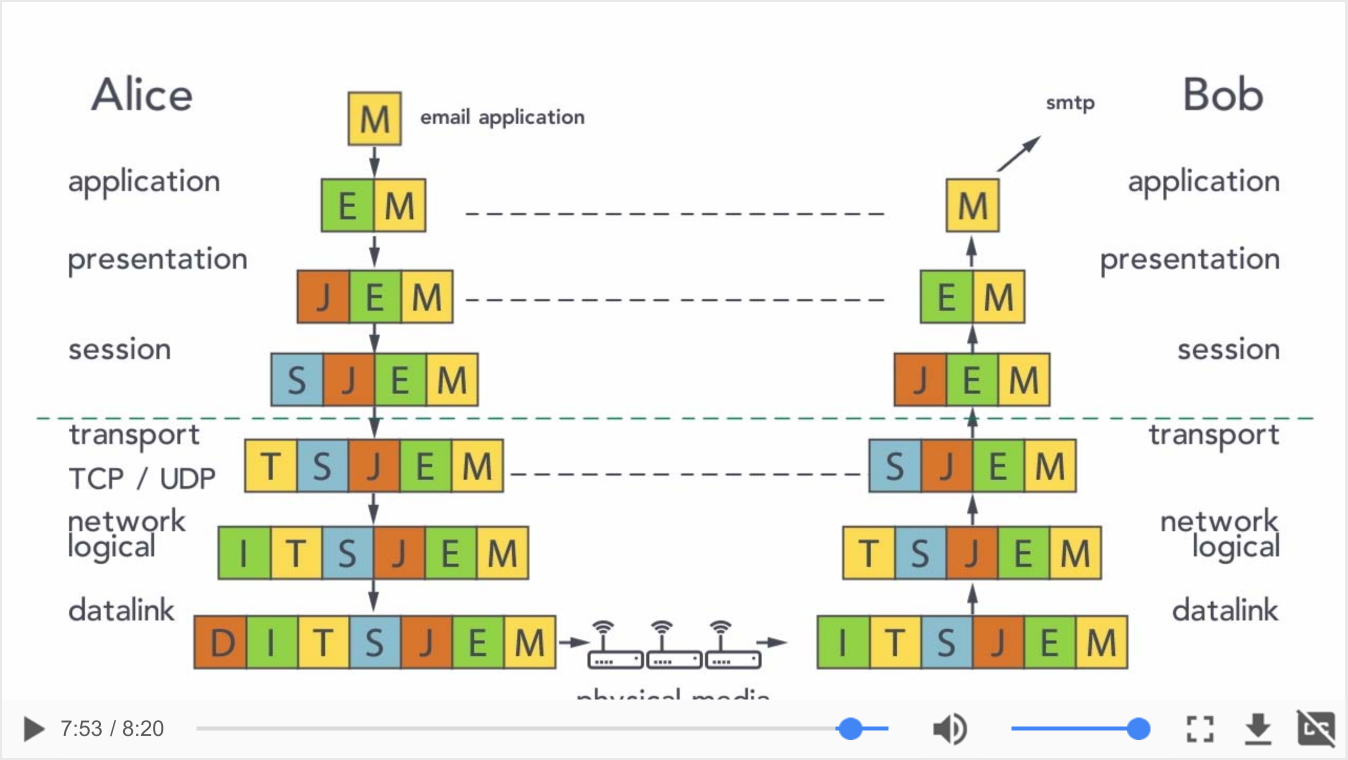
DATA LINK LAYER Reliable data delivery Includes LLC and MAC sub-layers
PHYSICAL LAYER Physical characteristics of the network media

TCP/IP

The TCP/IP model is commonly described as a four-layer model. It can be compared to the OSI model as follows:

OSI LAYER		**TCP/IP LAYER**	
7	Application	4	Application
6	Presentation		
5	Session		
4	Transport	3	Transport
3	Network	2	Network
2	Data Link	1	Link Layer
1	Physical		

The Layers of the OSI Model and Devices at Each Layer



▼ Transcript

The principals of communication are dependent on several different models. We have TCP/IP and we have OSI. OSI is an international standard 7498. It does the Open Systems interconnect model. That describes communication through seven distinct layers. Each layer has it's own function. Let's see, for example, if Alice has a message she needs to send to Bob. She writes that message in a format that can be transmitted across a network. Let's say, for example, she chose to use an email and she uses some type of email application. For example, Outlook. She writes the email and when she's done, she hits send. It then is passed to the application layer, the top layer of the seven layers of the OSI stack. It's important to remember that the application layer is not the application itself, it's the interface to the application, and when it receives that message to be transmitted, it knows this gonna be sent across a number of different operations until it gets to Bob. When it is received by the application layer on Bob's machine. It needs to know is this supposed to go to his browser? Is it suppose to go to a FTP server or is it suppose to go to his mail server? And therefore, the application layer here on Alice's machine is going to put an application header on there that will be used by the peer layer on Bob's machine. So when it receives this, it knows that his email and will be sent to his email engine. The application layer has now done it's job and passes the message down to the presentation layer. The presentation layer takes the data received from the higher layer, the application header and the message and ensures that's it's in the correct format to be transmitted. For example, sometimes we had to do changes in format from ASCII to EBCDIC or we did compression or decompression with MP3s. Or for example, with an email, if we're going to send a JPEG, one of the problems is that JPEGs don't transmit well through email. So we convert it into a format that can be transmitted, but then we need to have that header on the packet so that at the far end, Bob's application is able to turn it back into the correct format so that it can be processed by the application layer and the presentation layer would take this JPEG, convert it back and pass it across. We than have the session layer. The session layer is where we would log in or we'd manage the session information. Now since this is an email, we don't really have a session identifier, but if this was a TLS session or if we was logging into an FTP server, we'd put a header on here that would indicate the session information, because Bob, say for example, if he was a bank, could have hundreds of different sessions set up at the same time and that session information would be necessary for him to be able to associate this packet with the correct banking session. The next layer down is the transport layer. The transport layer is where we take quite a difference in how we handle the communication because now we are passing it down from preparing it to be sent to actually transmitting the data and the transport layer uses pretty much two main protocols. TCP and UDP. When it receives the information from the session layer, it puts on a TCP header. The TCP header ensures the traffic will make it all the way to the far end and it worries about things such as, for example, the delivery of that information so that none of the packets were actually lost in transport. It also worries about windowing. To ensure that we don't send too much traffic at once, the traffic can be received by Bob and processed. If we send too much, then Bob will start losing some of that traffic. So using windowing, we ensure that Alice never transmits more data than Bob can actually process. So TCP makes up for some of the weaknesses in the lower layers of the model. The network layer is the next layer down, and the network layer takes the information from the transport layer and adds on the logical address which, for us, is usually based on internet protocol or IP. It then passes the information to the datalink layer. The datalink actually provides the true address. We can say here that it takes the IP address and it associates it then with a datalink address and that datalink is the address of the next device along the network. For example, from your laptop, the datalink address would be that of the wireless access point. For the wireless access point, we'd put on the datalink address of the firewall. For the firewall, the datalink address of the router and, of course, across all the various routers and switches until it was received by Bob. Transmitting it then across various types of physical media. The physical media consisting of fiber, copper, or wireless. It goes through a number of steps here until it is received finally by the datalink layer on Bob's machine. The datalink layer then removes the datalink address or header for the last time. It's not gonna be needed anymore and passes it up to the network layer. The network layer receives it and removes the IP address that is no longer going to be needed and passes it up to the transport layer. The transport layer sends back in acknowledgement that the packet has been received and removes the transport header. Passes it to the session layer and so on until finally the message itself is sent to the correct location on Bob's machine. OSI describes all of the individual parts of a communications process so we understand the individual activities happening at each layer and encapsulates the data so that the other layers don't have to worry about the functions of a higher layer within the stack.

Layer 1: The Physical Layer

Layer 1 of the OSI model defines the physical nature of a connection. This includes the type of medium being used (copper, fiber, coax, microwave, free space optical, etc.). Data passed to Layer 1 from Layer 2 are converted into a stream of 1s and 0s as defined by the medium being used.

L1 devices include Repeaters (Regens), Amplifiers, and HUBs. Repeaters regenerate the 1 or 0 bits received and send them back out. These are used to help propagate the signal further down the transmission medium. Amplifiers will simply attempt to boost the energy level of the signal received and in some cases can inject errors into the bit stream. Neither device provides for any form of error detection, correction, or notification.

If two nodes on a network begin transmitting at the same time, they will corrupt the data and cause what is known as a collision. When a collision happens, the transmitting devices need to wait and attempt again.

Layer 1 is sometimes referred to as a Collision Domain.

Layer 2: The Data-link Layer

Layer 2 (L2) of the OSI model provides node-to-node transfer of data. This is a direct link between two directly connected devices on a network. Nodes are identified with a unique hardware address. L2 will take the stream of 1s and 0s from Layer 1 (L1) and convert them into a data frame. L2 will also validate the data from L1 and assure the data is correct. In some cases, L2 may be able to fix certain received bit errors. L2 also defines and manages flow-control between the two nodes.

L2 devices include Bridges and Switches. A Bridge or Switch will receive the entire L2 Frame, perform basic error detection, and forward the Frame out the appropriate interface(s). Bridges do NOT route frames, they only forward frames based on a very limited set of criteria.

There are three types of L2 frames: Unicast, Multicast, and Broadcast.

A Unicast frame has a specific destination address, in other words if on a network there are 4 nodes, A, B, C, D, and if Node A wished to send a frame to Node C, then it could do so by creating a Unicast frame with the Source Address being A and the Destination address being C. Generally, none of the other nodes would process this data unless another node had been set into promiscuous mode, then it would capture all traffic. This can be helpful for an administrator trying to analyze traffic or for an attacker trying to capture network traffic.

A Multicast frame has as its destination address a special group address. For example, Node A could send a Multicast frame to all Bridges on a network. In this case, each bridge on the network would process the frame, whereas each client workstation would ignore the frame.

A Broadcast frame has its destination address set to all ones “FF:FF:FF:FF:FF:FF”. All nodes will receive and process a frame sent to the Broadcast address.

L2 frames are bounded by Layer 3 (L3) devices. In other words, an L2 frame does not go past an L3 device.

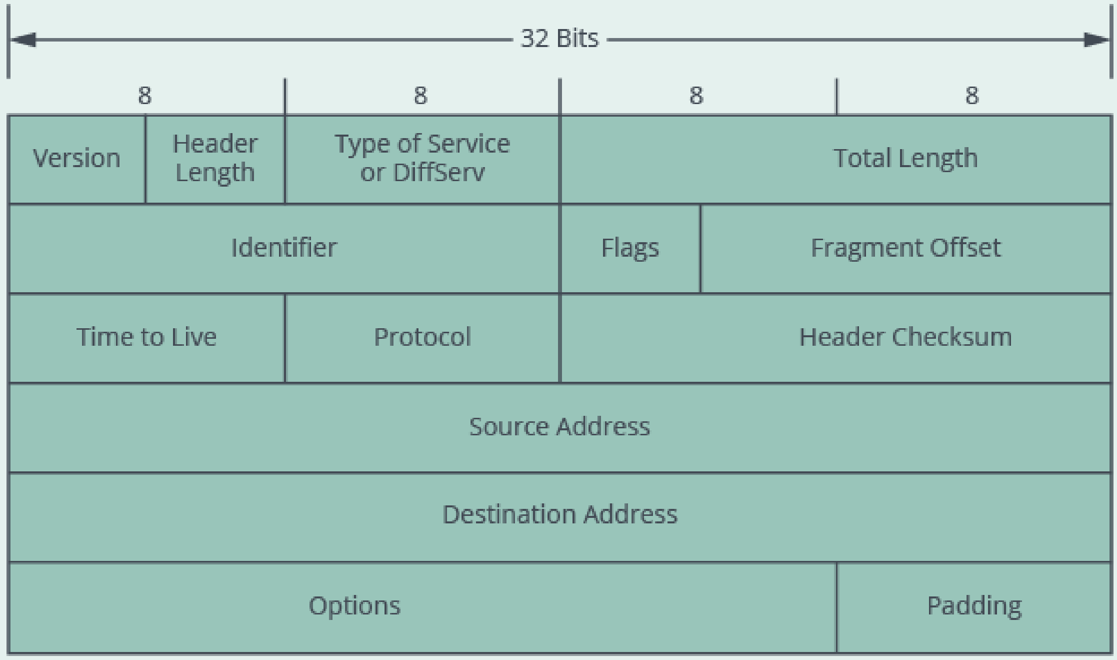
L2 is sometimes referred to as a “Broadcast Domain.”

Layer 3: The Network Layer

Layer 3 (L3) of the OSI model uses logical addressing to identify nodes on a network. It is important to understand that the addressing used in L3 is different than that used in L2. Message delivery at

L3 is not necessarily guaranteed to be reliable. Some of the various protocols at L3 include; IPv4/IPv6, RIP, IPsec, ICMP, IGMP, IPX, and others.

In today's global communications world, one of the most important L3 protocols is IPv4/IPv6. IP is part of the TCP/IP suite of protocols. IP provides for the logical addressing of nodes on a network, thus allowing packets to be sent through one or more networks to a destination node. In addition, IP provides for the ability to fragment packets so that they conform to L2 payload size requirements. IP is a connectionless protocol and does not guarantee delivery.



L3 devices typically are called Routers. Even a "Layer 3 Switch" is a router. Routers look at the destination IP address and make a routing or forwarding decision based on information contained in that router's local routing table. The local router's routing table defines the "next-hop" the packet needs to take. If no route exists in the local router, the router may use a "default gateway," a generic next-hop. If no default-gateway exists, the router will drop the packet. If a packet is destined for a faraway network, there may be multiple routers between the source node and the destination node. Each router passed through is called a hop.

Layer 4: The Transport Layer

Layer 4 (L4) creates an end-to-end connection between nodes. Within the TCP/IP suite the two common protocols are UDP (User Datagram Protocol) and TCP (Transmission Control Protocol).

UDP (defined in RFC-768) does not require that prior communications between nodes exist, or that a channel has been agreed to or set up. Thus UDP is a "connectionless protocol." UDP provides for data integrity via a checksum mechanism but does not provide for any method to detect lost packets, packets out of order, or duplicate packets.

Bits

0 **16**
31

SOURCE PORT NUMBER	DESTINATION PORT NUMBER
LENGTH	CHECKSUM

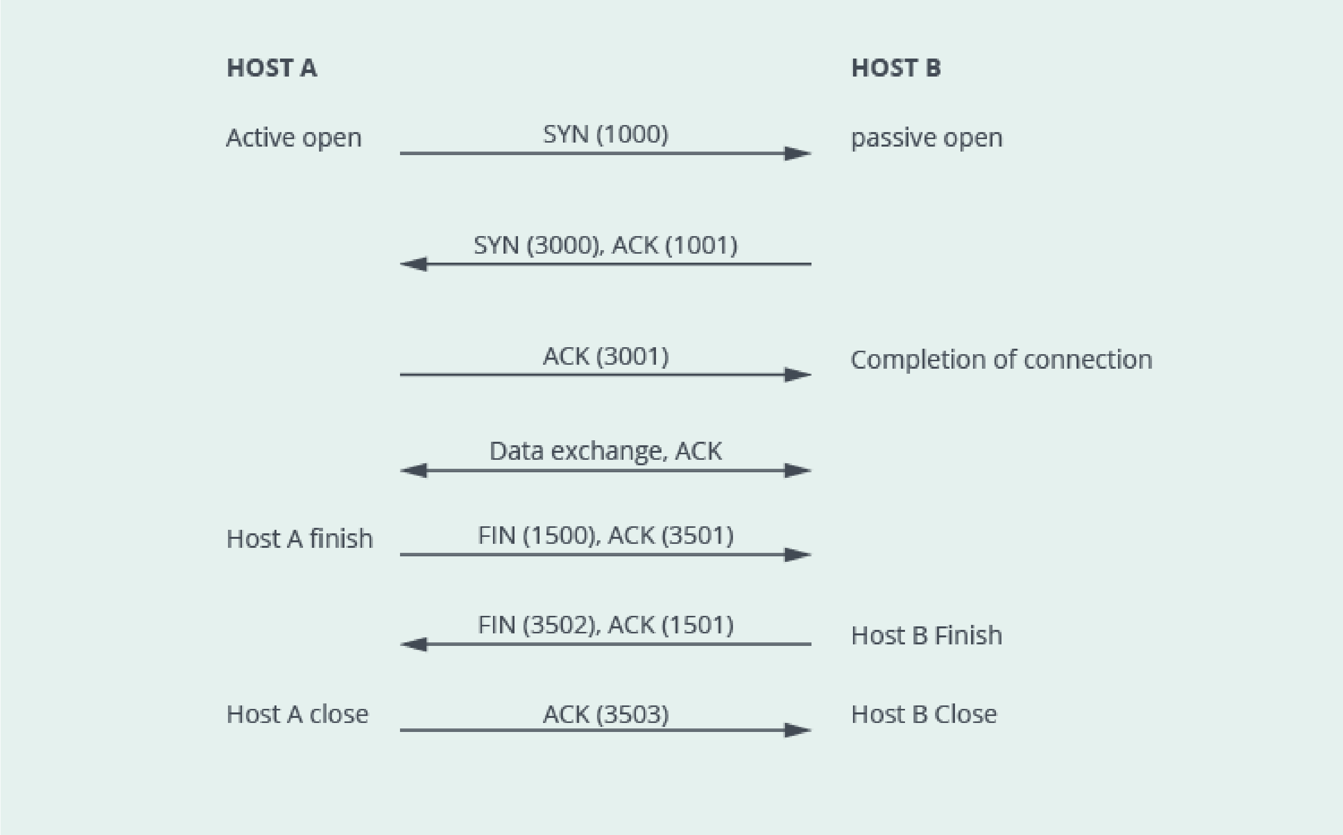
UDP is often used where the application program handles errors and thus removes the performance impact at L4 for such checking. Time-sensitive applications also use UDP because the loss of a packet is more acceptable vs. waiting for the packet to be re-sent. An example of a typical UDP application would be VoIP, real-time streaming, etc.

TCP or Transmission Control Protocol (defined in RFC-675, RFC-793, RFC-1883, RFC-2460, and many more) does require that prior communications and acceptance between nodes exist before user data can be transmitted. Thus, TCP is a "connection-based protocol". TCP is a complex protocol with many enhancements added over its many decades of service. At the heart of the protocol is what is known as the "Three-Way Handshake."

Bits

0 **8** **16**
31

<table>
<tr><td colspan="3">Source Port</td><td colspan="2">Destination Port</td></tr>
<tr><td colspan="5">Sequence Number</td></tr>
<tr><td colspan="5">Acknowledgment Number</td></tr>
<tr><td>Data Offset</td><td>Reserved</td><td>Code</td><td colspan="2">Window</td></tr>
<tr><td colspan="3">Checksum</td><td colspan="2">Urgent pointer</td></tr>
<tr><td colspan="4">Options</td><td>Padding</td></tr>
<tr><td colspan="5">Data</td></tr>
</table>


HOST A
HOST B
Active open
SYN (1000)
passive open
SYN (3000), ACK (1001)
ACK (3001)
Completion of connection
Data exchange, ACK
Host A finish
FIN (1500), ACK (3501)
FIN (3502), ACK (1501)
Host B Finish
Host A close
ACK (3503)
Host B Close

The Upper Layers

The lower layers process the transmission of the data while the upper layers prepare the data for transmission.

Layer 5 Session

Layer 5 establishes the session between the two parties that are communicating. Some protocols do not need a session such as email since it is asynchronous, but others such as https use a session to identify the packets that belong to an established connection.

Layer 6 Presentation

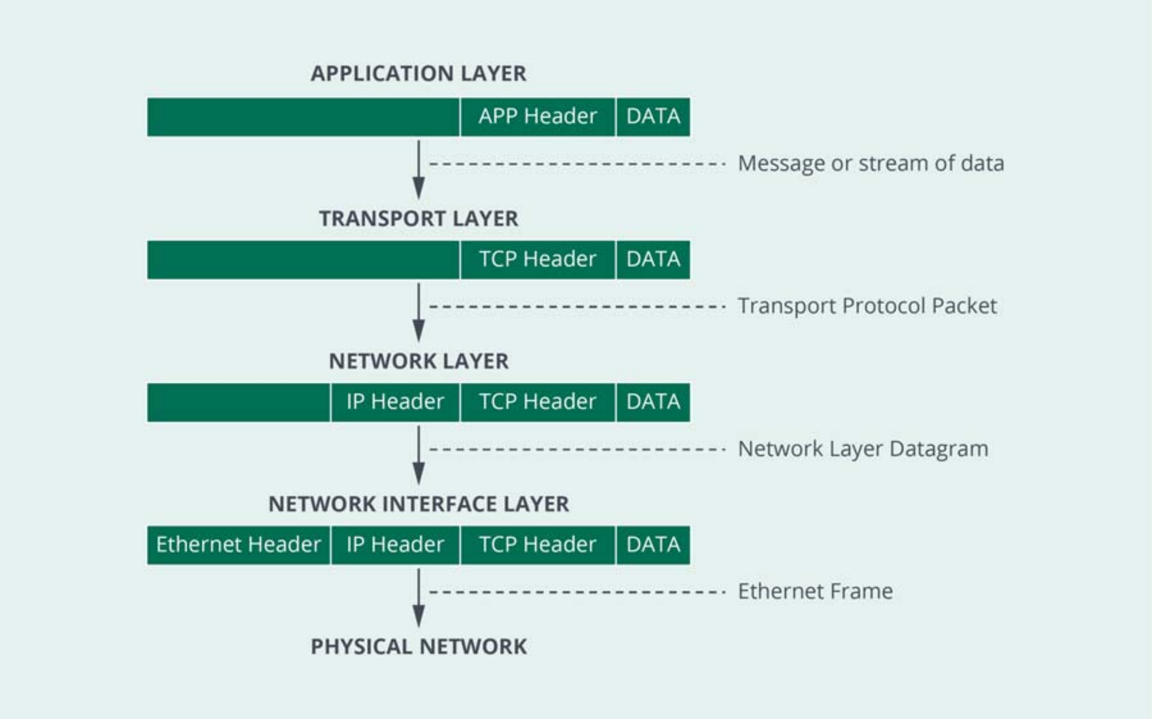
Layer 6 prepares a message for transmission and ensures it is in the correct format. This would include converting ASCII to EBCDIC, or doing compression or decompression on a message.

Layer 7 Application

The application layer is the interface to the application being used by the sender and receiver; for example, the interface that would accept an email from the sender's email software and then prepare it to be processed by the receiver's email engine.

Building a Packet

As a message is sent through the layers of the stack, headers are added on to prepare it to be routed and handled efficiently. This diagram shows the building of a packet.


APPLICATION LAYER
APP Header
DATA
Message or stream of data
TRANSPORT LAYER
TCP Header
DATA
Transport Protocol Packet
NETWORK LAYER
IP Header
TCP Header
DATA
Network Layer Datagram
NETWORK INTERFACE LAYER
Ethernet Header
IP Header
TCP Header
DATA
Ethernet Frame
PHYSICAL NETWORK

Summary

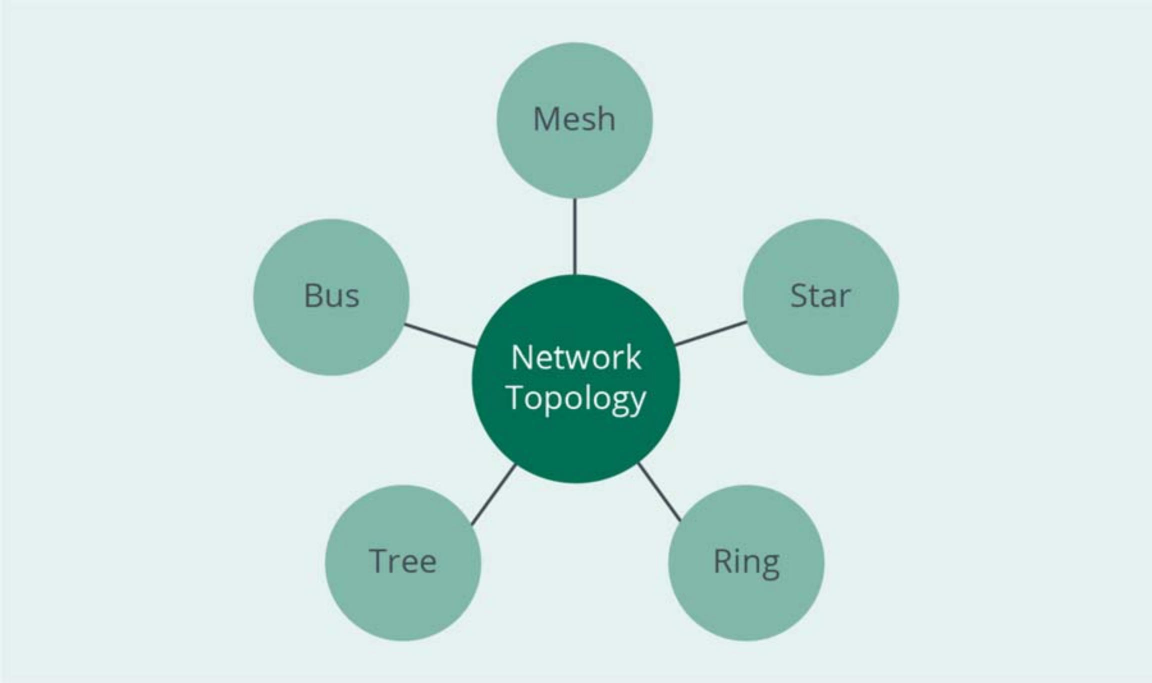
The use of the OSI and TCP/IP models help define the process of communications by breaking it into individual steps. Each layer has a specific function, and each layer interfaces with the other layers according to a defined format.

Transmission Overview

There are many ways to communicate using various medium and topologies. Each medium has advantages and disadvantages, and the choice of medium is often based on factors such as cost, bandwidth, operational environment, and security.

Network Topographies and Relationships

Networks typically have one or more topographical forms depending on the specific performance needs of the network.

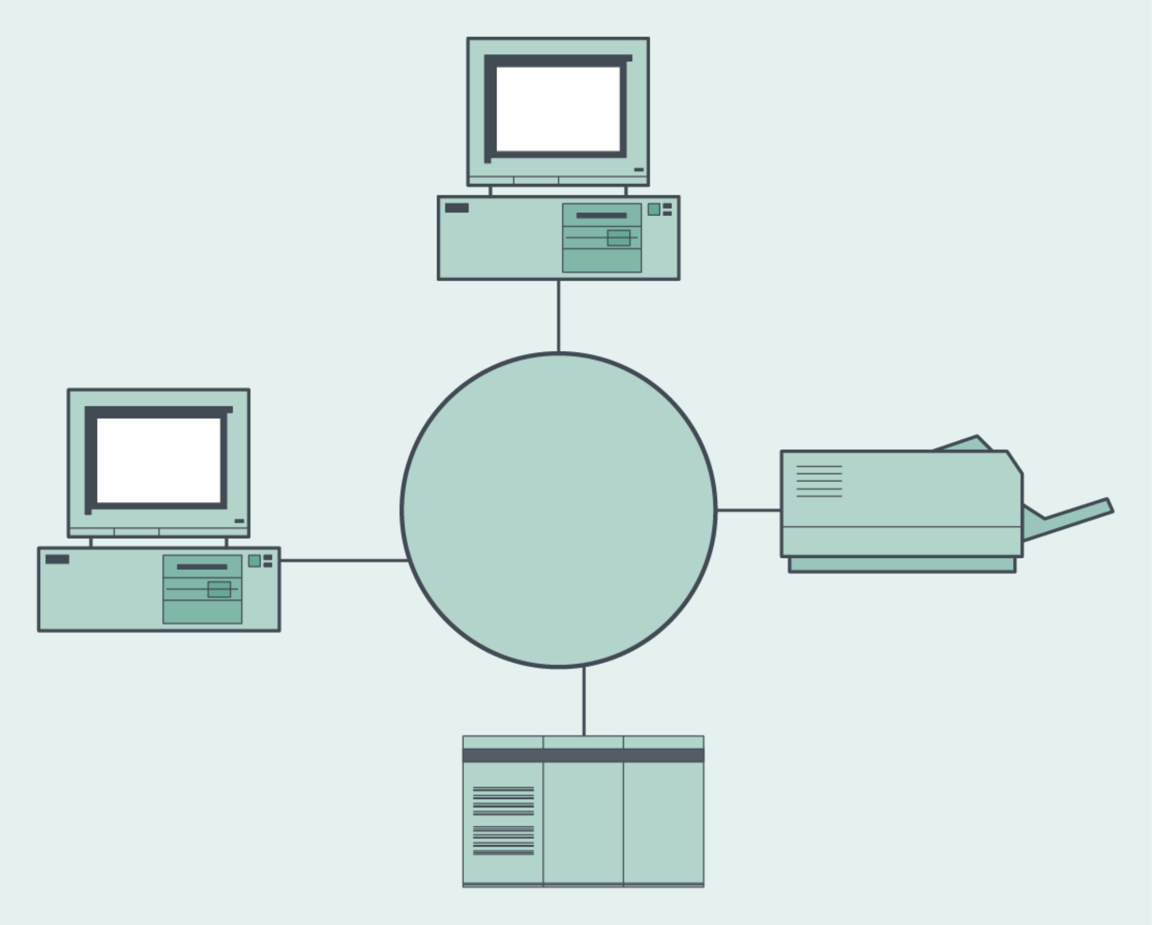


Topographical Models

These topographical forms include:

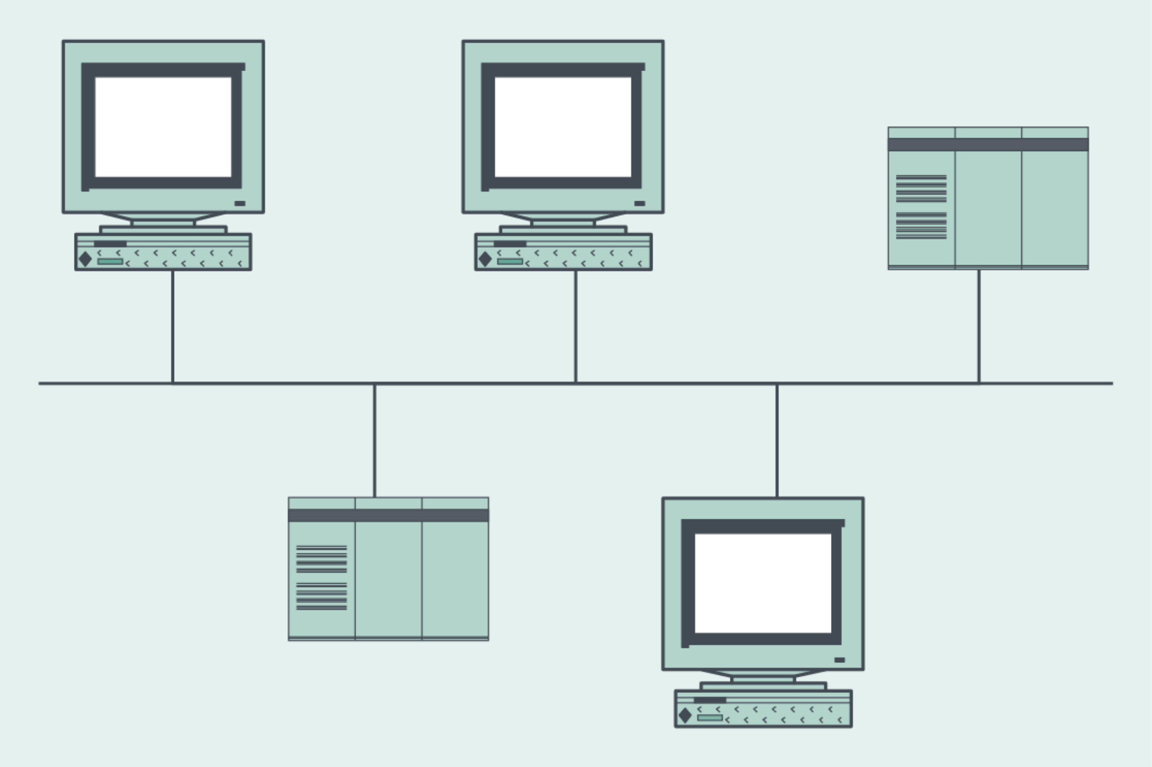
Ring

A Ring topology is a bus topology network that is a closed loop. Data traverses around the ring in a particular direction (clockwise or counterclockwise) and passes through each node. Each node on the ring retransmits the signal, which helps to keep the signal strong. If a node fails, it disconnects from the nodes to its left and right, and the topology heals. As workload increases, a Ring will scale better to handle the workload.



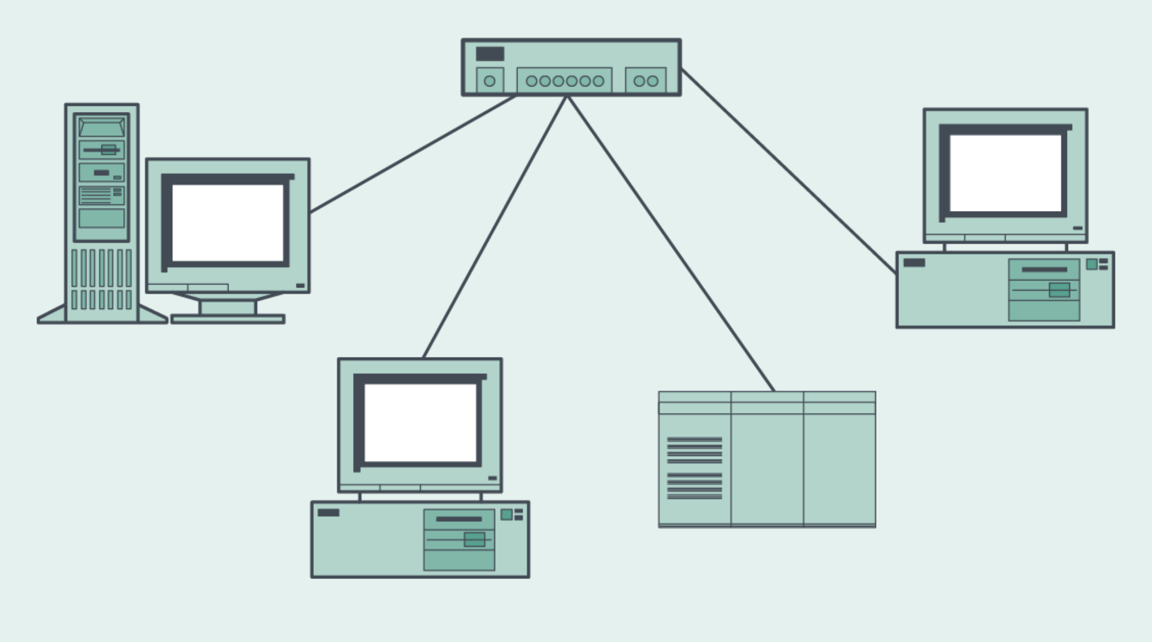
Bus

A Bus topology is made up of a single backbone cable in which each node is connected to this backbone cable. When a node wishes to send data, data is sent in both directions up/down the backbone cable. Should there be a failure (cable cut for example), then the data to all nodes will be impacted. This is a critical single point of failure for this topology.



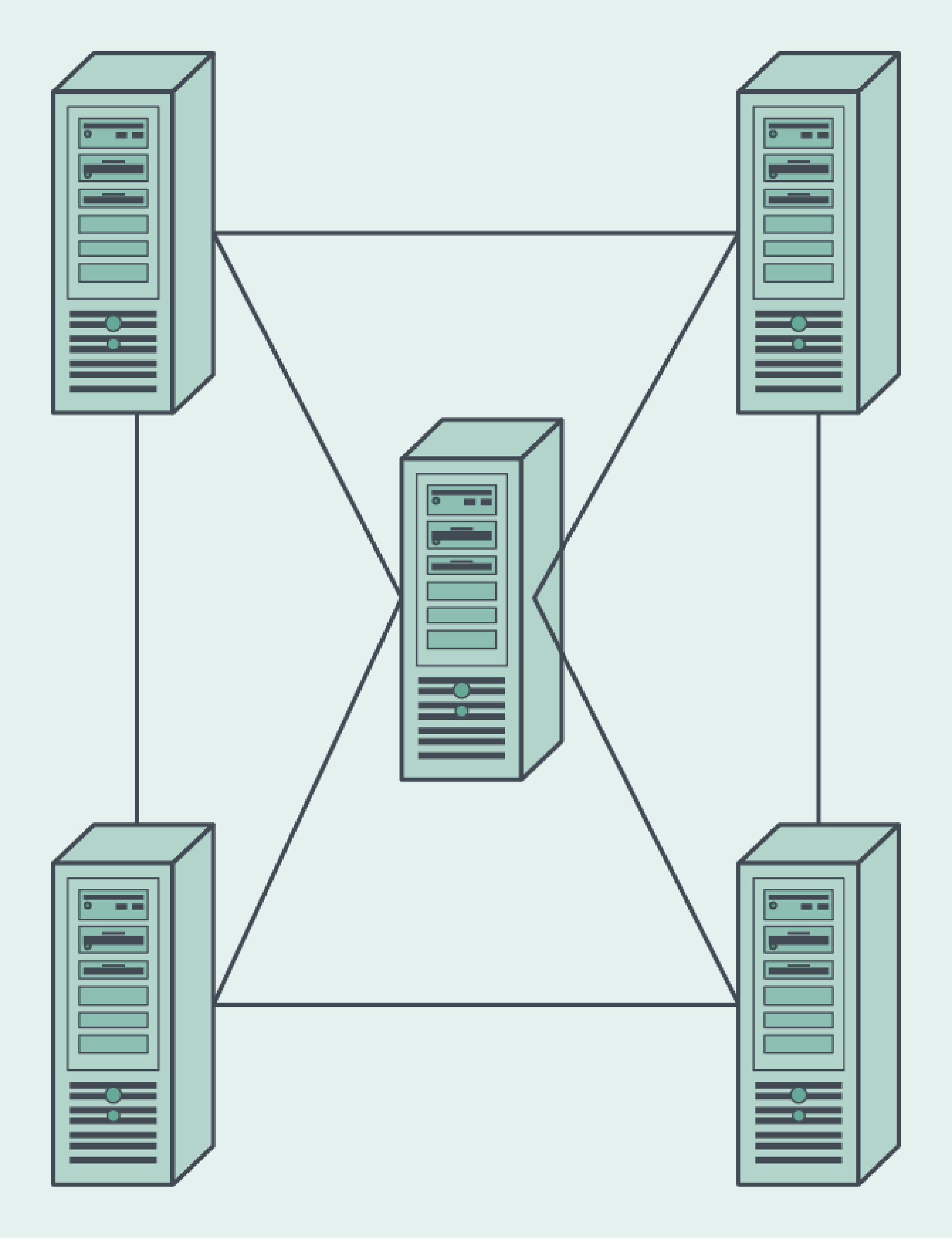
Star

A star topology is based on a single switch that every device connects to. The switch passes data between ports directly instead of propagating the data to every device like a bus topology does. The switch can also be connected to other switches, creating a tree. A switch failure is the single point of failure for this topology.



Mesh

A mesh network is used when high availability is required. Each device is connected to multiple other devices, thereby avoiding a single point of failure. This is an expensive option but will survive the loss of one or more nodes.



Commonly Used Ports and Protocols

When establishing connections between hosts, four identifiers are used to identify the specific connection: Source IP, Source Port, Destination IP, and Destination Port.

Within the TCP/IP protocol suite, a **port** number describes the endpoint process or daemon in the operating system. A port is identified by an unsigned 16-bit number, commonly known as a **port number**. When writing a network address containing a port number, the format is 192.0.2.10:80. The colon separates the IP address from the port number. In this example the port number is 80 (decimal).

The IANA (Internet Assigned Numbers Authority) is the responsible party for maintaining the registration of commonly used port numbers for well-known Internet services.

Port numbers range from 0 to 65535 and are broken down into three groups:

[Source RFC 6335]

Well-Known Ports:	port numbers between 0–1023
User Ports aka Registered Ports:	port numbers between 1024–49151
Dynamic/Ephemeral/Private:	port numbers between 49152–65535

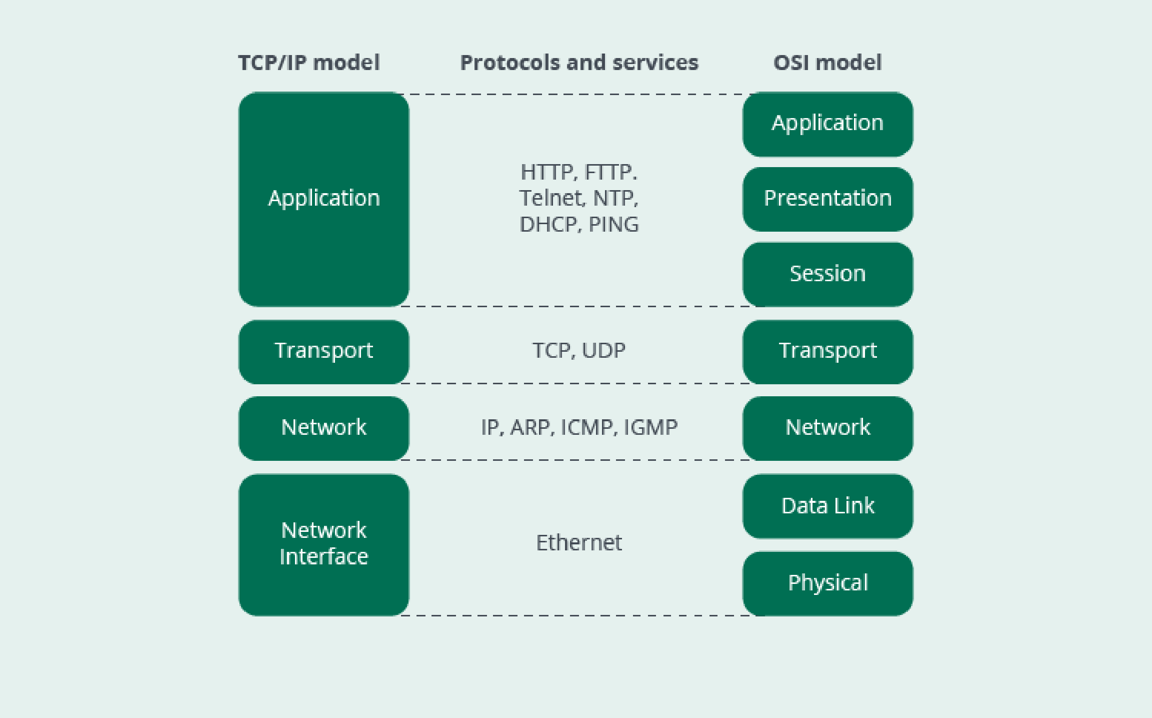
Well-known ports include:

20 and 21	FTP, File Transfer Protocol
22	SSH, Secure Shell
23	Telnet
25	SMTP, Simple Mail Transport Protocol
53	DNS, Domain Name System

80	HTTP, Hyper Text Transport Protocol
123	NTP, Network Time Protocol
443	HTTPS, Hyper Text Transport Protocol/Secure

Registered ports include:

1433/1434	MS-SQL Server
5060	SIP, Session Initiation Protocol (VoIP and more)



TCP/IP model	Protocols and services	OSI model
Application	HTTP, FTTP. Telnet, NTP, DHCP, PING	Application Presentation Session
Transport	TCP, UDP	Transport
Network	IP, ARP, ICMP, IGMP	Network
Network Interface	Ethernet	Data Link Physical

The Dynamic port range is used for short-lived connections, connections from a client to a server and will (at this time) never be assigned to a specific function or service.

It is important to note that just because a packet is using port 53, it does **not** mean that the traffic is actually DNS. Some years ago, a country attempted to ban VoIP by requiring all service providers to block port 5060. Everyone avoided the blocked port 5060 and just moved SIP / VoIP over to port 53. Since port 53 was also used for DNS, the destination server ultimately decided on if it was DNS or VoIP. Thus when building firewall rules, do not just assume that all port XX is in fact that type of traffic.

Control Network Access

Access control and monitoring (NAC, remediation, quarantine, admission)

Access to network resources can be controlled at various levels. Typically, one thinks of username/password as the control point. This permits or denies access based on user credentials; however, this does not control a device.

Access control based on the actual device is also highly useful. If a user brought their own laptop into the office and connected it to the network, then with their username / password, they could connect and download confidential data to their laptop. To prevent this, access control can also be extended to the device. If the device is not specifically listed, then no matter what the users' credentials are, that unapproved device cannot connect to the network.

This can be extended to prohibit devices that have not been scanned recently for viruses or do not have certain company software loaded on them.

Ports that are accessed with unapproved devices can then lock out the port and prohibit any further connection until IT concludes it is safe to unlock the port again.

Access control standards and protocols (IEEE 802.1X, Radius TACACS)

IEEE 802.1X

The IEEE (Institute of Electrical and Electronics Engineers) 802 is a family of standards that focus on networks that carry variable sized packets. IEEE 802.3 defines Ethernet, and 802.1 defines “Higher Layer LAN Protocols” such as bridging.

IEEE 802.1X defines PBNAC (Port Based Network Access Control). 1X provides an authentication method to allow devices to connect to a LAN or WLAN (Wireless LAN).

1X is broken down into three parties: A Supplicant, An Authenticator, and an Authentication Server.

The ***Supplicant*** is the device (such as a desktop, laptop, tablet computer) that wants to connect to the LAN/WLAN.

The ***Authenticator*** is the network device, such as a switch or a wireless access point.

The ***Authentication Server*** is a server running RADIUS or similar and supporting EAP (Extensible Authentication Protocol).

The supplicant is not allowed to connect to the network until the supplicant's identity has been validated and approved. The supplicant can provide credentials in a number of different forms, including username / password or digital certificate. The credentials are then forwarded to the Authentication Server for validation and approval.

There have been several revisions to the 802.1X protocol, most notably to resolve several security risks. For example: Once a device has been authenticated and approved to connect to the network, no further checks are done. Thus, it is possible to gain access to a port after the authentication is completed.

RADIUS (Remote Authentication Dial-In User Service) RFC 2865.

RADIUS provides centralized AAA (Authentication, Authorization, and Accounting) services for user who connect to various network devices. RADIUS was originally developed by Livingston Enterprises, Inc. in 1991 and was later adopted as an IETF standard. RADIUS is a client/server protocol that runs at the application layer and can use either UDP or TCP for transport. RADIUS provides more than just user authentication. With RADIUS, the network administrator can control a number of other policy attributes. For example: Mary can login, but a dynamic ACL is created that limits Mary access to certain network resources. Later John can connect on the same port but will have different access rights. RADIUS enjoys wide support and is the choice for other technologies such as IEEE 802.1X, VoIP and other services that need access control. Because RADIUS is widely accepted, it is often the target of attackers. Therefore, RADIUS systems must be well protected and backed up.

TACACS (Terminal Access Controller Access-Control System) RFC 927 and RFC 1492

TACACS was originally created in the mid-1980s and used for communicating with an authentication server. Originally developed by BBN Technologies, it was used to run the unclassified network known as MILNET for DARPA. Cisco Systems began using TACACS in its networking products and added several extensions. TACACS+ is a new version of the protocol that is not backwards compatible with TACACS. Unlike RADIUS, TACACS+ uses TCP for transport and thus does not have to build its own transmission control features into the protocol. Also, TACACS+ encrypts all data sent and thus is not as vulnerable to certain types of attacks as RADIUS is.

Summary

The design, installation, and operations of networks is an important role for the security practitioner. Networks provide critical infrastructure needed to support reliable business operations. A network should be designed to be resilient to failure and robust enough to continue to operate in adverse conditions.

Service Models Overview

Networks are the foundation of nearly every business process today. Without reliable networks, many business operations, departments, and objectives would be unable to function.

Network reliability requires a strategy to design and build an architecture free from single points of failure and protected from common attacks.

Network Attacks

Network security has two primary areas of focus: protecting the network itself from attack; and ensuring the network is not used to attack devices connected to the network.

Networks are often expected to operate with extremely high levels of availability—perhaps as high as 99.999% (5 nines) availability, where even a few seconds of outage per month would not be acceptable. This requires redundancy. Redundancy includes duplication of cabling and network devices, such as routers. A common problem is where duplicate network cabling still runs in the same conduit, leaving both cables susceptible to being cut or damaged at the same time. Redundant network devices need to be installed on separate racks with separate power supplies.

Networks are also susceptible to sniffing or eavesdropping, where an attacker can listen into (capture) traffic on the network. The attacker may conduct this as a passive attack where the attacker only captures traffic for analysis but does not alter or affect the traffic. An active attack is where the attacker alters (modifies) the traffic perhaps by inserting, deleting, or modifying the data on the network. Running a port scan is an example of an active attack since the scan injects traffic onto the network.

Networks can be protected through the use of many different devices such as Firewalls, Gateways, Intrusion Detection and Intrusion Prevention Systems (IDS/IPS), and router configurations. The security practitioner needs to ensure that network devices are configured correctly and hardened to resist attacks. Hardening disables all unnecessary services and features that could present an additional attack surface for an attacker to exploit.

Protocol-based Attacks

Networks communicate through the use of protocols that define the structure of network communications. Many protocols in use today have identified vulnerabilities that can be exploited by an attacker. This lack of security is due to the focus on communications and function during the development of the protocols without considering the risk of a person misusing the protocols to disable network function.

Physical Layer

The risk at the physical layer is primarily related to the theft of equipment (cabling, repeaters, etc.,) and damage to cabling or radio wave jamming. This risk of cable damage may be reduced by placing cable into conduit to protect it from accidental damage. Cable locators can avoid damage to cable by construction crews. It is also important to lock wiring closets and telephone rooms in buildings to prevent unauthorized access.

The choice of communications medium is also important. All communications are subject to attenuation if the cable runs are of an excessive length. When cabling must run in an area of high electromagnetic interference, the use of fiber optics cable is preferable. Shielded cable may also prevent interference from external radio or electromagnetic interference. Twisted cable break up the electromagnetic fields created when an electrical current flows over a cable thereby preventing crosstalk.

DataLink Layer

The DataLink layer connects two adjacent devices on a network. This requires using the MAC (Media Access Control) address of the two adjacent devices for transmitting the traffic between the devices. The MAC address will be cross-referenced with the logical address (the assigned Internet Protocol (IP) address), using Address Resolution Protocol (ARP). ARP is a noisy protocol that calls out to the devices on the network to learn which device is currently associated with a particular IP address. The correct device should reply back, and the response is then recorded in an ARP table so that subsequent traffic can be routed to the correct device. However, poisoning the ARP table can allow an attacker to capture data intended for another person/device.

Wireless communications operate at the DataLink layer, and these are subject to interference by blocking the signal, or jamming by flooding the channel with other traffic or noise.

IP Attacks

Internet Protocol is the primary method of communicating over many networks today. Currently most of the traffic is based on Internet Protocol version Four (IPv4). IPv4 was not built with security in mind and is subject to a wide range of attacks. It is relatively simple to spoof an IP originating address so that traffic from an attacker would appear to come from another address altogether. IP is also subject to overlapping fragments, teardrop, final fragment, and LAND attacks. Most of these attacks were intended to cause a denial of service where the victim's equipment would be disabled or suffer degraded performance.

The Internet (Network) layer also uses protocols such as ICMP (Internet Control Message Protocol) to verify connectivity between devices on a network. This protocol has been misused in several ways over the years as the Ping of Death and SMURF attacks. An attacker can use ICMP to map out a network and trace the route traffic may take as it traverses a network. The transition to IPv6 was intended to prevent many attacks associated with IPv4.

Transport Layer

The transport layer is also subject to attacks such as SYN Flood, FIN, TCP half-open and Fraggle. These attacks can be used to disable a victim's systems, perhaps as a part of a botnet or Distributed Denial of Service (DDoS) attack.

Application Layer Attacks

The application layer in the TCP/IP model includes the Session, Presentation, and Application layers of the OSI model. There are many attacks at these layers related to the choice of weak or insecure protocols such as SNMP v1 and v2, TFTP, and SMB.

The security practitioner should ensure that the secure protocols are chosen for network communications or that they are run over a secure channel (tunnel) such as IPSec to protect them.

Domain Name System (DNS)

For most people, the Internet would not work without the domain name system. The Internet operates on IP addresses, not on domain names. The domain www.isc2.org is associated with an IP address that is required for routers to route the traffic. The DNS system is the cross-reference tool used to provide the IP address and other data needed to route the traffic. The DNS record for www.isc2.org is as follows as shown by whois:

```
Domain Name: ISC2.ORG
Domain ID: D4518149-LROR
Creation Date: 1996-11-12T05:00:00Z
Updated Date: 2015-02-12T18:59:13Z
Registry Expiry Date: 2022-11-11T05:00:00Z
Sponsoring Registrar: GoDaddy.com, LLC (R91-LROR)
Sponsoring Registrar IANA ID: 146
WHOIS Server:
Referral URL:
Domain Status: clientDeleteProhibited --
http://www.icann.org/epp#clientDeleteProhibited
Domain Status: clientRenewProhibited --
http://www.icann.org/epp#clientRenewProhibited
Domain Status: clientTransferProhibited --
http://www.icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited --
http://www.icann.org/epp#clientUpdateProhibited
Registrant ID: CR164721558
Registrant Name: Registration Private
Registrant Organization: Domains By Proxy, LLC
Registrant Street: DomainsByProxy.com
Registrant Street: 14747 N Northsight Blvd Suite 111, PMB 309
Registrant City: Scottsdale
Registrant State/Province: Arizona
Registrant Postal Code: 85260
Registrant Country: US
Registrant Phone: +1.4806242599
Registrant Phone Ext:
Registrant Fax: +1.4806242598
Registrant Fax Ext:
Registrant Email: ISC2.ORG@domainsbyproxy.com
Admin ID: CR164721560
Admin Name: Registration Private
Admin Organization: Domains By Proxy, LLC
Admin Street: DomainsByProxy.com
Admin Street: 14747 N Northsight Blvd Suite 111, PMB 309
Admin City: Scottsdale
Admin State/Province: Arizona
Admin Postal Code: 85260
Admin Country: US
Admin Phone: +1.4806242599
Admin Phone Ext:
Admin Fax: +1.4806242598
Admin Fax Ext:
Admin Email: ISC2.ORG@domainsbyproxy.com
Tech ID: CR164721564
Tech Name: Registration Private
Tech Organization: Domains By Proxy, LLC
Tech Street: DomainsByProxy.com
Tech Street: 14747 N Northsight Blvd Suite 111, PMB 309
Tech City: Scottsdale
Tech State/Province: Arizona
Tech Postal Code: 85260
Tech Country: US
Tech Phone: +1.4806242599
Tech Phone Ext:
Tech Fax: +1.4806242598
Tech Fax Ext:
Tech Email: ISC2.ORG@domainsbyproxy.com
Name Server: NS3.P05.DYNECT.NET
Name Server: NS1.P05.DYNECT.NET
Name Server: NS2.P05.DYNECT.NET
Name Server: NS4.P05.DYNECT.NET
Name Server:
DNSSEC: signedDelegation
DS Created 1:2015-02-12T18:59:12Z
DS Key Tag 1:45922
Algorithm 1:5
```

```
Digest Type 1:1
Digest 1:A8A7BA429A3B965421B6662234E303B79E039A01
DS Maximum Signature Life 1:1814400 seconds
DS Created 2:2015-02-12T18:59:12Z
DS Key Tag 2:30589
Algorithm 2:5
Digest Type 2:1
Digest 2:9BFB97561AB98F76417178E07F74144E273D0D37
DS Maximum Signature Life 2:1814400 seconds
```

Extract from whois.net/icann.org

As can be seen, this domain is registered through a proxy service that hides some of the information about the domain. The owner of the domain is responsible to ensure that the domain registration is kept current and not allowed to lapse. Any organization that wishes to register a name associated with a new product or service should register the name as soon as possible to prevent someone else from registering the name first. This type of attack (pharming) can cost the organization a lot of money and time in regaining the name.

Traffic Shaping

Traffic shaping is used to throttle or control the flow of network traffic by allowing higher priority packets to have precedence. This practice would hold back or relay lower priority traffic. The problem with this is when a large Internet Service Provider (ISP) restricts the traffic of a competitor or reseller. This may lead to a two-tiered network model where preferential service is granted to a customer for an additional fee and interfere with the concept of net neutrality that discourages such practices.

There are advantages to using traffic shaping in the corporate environment since it can grant preference to business-related traffic over casual Internet surfing or non-essential communications. If an organization is seeing network congestion due to streaming media usage, then traffic shaping may help manage network traffic flows in a way to support the business. The risk, however, is that traffic shaping may slow down and affect other streaming types of traffic that should receive priority, such as voice-over IP (VOIP).

Network Architectures

Network segmentation is an important part of network security. Segmentation restricts access between domains, allowing sensitive data in a more secure domain from being accessed by personnel that have access to a less secure domain. For example, a customer may access the web application of the organization, which is hosted on a web server located in a transitional subnet commonly known as a Demilitarized Zone (DMZ). This area is accessible to outsiders and subject to being overrun or compromised; therefore, no sensitive data should be kept in a DMZ. Any process that needs to execute from within the DMZ to retrieve data from the internal network should be subject to careful controls and whitelisting. Whitelisting would only permit pre-approved processes to access the internal networks from the DMZ.

The DMZ is an example of an extranet (an external network segment) placed “outside” of the organization’s internal systems and networks. It can be compared to the front lobby of an organization’s headquarters building. Almost anyone may be able to enter the lobby, but only trusted personnel can go from the lobby into the internal network.

Many organizations will also have an extranet used for remote workers or business partners that want to connect to the organization. An extranet usually requires some form of authentication so that only trusted persons can enter the extranet. This differs from a DMZ, since usually anyone can enter the DMZ. In the extranet, the organization may locate a VPN concentrator or other tools specifically designed to support external parties. A remote worker would connect to the VPN concentrator and from there into the internal network once they were authenticated and the traffic was secured.

Summary

The security and reliability of networks comprises a significant part of many security practitioners' responsibilities. There are many factors that need to be built into network security and management and this course is only able to scratch the surface of these areas. The security practitioner should work with network architects and administrators to incorporate security practices into network operations.

Manage LAN-based Security Overview

Separation of Data Plane and Control Plane

In the past, protocols used to control how a firewall, switch, or router handled forwarding user data packets that were also sent in the same connection as the user data.

This “In-Band” communication process created several risks: first, if the data path broke (fiber cut, bad interface card, etc.), then you also lost control over the device.; second, attackers could learn about your network and thus control it by sending their own control packets in the data flow.

This type of in-band attack isn’t new. Many years ago, hackers were able to control the national phone system by sending certain tones down the same connection as a regular phone call. This enabled them to control the phone switch equipment and thus obtain free phone calls and place calls to other places. Today the same can be done with certain routing protocols, and if an enterprises network does not protect against this, it can cause a number of security issues.

To help prevent these types of risks, today’s modern networks have split the control of our network devices away from the data forwarding parts of our network. We call these the “Control Plane” and the “Data Plane.”

The Control Plane (CP) is used to pass or signal control information to the network device, which will affect how the device forwards traffic on the Data Plane (DP).

These concepts can be leveraged within the enterprise by having a separate network communicate with the routers, switches, and firewalls for control and management purposes.

Segmentation (e.g., VLAN, ACL’s, etc.)

Networks can be segmented for a number of reasons and in a number of different ways. Network administrators may wish to segment a network based on the role, function, and resources needed for that network. For example: the sales department has different needs than the accounting department. Historically this would be done with physical networks, which required different cabling and equipment.

Over time, protocols were enhanced to allow the virtualization of these physical networks, now known as VLANs (Virtual LAN). VLANs leverage the physical network assets (cables, switches, etc.,) but insert a unique label called the VLAN ID into the packet. This tells the switches which LAN this packet is a member of. VLAN enabled switches enforce isolation between VLANs by not allowing packets of different VLAN IDs to be sent to non-member ports. Just as in a physically separated network, a Router is used to pass traffic between different VLANs.

It is important to note that if an attacker has gained access to the network, they may be able to see different VLANs depending on where they compromised the network.

ACLs (Access Control Lists) can further restrict access to LAN resources. ACLs can be applied at the host or server, switch, and router. ACLs help provide another layer of segmentation and control on the LAN.

Operate and Configure Network-Based Security Devices

Firewalls and Proxies

When building a house or a commercial structure, designers, regulators, and users want to mitigate the spread of a fire. So throughout the structure, certain types of walls are built to withstand the forces of fire. They are called “Firewalls”.

In computer networks, designers, regulators, and users want to limit external and internal access to the networks, so they install **firewalls** or **proxies**.

Different types of firewalls exist; State-less, State-full, and Deep Packet Inspection (DPI). Each has its strengths and weaknesses.

> A proxy is a type of firewall that sits in the middle between the user and the service the user is trying to access. The proxy creates two connections for each session the user is creating: one session between the user and the proxy and another session between the proxy and the service. This allows the proxy to examine the traffic between the user and the service at a much deeper level. One could say that a proxy is a management approved “man in the middle” device.

When designing firewall requirements, it is important to have a solid understanding of the organization’s needs and access requirements. Developing firewall rule-sets is an ever-evolving process that must be constantly monitored and validated. The rules you create today may not be effective tomorrow. Every time a new application, service, external source, etc. is added or modified, the firewall rules must be revalidated. Further it is critically important that firewall rules be backed up / archived so in the event of a disaster, the rules can be put back into operation as quickly as possible.

Firewall rules must take into consideration the directional flow of traffic to be controlled.

For example: You need to allow web (HTTP) traffic for your users.

A simple firewall rule of:

Permit Any equal 80 (Permit Any Source, Any Destination that is port 80 (HTTP)) would meet the requirement. However, this rule also would allow for external users to access rogue web servers or internal only web servers from the outside. This is because the rule is matching on ANY IP address for the Source or ANY IP address for the destination, as long as it has a destination port of 80 (HTTP).

A better rule would be:

Permit <Internal IP Range> Any equal 80

This rule now limits the SOURCE IP address to only those within your organization, while allowing them to connect to ANY external IP address with a destination port of 80.

Still this rule is not ideal. One should be matching on TCP state as well, such that there would have to be a SYN packet, originating from the inside network to the outside, that a SYN ACK and thus the entire three-way handshake was complete. Further there should be some form of session time-out such that if there were no traffic between the hosts, the dynamic portion of the rule would be torn down.

Attackers will poke at your network to look for holes in the rules and attempt to exploit them.

You must log your firewall rules, and review those logs to look for things that are not normal. Do not just blindly assume that it doesn't matter what packets are being blocked /dropped by your firewall. In many cases, those dropped packets can tell you about other security issues on your network. It could indicate that you have a compromised computer inside your network.

Many firewalls have an implicit "drop everything" rule at the end. It is best to have an explicit "drop everything" at the end. This helps make sure that you have complete control and visibility over what is being permitted and what is being dropped.

Firewalls can consume large amounts of processing and memory resources. Deep Packet Inspection based firewalls have much more work to do, compared to simple packet level firewalls. The security professional must also monitor the firewall and its resources to make sure that resource exhaustion does not occur and negatively impact business operations.

Attackers also know this! They will attempt to overload your firewall. In some cases, IT folks have “disabled the firewall” because it was preventing users from getting their job done. The attacker has just won!

Network Intrusion Detection/Prevention System

Intrusion Detection Systems (IDS), and Intrusion Prevention Systems (IPS) are purpose-built tools that either detect that a system has been intruded on or can attempt to prevent a system from being intruded on. IDS/IPS typically live on a host computer, a server, a workstation, etc. They are looking at the local activity.

A NIDS (Network IDS) or NIPS (Network IPS) is looking at some portion of the network and thus providing cover for the network instead of a particular host.

NIDS will evaluate network traffic flows and based on a range of configurable rules, alert IT staff of possible compromises. A NIDS does not typically try to mitigate the event. This is where a NIPS comes into place. A NIPS is similar to a NIDS but will also try to mitigate the attack by communicating with firewalls and routers to block or redirect the intruding traffic. Thus, a NIPS is both a detection and mitigation system in a single service.

The placement of a NIDS or NIPS is an important network design decision. Some NIDS / NIPS are "in-line" with the packet flow and thus could be a point of failure on the network. Other systems sit off to the side and listen to traffic via a tap or monitor port, so the failure of the system does not directly impact traffic flow.

It is recommended that console / administrative access to a NIDS/NIPS system be limited and on a separate network.

There are a great number of both open-source / community supported and commercial IDS/IPS (host or network) systems available. Which one is correct is really based on the capabilities and needs of a particular organization. Almost all IDS/IPS systems generate large amounts of log data that can overload the IT security team. Combining visualization tools to help create meaningful visualizations of events can be useful for quick responses.

Routers and Switches

Routers are a OSI Layer 3 device and are primarily designed to forward traffic between different Layer 3 networks. Given the volume of traffic, much of this forwarding decision is now done in purpose-built hardware. This eliminates bottlenecks created by having the packet forwarding decision done in software / CPU. Routers can also act as firewalls via limited ACLs (Access Control Lists); however, it is critically important to know how your specific router will handle ACLs. Does it handle them in dedicated hardware or does it pass traffic for ACL handling up to the CPU? ACL traffic going to the CPU can quickly cause CPU overload and affect the entire router. In general, routers should route. A firewall could be placed in front of, or behind, the external facing router.

Routers should have certain ACLs created to prevent and limit access to the routers control / management interface. Services not used on the router should be explicitly disabled. Services, such as RADIUS or TACAS, should be used to control user authentication to the router. Router logs should be constantly reviewed, and the IT staff should make sure that a current and correct copy of every router's configuration is maintained / updated on a regular basis.

Switches (Layer 2 or Layer 3): The above pretty much applies to them as well.

Summary

Network devices can provide excellent protection from many threats; however, they require careful configuration and monitoring to ensure they work effectively.