The Anatomy of the IP Network, Part 2

November 10th 2014 - 02:00 PM

by Gary Olson, President, GHO Group

Courtesy Stuart Miles, FreeDigitalPhotos.net

This is the second in the series and here we will begin to get into a more granular discussion of the IP addresses and network transmission protocols. It is important to understand the different transmission and addressing protocols as devices, applications and systems each have specific requirements based on their role in the IP architecture.

Network Layers

First, we need to clear up a little confusion. When we are looking at the construct of the IP network technology, the features and functionalities of routers and switches are identified by layers. These layers are the technical construct of the Ethernet based IP network. It should not be confused with the discussion about the business and production layers (departments) that the network integrates to enable interaction with the business processes and workflows.

There is a published standard for Ethernet that defines the entirety of the hardware, communication and transmission protocols of the IP network. This is The Open Systems Interconnection (OSI), considered the basic reference model that was adopted as a joint effort by the International Standards Organization (ISO) and International Electrotechnical Commission (IEC). The OSI model is a seven layer network definition and standard that's maintained by the ISO under ISO/IEC 7498-1. The following describes each of the Layers, their role within the network and some of the protocols each layer supports. This topology are the core and foundation of all Ethernet and applies to other networks as well (ie. ATM,

SONET, x.25, FDDI, etc)

The seven layers are illlustrated here.

OSI Model			
	Data unit	Layer	Function
Host layers	Data	7. Application	Network process to application
		6. Presentation	Data representation, encryption and decryption, convert machine depen to machine independent data
		5. Session	Interhost communication, managing sessions between applications
	Segments	4. Transport	Reliable delivery of segments between points on a network.
Media layers	Packet/Datagram	3. Network	Addressing, routing and (not necessarily reliable) delivery of datagrams points on a network.
	Bit/Frame	2. Data link	A reliable direct point-to-point data connection.
	Bit	1. Physical	A (not necessarily reliable) direct point-to-point data connection.

Image courtesy: Wikipedia

Layer 1 - Physical layer:

This is the electrical mechanical and physical specifications all the hardware that will make up the network. This includes hubs, switches, Copper and Fiber Optic cable (ie. distances, impedances, signal timing, etc.) including the connectors and connection pin-outs. (ie. RJ45 for Category 5, 5E and 6). Layer 1 includes the frequency and modulation coding for Wi-Fi. Layer 1 is where the actual bandwidth of the network is determined and managed.

Layer 2 - Data link layer

This layer is commonly used in switches and data transport that includes the protocols of how these devices communicate with each other.

- The Media Access Control (MAC) address is a unique ID assigned to each network connection per device and controls their access to data and the permission to transmit it.
- The Point-to-Point protocol (PPP) is one part of this layer

Layer 3 - Network Layer

This is the most commonly known layer. A network is defined as an interconnected set of devices each with its own address which enables the communication of messages and data between the devices using the address of the device and finding the best path (route) to deliver the message and data. This is the layer where the IP addresses of the network are assigned, managed and controlled using a number of management protocols. This is where the IPV4, IPV6 and MAC addresses are managed.

Layer 4 – Transport Layer

The transport layer can be compared to how delivery services handle packages. They classify each

package and then send it to a destination. The transport layer acknowledges the delivery of the packet and if there are no errors, sends the next packet.

The transport layer is where Transmission Control Protocol (TCP) and UDP communicates within the Internet Protocol (IP)

Layer 5 – Session Layer
This is a software layer that controls the actual communication between computers and devices. It establishes, manages and terminates the connections between the device and server/workstation application. The session layer is where full duplex, half duplex and simplex connections are managed in the network.

Layer 6 – Presentation Layer
The presentation layer is what insures that packets sent out by the application layer of one network system is readable by the application layer of another network system. Common protocols in this layer are MIME, SSL, ASCII, MIDI and MPEG.

Layer 7 – Application Layer 7
This layer is closest to the end user. In the IP network, the application layer and the end-user interact directly with the software application. The application layer is how software applications communicate with other applications on the network. Some of these are web services, file transfer and mail. Some of the protocols are DNS, FTP, HTTP, DHCP, SMTP and SNMP.

IP Addresses and Protocols
In the first article of this series, ICANN and IANA were discussed as the organizations responsible for assigning IP public IP addresses and protecting specific ranges for private IP addressing. There are multiple IP addressing schemas and transmission protocols. There is the IPV4 and IPV6 addressing protocol, the media access control (MAC) address, Uni-cast and Multi-cast protocols; and TCP (Transmission Control Protocol) or UDP (User Datagram Protocol). All of these are important to understand.

Transmission Protocols

- **IP – Internet Protocol -** This is the protocol used to encapsulate data for sending between networks. It has routing functionality that enables inter-networking. This is how the Internet was created. IP delivers packets from a source application to destination application or to a device based on an IP address embedded in the packet header.
- **TCP - Transmission Control Protocol -** This is the protocol most applications use to transmit packets across the Internet. This is the primary protocol used when an application needs to send a large amount of data across the Internet. TCP is optimized for accurate delivery rather than timely delivery and can introduce latency. TCP has built in error checking and correction making it less efficient for transmitting files and packets that are time sensitive.
- **User Datagram Protocol (UDP) -**This was developed to solve the issue of sending large files and the latency associated for the error checking of TCP. This is a simpler transmission protocol than

TCP. It is accomplished by removing the handshaking, error checking and other protections found in TCP. Time-sensitive applications will use UDP and have the application apply error checking and correction.

- **Unicast** is when a packet is sent from a single source to a specific destination over the network. This is point to point and very bandwidth intensive. This is the most common form of transmission on internal networks (LANs) and the Internet. All IP networks support unicast and the applications that are the most familiar are http, smtp, and ftp. TCP only supports Unicast.
- **Multicast** - Multicasting is delivering the same packet simultaneously to a group of devices or applications. Multicast provides dynamic many-to-many connectivity between a set of senders and a group of receivers. The format of IP multicast packets is identical to unicast packets with a special class of destination IP address (class D IPv4 address) which denote the specific multicast group. Multicast applications must use the UDP transport protocol. Within a multicast environment the devices and applications receive only the stream of packets they have been configured to by having a unique multicast group address).

IP Addressing

- **IPV4 - Internet Protocol Version 4 -** This is based on a 32bit address in four 4 byte segments separated by a period or "dot" called octets (172.234.111.254). While this is the most recognisable address format, the global proliferation of IP connected devices has used up the available IPV4 ~4.8 billion public addresses.
- **IPV6 – Internet Protocol Version 6** – IPV6 was created to resolve the issue that IPV4 had used all available addresses within the 32bit address range. This is now based on a 128bit address in eight hexadecimal segments, which for all practical purposes will have enough addresses for the foreseeable future. The IPV6 format is eight groups of four hexadecimal numbers (2001:0db8:85a3:0042:1000:8a2e:0370:7334) that are separated by a colon instead of a dot. There are efforts being made to create abbreviations of the full hex address.
- **MAC Address** – This is a unique ID assigned to every network interface or adapter that is connected on the physical network. The MAC address is typically assigned by the manufacturer of the network interface controller (NIC) stored in the hardware or firmware. The MAC address is usually an encoded version of the manufacturer's registered identification number and in a 48bit format.
- **Multicast –** In the same way IANA has reserved blocks of addresses for private networks, they have also assigned s range for Multicast addresses. The reserved range for Multicast is 224.0.0.0 to 239.255.255.255. There are certain addresses that have been reserved by IANA for specific use. One example is the Precision Time Protocol (PTP) which synchronizes time across the network to all connected time devices or applications.

The importance of understanding the addressing and transmission protocols because all devices and applications have specific configuration requirements to communicate across the network and in the instance of file transfer guarantee reliable delivery of the file.

The series will continue with Part 3, Network Topology and Network Design Considerations.

This is part of Olson's continuing series "Smoothing the Rocky Road to IP". Other articles include:

The Anatomy of the IP Network, Part 1

The Anatomy of the IP Network, Part 2

The Anatomy of the IP Network, Part 3

Changing Technology: Panacea or Pandemonium

ASSOCIATED RESOURCES:

The Anatomy of the IP Network, Part 1

The Anatomy of the IP Network, Part 3