Advanced IP Networking Series: “The Network of Networks“

Wayne M. Pecena, CPBE, CBNE
Texas A&M University
Office of Information Technology
Educational Broadcast Services
"Advanced IP Networking Series: The Network of Networks"

Advertised Webinar Scope:
The first of the series offered in 2014 will focus upon implementation of multiple isolated, but structured networks built upon a common physical infrastructure. Isolated networks examples will include performance, security, and policy factors that may be used in implementation decisions. Implementation examples will use actual network equipment configuration.

Prerequisite Knowledge:
Attendees should have knowledge of IP networking concepts that includes OSI Layers 1-3, Ethernet switching, IP routing, and VLAN principals.

Webinar Outline:

- The 15 Minute IP Networking Review
- Why Multiple Networks?
- The Ethernet Switch in Detail
- The Virtual Local Area Network (VLAN)
- VLAN Implementation & Examples
- Summary – Q&A
The 15 Minute IP Networking Review
What is a Network?

• The Foundation for Human Interaction.
• A Group of Computers That are Interconnected to Share Resources and Information.
• A group of Hosts That Share a Common Address Scheme.
• Networks are often defined by their geographic reach:
  – Local Area Network - LAN
  – Wide Area Network - WAN
  – Metropolitan Area Network - MAN
  – Campus Area Network – CAN
• Networks Can Be Defined By Their Function:
  – Storage Area Network - SAN
5 Things Required To Build a Network

• **Send** Host
• **Receive** Host
• **Message** or Data to Send Between Hosts
• **Media** to Interconnect Hosts
• **Protocol** to Define How Data is Transferred
The OSI Model

Open Systems Interconnection (OSI) Model
Developed by the International Organization for Standardization (ISO)

A Conceptual Model – Abstract in Nature – Modular in Structure
The OSI Model Does Not Define Standards – Standards Are Built From the OSI Model
The OSI Model Defines How Data Traverses From An Application to the Network
The OSI Model Describes How Devices & Protocols Interact
Encapsulation

Data is “Encapsulated” As It Travels Through the “Stack” From Application
Encapsulation & De-Encapsulation
The Network Today!
The “de facto” Standard

- Layer 1 is **Ethernet** based Copper, Fiber, or WiFi in the LAN
- Layer 2 is **Ethernet**
- Layer 3 is **IP**

“I don’t know what the future network will be, but it will be Ethernet!”

Bob Metcalf
*Father of Ethernet*
Layer 2 Standards:
IEEE- Institute of Electrical & Electronic Engineers

• Project 802
  Ethernet Standards:
  – 802.1 Bridging
  – 802.3 Ethernet
  – 802.11 Wireless

http://standards.ieee.org/about/get/

IEEE 802 standards are included in the program after they have been published in PDF for a period of six months. To download these documents, you must first agree to our Terms of Use. Please select a category below for a full listing of available standards.

IEEE 802®: Overview & Architecture
IEEE 802.1™: Bridging & Management
IEEE 802.2™: Logical Link Control
IEEE 802.3™: Ethernet
IEEE 802.11™: Wireless LANs
IEEE 802.15™: Wireless PANs

IEEE 802.16™: Broadband Wireless MANs
IEEE 802.17™: Resilient Packet Rings
IEEE 802.20™: Mobile Broadband Wireless Access
IEEE 802.21™: Media Independent Handover Services
IEEE 802.22™: Wireless Regional Area Networks
Layer 3 Standards:
IETF – Internet Engineering Task Force

- **Request for Comments – RFC’s**
  - The “Standards Bible” of the Internet
  - Used to Explain All Aspects of IP Networking
  - Nomenclature “RFC xxxx”

- **Requirement Levels:**
  - Required
  - Recommended
  - Elective
  - Limited Use
  - Not Recommended

[www.rfc-editor.org/rfc.html](http://www.rfc-editor.org/rfc.html)
The Layer 2 Ethernet Frame

An Ethernet II (DIX) Frame

<table>
<thead>
<tr>
<th>Preamble</th>
<th>Destination Address</th>
<th>Source Address</th>
<th>Type</th>
<th>Data</th>
<th>CRC</th>
<th>IF Gap</th>
</tr>
</thead>
<tbody>
<tr>
<td>8 BYTES</td>
<td>6 BYTES</td>
<td>6 BYTES</td>
<td>2 BYTES</td>
<td>46 – 1500 BYTES VARIABLE</td>
<td>4 BYTES</td>
<td>12 BYTES</td>
</tr>
</tbody>
</table>

frame length

64 Byte Minimum

< 64 bytes results in a “runt” frame
Ethernet Frame Flow Through Network

MAC Address Changes As Frame Passes Through the Network
Addressing Review

- **MAC Address** – 6 Bytes – Hexadecimal Notation - **00:12:3F:8D:4D:A7**
  - Layer 2 **Physical Address** (local network segment)
  - Fixed – Assigned by NIC Mfg.
  - Local Scope

- **IP Address** – 4 Bytes – Dotted Decimal Notation - **172.15.1.1**
  - Layer 3 **Logical Address** (global routed)
  - Can Change – Determined by Network - Assigned by User
  - Global Scope

![Simplified Representation of IP Packet and Ethernet Frame](image-url)
MAC Address Formats
Always 48 Bits – Always Expressed as Hexadecimal

Can Be Represented in Several Formats:

00:A0:C9:14:C8:29
00-A0-C9-14-C8-29
00A0.C914.C829
Hubs, Switches. & Routers

*A Summary!

• **Hub**
  – Layer 1 Device
  – Acts as a Repeater - All Incoming Frame FWD Out Every Other Port
  – Half-Duplex Based – CSMA/CD Algorithm Controlled
  – No Intelligence – Collision & Broadcast Domain Across All Ports

• **Switch**
  – Layer 2 Device – Originally Called “Forwarding”- Now Called “Switching”
  – Full Duplex Based
  – Intelligence Based – Selectively Forwards Frame to a Port
  – Each Port is a Collision Domain (assuming one device per port)
  – Each Switch is a Broadcast Domain

• **Router**
  – Layer 3 Device
  – Forwards Packets Between Different Networks
  – Separates Broadcast Domains
  – Each Interface is a Collision Domain
Why Multiple Networks?
The Network

• One Network – Single Broadcast Domain
  – “Flat” Topology

• Multiple Networks – Individual Broadcast Domains
  – “Segmented”
    • Policy
    • Regulation
    • Security
    • Performance
Understanding Broadcast Domains & Collision Domains
Collision Domains & Broadcast Domains

11 Collision Domains
3 Broadcast Domains
The Ethernet Switch in Detail
Managed vs Un-Managed Ethernet Switches

- **Managed Switch**
  - User Configurable
  - Provides Ability to Control & Monitor Host Communications
  - Port Configuration, Security, & Monitoring
  - VLAN Implementation
  - Redundancy Supported (STP)
  - QoS (Prioritization) Implementation
  - Port Mirroring

- **Un-Managed Switch**
  - Fixed Configuration
  - “Plug & Play”
  - Provides Basic Host Communications
  - Cheaper
Ethernet Switch Functions

• Learn MAC Addresses
• Filter Ethernet Frames
• Forward Ethernet Frames
• Flood Ethernet Frames
• Allow Redundancy (Avoid loops where redundant links exist)
• Can Provide Port Security Features
Ethernet Switching Fundamentals
“Bridging”

- **Switches Allow Segmentation of Network**
  - Allows Dedicated Bandwidth and Creates Point-Point Communication
  - Increased Throughput Due to Zero or Minimal Collisions
  - Provides Full-Duplex Operation
  - Increased Security Capability

- **Switches Selectively Forward Individual “Frames” from a Receiving Port to a Destination Port**
  - Builds Internal Table of Destination Address on each Port
  - Forwards Ethernet Frame if in Table
  - Floods Ports if Frame Not in Table OR a Broadcast Frame
Learning a MAC Address

VLAN 1 is Special

Switch MAC Address Table
“Content Addressable Memory (CAM) Table”

<table>
<thead>
<tr>
<th>MAC ADDRESS</th>
<th>PORT</th>
</tr>
</thead>
<tbody>
<tr>
<td>08-3e-8e-11-11-11</td>
<td>A1</td>
</tr>
<tr>
<td>08-3e-8e-22-22-22</td>
<td>A2</td>
</tr>
<tr>
<td>08-3e-8e-33-33-33</td>
<td>A3</td>
</tr>
<tr>
<td>08-3e-8e-44-44-44</td>
<td>A4</td>
</tr>
</tbody>
</table>

A Real MAC Address Table

<table>
<thead>
<tr>
<th>Vlan</th>
<th>Mac Address</th>
<th>Type</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1</td>
<td>0014.1c40.b080</td>
<td>STATIC</td>
<td>CPU</td>
</tr>
<tr>
<td>A1</td>
<td>0100.0ccc.cccc</td>
<td>STATIC</td>
<td>CPU</td>
</tr>
<tr>
<td>A1</td>
<td>0100.0ccc.cccd</td>
<td>STATIC</td>
<td>CPU</td>
</tr>
<tr>
<td>A1</td>
<td>0100.0cdd.dddd</td>
<td>STATIC</td>
<td>CPU</td>
</tr>
<tr>
<td>1</td>
<td>0000.aa67.64c5</td>
<td>DYNAMIC</td>
<td>Fa0/14</td>
</tr>
<tr>
<td>1</td>
<td>0000.aa70.d9b9</td>
<td>DYNAMIC</td>
<td>Fa0/7</td>
</tr>
<tr>
<td>1</td>
<td>0001.e641.96cd</td>
<td>DYNAMIC</td>
<td>Fa0/2</td>
</tr>
<tr>
<td>1</td>
<td>0004.00d5.285d</td>
<td>DYNAMIC</td>
<td>Fa0/18</td>
</tr>
<tr>
<td>1</td>
<td>0007.50c4.3440</td>
<td>DYNAMIC</td>
<td>Fa0/2</td>
</tr>
<tr>
<td>1</td>
<td>0008.74a5.9ee0</td>
<td>DYNAMIC</td>
<td>Fa0/8</td>
</tr>
<tr>
<td>1</td>
<td>0009.0f0a.6974</td>
<td>DYNAMIC</td>
<td>Fa0/12</td>
</tr>
</tbody>
</table>
The Virtual Local Area Network “VLAN”
Virtual Local Area Network – VLAN

• Allows Separation or Segmentation of Networks Across a Common Physical Media
  – Creates Subset of Larger Network
  – VLAN Control of Broadcast Domains – Each VLAN is a Broadcast Domain
  – Architecture Flexibility
  – Security

• Static Port Based VLAN(s)
  – Most Popular
  – Manual Configuration
  – Switch Port Security Features

• Dynamic Port Based
  – MAC-Based VLAN(s)
    • Assignment Based Upon MAC Address
  – Protocol-Based VLAN(s)
    • Assignment Based Upon Protocol
VLAN Example

Switch Port Type Configuration:

Access Link – Member of One VLAN Only Connects to a Host
Trunk Link – Carries Traffic From Multiple VLANS Between Switches
Switch Interface Configuration

- **Interface Config:**
  - TRUNK
  - Blue VLAN
  - Green VLAN

- **Switch 1**
  - Access Interface

- **Switch 2**
  - Access Interface

- **Switch 3**
  - Access Interface

- **Interface Config:**
  - TRUNK
  - Blue VLAN
  - Red VLAN
  - Green VLAN
No Connectivity Exists Between Broadcast Domain, Networks, or Subnets!
Adding the VLAN Tag

**ETHERNET FRAME**

<table>
<thead>
<tr>
<th>PREAMBLE</th>
<th>DESTINATION MAC ADDRESS</th>
<th>SOURCE MAC ADDRESS</th>
<th>TYPE</th>
<th>DATA</th>
<th>CRC</th>
</tr>
</thead>
</table>

**802.1Q ETHERNET FRAME**

<table>
<thead>
<tr>
<th>PREAMBLE</th>
<th>DESTINATION MAC ADDRESS</th>
<th>SOURCE MAC ADDRESS</th>
<th>TAG</th>
<th>TYPE</th>
<th>DATA</th>
<th>CRC</th>
</tr>
</thead>
</table>

**802.1Q TAG**

- TPID "0X8100"
- PRI
- CFI
- VLAN ID

**NEW**
The 802.1Q Tag in Detail

- **TPID**: Tag Protocol ID “0x8100” 16 bits
- **PRI**: Priority 3 bits
- **CFI**: Canonical Format ID 1 bit
- **VID**: VLAN Identifier 12 bits

**TAG CONTROL INFO**

2 bytes

<table>
<thead>
<tr>
<th>TPID</th>
<th>TCI</th>
</tr>
</thead>
</table>

2 bytes

<table>
<thead>
<tr>
<th>TPID</th>
<th>PRI</th>
<th>CFI</th>
<th>VID</th>
</tr>
</thead>
</table>

**802.1Q Tag Length = 32 bits or 4 bytes**
Where Does Tagging Occur?

Tag added to frame at Egress trunk interface / Tag stripped at Ingress trunk interface
VLAN Implementation & Examples
VLAN Configurations

LAN #1
LAN #2

Physical Separate Networks

VLAN Implementation

VLAN #1
VLAN #2

Inter-Switch Links

VLAN #1
VLAN #2
VLAN #1
VLAN #2
Trunk Link

VLAN #1 & #2

Trunk Inter-Switch Links

VLAN #1 & #2

Trunk Inter-Switch Links
Servers can have “Trunk” interfaces as well, especially in the virtualized data center environment.
Conceptual Configuration:
define vlan 100 & 200 in switch
set port 2 mode to access
set port 14 mode to access
set port 23 mode to trunk
allow vlan 100 & 200 on trunk port

Exact configuration command will vary by switch model / IOS version
Practical VLAN Configuration – 2
Cisco to HP Switch

Conceptual Configuration:
define vlan 100 & 200 in switch
set port 2 mode to access
set port 14 mode to access
set port 23 mode to trunk
allow vlan 100 & 200 on trunk port

Conceptual Configuration:
define vlan 100 & 200 in switch
set port 7 as untagged vlan 100
set port 24 as untagged vlan 200
set port 18 as tagged vlan 100 & 200

Cisco Terminology
Access Mode
Trunk Mode

HP Terminology
Untagged
Tagged
Takeaway Points

• **VLANs** Allow a Common Physical Infrastructure to Support Multiple Isolated Networks

• Each Network, Subnet, or VLAN is a **Broadcast Domain** With a Unique IP Address Scheme

• Ethernet Switches Minimize **Collision Domains**

• IP Routing Must Be Used for Communications Between VLANs

• IP Routers Create **Broadcast Domains**

• Network Traffic May Be Isolated Because of:
  – Policy
  – Regulations
  – Security
  – **Performance**

• An Ethernet Frame is “Tagged” to Denote VLAN Membership on a Trunk Interface
Further Study:

Suggested Study Books for CBNE Exam:
- Video Systems in an IT Environment by Al Kovalick
- Communications Systems and Networks, 3rd edition by Ray Horak
- LAN Wiring, 3rd Edition by James Trulove
- Network Warrior by Gary Donahue
- Ethernet: The Definitive Guide by Charles Spurgeon
- IP Address Management Principles and Practice by Timothy Rooney
- Digital Rights Management: Protecting and Monetizing Content by Joan Van Tassel
- Networking for Dummies, 9th edition by Doug Lowe
- Cisco CCNA Simplified by Paul Browning
CBNT
Certified Broadcast Networking Technician
• This certification is designed for persons who wish to demonstrate a basic familiarity with networking hardware as utilized in business and audio/video applications in broadcast facilities.

• Exam Focus:
  – Network topologies and layouts
  – Common network protocols
  – Wiring standards and practices
  – Maintenance, troubleshooting and connectivity issues
  – Challenges unique to broadcast-based networks

CBNE
Certified Broadcast Networking Engineer
• This certification is an “Advanced” level that reflects the skill and knowledge that will be required in today's world of converged IT and broadcast engineering.

• Exam Focus:
  – Audio/Video over IP
  – Digital Content Management
  – Video Systems in an IT World
  – Data Transmission Systems
  – General IT Hardware
There's more to networking than just hooking things up.
Thank You for Attending!

Wayne M. Pecena
Texas A&M University
w-pecena@tamu.edu
N1WP@tamu.edu

979.845.5662