Client IP Parameters

The topic of addressing is fundamental to network operation and extends to all endpoints and intermediate nodes. In fact, the topic of addressing includes DHCP, DNS, and NAT topics on the CCNA exam. All network nodes whether they are endpoints or intermediate nodes are uniquely identified by one or more physical and/or logical addresses.

Each address is associated with a network interface for communication. For example, switch ports are operational with only a physical MAC address. Endpoint network interfaces on hosts have a physical MAC address and logical IP address.

Today, most IP addressing of client hosts is assigned from a DHCP server. The host sends a request for assignment of IP address along with default gateway and DNS server address. There is dynamic configuration from the DHCP server for host IP parameters. It is important to verify IP parameters are correct for normal operational state.

The host command **ipconfig /all** is available from a Windows command prompt. It displays a list of all IP parameters and MAC addresses. The equivalent host command is **ipv6config /all** for network interfaces with IPv6 addressing. Linux-based hosts as well that have host command **ifconfig -a** that is available to verify similar settings.

Example: Windows Client IP Configuration Parameters

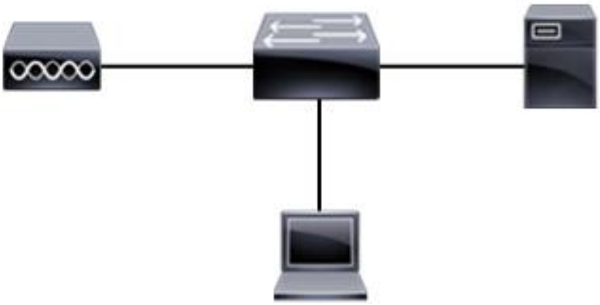
```
c:/> ipconfig /all

GigabitEthernet0 Connection: (default port)

Connection-specific DNS Suffix

Physical Address : 0007.EC0D.ED75

Link-local IPv6 Address : FE80::207:ECFF:FE0D:ED75

IPv4 Address : 192.168.1.1

Subnet Mask : 255.255.255.0

Default Gateway : 192.168.1.254

DNS Servers : 192.168.3.1

DHCP Servers : 192.168.3.1

DHCPv6 Client DUID : 00-01-00-01-15-7D-1C-DC-00-07-EC-0D-ED-75
```

Network Components

Layer 2 Switches

The primary purpose of a network switch is to connect wired and wireless endpoints to the production network. Layer 2 switches are comprised of switch ports that create a collision domain per port. VLANs are supported to define and limit broadcast domains. They work in concert to optimize network performance and forward traffic at the access layer.

Figure 1 Layer 2 Access Switch



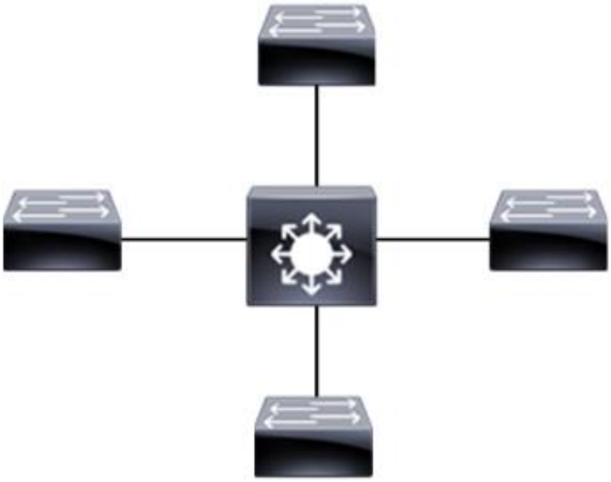
Layer 2 switches have no knowledge of IP addressing and do not provide routing services. They examine the destination MAC address of each arriving frame and forward out a switch port to a destination endpoint. The switch does a MAC address table lookup to select the correct switch port associated with a destination MAC address. Some network services at the access switch include port security, DHCP snooping and QoS.

Multilayer Switches

There has been a proliferation of endpoint connections at the access layer that includes both wired and wireless clients. Multilayer switches are an aggregation point for access layer traffic. They provide switching and routing services between the access layer and traditional routers.

VLANs are configured on switch access ports while some ports are defined as routed ports for connection to routers. Multilayer switches are sometimes called Layer 3 switches. They support default gateway services for hosts configured with an SVI. In addition, routed ports will rewrite frames and proxy ARP requests.

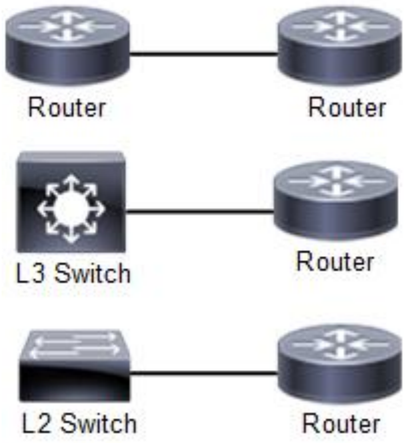
Figure 2 Layer 3 Switch Topology



Routers

Routers are primarily responsible for subnet interconnection and best path selection. They forward packets between different subnets, VLANs and across the WAN based on a routing table lookup. They are often deployed to connect data centers, cloud and branch offices.

Figure 3 Router Topology Connections



Router operation is based on build a routing table with routes advertised from neighbors along with connected subnets and configure (static) routes. Each route is comprised of a network prefix, metric and next hop address. The router examines the destination IP address field of an incoming packet and selects the route based on a routing table lookup.

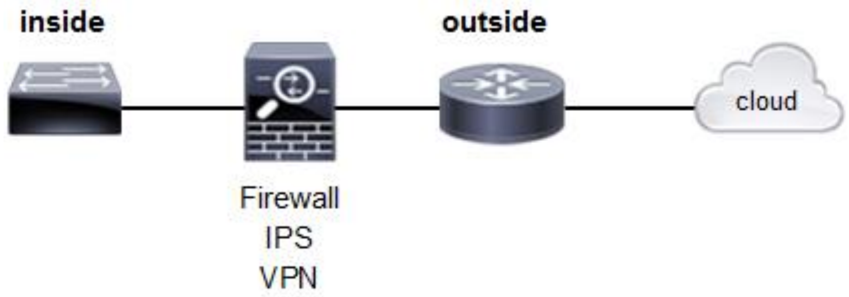
There is a frame rewrite of the source and destination MAC address. Finally any ACL and QoS marking is applied and packet is forwarded to the next hop router (neighbor). There are a variety of network services in addition to routing such as default gateway, DHCP services, proxy ARP and load balancing.

Next-Generation Firewall

Cisco Next-Generation Firewalls (NGFW) is a security appliance that optimizes security for connecting directly to internet-based and cloud services. That includes data center, branch office, remote and mobile devices. The newer Cisco firewall provides inbound/outbound stateful packet inspection to the application-layer.

There are newer integrated security services as well. For example, intrusion prevention sensors (IPS) examine inbound and outbound packets for vulnerabilities, exploits, worms and viruses. There are a variety of mitigation actions available that are configurable.

Figure 4 Next-Generation Firewall Services

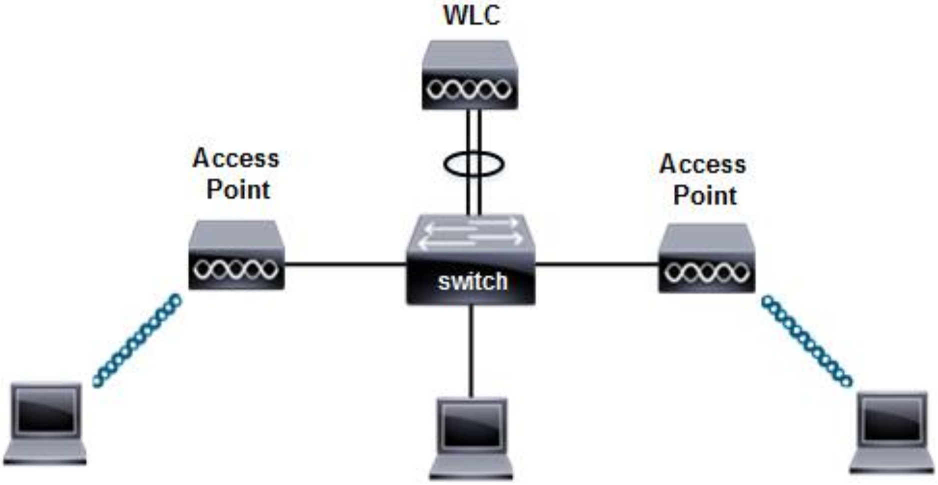


IPsec VPN connections can be terminated at firewalls so encryption is extended and offloaded from internet routers. Cisco CWS is a firewall service as well for preventing malware attacks. The service is essentially cloud-based with the firewall acting as an endpoint.

Wireless LAN Controller (WLC)

The complexity and growth of wireless infrastructure requires a solution specifically for managing access points. Cisco wireless LAN controller is responsible for deploying and managing access points. They provide dynamic RF optimization of wireless cells. It is a newer centralized management model for wireless with many advantages.

Figure 5 Wireless LAN Controller

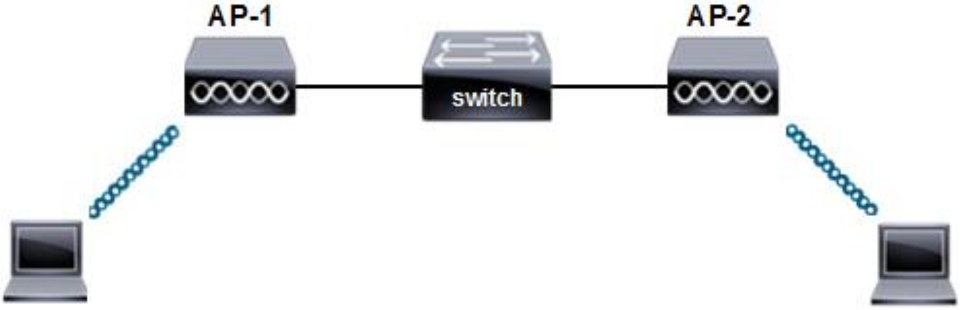


Consider that WLC deploys seamlessly with Cisco DNA for automation and programmability paradigm. For example, it is much easier to push new or update existing configuration to hundreds of access points simultaneously. Software updates and user policies are easier to deploy to access points as well much faster. All access points discover and connect to the nearest controller for configuration and operational control. Older autonomous access points must be upgraded to Cisco Lightweight Access Point (LAP) software to support controllers.

Wireless Access Points

As the name suggests, wireless access points provide an entry to the wired network. They are deployed to extend coverage and availability to the production network. In addition, access points are a foundational component of Cisco Unified Wireless Network (CUWN).

Figure 6 Wireless Access Point



The network access is often temporary and mobile in nature for a variety of user endpoints. It is a reliable backup as well when segments of the wired network are not operational.

Cisco access points are Layer 2 network devices with operation similar to older bridges. They examine incoming frames from multiple wireless clients sharing a common wireless cell. There is much less throughput attributed to the fact that a wireless RF cell is shared half-duplex media. Collisions are quite common with half-duplex media mode. The number of retransmissions increase particularly as you add more wireless clients.

There is a wired-side network interface that uplinks to a network switch and wireless-side comprised of a radio interface. Some access points support multiple radios that each define a separate wireless cell and RF characteristics defined by the radio type.

Table 1 Traffic Domains

Device Type	Description	Traffic Flow
bridge	broadcast domain	half-duplex
access point	collision domain	half-duplex
*switch port	collision domain	full-duplex
VLAN	broadcast domain	not physical interface
router interface	broadcast domain	full-duplex

* half-duplex switch ports are not configured on Gigabit interfaces unless required for compatibility with third party equipment or older devices.

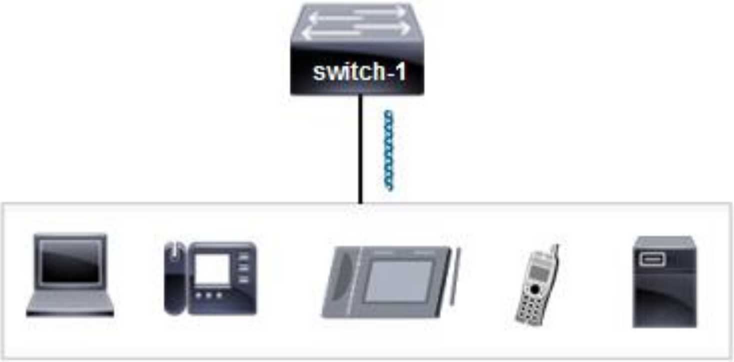
Cisco DNA Center

The purpose of Cisco DNA Center is to enable both automation and network programmability across a global network infrastructure. It is a sophisticated management platform for wired, wireless and virtualized connectivity with characteristics of SDN. Cisco has developed a management solution that provides global, real-time awareness of network operational state. Automation is key to updating software, push configuration state and analytical reporting. The primary services include policy management, provisioning, design and assurance. Network data is collected from across the network to an appliance where connection is via NMS station.

Network Endpoints

Common to network infrastructure are endpoints and intermediate nodes. The communication media, whether wired or wireless is the transport for data messages. Endpoints as originators and/or responders to requests for applications and services. Intermediate nodes are responsible for connecting endpoints and forwarding data messages.

Figure 7 Network Endpoint Examples



Intermediate nodes include switches, routers, access points and firewalls. There are a variety of endpoints from computers, IP phones, tablets, cell phones and servers. They are originator and termination points for application and services. Consider as well there are physical and virtual endpoints along with intermediate nodes.

Table 2 Network Services

Device Type	Network Services
router	route selection, logical addressing, default gateway, frame rewrite, proxy ARP
L2 switch	access layer, endpoints, frame switching
L3 switch	traffic aggregation, frame switching, route selection, default gateway, frame rewrite
access point	access layer, bridging frames to wired network
wireless controller	manage access points, RF management, frame rewrite, proxy ARP, DHCP
firewall	network security, stateful packet inspection, IPS, malware detection, VPN

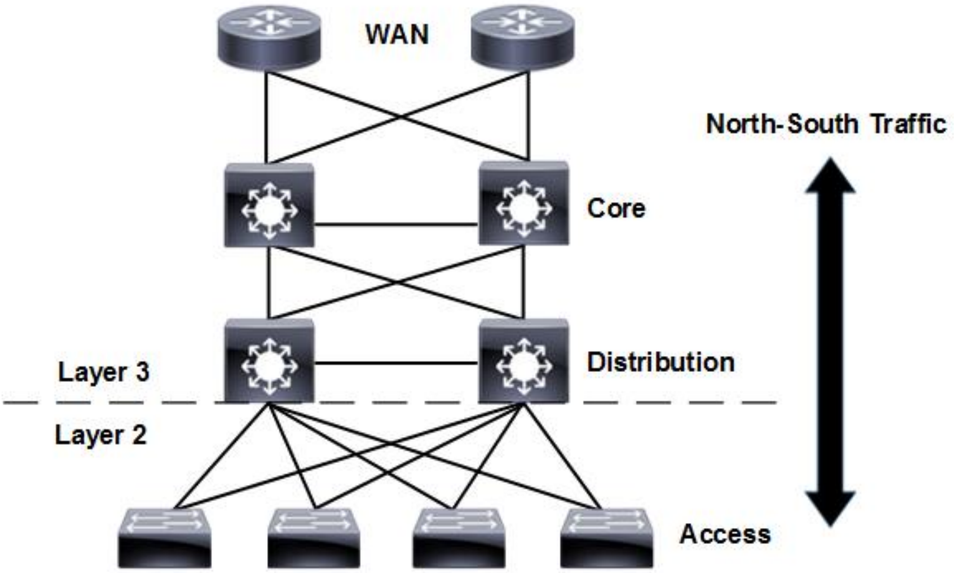
Data Center Architecture

The current data center design is transitioning over to new architecture. The reason has to do with how applications are changing. Traditionally, most applications existed only on a single server that multiple clients accessed. The advent of complex web-based applications has changed that. There are now applications that utilize multiple servers in an N-Tier architecture. Traffic has shifted from north-south to east-west where most throughput is now between different servers. The result is that data center infrastructure architecture is shifting as well.

3-Tier

Most enterprise data center architecture has been designed based on an older 3-Tier model. There are three distinct layers comprised of access, distribution and core switches. Traffic is isolated to each layer for performance and security unless routing services are required. There are well-defined L2 and L3 boundaries. All access layer switches are homed to each distribution multilayer switch for redundancy. The main purpose of distribution layer is to aggregate traffic and provide first-level routing services. There are redundant connections as well between distribution and core multilayer switches. There is fast transport of packets arriving at core switches across switching domains and WAN.

Figure 8 3-Tier Data Center Architecture

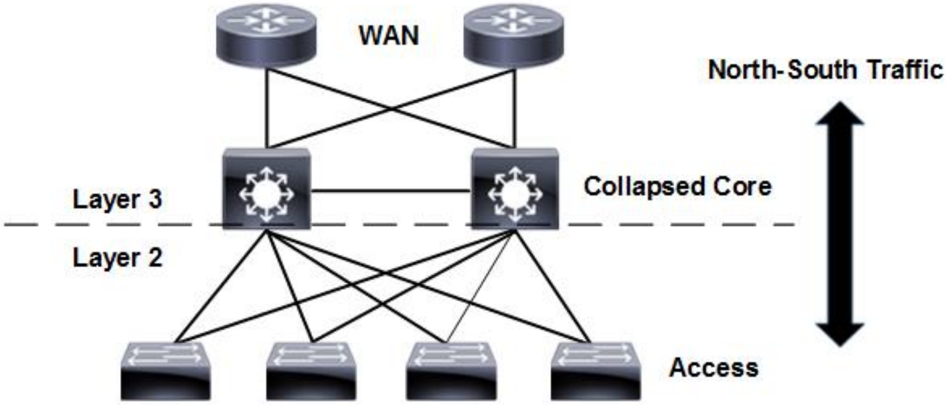


This data center architecture is more expensive to deploy and manage however it is scalable for medium and large data centers. It is typically deployed to traditional data centers where there is mostly north-south application traffic.

2-Tier

Cisco developed 2-Tier data center architecture or collapsed core as an alternative to 3-Tier model. The distribution and core switch is collapsed into a single multilayer switch. All access layer switches are homed to each multilayer switch for redundancy. As a result, multilayer switches provide all network services of aggregation and fast transport. Collapsed core is cost effective however less scalable and suited for smaller data centers. It is typically deployed to traditional data centers where there is mostly north-south traffic.

Figure 9 2-Tier Data Center Architecture



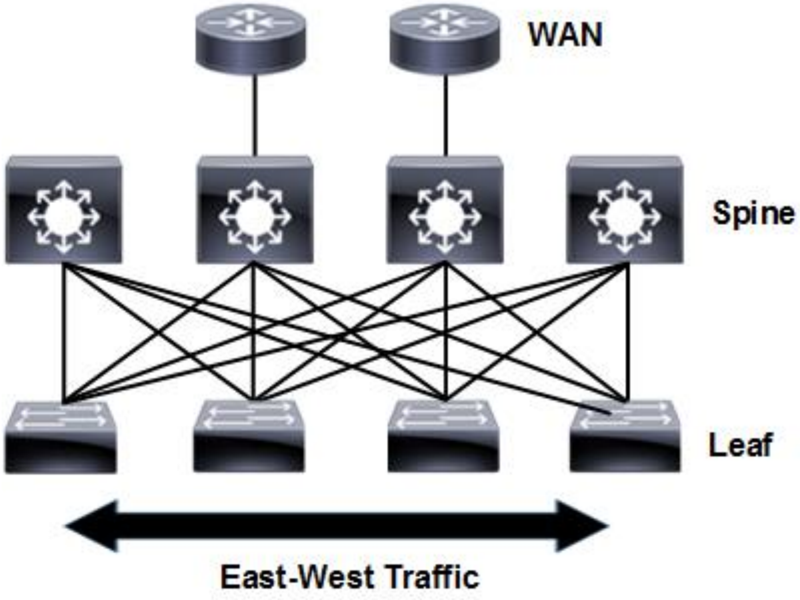
Spine-Leaf

More recently, cloud computing, virtualization and programmability has changed traditional data center architecture. Traffic flow is now mostly east-west for data centers with virtualized servers and N-tier applications. The common characteristic of newer web-based applications is multiple server-server transactions. It is a distributed application model where most traffic moves between servers.

Cisco is now promoting what is called CLOS Spine-Leaf architecture. It is comprised of a 2-Tier layered design with switches connected via full mesh topology. There are leaf switches connected in a full mesh topology to each spine switch.

As a result, each switch is only a single-hop to a neighbor for fast low latency connections. Newer fabric architecture defines a physical underlay and virtual overlay that supports L2 and/or L3 designs. The virtual overlay is unique to Spine-Leaf and required for programmability and SDN applications. Cisco DNA Center is based on fabric architecture.

Figure 10 Spine-Leaf (Clos) Data Center Architecture



WAN Topology

Current network architecture is based primarily on LAN, WAN and cloud. The purpose of WAN infrastructure is interconnection of external locations. WAN routers are designed to connect and forward packets between locations at much lower bandwidth. It is a point where QoS is applied to classify traffic and optimize performance. That could include data centers, branch offices and cloud. In addition, there is the idea of multiple routing and management administrative domains.

For example, connecting an on-premises data center to AWS cloud servers would require WAN infrastructure. The internet router is located in private and public addressing domains. There is a private on-premises administrative domain and an ISP administrative domain. AWS cloud is a third administrative domain. As mentioned, most traffic resides at data centers by design.

AWS cloud is an example of multiple administrative domains within the same data center. Amazon AWS manages physical infrastructure while each tenant is an administrative domain. There is some managed coordination as well that adds complexity.

Figure 11 WAN Topology

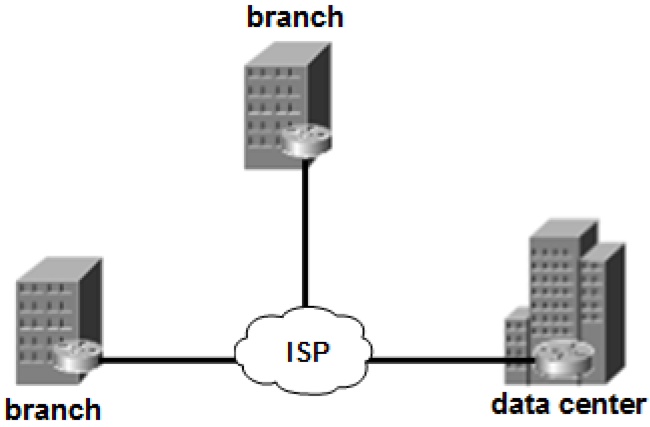
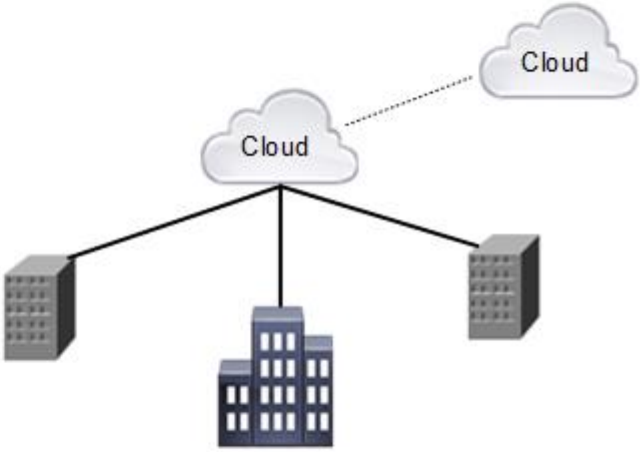


Figure 12 On-Premises and Cloud Topology



Physical Interfaces and Cabling

The current de facto physical standard for switching infrastructure is Ethernet. It is a network protocol standard that defines network interface signaling, distance, speed and media type. In fact, there are multiple Ethernet standards now available. Ethernet is most often associated with LAN infrastructure, however it can be extended across WAN with Metro Ethernet. It is a Layer 2 protocol based on physical MAC addressing only. It has evolved from an older shared (bridge) media to what is now faster point-to-point switch connections.

Currently the most popular Ethernet standard is still Gigabit Ethernet. It is deployed at access layer switch ports for connecting to endpoints and wireless access points. There are now faster 10 Gbps and 40 Gbps Ethernet interfaces available used mostly for switch and building interconnection. Quite impressive is 100 Gigabit Ethernet as well for switch interconnection with the highest traffic loads..

Cabling Media Type

Ethernet physical layer signaling standards are based on media type support (copper or fiber), distance limitations and the maximum speed. Fiber media is used mostly for interconnection of network devices and rarely for connecting endpoints. Campus buildings are connected via fiber media as well with reliable faster transport. Copper cabling media is limited to 100 meters as a result of crosstalk and signal attenuation.

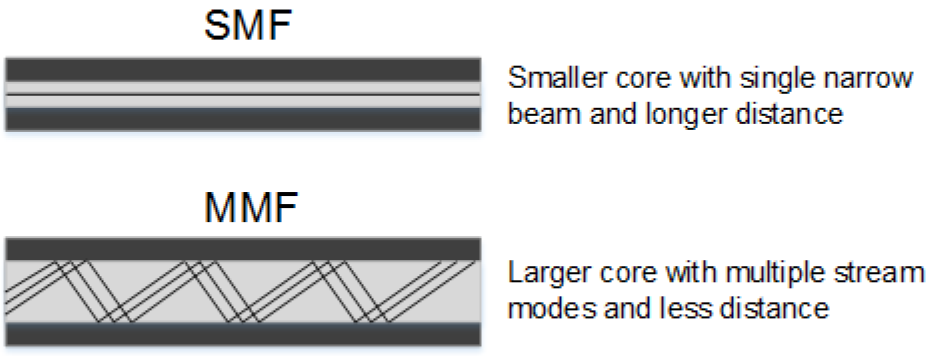
Copper Media

Traditional copper-based media is used mostly for connecting host and server endpoints to an Ethernet access switch. In fact, it was all copper cabling until faster speed and longer distance required new fiber media. Copper media available include Cat 5, Cat 5e and Cat 6 standards. The difference is distance and speed limitation as shown with Table 3. Modern data centers and branch offices will deploy at least Cat 5e to support Gigabit interfaces.

Single-Mode Fiber vs Multi-Mode Fiber

The primary difference between single-mode fiber (SMF) and multi-mode fiber (MMF) is distance. There are some differences in how light is sent across fiber core between source and destination interfaces as well. For example, SMF is characterized by a smaller fiber core where a laser sends a single stream of light pulses. MMF is based on a less expensive LED that sends multiple light beams down a larger fiber core.

Figure 13 Comparing SMF and MMF Cabling Media


SMF
Smaller core with single narrow beam and longer distance
MMF
Larger core with multiple stream modes and less distance

That technique is called modal dispersion and causes higher loss that lowers bandwidth and limits distance. Typical usage for MMF cabling is for switch and router interconnections within the data center. MMF is also deployed to connect buildings. SMF cabling is used for longer distance runs or sometimes between closets/floors in a large building. It is all based on distance, speed and tolerance for loss.

Table 3 lists the most common Ethernet standards with supported media type, speed and distance specifications. There are various transceivers and connectors specified with each Ethernet standard as well. Fiber media connectors include LC and SC while copper media is older RJ-45 connectors.

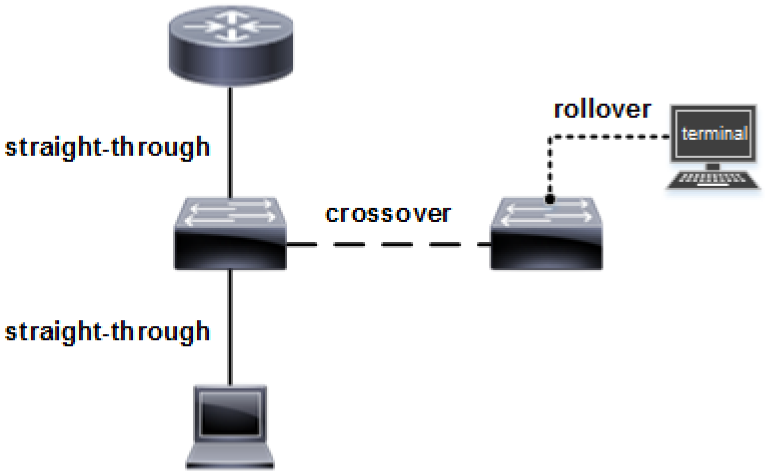
Table 3 Common Ethernet Standards

1000Base-LX/LH	Single-mode Fiber, 1 Gbps, 10 km
1000Base-SX	Multi-mode Fiber, 1 Gbps, 220 - 550 m
100Base-TX	Cat 5, Copper, Fast Ethernet, 100 m
1000Base-T	Cat 5, Copper, 1 Gbps, 100 m
10GBase-T	Cat 6, Copper, 10 Gbps, 55 m
1000Base-LX	Multi-mode Fiber, 1 Gbps, 550 m, SMF (5 km)
1000Base-ZX	Single-mode Fiber, 1 Gbps, 70 km

Cabling Types

Most of the cabling currently deployed to a modern network is comprised of straight-through copper. That is the cabling type used for connecting endpoints to a network switch. Connect dissimilar network devices with a straight-through cable type. Network devices from the same class are connected with a crossover cable type. Connecting switch to switch for example, would require a crossover cable to flip the Tx and Rx pins. There are a variety of WAN cables that are customized for each protocol standard. Most have been based on a serial interface standard.

Figure 14 Network Cabling Types



The rollover cable is a Cisco proprietary cable designed specifically for connecting to the console port of a Cisco device. It is often used for initial configuration and where remote management isn't an option. Terminal emulation software is available with PuTTY or SecureCRT. The following describes the correct usage for each cable type.

Table 4 Network Cabling Types

straight-through	dissimilar device type	switch to router switch to host
rollover	console port	laptop to console
crossover	same device type	switch to switch router to router
serial	router to CSU/DSU	WAN

Power over Ethernet

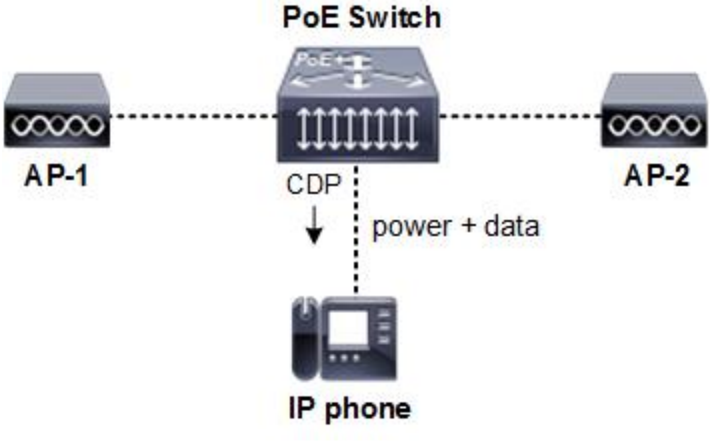
The proliferation of wireless and IP phones is the primary reason for Power over Ethernet (PoE) on access switches. There are newer applications as well such as surveillance cameras and security card readers that support PoE as a power source. The advantage of PoE is that data messages are sent across the same cable used to power the device. PoE is cost effective, eliminating the need for common electrical wiring and installation costs. It extends power as well to access points and cameras that are often located where there are no power outlets.

Power over Ethernet is comprised of cabling, power source equipment (PSE) and powered devices (PD). The supported cabling is standard copper UTP Cat5 (twisted pair) deployed to most buildings. It is the cabling used by endpoints for connecting directly to a network switch. Cisco has various PoE enabled switches referred to as power source equipment where endpoints connect for network access. All powered devices have an Ethernet interface as well that must support the PoE standard of the connected switch.

PoE Operation

The network switch negotiates power level with a powered device when the link is connected via CDP. For example, an IP phone will advertise its power class to the switch on startup. The network switch detects and allocates power to the IP phone based on the class and power usage of the endpoint. In fact, switches manage a power budget that is based on all PoE enabled devices.

Figure 15 Power over Ethernet (PoE)



When the IP phone is turned off, any power usage is designated as available for new connections. Industry standards and vendor standards specify minimum and maximum watts available per class along with cabling twisted pairs used.

Any endpoint that does not support power detection (negotiation) is a class 0 device. PoE power class 1 to class 3 support power detection and autoconfiguration of power level up to 802.3af PoE standard. Finally, there is power class 4 that is only available with the newer 802.3at PoE standard. Cisco has PoE+ brand that is based on the 802.3at standard. The next-generation 802.3bt (Cisco UPoE) is designed for higher wattage to support security card readers and kiosk terminals for example. The following events occur when a powered device exceeds administrative maximum power value.

- Syslog error message is sent
- Switch port is shut down and error-disabled
- Previously allocated power is made available

Configuration of PoE on Cisco network switches is straight-forward. The default setting on any switch port is **auto**. That detects power class and allocates maximum power based on class to the powered device initially.

```
switch(config-if)# power inline auto
```

After additional CDP negotiation, the switch will then adjust power level. Alternatively, static mode pre-allocates maximum power allowed to the attached device. There is an option as well to assign no power or disable PoE on the switch port.

Identifying Interfaces and Cabling Issues

The most common source of interface errors are switch duplex and speed mismatch. Consider the variety of Ethernet standards, cabling media, transceivers, and connectors. There is additional complexity as well when connecting third-party equipment. Ethernet is a standard and hardware vendors are often not 100% compliant. The result is that link negotiation between switches for communication can cause errors. Most often there is degraded performance, timeouts, or connection to server dropped.

Duplex Mode

Full-duplex is the most common transmission mode between network nodes. All network nodes whether they are endpoints or network devices (intermediate nodes) are connected via network interfaces. The main advantage of full-duplex is simultaneous upstream and downstream traffic between nodes. That effectively doubles the available bandwidth. Gigabit Ethernet for example provide 2 Gbps aggregate throughput per port with full-duplex mode setting. Switch interfaces that are connected must use duplex and speed setting that match or configure auto-negotiation to prevent port collisions.

Figure 16 Cisco Network Interface Duplex Modes

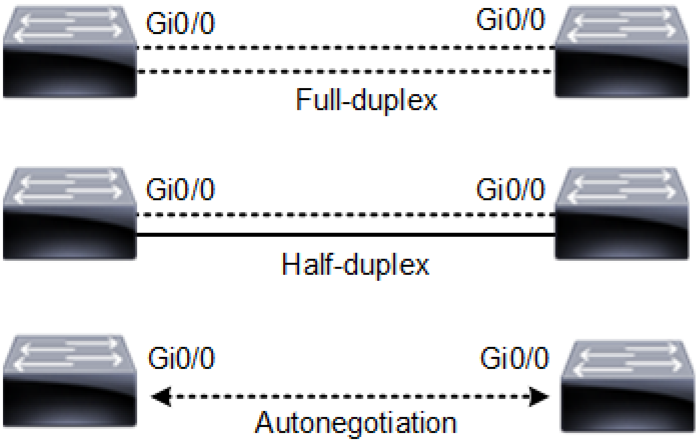


Figure 16 illustrates full-duplex, half-duplex and autonegotiation modes. The dotted line is active traffic is one direction on the same interface. Cisco recommends that you configure autonegotiation mode (default) on switch interfaces.

The command **duplex auto** configures autonegotiation of duplex mode on a switch interface. There is the option to hard code duplex with the interface command **duplex full** as well. Traffic on a half-duplex link flows in only one direction at a time. The switch must wait before sending packets if the interface is busy. There is 50% less bandwidth available at any time as a result. Some half-duplex deployments are still used on older devices or multivendor compatibility. Configuration of speed on network interfaces is important as well.

You can connect switch interfaces that operate at different speeds however it is not recommended. The solution is to set both interfaces to the lowest common speed supported on each interface. That requires hard-code of interface speed or autonegotiation mode. For example, Fast Ethernet (100 Mbps) and Gigabit Ethernet (1000 Mbps) would require **speed 100** or **speed auto** configured on both switch interfaces.

Network Interface Status

The operational state of a Cisco network interface is either **up**, **down**, or **administratively down**. Layer 1 is the interface (Ethernet, Serial etc.) and Layer 2 is the data link to neighbor.

Interface = Layer 1, Line protocol = Layer 2

The normal status of a network interface is **up/up**. The **shutdown** interface command would change interface status to administratively down. (**down/down**). The following IOS commands can verify operational status of all network interfaces on a Cisco device.

```
show ip interface brief
show protocols
```

The following IOS command displays the operational status and errors on a specific network interface.

```
show interfaces gigabitethernet1/1
```

GigabitEthernet 1/1 ***up****, line protocol* ***up*** *(normal state)*

Interface Errors

The misconfiguration of duplex setting between switches cause collisions on a switch port. The late collisions interfaces counter increase as a result. Note that duplex mismatch has no effect on the operational state of interfaces (up/up). Packets are still forwarded however performance is often affected.

The output of **show interfaces** display interface errors such as runts, giants, collisions and CRC. The most common cause of CRC and runts is collisions. Gigabit Ethernet switch ports have eliminated collisions unless there is a configuration error or defective hardware. Collisions can occur when network interface hardware or cabling is defective as well. Giant frames (1600 bytes) result either from faulty interface hardware or MTU misconfiguration on an interface.

The high number of input errors and CRC errors indicate a Layer 1 issue between switches. The local switch is sending frames that are corrupt when they arrive at the neighbor switch. The most probable cause is duplex mismatch between the switch interfaces or cabling errors. The switch ports must agree on duplex setting. Gigabit Ethernet ports do not support half-duplex at all. The older 10/100/1000 interfaces permitted half-duplex with lower speed settings.

Root Cause Errors

Layer 1 = defective cabling/network interface, duplex or speed mismatch

Layer 2 = encapsulation mismatch, spanning tree error, clocking errors.

TCP vs UDP Transport

TCP provides reliable, connection-oriented connectivity with error recovery, flow control and retransmission. The purpose is to detect, prevent and correct packet drops. It is less efficient than UDP with increased overhead and packet processing.

UDP is faster than TCP however it is connectionless with no packet delivery guarantee (best effort). UDP is most suited to applications and protocols where some packet loss is acceptable. Data integrity check is performed with CRC/FCS checksum on frames arriving at destination. UDP datagrams with errors are discarded so only error detection is provided. Some applications such as video streaming prefer UDP where there is less latency from TCP retransmissions.

Table 5 TCP vs UDP Comparison

TCP	UDP
transport layer	transport layer
connection	connectionless
flow control	no flow control
error recovery	error check / discard
data integrity checksum	data integrity checksum
slower	faster
TCP window size	no windowing
ordered data	unordered data
guaranteed delivery	best effort
segment	datagram
retransmission	no retransmission
HTTP, Telnet, SSH, FTP	DHCP, SNMP, VoIP, Video

All network applications are either designed for TCP or UDP transport protocol. In fact, most applications today are HTTP (TCP 80) and based on TCP transport. There are UDP applications however they are often network protocols such as SNMP and NTP for example.

TCP Protocol Features

Consider that most applications are web-based (HTTP) whether intranet or internet and rely on TCP transport protocol. TCP protocol is connection oriented with various features to prevent packet loss, error detection and retransmission.

TCP Flow Control

The host and server endpoints send TCP ACK messages to acknowledge receipt of data messages. There is packet sequencing to track when packets arrive at the destination. The destination endpoint sends an alert to the source endpoint when any packets do not arrive. Any dropped packets are detected and retransmitted.

Queueing

Cisco network Interface have temporary memory called queues. TCP is designed to queue packets on network interface when there is network congestion. That prevents packet loss instead of only discarding them. Any applications that are UDP-based will discard packets.

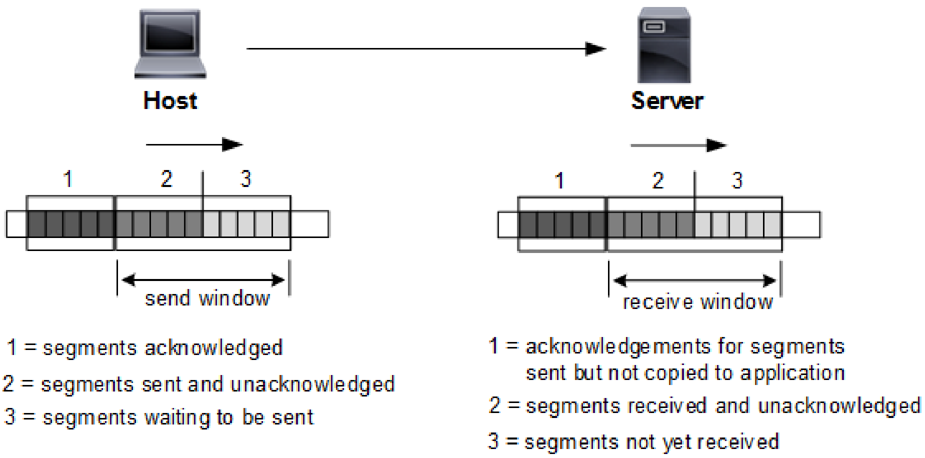
Data Integrity Check

CRC/FCS frame checksum is a technique used to verify data content integrity. The frame is discarded where there is a mismatch between the original checksum value and the frame arriving at destination. The data message is discarded if there is a mismatch. Data integrity is verified however this is not used to detect packet loss during transmission.

TCP Sliding Window

This is a flow control technique that prevents packet loss instead of actually detecting it. The send and receive window size are negotiated to manage the data forwarding rate between endpoints. That prevents packet overrun and retransmissions.

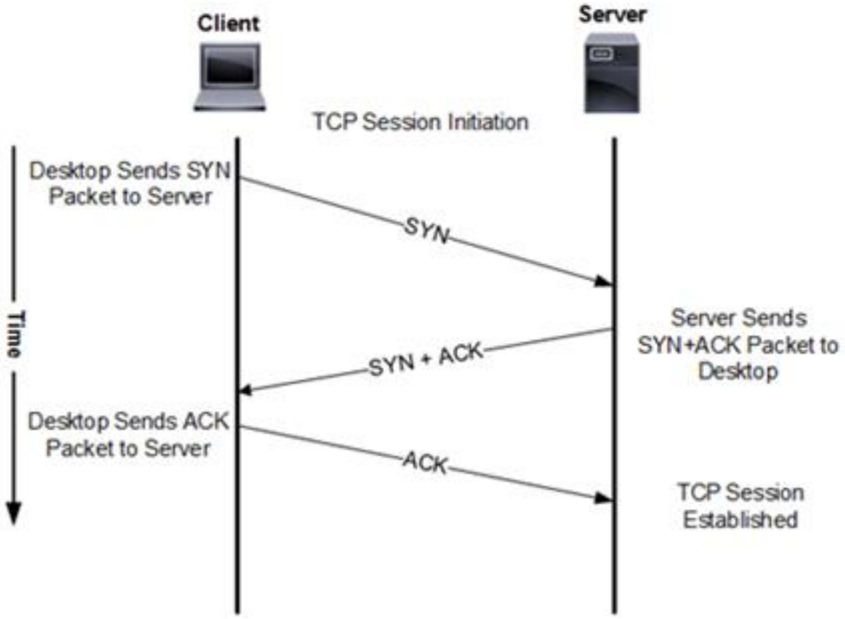
Figure 17 TCP Sliding Window for Endpoint Communication


Host
Server
1
2
3
send window
receive window
1 = segments acknowledged
2 = segments sent and unacknowledged
3 = segments waiting to be sent
1 = acknowledgements for segments sent but not copied to application
2 = segments received and unacknowledged
3 = segments not yet received

TCP Session Establishment

TCP is a connection oriented transport layer protocol that provides connection setup, flow control, congestion management and connection termination. The server listens on specific TCP ports for any connection request from a client host.

Figure 18 TCP 3-Way Handshake Messages


Client
Server
TCP Session Initiation
Desktop Sends SYN Packet to Server
SYN
Time
Server Sends SYN+ACK Packet to Desktop
SYN + ACK
Desktop Sends ACK Packet to Server
ACK
TCP Session Established

The following explains 3-Way TCP handshake for endpoint session setup as shown with Figure 18.

1. TCP session starts with host assigning a random sequence number to **SYN** TCP message and sending it o server.

2. The server assigns a random sequence number to the packet and sends **SYN/ACK** to the host.

3. The host receives **SYN/ACK** message and sends **ACK** TCP message to the server.

4. Figure 17 describes how TCP sliding window shifts the send window as the receiver sends ACKs for additional packets.

Table 6 Application Ports

Application	**Port**
Telnet	TCP 23
SMTP	TCP 25
FTP	TCP 21
HTTP	TCP 80
SNMP	UDP 161
DNS	TCP 53 | UDP 53
HTTPS	TCP 443
SSH	TCP 22
TFTP	UDP 69

Table 7 TCP/IP Architecture Model

Layer	Network Infrastructure	Visibility
Application	host server firewall proxy server	HTTP, SSH, Telnet, DNS, SNMP FTP, TFTP, DHCP, NTP, JSON
Transport	firewall	application ports (**TCP/UDP**)
Internet	router, multilayer switch, firewall	routing, IP addressing (**IP**)
Data Link	switch, access point, wireless controller	switching, wireless, MAC address (**Ethernet**)
Physical	cabling, transceiver, modem, antenna, repeater	transmit binary bits (**1000Base-T**)

Virtualization Services

The primary components of a virtualized solution include hypervisor, virtual machine (VM) and server hardware. The number of virtual machines (VM) that can be supported on a single server is based on memory, CPU, switch uplink speed and hard disk space.

Cisco network virtualization model includes tenant segmentation, security policies and virtual machines. Tenant traffic is segmented with various techniques for path isolation. Network access is managed with security policies and virtual network services based on virtual machines (VM).

Primary services of the virtualization model:

- Network access control
- Tenant segmentation
- Virtual machines (VM)

The primary characteristics of cloud computing architecture:

- Resource pooling
- Elastic capacity
- Metered billing
- Multi-tenancy
- Anywhere access

Virtualization Advantages

The advantage of virtualization is the decreased costs for shared network infrastructure and lower support costs.

Cost Effective

Fewer physical servers are required for the same number of applications. Less data center cabling, power and cooling is required.

Optimized Hardware Usage

Server hardware is utilized at much higher rates with multiple virtual machines. That is preferable to physical servers staying idle when a single application is deployed.

Network Management

Virtual servers (VMs) are abstracted from hardware making them agile and easier to manage. The virtualized environment is a shared infrastructure model. Encryption is available with physical and virtual servers as a network service.

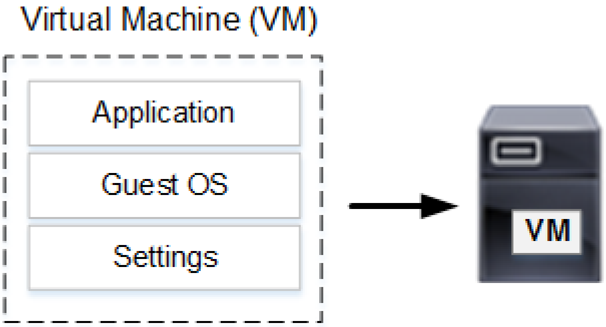
Faster Deployment

Deployment is faster with bundled application that can be copied, distributed and activated when required.

Virtual Machine (VM)

The server hardware at data centers is often not 100% utilized. The advent of server virtualization has consolidated applications to fewer physical servers. It is cost effective and optimizes available hardware. The virtual machine (VM) is a separate logical machine with its own operating system and application. The request for server hardware is made to hypervisor. Each virtual machine is assigned a percentage of CPU, memory, disk space and network interface hardware based on system requirements.

Figure 19 Components of Virtual Machine



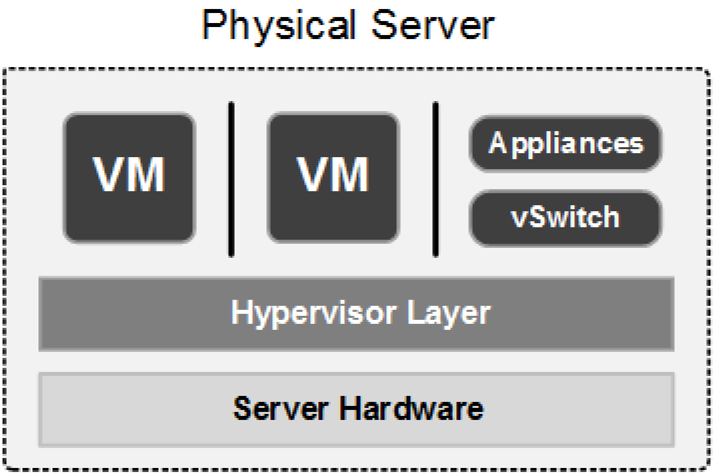
Hypervisor

There are often multiple virtual machines (VM) installed on each physical server. VM is packaged with an application and operating system that is already configured. The hypervisor is intermediary software layer that manages and arbitrates requests for hardware from all virtual machines on the physical server. It abstracts server hardware from virtual machines so the hardware can be shared. There are two hypervisor architectures available today.

Bare Metal Hypervisor

Type 1 is referred to as a bare metal hypervisor. It is a native hypervisor that communicates directly with server hardware shown with Figure 20. The advantage is faster response time and optimized security. Guest operating system on each virtual machine (VM) sends requests for server hardware through APIs. The disadvantage is when there is underlying hardware not supported by the hypervisor. The current versions of type 1 hypervisor communicate directly with the server processor to increase workload capacity with pipelining requests from multiple VMs.

Figure 20 Type 1 Hypervisor



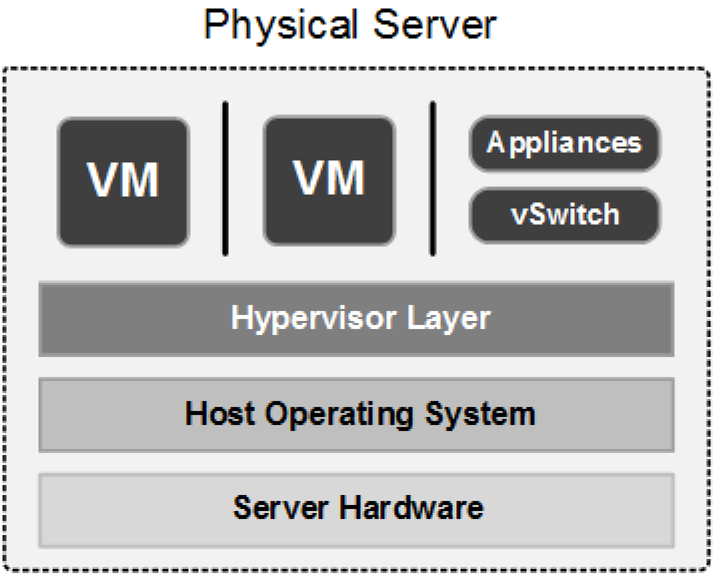
Hosted Hypervisor

This is referred to as a hosted or embedded hypervisor. It is a process on the server between virtual machines (VM) and host operating system. The hypervisor arbitrates requests from VMs. The requests for hardware are sent to the host operating system installed on the physical server. The amount of latency is increased when requests are routed through host operating systems. Containerization is a new architecture not based on a hypervisor. Virtual machine is packaged with the required application and system files except an operating system. VMs all share the host operating system to virtualize operating system for increased scalability.

Server Hardware

The standard data center architecture is based on Top of Row (ToR) access switch that connect to multiple servers. The physical servers have enough CPU processor, disk drive and system memory to share among multiple virtual machines. There are often multiple network interface cards (NIC) for high speed uplink to the access switch. The network server hardware is independent and abstracted from virtual machines

Figure 21 Type 2 Hypervisor


Physical Server
VM
VM
Appliances
vSwitch
Hypervisor Layer
Host Operating System
Server Hardware