Fundamental Networking Topics
www.globalipv6.com

Overview

Knowing the basics about networking can make learning more advanced topics easier. This white paper is written to aid in explaining the fundamental terminology and services that are offered today and even legacy technologies which are often referenced to. Even though the OSI model has been around for a number of years; and often reference as "outdated" it is still commonly used when troubleshooting networking issues, relating network services, identifying hardware or discussing how protocols are layered in a stack. For example, someone may simply say "I cannot ping the server, it must be a layer three issue". By mentioning layer 3 immediately you think IP and routing issues.

Another topic for discussion is switch types and how they are used in the network. Switching technology has become very advanced offering a number of different services supported at different layers of the OSI model. These days we have different layer switching types available for example; *Layer 2 switching, Layer 3 switching, Layer 4 switching, multi-layer switching,* along with *core, access* and *distribution switches* which are a few terms and switch types available. The different "Layer" switches quite simply refer to three different and unique addressing schemes (Layer 2, 3, and 4) used in networks now to move information from a source network device to some destination network device. A further challenge is the efficient deployment of switches in the enterprise system throughout the company itself. This can lead to another technology burden for both management and technicians. Not only is there the confusion about types of switches, but also the location in which they are deployed, along with switch configuration issues. To better understand switching technologies then, one must first understand the basics about computer networking.

Table of Contents

OSI Model

OSI History

The OSI (Open System Interconnection) model was developed in 1984 by *International Organization for Standardization (ISO)* and has become the primary architectural model for network communications. The model was created to help identify technologies, protocols and services at different layers. Prior to the OSI model was a four layer TCP/IP model used for a number of years. The TCP/IP model was adequate for its time, but as more technologies and protocols became available, a more granular model was needed.

OSI Model

Like the earlier TCP/IP model the OSI model is used to reference technologies, services and protocols at different layers. Unlike the TCP/IP model the OSI offeres three additional layers for additional granularity. SI is a seven-layer reference model that defines different services or functions of a network operating system at each layer. These functions must be executed by software and hardware for two networked components to converse. The OSI model is a valuable reference that furnishes everyone a common ground for education and discussion. In normal conversations, the OSI model is often referenced to identify a specific piece of hardware or service. As an example, consider a common question asked: “Is that a layer 2 or layer 3 switch that you are installing”? The reference by layer questions whether the switch is a MAC (Media Access Control) address based or IP (Internet Protocol) address based switching device (discussed later). Switches are often referred to as layer “x” switches in place of their actual model numbers.

Seven Layer Model

The OSI model is broken into seven different layers. The lower four layers assist in moving data through the network. The upper three layers support applications between different network devices.

Applications	**Application**	***FTP, TFTP, BGP, RIP, DNS, HTTP, SNMP, Telnet***
	Presentation	***Encryption, Compression, Encoding, Translational***
	Session	***NetBui, NetBios, Naming Conventions, Windows Workgroup***
Data Movement	**Transportation**	***TCP, UPD, Segments, Port Numbers Layer 4 Switching***
	Network	***IP Protocol, Routing, Subnetting, Layer 3 Switching***
	Data link	***MAC Address, L2 Switches, Ethernet, PPP, HDLC, Frame Relay***
	Physical	***Cables, Connectors, Voltage, Hub, 1s and 0s***

Seven layers defined

- **Layer 7 Application Layer**: A protocol (rule carried out by software or hardware) residing at this layer supports the application running in memory on a network device. For example, if an email is sent then SMTP (Simple Mail Transfer Protocol) is used for encapsulating the email and forwarding it to the next supported layer.

- **Layer 6 Presentation Layer**: Translates from application to network format and vice-versa. This way all different formats from different sources are converted into one uniform format enabling all OSI layers to communicate. Furthermore, for security, data encryption may be used to encrypt the data before leaving a device and decrypt it at the receiving device. Encryption, if used, is another example of a Presentation Layer functionality.

- **Layer 5 Session Layer**: Session Layer helps keep track of login sessions. It primarily establishes and terminates session-to-session layer communications between communicating devices. This is a common layer supported by both mainframes' operating systems and Microsoft operating system services, Netbios and NetBeui.

- **Layer 4 Transport Layer**: In TCP/IP networking, the two primary protocols at this layer are TCP (Transmission Control Protocol) and UDP (User Datagram Protocol). The main difference between the two protocols lies in issues of reliability and speed: TCP provides reliable but slow data transmission; UDP provides fast but unreliable (or "best-effort-basis") data transmission. TCP establishes connections between two hosts (networked computers for example) using "sockets." A socket is an address pair determined by: the IP addresses (Layer 3 addresses); and the assigned software "port" number which defines an Application Layer service. These software port numbers are used by Layer 4 switches to forward data according to the Application represented by the software port number. TCP tracks data packets being both sent and received, which offers a reliable "connection-oriented" service between communicating devices. This layer is often referred to as the end-to-end layer.

- **Layer 3 Network Layer**: The Network Layer is responsible for moving (or routing) data from network to network. On the Internet, IP (Internet Protocol) is supported at this layer. IP protocol contains a 32-bit address used to route IP packets through networks (if running TCP/IP) and the Internet (which runs on TCP/IP). Both routers and Layer 3 switches operate at this layer since both type devices make their forwarding decisions based on IP addresses.

- **Layer 2 Data Link Layer**: One of the key components found at this layer is the MAC (Media Access Control) address. The MAC address is a unique 48-bit or 12-digit hexadecimal value, which is unique to each NIC (Network Interface Card). The MAC address is used within a frame to address other network devices. Each network device installed with a NIC (Network Interface Card) would have a unique MAC address burned into its ROM (Read Only Memory) chip. A switch will use this address to make forwarding decisions. Since this address resides at Layer 2, a switch using this address is referred to as a Layer 2 switch.

- **Layer 1 Physical Layer**: The physical layer supports technologies that make no forwarding decisions. The physical layer is often referred to as the electrical layer. This is the layer where all network cabling resides including all connectors and terminations. As data moves through the network, electrical voltage levels are created to represent either ones or zeros referred to as binary encoding. An older legacy device found at this layer is a hub. A hub is used to connect many devices together allowing these devices to share electrical voltages (data) between each device. Unfortunately, these hubs are un-intelligible forwarding devices, which means they do not make intelligent forwarding decisions, so any frames received are flooded to all other devices connected to the hub.

What is a Data Frame

Destination MAC	Source MAC	Type Field	Data	FCS
6 bytes	6 bytes	2 bytes	Variable Length	4 bytes

A data frame is used to send data through a network. One could compare a data frame to a FedEx package. When a FedEx package is sent, it contains both a source and destination address. A frame is similar in that it contains both a source and destination MAC address. The MAC address would uniquely identify both the source and destination network interface card. Each Network Interface Card has a unique 6-byte or 12-digit (hexadecimal) number (for example, 00-21-56-EF-4D-AB) burned into it. Devices use their MAC address to communicate with other network devices on the same network. If the network is Ethernet, then the MAC address is the unique Ethernet NIC address burned into each card.

The FedEx package carries some form of content located inside the FedEx package. The enclosure of content can also be referred to as *encapsulation* since the content (data) is sealed inside the FedEx envelope. Like a FedEx package, a data frame will also enclose or encapsulate its data inside the frame. The part of the frame that gets encapsulated is called the *Data Header.* Not only

does the data header include data content, but also includes all protocols supporting the data transfer and application running above Layer 2. For example, if a user were to send out an email, then the data header would not only contain the user's email, but would also contain an IP protocol header, TCP protocol header and SMTP protocol header required to support the transmission of the email.

Frame Header Breakdown

Destination MAC	Source MAC	Type Field	IP	TCP	HTTP	FCS
6 bytes	6 bytes	2 bytes		Data		4 bytes

Destination Address: Unique six-byte or 48-bit address burned into a network interface card. This address identifies the destination of the frame.

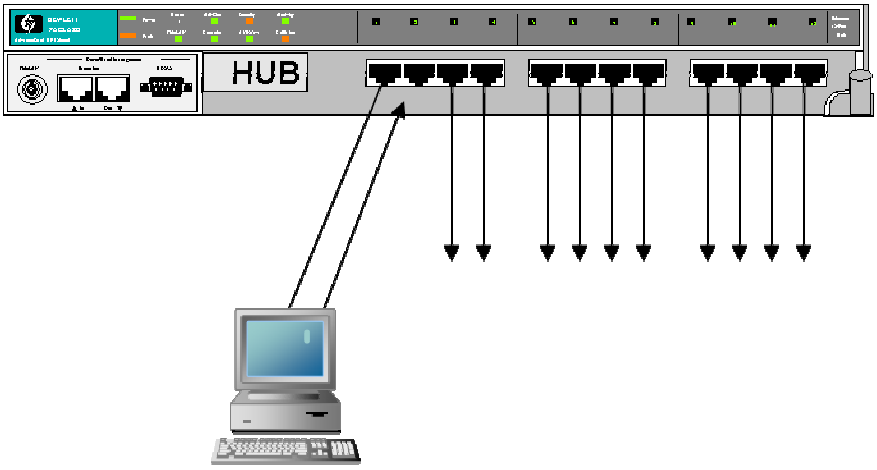
Source Address: Unique six-byte or 48-bit address burned into a network interface card. This address identifies the source of the frame.

Type Code: The type code identifies the next protocol after the data link header. Each protocol is assigned a unique 2-byte number that identifies the protocol only.

Data Header: Contains data being transferred on the network including all protocols required to support the data transfer. In this example, the data header is encapsulating the protocols IP, TCP and HTTP.

What is a Hub?

A hub is used to connect devices together allowing these devices to share electrical voltages (data) between each device. Hubs were early access points giving network devices connection into a network. Most companies would use a Layer 2 switch as an access point device in place of a hub today.



Example of hub connectivity

In the above diagram all network devices are connected into the hubs. Workstation A is forwarding its payroll reports to the payroll server. Since the hub makes no intelligent forwarding decisions, workstation A's network traffic is propagated through the network. All devices connected into either hub will receive workstation A's network traffic. If a protocol analyzer (device used to capture network traffic and display it), were connected into either hub it would capture the traffic. This could be a security breach.

Reasons for not using hubs

- *Shared bandwidth* – All devices plugged into the hub share the exact same bandwidth with all other devices. As more devices are added within the same hub or hubs linked together, network performance degrades.
- *Collisions* – If two or more devices communicate at the same time a collision occurs within the hub. Any part of the network where two or more devices share bandwidth is considered to be within the same collision domain.
- *Security* – Since all traffic forwarded to a hub is propagated out all ports a security issue arises. Devices designed to capture traffic (protocol analyzers) can view any data header that's not encrypted, viewing email content, payroll reports and other vital company information.

Switching Introduction

As network bandwidth requirements continued to increase from initial 10Mbps to100Mbps and now 1000Mbps (gigabit speeds), the demand for faster interconnectivity devices surfaced. Switching technology was created to handle the increased bandwidth speeds that faster PCs and more time sensitive applications demand as well as the ever increasing volumes of data sent over networks. Switches are categorized within most companies' network designs as access, distribution or core (backbone) switches. Each of these devices works within a network structured hierarchical model called the access layer, distribution layer and core layer. Each of these layers can be defined as:

- The **access layer** uses low-end to moderate-end switches used as an entry point for network devices like workstations, laptops and networked printers. Access switches are usually found within the wiring closet allowing devices network access. Dell's access switches may be represented by the PowerConnect 2000, 3000 and 5000 series switches.
- The **distribution layer** defines the point between the access and core layer. The primary function at this layer is to route IP packets between the access and core layers. Basic traffic management using filtering is found at this layer, supporting "access control lists" which are used to filter specified network traffic. Dell Computer offers two types of distribution switches within their Vesuvio PowerConnect line called 6024 and 6024F switches.
- The **core layer** is designed as a high-speed network backbone. If utilized, this is where distribution switches collapse into for fast packet forwarding. The core layer is designed to transport high volumes of traffic to specific enterprise locations. No traffic management takes place at this level. It is designed specifically for high-speed transfer of data. At this time Dell Computer does not offer any high-end core switches.

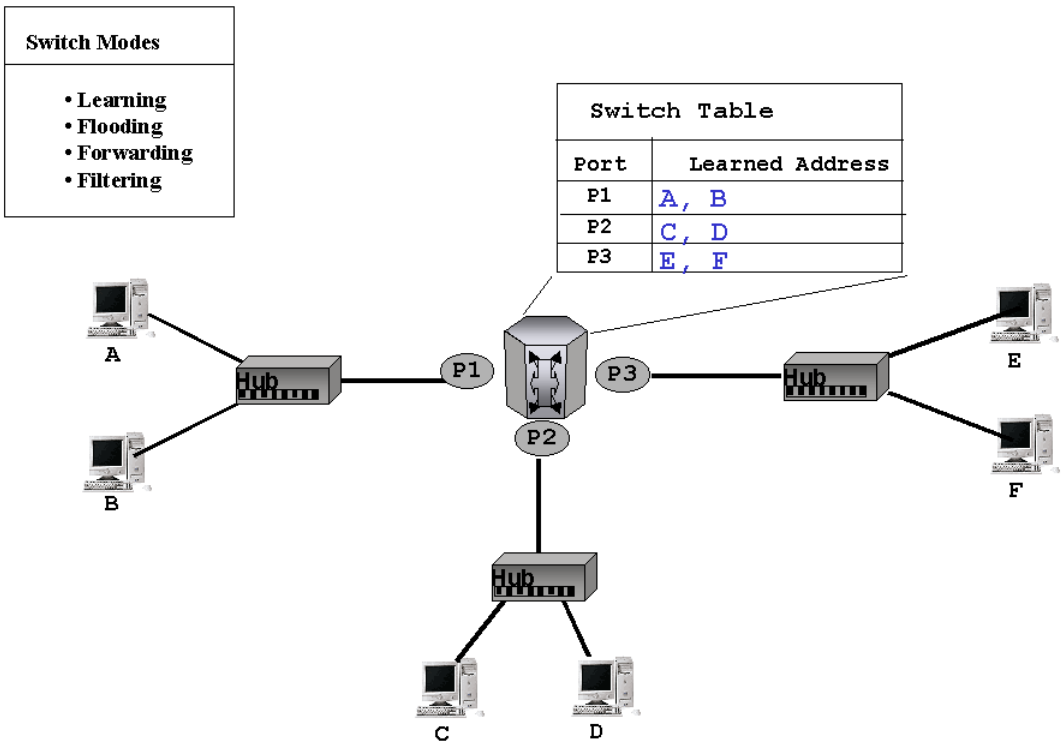
Why are switches so fast?

With the vast demand for more bandwidth and faster PCs, switching technology has evolved to efficiently carry the additional data loads through the network. Unlike slower legacy devices like routers or bridges, switches operate at much higher speeds allowing data packets to be forwarded at greater throughput rates. So why are switches so much faster compared to older legacy hardware? The answer is a technology called ASIC (Application Specific Integrated Circuit). ASIC allows software instructions to be written within a hardware chip. Before ASIC, intelligent devices made their forward decision based on a software program residing in memory that caused latency problems (slower forwarding times). With ASIC the software program now resides embedded in a hardware chip called ASIC. Therefore when a switch receives a frame, it reads its

forwarding decision in hardware (wire speeds) that reduces the forward latency experienced in older legacy equipment.

Layer 2 switch operation

Unlike hubs, that do not make forwarding decisions, switches use MAC addresses for their forwarding decisions.



In the above diagram a switch has been added to the network along with various segments connecting through hubs.

Switch operations involve four processes:

- ***Learning process***
  As network devices communicate on the network the switch will learn their MAC address. A switch can only learn from the source MAC address located within the frame. Once the switch learns the MAC address it stores the learned address and the port it learned it on in its forwarding table (in

Random Access Memory). In the above figure, for example, the first time workstation A sends a frame, the switch reads A's MAC address in the Source Address portion of the frame and enters that (abbreviated as "A" in the figure) in its RAM switching table.

- ***Flooding process***
  Workstation A is sending a frame to workstation E. When workstation A sends the frame the switch will learn workstation A's MAC address as stated above. At this time the switch does not know where workstation E is located since workstation E is not in its forwarding table. When a switch does not know where a device is located it will then forward a received frame out all ports except the port the frame entered. This process is called the flooding process.

- ***Forwarding process***
  Workstation A is sending workstation E a data frame. This time the switch knows where workstation E is located. Since the switch now knows where workstation E is located the switch will only forward out that specific port. Once a switch learns where devices are located, it will only forward out that specific port.

- ***Filtering operation***
  Workstation A and Workstation B are communicating within the same segment. Once the switch has learned where both devices are located and since they are both on the same segment, the switch will filter (drop) their frames.

Layer 3 Switching

Layer 3 switching refers to the network layer within the OSI model. Devices that use IP for their forwarding decisions are referred to as Layer 3 devices. Two common devices used as layer 3 technology are both routers and L3 switches. The distinguishing factor between the router and the L3 switch is how the IP forwarding decisions are processed: in routers it is by software; in L3 switches it is with ASIC chips. Layer 3 switches therefore are low latency devices in comparison.

The traditional layer 3 device is a router. A router is used to route IP packets, but also has the ability to route other *legacy* layer 3 protocols, i.e. Novel's IPX, Appletalk DDP, Banyan Vines VIP, Decnet DRP etc. where L3 switches usually only route IP packets. Since most companies predominantly run only TCP/IP, and the Internet is IP based, switches are not currently expected to fulfill multi-protocol switching support. Network routes are learned using some form of routing protocol, i.e. RIP 1, RIP 2, OSPF to learn the location of different networks. When a new network is learned it is stored in a router's *routing table*. A routing table lists networks located throughout the company including the best path (determined by a value called a metric) to the destination network.

Layer 3 switches would generate the routing table in the same manner, but once generated, the IP forwarding decision process would be executed in ASIC chips versus software in routers. Thus IP packet forwarding is much faster in Layer 3 switches.

Layer 4 Switching

Layer 4 switching is common and is accomplished by using the Application Layer service assigned software port number to forward the frame of data. Every Application Layer service (email, file server services, telnet, web service, etc.) is assigned a "well known port number" by the Internet Engineering Task Force (IETF). An example of a Layer 4 switching need is to load balance file servers containing identical databases. The Layer 4 switch can examine the service requested in the data frame, determine the most available server to provide that service, and forward that request to that server. Even though the switching decision is being made based on the Application Layer service (OSI Layer 7), the switching is called Layer 4 switching because the IETF "well known port number" identifying the service resides inside the Layer 4 (Transport) header in the data frame.

Network Design

Overall network designs have changed since the implementation of switching technology. Before switching, routers were installed as both distribution and core layer devices. At that time, majority of bandwidth speeds average anywhere from 10 Mbps to 100 Mbps. With the creation of Gigabit Ethernet faster forwarding devices were required to keep up with bandwidth demands. Since bandwidth issues have become a major concern switches are now used in areas where routers once were.

Hierarchical Network Design

Over the years network design has migrated into five primary layers called the Access, Distribution, Core, DMZ and WAN layers. Each of these layers performs specific network functions within their designated layer. Using a model approach allows network designers to focus on specific functions required within each hierarchical layer. As network growth increases, each layer can be expanded to allow for network growth, bandwidth requirements or even additional security needs.

Five network layers

- ***Access Layer***
  The access layer is the point where devices are granted access into the network. Access devices are installed within a company's cabling or telecommunication closets. This is the layer where cables terminate from users' cubicles, offices allowing access into a company's network. The access device is usually a low end to moderate size Layer 2 switch. Dell's PowerConnect series 2000 and 3000 are excellent examples of access layer switches.

- ***Distribution Layer***
  The distribution layer is the routing layer between the access and core layer. The primary function, at this layer, is to route (IP) traffic between the access and core layers. A distribution switch is an aggregation point for many access layer switches and must have the ability to route large amounts of traffic between both layers. Dell's PowerConnect series 6000 (Vesuvio) switches are excellent distribution switches.

- ***Core Layer***
  The core layer is the backbone of the network. Its main responsibility is to forward large amounts of data quickly and reliably. All traffic enters into the core layer through the distribution layer. Once the core

layer has forwarded the data, it is delivered back into the distribution layer.
Typically only one subnet would encompass the core layer. Since routing is not performed at this layer, the distribution switches would use one single IP subnet to route through the core. The primary function at this layer is forwarding packets at very high speeds.
At this time, Dell Computer does not offer any core layer type switches.

- ***DMZ Layer***
  The DMZ (demilitarized zone) is the area between a company's enterprise system and the Internet. This is the layer where a security administrator decides WAN (wide area network) access rights. Security *firewalls* function within this layer. A firewall performs many different functions granting and denying specified network traffic. A firewall allows many different layers of granularity, to filter within a frame, packet, datagram or data header.

  Listed are different forms of filtering traffic:

  - Packet filtering
  - Access Control Lists
  - SMLI (stateful multi-layer inspection)
  - Proxy Services
  - NAT services (network address translation)

- ***WAN access layer***
  The WAN (wide area network) access layer relies on some type of third party service provider transporting voice, data, video, etc. among geographically dispersed locations and/or Internet locations. Service providers may include one or more of the following services:
  - Public Switched Telephone Network (PSTN): for example T-1 and T-3 lines, ISDN, DSL, SONET, and other physical transport services;
  - Packet Switched Data Networks (PSDN): for example, Frame Relay and ATM transport services;
  - Internet Service Providers (ISP): providing transport services over the Internet, usually using Virtual Private Network (VPN) technologies.

  The WAN access layer is often referred to as the edge network allowing external network communication. The most common WAN device is a router offering network access, WAN access and filtering (security) capabilities. Often a router works in conjunction with a firewall offering network security.

Switch VLAN Technology

As networks have grown in size, companies have resorted to VLANs (virtual local area networks) to assist with controlling traffic congestion. Basically, a VLAN is a collection of physical L2 switch ports, or MAC addresses grouped together to contain traffic within an assigned group. Benefits of VLANs include bandwidth preservation, bandwidth dedication (e.g. for VoIP traffic), decreased total cost of ownership with increased performance, and network security.

Broadcast problems

A “broadcast” data frame is one intended to reach every networked device in a network, and to be processed by every one of those devices. In a data frame, a broadcast is denoted by a unique Destination MAC address of all F’s (FF-FF-FF-FF-FF-FF). Many applications or protocols support broadcast addressing to reach all network devices.

Benefits of using broadcast addressing:

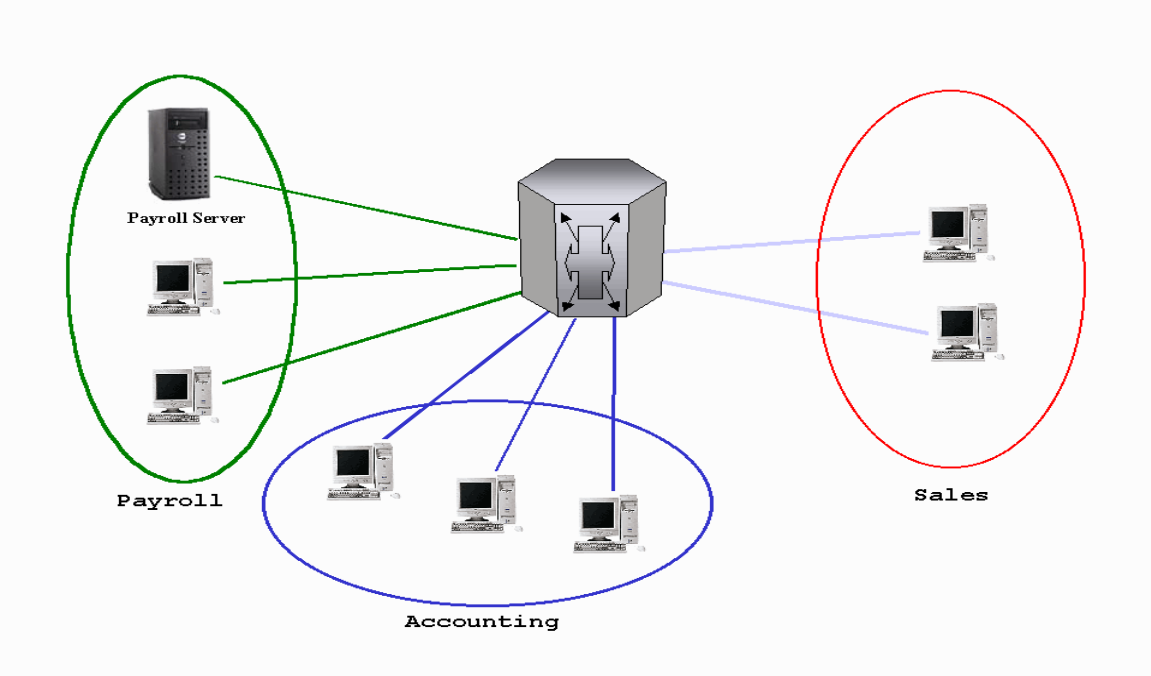
- A source device does not need to know all workstations’ MAC addresses in order to communicate with them.
- One frame addressed as a broadcast can reach all devices within same network.

Disadvantages of broadcast addressing:

- Switches will flood a broadcast message out all ports, which can cause broadcast “storms”.
- All devices receive the broadcast frame on the same network, whether they “need it” or not.
- Since the frame is addressed as a broadcast all devices must process the frame, wasting valuable CPU utilization on unnecessary traffic.

Switch operation

To combat the problems associated with broadcast traffic, VLANs were created. By creating a VLAN, broadcast traffic can be isolated only within a specific VLAN group reducing the number of broadcasts flooded within the network. A VLAN group may be a remote location, specific department, or cluster of segmented devices.



Isolating conversations

For example, consider a payroll department for setting up a VLAN. It may be desired to contain or control all traffic in and out of the payroll department. There may be concern with internal personnel hacking the payroll server.

A solution is to group all employees working in the payroll department into the same VLAN. Each device could be grouped by simply associating their attached port with a specific VLAN number. This way all internal traffic stays local and any external traffic is filtered.

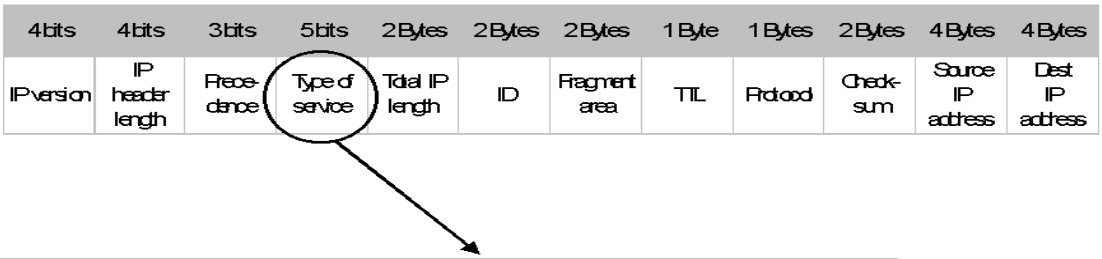
IP Overview

The Internet Protocol resides at the OSI network layer (Layer 3) offering a connection-less (fast but unreliable) service between communicating devices. IP makes no guarantee for data reliability, packet loss, error detection or error correction.

IP's primary function is addressing inter-communication devices allowing them to communicate based on a logical assigned address. IPv4 (IP version 4 is the current version of IP running commercially) supports a 32-bit address that can either be statically or dynamically assigned to a network device. (Note that IPv6, sometimes designated as IPng for IP next generation, supports a 128 bit address, is running in a private network of universities and other entities, and Layer 3 hardware and software are on the market to handle these IPv6 address and protocol. For example, Windows XP is IPv6 capable.) IP offers two primary forms of QoS (Quality of Service) support. Applications configured for QoS can take advantage of faster forwarding rates when congestion is experienced through the network.

IP Quality of Service

IP QoS (Quality of Service) is designed to allow prioritization to specific IP data packets (e.g. for VoIP traffic) through a network. The IP header supports two different types of prioritization called precedence and type of service.



4 bits	4 bits	3 bits	5 bits	2 Bytes	2 Bytes	2 Bytes	1 Byte	1 Bytes	2 Bytes	4 Bytes	4 Bytes
IP version	IP header length	Prece-dence	Type of service	Total IP length	ID	Fragment area	TTL	Protocol	Check-sum	Source IP address	Dest IP address

Precedance Field			Type of Service Bits				
			Delay	Throughput	Reliabilitiy	Cost	Reserved
0	0	0	1	0	0	0	0
0	0	0	0	1	0	0	0
0	0	0	0	0	1	0	0
0	0	0	0	0	0	1	0
0	0	0	0	0	0	0	0

The type of service header defines four different types of services. Each of these four headers supports a form of QoS supported by applications configured for QoS.

- Delay - Setting the delay bit to one defines the frame as a high priority routed frame. When a router receives a frame, with the delay bit set to

one, then it tries to find the path with the least amount of delay if it's available.

- Throughput - Routers receiving a throughput set to one, will attempt to find the path with the highest throughput available to route the frame.

- Reliability - When set to one, informs the router the packet is to travel over the route with the least chance of data loss.

- Cost - Informs a router to use the lowest monetary cost path through the network. The standard is written within RFC's (Request for Comments) 791 and 1349.

- Reserved – Reserved for future use.

The precedence header defines the importance of data located within the IP header. Routers or Layer 3 switches receiving this header can identify the level of importance defined by the binary number. The higher the binary number, the more important is the data.

Normally IP packets are set to value 000 identifying normal routing. When a router's or switch's buffer gets full it must begin dropping data packets. If all data packets are set to precedence value 000 then it simply dumps the oldest packets in its queue. If it had packets with both precedence values set to 000 (normal routine) and 001 (priority) the router would drop all IP packets with precedence value set to 000 first before dropping precedence packets set to 001.

IP DSCP Technology

A newer technology has emerged replacing IP Precedence and Type of Service headers called DSCP (differentiated service code point) allowing improved quality of service support. The IETF (Internet Engineering Task Force) Differentiated Service Working Group has proposed a standard (RFC 2474 and 2475). The RFC standards are written to replace the current IP version 4 type of service field with a new DSCP field. The new DSCP field offers six different fields allowing additional quality of support for supported applications.

DSCP Highlights

- Open System Standard
- Written and approved under RFC 2474
- Uses six identification bits
- Allows for up to 64 different classes of service
- Replaces IP version 4 ToS field

Other Emerging Technologies

Power over Ethernet Standard

PoE (Power-over-Ethernet) is an open system technology written under the IEEE (Institute for Electrical and Electronic Engineers) 802.3af standard. The technology is used to supply electrical power to network devices over available network cable pairs.

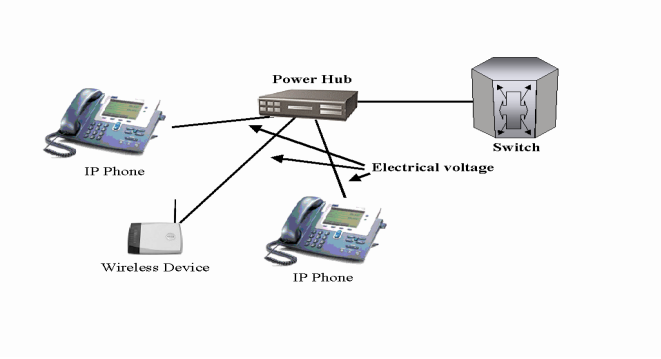
Power over Ethernet explained

Wireless LANs and voice over IP continue in popularity and continued deployment. One problem faced is supplying electrical voltage to these devices. Each of these devices requires an electrical outlet for power. If a power outage occurs, the IP telephone is unusable. To provide fail safe backup, either a standard backup circuit switched service telephone is necessary, or costly UPS and distributed outlets must be installed.

However, a new technology called PoE can be installed replacing the need for an electrical outlet. A typical Ethernet installation uses Cat5 or higher rated wiring. A normal Ethernet cable has 8 wires, where only four out of 8 wires are used for data transfers. PoE takes advantage of the 4 unused wires by supplying 48 volts of electricity over them. With POE a cabler only needs to run one Ethernet cable providing both network connectivity and power to the device. Once the power sourcing equipment detects the presence of the client, it then supplies electrical power eliminating the need for power outlets. By using PoE technology, no longer are peripheral devices restricted to power outlets.

PoE Implementation

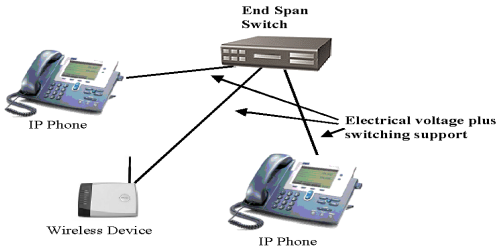
Instead of plugging a user's networked device directly into a switch, instead it will terminate in a *power hub*. A power hub will reside between the network client and network switch. PoE devices will forward data traffic to the "power hub" which then in return forwards the data onto the network switch.
Example 1:



Example 1: Power Hub

PoE end span solution

Some vendors are offering “end span” switches which provide PoE directly from the switch to end device thus eliminating the need for the power hub illustrated in Example 1:



Example 2: End Span

With end span only one network device is required servicing both electrical power and network connectivity.

Voice over IP Introduction

VoIP (Voice over IP) eliminates the need for maintaining both a voice and data network. Converging voice, data and video over one network reduces the cost of managing both a voice and data network. In the long run, VoIP can reduce system cost and operation management since both technologies are embedded within one network infrastructure.

There are issues that need to be considered when setting up a VoIP network. Without such due diligence network traffic could be severely degraded affecting both data and voice traffic. Listed are two factors to consider when setting up a VoIP network.

- Latency – In VoIP network, latency is a measurement of time it takes a voice packet generated by an IP phone, to reach the destination IP phone. Poor quality will experience delay in a voice conversation as experienced with some overseas calls.
- Packet loss – Packet loss in voice conversation is acceptable as long as the loss is spread out over long time periods. Since VoIP runs on top of the UDP (connection-less service) protocol, the lost voice packets are not retransmitted nor would they want to be since retransmission would only slow the transmission down further and the retransmitted packet would be out of sequence- clearly unacceptable. Minimal packet loss is acceptable since the human hearing mechanism can still function to understand the received voice.

With QoS support, IP voice packets would carry a higher priority over data packets helping to assure their delivery. If congestion occurred within the switches, higher priority packets (i.e. VoIP) would take precedence over lower priority data packets.

For training classes please contact:

Globalipv6
Sales@globalipv6.com or mark@globalipv6.com
www.globalipv6.com