IP Networking for Broadcast Engineers

Advertised Presentation Scope:
Course Level: Intermediate to Advanced Level

IP Networking for Broadcast Engineers is an intensive instructor-led class focused on major IP networking topics. The goal is to equip the broadcast engineer with the knowledge and understanding of IP networking fundamentals. The morning will focus on the principals of IP networking including the OSI and TCP models, physical layer technologies, IP addressing, IP subnetting, and applying best practices in the design of an IP address plan.

The afternoon will focus on applying the morning fundamentals to the understanding of routing protocols, switching fundamentals, VLAN implementation, and security best practices in network design.

The lecture will be supplemented with network design examples presented by virtual demonstration and class exercises designed to apply learned concepts in a practical manner. Students will receive a complete set of class notes, class exercises, and reference materials.

My Goals & Deliverables:

- Awareness of Major IP Networking Topics (broadcast application focused)
- Understanding of Topic Fundamentals & Practical Application Principals
- Where to Obtain Further Knowledge
- Foundation for CBNE Certification Exam
SBE Networking Certifications

**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 (coming in 2012)**
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
National SBE Certification Committee continues CBNE exam construction

by Terry Baun, CPBE, AMD, CBNT, SBE Certification Committee Member

You might think that creating a new level of SBE Certification based on practices already exist in the industry might be a relatively simple task, but let me assure you that is not the case.

Although drawing on the general configuration of the CBNT, the creation of the “advanced level” CBNE has been particularly challenging due to the vast rate of change in the IT industry and the field of video and audio playout and storage. With every minute, the distinction between media engineering and IT grows smaller, yet each still retains areas of knowledge that must be integrated with the other as we move forward with this technology.

Steps are being made. As you are reading this SBE hopes to have a final set of beta tests completed and fine-tune the question database and eliminate questions that are either too difficult or not difficult enough. Hopefully, there will be some crossover between CBNE subject matter (particularly in the revised question set currently in use) and the new CBNE questions. But what we hope to accomplish is to create a meaningful examination reflecting the knowledge and skills that are and will be required when working in today’s converged world of broadcast, media, and IT deployment. Remember, too, that the multiple-choice portion of the examination is “open book,” with the use of standard reference texts, tables, and calculators allowed. Previously-prepared notes, old exams, or other such study materials are not permitted.

Because the CBNE is an advanced level certification, as opposed to the CBNT technology-level, we are incorporating an essay question in the mix to allow candidates for CBNE a more free-form opportunity to demonstrate their knowledge of the subject matter. As with all advanced level certification exams, three essays will be provided and the candidate will be able to choose the one they wish to answer.

The essay questions are selected by the Certification Committee specifically for each applicant, based upon that applicant’s knowledge and experience as reflected in their certification application. Remember that all essay questions are strictly closed book, and not books, notes, or study materials of any kind are allowed to be used during that portion of the examination.

A Certificate Preview for this examination will be available prior to administration of the first CBNE exam, which we hope can take place by the end of 2012.

Society adds Best Social Media Site to annual SBE National Awards

A new award has been added to the list of honors presented by the society. The award for Best Social Media Site will recognize the chapter that best uses social media to update broadcast engineers on SBE chapter information and inform members pertinent to the engineering world.

In recent years, the up-to-the-minute, social media sites, such as, Facebook, Twitter, and LinkedIn have become useful communication tools for chapters and members.

This award allows members to recognize those who make a difference by keeping members connected to the SBE and the field of broadcast engineering. Nominations for this and other awards must be received by June 15.

For more information on all the awards and nomination forms, visit the Awards page under Membership on the SBE website. For questions, contact the SBE Awards Chairman Ralph Beamer, at SBEawards@broadcastoperations.net or the SBE Certification Director Megan Chappel, at mbchappel@sbe.org.

SBE Certification Exam Schedule

<table>
<thead>
<tr>
<th>Dates</th>
<th>Location</th>
<th>Application Deadline</th>
</tr>
</thead>
<tbody>
<tr>
<td>April 17</td>
<td>NAJ Show</td>
<td>March 23</td>
</tr>
<tr>
<td>June 1-14</td>
<td>Local Chapters</td>
<td>April 15</td>
</tr>
<tr>
<td>Aug. 3-15</td>
<td>Local Chapters</td>
<td>June 15</td>
</tr>
<tr>
<td>Nov. 2-12</td>
<td>Local Chapters</td>
<td>Sept 14</td>
</tr>
</tbody>
</table>
Certification Exams

MY DISCLAIMER

This class should not be considered a certification preparation class.

However the material presented will provide an excellent background in IP networking technology for those pursuing the SBE Certified Broadcast Networking Technologist (CBNT) or the Certified Broadcast Networking Engineer (CBNE) certifications.

Why Is This NOT a Preparation Class?

1. I have no personal knowledge of the certification exam question pools.
2. The published exam scope covers more than just IP networking.

What I Will Do With Regards to the CBNE:

1. Cover IP Networking Technology fundamentals and focus on topics which represents 60-70% of published exam content scope
2. Tailor network design examples towards possible CBNE “essay” questions
3. Provide suggested self-study material sources to address missing exam content
IP Networking for Broadcast Engineers
Course Outline

• 1. Introduction & Standards Organization Overview
• 2. OSI Reference Model
• 3. TCP Reference Model
• 4. TCP/IP Protocols
• 5. TCP and UDP Fundamentals
• 6. IP Addressing (IPv4)
• 7. IP Addressing (IPv6)
8. Switching & Routing Fundamentals
9. QoS Basics
10. Controlling Network Traffic & Security
11. Network Design Practical
12. Additional CBNE Topics:
   – Broadcast Digital Content Management & Workflow
   – General Server Hardware
   – Wireless Networking
1. Introduction & Standards
Organization Overview
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
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
Network Device Evolution

- **Repeater or Hub**
- **Bridge**
- **Switch**
- **Router**

Typical Devices Found

- **Sorta Layer 2**
- **Layer 2 Devices**
- **Layer 3 Device**
Network Topologies

- Bus Topology
- Mesh Topology
- Ring Topology
- StarBus Topology
Introduction

• **IP Networking – A Brief History:**
  – Development Began in the Early 70’s
  – **Goal** - Vendor Independent & Survivable Networking for DoD ARPAnet
  – The Name “internet” Came into Use for “Interconnecting ARPANet Sites”
  – Internet Protocol Version 4 Completed in 1978 – **IPv4**

• **Nomenclature Clarification:**
  – “internet” or “internetwork” means to interconnect networks
  – “Internet” refers to a specific global network of TCP/IP based systems
The Early Days

- First "Router" was the "Interface Message Processor – IMP"
- Developed in the late-60’s for ARPANET
- First message "lo" was sent on October 29, 1969 from UCLA to the Stanford Research Institute
- After recovery from a system crash, the word "login" was successfully transmitted
- *Life Has Never Been the Same Since!*

ARPANET Logical Map, March 1977

(Illustration of a network map showing connections between various locations like UCLA, Stanford, and others.)
Standards Organizations

De Jure & De Facto

• **IETF** – Internet Engineering Task Force
  – The Internet Standard **RFC’s** Originate Here
• **IEEE** - Institute of Electrical & Electronic Engineers
  – Ethernet & Wireless LAN Standards
• **EIA** – Electronic Industries Association
  – Focused on Physical Layer Standards
• **ISO** – International Standards Organization
  – OSI Reference Model Creation
• **ITU** – International Telecommunications Union
  – Global Telecommunications Standards (ie PSTN)
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
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
ITU – International Telecommunications Union

• ITU-T Sector:
  – ITU-T G-Series TRANSMISSION SYSTEMS AND MEDIA, DIGITAL SYSTEMS AND NETWORKS
  – ITU-T H-Series AUDIOVISUAL AND MULTIMEDIA SYSTEMS
  – ITU-T I-Series INTEGRATED SERVICES DIGITAL NETWORK
  – ITU-T X-Series DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

http://www.itu.int/ITU-T/info/structure.html
2. OSI Reference Model
Opens Systems Interconnection Reference Model (OSI stack)
OSI Model
The TCP/IP Architecture Begins Here

- **International Standards Organization (ISO) - Open Systems Interconnection Model**
  - Layered Model to Standardize the Networking Process
  - Guidelines to Provide Vendor-Independent Interoperability
  - Detailed by ITU-T X.200 Series of Recommendation
- Provides an *abstract description of the network communications process*
- Serves as a *Reference Model* + Associated Protocols
- Layers also reference to by numbers 1 – 7
  - Each Layer Relies on the Previous Layer and is Transparent to the Next Higher Level
    - *A Layer Only Interacts With the Layer Below It*
    - *A Layer Only Provides Capability for the Layer Above to Interact With It*
- Data is *Encapsulated* As It Travels Through the Model
OSI Model

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

Data Flow Layers

Application Layers

7 Application
6 Presentation
5 Session
4 Transport
3 Network
2 Data Link
1 Physical

Protocol Data Unit PDU

TCP / UDP SPX
IP IPX, ICMP, X25
Ethernet Token Ring, DECnet
Packet (Datagram)

Bits (data stream)

TCP / UDP SPX
IP IPX, ICMP, X25
Ethernet Token Ring, DECnet
Packet (Datagram)

Bits (data stream)

“All People Seem To Need Data Processing” OR “Please Do Not Throw Sausage Pizza Away”

“Some People Fear Birthdays”
Encapsulation

Data is “Encapsulated” As It Travels Through the Model
Encapsulation & De-Encapsulation

Application
Presentation
Session
Transport
Network
Data Link
Physical

TCP Header Upper Level Data
IP Header Data
LLC Header Data CS
MAC Header Data CS

0110010111001000111000111010

PDU
Segment
Packet
Frame

Application
Presentation
Session
Transport
Network
Data Link
Physical

Upper Level Data
Real – World OSI Model
RFC 2321

Important to Recognize During Troubleshooting

<table>
<thead>
<tr>
<th>Layer</th>
<th>Error ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>10</td>
</tr>
<tr>
<td>Religious</td>
<td>9</td>
</tr>
<tr>
<td>Political</td>
<td>8</td>
</tr>
<tr>
<td>Application</td>
<td>7</td>
</tr>
<tr>
<td>Presentation</td>
<td>6</td>
</tr>
<tr>
<td>Session</td>
<td>5</td>
</tr>
<tr>
<td>Transport</td>
<td>4</td>
</tr>
<tr>
<td>Network</td>
<td>3</td>
</tr>
<tr>
<td>Data Link</td>
<td>2</td>
</tr>
<tr>
<td>Physical</td>
<td>1</td>
</tr>
</tbody>
</table>

ID10T Errors Occur Here
The Physical Layer - 1

Receives frames from the Data Link layer
Places bits onto the physical network medium
Controls the signaling
Takes bits off the physical network medium
Sends constructed frames to the Data Link Layer
Ethernet Media Evolution

Topology Also Migrates from “Bus” to “Star” Based
## Ethernet Cable Wiring - Straight

### T568A Pin Out

<table>
<thead>
<tr>
<th>RJ45 Pin #</th>
<th>Wire Color (T568A)</th>
<th>Wire Diagram (T568A)</th>
<th>10Base-T Signal 100Base-TX Signal</th>
<th>1000Base-T Signal</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>White/Green</td>
<td><img src="image1.png" alt="Diagram" /></td>
<td>Transmit+</td>
<td>BL_DA+</td>
</tr>
<tr>
<td>2</td>
<td>Green</td>
<td><img src="image2.png" alt="Diagram" /></td>
<td>Transmit-</td>
<td>BL_DA-</td>
</tr>
<tr>
<td>3</td>
<td>White/Orange</td>
<td><img src="image3.png" alt="Diagram" /></td>
<td>Receive+</td>
<td>BL_DB+</td>
</tr>
<tr>
<td>4</td>
<td>Blue</td>
<td><img src="image4.png" alt="Diagram" /></td>
<td>Unused</td>
<td>BL_DC+</td>
</tr>
<tr>
<td>5</td>
<td>White/Blue</td>
<td><img src="image5.png" alt="Diagram" /></td>
<td>Unused</td>
<td>BL_DC-</td>
</tr>
<tr>
<td>6</td>
<td>Orange</td>
<td><img src="image6.png" alt="Diagram" /></td>
<td>Receive-</td>
<td>BL_DB-</td>
</tr>
<tr>
<td>7</td>
<td>White/Brown</td>
<td><img src="image7.png" alt="Diagram" /></td>
<td>Unused</td>
<td>BL_DD+</td>
</tr>
<tr>
<td>8</td>
<td>Brown</td>
<td><img src="image8.png" alt="Diagram" /></td>
<td>Unused</td>
<td>BL_DD-</td>
</tr>
</tbody>
</table>

### T568B Pin Out

<table>
<thead>
<tr>
<th>RJ45 Pin #</th>
<th>Wire Color (T568B)</th>
<th>Wire Diagram (T568B)</th>
<th>10Base-T Signal 100Base-TX Signal</th>
<th>1000Base-T Signal</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>White/Orange</td>
<td><img src="image9.png" alt="Diagram" /></td>
<td>Transmit+</td>
<td>BL_DA+</td>
</tr>
<tr>
<td>2</td>
<td>Orange</td>
<td><img src="image10.png" alt="Diagram" /></td>
<td>Transmit-</td>
<td>BL_DA-</td>
</tr>
<tr>
<td>3</td>
<td>White/Green</td>
<td><img src="image11.png" alt="Diagram" /></td>
<td>Receive+</td>
<td>BL_DB+</td>
</tr>
<tr>
<td>4</td>
<td>Blue</td>
<td><img src="image12.png" alt="Diagram" /></td>
<td>Unused</td>
<td>BL_DC+</td>
</tr>
<tr>
<td>5</td>
<td>White/Blue</td>
<td><img src="image13.png" alt="Diagram" /></td>
<td>Unused</td>
<td>BL_DC-</td>
</tr>
<tr>
<td>6</td>
<td>Green</td>
<td><img src="image14.png" alt="Diagram" /></td>
<td>Receive-</td>
<td>BL_DB-</td>
</tr>
<tr>
<td>7</td>
<td>White/Brown</td>
<td><img src="image15.png" alt="Diagram" /></td>
<td>Unused</td>
<td>BL_DD+</td>
</tr>
<tr>
<td>8</td>
<td>Brown</td>
<td><img src="image16.png" alt="Diagram" /></td>
<td>Unused</td>
<td>BL_DD-</td>
</tr>
</tbody>
</table>

*Pin 1 is the reference point for both T568A and T568B pin outs.*
# Ethernet Cable Wiring - Cross

<table>
<thead>
<tr>
<th>RJ45 Pin # (END 1)</th>
<th>Wire Color</th>
<th>Diagram End #1</th>
<th>RJ45 Pin # (END 2)</th>
<th>Wire Color</th>
<th>Diagram End #2</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>White/Orange</td>
<td></td>
<td>1</td>
<td>White/Green</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Orange</td>
<td></td>
<td>2</td>
<td>Green</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>White/Green</td>
<td></td>
<td>3</td>
<td>White/Orange</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Blue</td>
<td></td>
<td>4</td>
<td>White/Brown</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>White/Blue</td>
<td></td>
<td>5</td>
<td>Brown</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Green</td>
<td></td>
<td>6</td>
<td>Orange</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>White/Brown</td>
<td></td>
<td>7</td>
<td>Blue</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Brown</td>
<td></td>
<td>8</td>
<td>White/Blue</td>
<td></td>
</tr>
</tbody>
</table>

Crossover Ethernet Cable Pin Outs
Ethernet Cable Types

Cable Type Legend
- EIA/TIA-568B Straight-Through
- EIA/TIA-568B Cross-Over
- EIA/TIA-568A MDI
- EIA/TIA-568A MDIX

Router 1
- Ethernet 0
- Ethernet 1
- MDI
- MDIX

Router 2
- Ethernet 0
- Ethernet 1
- Ethernet 3
- MDI
- MDIX

Router 3
- Ethernet 0
- Ethernet 1

Router 1 connected to Router 2 via an Ethernet cable labeled 'EIA/TIA-568B' (Straight-Through), and Router 2 connected to Router 3 via an Ethernet cable labeled 'EIA/TIA-568B' (Cross-Over).
Ethernet Auto-Negotiation

• Auto Configuration of Port Duplex & Speed
  – Utilizes Ethernet FLP & NLP Bursts
• Duplex – Half Duplex or Full Duplex
• Speed - 100 / 1000 Mbps
• Be Careful With Depending Upon Auto-Negotiation
  – 10 Mbps Full Duplex is Not a Valid Mode
  – 100 Mbps Half Duplex Indicates Auto-Negotiation Failure
  – Duplex Mismatch = Poor Performance = CRC Errors

• Best Practice – Static Configure Infrastructure
Duplex Mismatch Result

When Duplex Mismatch Occurs:
High Collision Rate Results, thus Performance Reduced
## Ethernet

### Physical Medium

<table>
<thead>
<tr>
<th>IEEE</th>
<th>Cable Designation</th>
<th>Topology</th>
<th>Speed / Duplex / Media</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.3</td>
<td>10-Base-5</td>
<td>Bus</td>
<td>10Mbps / Half / Thicknet</td>
</tr>
<tr>
<td>802.3</td>
<td>10-Base-2</td>
<td>Bus</td>
<td>10Mbps / Half / Thinnet</td>
</tr>
<tr>
<td>802.3</td>
<td>10/100-Base-T</td>
<td>Star</td>
<td>10/100 Mbps / Half-Full / UTP</td>
</tr>
<tr>
<td>802.3u</td>
<td>100-Base-T</td>
<td>Star</td>
<td>100 Mbps / Half-Full / UTP (Cat 5)</td>
</tr>
<tr>
<td>802.3u</td>
<td>100-Base-FX</td>
<td>Star</td>
<td>100 Mbps / Full / MM Fiber</td>
</tr>
<tr>
<td>802.3ab</td>
<td>1000-Base-T</td>
<td>Star</td>
<td>1000 Mbps / Full / UTP (Cat 6)</td>
</tr>
<tr>
<td>802.3z</td>
<td>1000-Base-SX</td>
<td>Star</td>
<td>1000 Mbps / Full / MM Fiber</td>
</tr>
<tr>
<td>802.3z</td>
<td>1000-Base-LX</td>
<td>Star</td>
<td>1000 Mbps / Full / SM Fiber 1310nm</td>
</tr>
<tr>
<td>802.3z</td>
<td>1000-Base-ZX</td>
<td>Star</td>
<td>1000 Mbps / Full / SM Fiber 1550nm</td>
</tr>
</tbody>
</table>

and 20 Gigabit, 40 Gigabit, & 100 Gigabit Ethernet are emerging ……
The OSI Model & Ethernet Types

Data Link Layer

Physical Layer

LLC

MAC

Physical Layer

Ethernet

802.2

Ethernet 802.3

Ethernet 802.3u

Fast Ethernet

Ethernet 802.3z

Gigabit Ethernet

Ethernet 802.3ab

Gigabit Ethernet (copper)

Token Ring 802.6

FDDI
Ethernet GBIC & SFP Modules

“Giga-Bit Interface Converter” - GBIC Transceiver
SC Fiber Connector

“Single Form-factor Pluggable” – SFP (mini GBIC) Transceiver
LC Fiber Connector

Copper or Optical Based Transceiver to Provide Flexible Physical Interface

- 1000Base-T (some support 100/100-Base-T as well)
- 1000Base-SX / LX / ZX - Multi-Mode / Single-Mode Fiber
Fiber Optic Connector Types
Power Over Ethernet – “POE”

Nominal POE Voltage: 48 vdc
(44-57 vdc)

IEEE 802.3af
15.4 watts of power per port
IEEE 802.3at
32.4 watts of power per port
WAN Technology

- Generally Categorized as Dedicated, Circuit Switched, or Packet Switched:
  - Dedicated
    - T-Carrier (data)
    - Optical Carrier
  - Circuit Switched
    - ISDN – BRI
    - ISDN – PRI
    - T-Carrier (voice)
  - Packet Switched
    - X.25
    - Frame Relay
    - ATM
    - ADSL / HDSL
    - Metro Ethernet Offerings
WAN Component Example

Point – Point T-1 or DS-1

Possible Interfaces That Might Be Found:

- EIA/TIA-232
- EIA/TIA-449
- V.35
- X.21
- EIA-530

Network connections at the modem or CSU/DSU.
## WAN Link Types

<table>
<thead>
<tr>
<th>Line Type:</th>
<th>Signaling Type:</th>
<th>Bit Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>64</td>
<td>DS0</td>
<td>64 kbps</td>
</tr>
<tr>
<td>T1 or DS1</td>
<td>DS1</td>
<td>1.544 Mbps</td>
</tr>
<tr>
<td>T3 or DS3</td>
<td>DS3</td>
<td>44.735 Mbps</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SONET OC:</th>
<th>SONET STS:</th>
<th>Bit Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>OC-1</td>
<td>STS-1</td>
<td>52 Mbps</td>
</tr>
<tr>
<td>OC-3</td>
<td>STS-3</td>
<td>155 Mbps</td>
</tr>
<tr>
<td>OC-12</td>
<td>STS-12</td>
<td>622 Mbps</td>
</tr>
<tr>
<td>OC-48</td>
<td>STS-48</td>
<td>2400 Mbps</td>
</tr>
<tr>
<td>OC-96</td>
<td>STS-96</td>
<td>5000 Mbps</td>
</tr>
</tbody>
</table>
DS1 Configuration

• DS1 or T1 Types:
  – Channelized (voice)
  – PRI (ISDN) (voice or data)
  – Clear Channel (data)

• Encoding
  – AMI (voice)
  – B8ZS (data)

• Framing
  – D4 Super Frame (voice)
  – Extended Super Frame (data)

• Timing
  – Must specify source
The Data Link Layer - 2

Network Layer Packets Encapsulated into Frames

Hardware Addressing Scheme Implementation

Unique Sub-Layers: LLC & MAC
The Data Link Sub-Layers:

**Data Link Functions:**
- Package Frames
  - LLC Sublayer
  - Flow Control
  - Error Control (CRC)
  - Synchronization
- Transmit Frames
- Control Flow
- Error Correction
- Network ID
- MAC Sublayer
  - Physical Addressing (MAC Address)
  - Transmitting On The Media

**Data Link Frames:**
- Are Likely Ethernet Layer 2 Protocol Data Units
- But, they could be:
  - Token Ring Layer 2 Protocol Data Units
  - Frame Relay Layer 2 Protocol Data Units
Ethernet Basics
IEEE 802.3

• The “de facto Standard” of Networking Today!
• Based Upon Contention-Access to the Wire
• 4 Basic Building Blocks of the Ethernet System
  – The Ethernet Frame
    • 802.3 Raw Early Novell Netware IPX
    • 802.2 LLC Current Novell NetWare IPX
    • Ethernet II (DIX) TCP/IP
    • Ethernet SNAP IPX, AppleTalk v2
  – The Ethernet Frame
  – Media Access Control Protocol
  – Signaling Components
  – Physical Medium

<table>
<thead>
<tr>
<th>Preamble</th>
<th>Destination MAC address</th>
<th>Source MAC address</th>
<th>Type/Length</th>
<th>User Data</th>
<th>Frame Check Sequence (FCS)</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>6</td>
<td>6</td>
<td>2</td>
<td>46 - 1500</td>
<td>4</td>
</tr>
</tbody>
</table>
## Ethernet Frame – Layer 2

### 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>
</tr>
</thead>
<tbody>
<tr>
<td>8 BYTES</td>
<td></td>
<td></td>
<td></td>
<td>46 – 1500 BYTES</td>
<td>4</td>
</tr>
<tr>
<td>6 BYTES</td>
<td></td>
<td></td>
<td>2</td>
<td>VARIABLE</td>
<td></td>
</tr>
<tr>
<td>6 BYTES</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2 BYTES</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Invalid FRAME Lengths:
- < 64 BYTES = “RUNT” FRAME
- > 1518 BYTES = “GIANT” FRAME

**Note** – Preamble Not Used in Frame Length Calculation

#### 64 Byte Minimum

---

---
MAC Address
“Media Access Control” Address

- Known as Hardware Address or Physical Address
- 48 bit / 6 Byte Unique Address in Hardware
- Expressed as 6 Groups of 2 Hex Characters
  **00:A0:C9:14:C8:29**
- 1st 3 Bytes = Organizational Unit Identifier “OUI”
  00:A0:C9 OUI Assigned to Intel
- 2nd 3 Bytes = Network Interface Controller “NIC”
  14:C8:29 is Unique to Hardware
- Also Expressed as: 00-A0-C9-14-C8-29
  00A0.C914.C829

**MAC Lookup:**
Ethernet Media Access Control Protocol
Carrier Sense Multiple Access with Collision Detection – “CSMA/CD”

• **CSMA/CD Process:**
  – Listen Before Sending
  – Detect Collisions
  – Jam Signal & Random Backoff
Some Ethernet Trivia

- **Conceptually Based Upon “ALOHA NET”**
  - Developed as a “Wireless” Network by Norman Abramson & colleagues
  - Deployed at the University of Hawaii in 1971

- **Later Refined at Xerox PARC in 1973**
  - Bob Metcalf & David Boggs “Fathers of Ethernet”

- **More Ethernet History:**
  
  http://ethernethistory.typepad.com/
The Network Layer - 3

Internetwork Communications Focused:

Packet Delivery from Source Host To Destination Host

Logical Addressing Scheme Implementation

Routing Decisions via Routing Protocols
IP Packet – Layer 3
RFC 791

<table>
<thead>
<tr>
<th>Field</th>
<th>Length</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version (4)</td>
<td></td>
<td>IP Protocol Version</td>
</tr>
<tr>
<td>Header (4)</td>
<td></td>
<td>Header Options</td>
</tr>
<tr>
<td>Precedence / Type (8)</td>
<td></td>
<td>Precedence Options</td>
</tr>
<tr>
<td>Identification (16)</td>
<td></td>
<td>Identification</td>
</tr>
<tr>
<td>Flag (3)</td>
<td></td>
<td>Flag</td>
</tr>
<tr>
<td>Offset (13)</td>
<td></td>
<td>Offset</td>
</tr>
<tr>
<td>Protocol (8)</td>
<td></td>
<td>Protocol Number</td>
</tr>
<tr>
<td>Time to Live (8)</td>
<td></td>
<td>Time to Live</td>
</tr>
<tr>
<td>Source IP Address (32)</td>
<td></td>
<td>Source IP Address</td>
</tr>
<tr>
<td>Destination IP Address (32)</td>
<td></td>
<td>Destination IP Address</td>
</tr>
<tr>
<td>Options &amp; Padding (0 or 32)</td>
<td></td>
<td>Options and Padding</td>
</tr>
<tr>
<td>Packet Payload (Transport Layer Data)</td>
<td></td>
<td>Packet Payload</td>
</tr>
</tbody>
</table>

32 bits
20 Bytes
Ethernet Frame In More Detail

MAC Layer

Preamble 64 Bits
Destination Address 48 Bits
Source Address 48 Bits
Type 16 Bits
Data 46 - 1500 Bits
FCS 32 Bits

Transport Layer

IP Header
Source Address
Destination Address
Data

172.15.1.1
The Transport Layer - 4

- Implements Reliable End-End Data Transport
- Implements Error Detection / Correction
- Establishes Virtual Connect Between Hosts
- Provides Segmentation, Sequencing, Flow Control
Ports
RFC 1700

• Applications Are Indexed by a “Port Number”
• Allows Datagrams to be Multiplexed Between Applications

• Port Numbers Can Be Between 0 - 65535
  – 0–1023 Are Considered Reserved
  – 1024–49151 Can Be Registered
  – 49152–65535 Are Considered Dynamic or Private

• TCP and UDP Port Numbers Are Independent
Common Port Numbers

- **RESERVED PORTS**
  - **“System Port Numbers”**
    - Port 20 / 21 – FTP “File Transfer Protocol”
    - Port 23 – TELNET
    - Port 53 – DNS “Domain Name Service”
    - **Port 80 – HTTP**
    - Port 110 – POP3 “Post Office Protocol”
    - Port 123 – NTP “Network Time Protocol”
    - Port 161 – SNMP “Simple Network Management Protocol” (UDP)
    - Port 443 - HTTPS

- **REGISTERED PORTS**
  - **“User Port Numbers”**
    - Port 1720 – H.323 Video Call Setup
    - Port 1812 – RADIUS Authentication
    - Port 2000 – CISCO “Skinny”
    - Port 3074 – “X-Box” Live
    - Port 4664 – Google Desktop
    - Port 5004 – RTP “Real Time Transport Protocol”
    - Port 5060 – SIP “Session Initiation Protocol”
    - Port 5631 – PC Anywhere
    - Port 8080 – Alternate HTTP

http://www.iana.org/assignments/port-numbers
Sockets

- A "Socket" is a combination of an IP Address & A Port Number
- Used for Client-Server Application Interaction
- IP Address + Port Number = Socket

IP Address: 10.10.10.10
Port Number: 80

Socket: 10.10.10.10:80
### Ports & Sockets

#### Ports

**RFC 1700**

- Allows Datagram Multiplexing Between Applications
- **Port Numbers Can Be Between 0 - 65535**
  - 0–1023 Are Considered Reserved
  - 1024–49151 Can Be Registered
  - 49152–65535 Are Considered Dynamic or Private
- TCP and UDP Port Numbers Are Independent

#### Sockets

- A “Socket” Is a Combination of an IP Address & A Port Number
- Used for Client-Server Application Interaction
- IP Address + Port Number = Socket
  
  **Socket**: `10.10.10.10:80`
3. TCP Reference Model
An Implementation of the OSI Model
TCP/IP Model
DOD Model Stack or TCP/IP Model Stack Focused on IP

**OSI Model**
- Application
- Presentation
- Session
- Transport
- Network
- Data Link
- Physical

**DoD Model**
- Application
- Host to Host
- Internet
- Network

**TCP/IP Model**
- Application
- Transport
- Internet
- Network Interface

TCP/IP Focused
The Models in Comparison

<table>
<thead>
<tr>
<th>The OSI Model</th>
<th>TCP/IP Model</th>
<th>Encapsulation</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>Application</td>
<td>4</td>
</tr>
<tr>
<td>6</td>
<td>Presentation</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Session</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Transport</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>Network</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>Data Link</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>Physical</td>
<td></td>
</tr>
</tbody>
</table>

The OSI Model is a conceptual framework model independent of protocol.

The TCP/IP Model is an implementation of the OSI Model that describes the framework of the TCP/IP protocol suite.

TCP/IP describes how data is addressed, routed, and formatted for end-end connectivity between computer hosts.
4. TCP/IP Protocols
(TCP/IP Application Layer Protocols)

ARP, DNS, DHCP
HTTP, SMTP, FTP, Telnet, and the list goes on......
Primary TCP/IP System Protocols:

• **ARP** – Address Resolution Protocol

• **DHCP** – Dynamic Host Configuration Protocol

• **DNS** – Domain Name System

• **ICMP** – Internet Control Message Protocol
ARP Operation

Host 1:
192.168.1.10
00:07:E9:D4:EC:9A

Host 2:
192.168.1.20
00:07:E9:D4:EC:9B

Host 3:
192.168.1.30
00:07:E9:D4:EC:9C

Host 4:
192.168.1.40
00:07:E9:D4:EC:9D

Host 5:
192.168.1.50
00:07:E9:D4:EC:9E
DHCP Operation

Client

DHCP Discover – IP Address Request
DHCP Offer – IP Address Offer
DHCP Request – Select IP Address
DHCP ACK – Ack IP Address

DHCP Server

Router
Configured for DHCP Server

Must define:
- IP Pool
- Lease Period (default = 8 days)

DHCP provides IP Address & Mask.
DHCP can also provide the Default Gateway, Domain Name, DNS Server Info, & Time Server Info
DNS Operation

- DNS Provided:
  - Manual Configuration (Hosts file)
  - Dynamic Configuration via DNS Server
    - Primary Server – Authoritative Server – Master Zone File
    - Secondary Slave Server
    - Caching Server

```
C:\Documents and Settings\user>nslookup
Default Server: dns-cache-1.net.tamu.edu
Address: 128.194.254.1

> set querytype=soa
> tamu.edu
Server: dns-cache-1.net.tamu.edu
Address: 128.194.254.1

Name: tamu.edu
Class: IN
TTL: 604800
Serial: 90025915
Refresh: 7200 (2 hours)
Retry: 3600 (1 hour)
Expire: 604800 (7 days)
Default TTL: 28800 (8 hours)
  primary name server = ns1.tamu.edu
  responsible mail addr = dns.tamu.edu
  nameserver = ns2.tamu.edu
  nameserver = ns3.tamu.edu
  nameserver = ns1.tamu.edu
ns1.tamu.edu  internet address = 128.194.254.4
ns2.tamu.edu  internet address = 128.194.254.5
ns3.tamu.edu  internet address = 192.195.87.5
```
DNS Hierarchy

Root DNS Servers
www.root-servers.org

Top Level Domain Servers
.com
.org
.edu

Secondary – Level Domain Servers
ClearChannel.com
SBE.org
TAMU.edu

DNS Client
DNS Example
ICMP

• Sends Error & Control Messages Between Hosts – Common Messages Include:
  – Echo
  – Echo Reply
  – Destination Unreachable
  – Time Exceeded
  – Source Quench
  – And Others ......
ICMP Messages:

- Platform Utilized by Ping & Traceroute Utilities

<table>
<thead>
<tr>
<th>Type</th>
<th>Name</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Echo Reply</td>
<td>[RFC792]</td>
</tr>
<tr>
<td>1</td>
<td>Unassigned</td>
<td>[JBP]</td>
</tr>
<tr>
<td>2</td>
<td>Unassigned</td>
<td>[JBP]</td>
</tr>
<tr>
<td>3</td>
<td>Destination Unreachable</td>
<td>[RFC792]</td>
</tr>
<tr>
<td>4</td>
<td>Source Quench</td>
<td>[RFC792]</td>
</tr>
<tr>
<td>5</td>
<td>Redirect</td>
<td>[RFC792]</td>
</tr>
<tr>
<td>6</td>
<td>Alternate Host Address</td>
<td>[JBP]</td>
</tr>
<tr>
<td>7</td>
<td>Unassigned</td>
<td>[JBP]</td>
</tr>
<tr>
<td>8</td>
<td>Echo</td>
<td>[RFC792]</td>
</tr>
<tr>
<td>9</td>
<td>Router Advertisement</td>
<td>[RFC1256]</td>
</tr>
<tr>
<td>10</td>
<td>Router Solicitation</td>
<td>[RFC1256]</td>
</tr>
<tr>
<td>11</td>
<td>Time Exceeded</td>
<td>[RFC792]</td>
</tr>
<tr>
<td>12</td>
<td>Parameter Problem</td>
<td>[RFC792]</td>
</tr>
<tr>
<td>13</td>
<td>Timestamp</td>
<td>[RFC792]</td>
</tr>
<tr>
<td>14</td>
<td>Timestamp Reply</td>
<td>[RFC792]</td>
</tr>
<tr>
<td>15</td>
<td>Information Request</td>
<td>[RFC792]</td>
</tr>
<tr>
<td>16</td>
<td>Information Reply</td>
<td>[RFC792]</td>
</tr>
<tr>
<td>17</td>
<td>Address Mask Request</td>
<td>[RFC550]</td>
</tr>
<tr>
<td>18</td>
<td>Address Mask Reply</td>
<td>[RFC550]</td>
</tr>
<tr>
<td>19</td>
<td>Reserved (for Security)</td>
<td>[Solo]</td>
</tr>
<tr>
<td>20-29</td>
<td>Reserved (for Robustness Experiment)</td>
<td>[ZSu]</td>
</tr>
<tr>
<td>30</td>
<td>Traceroute</td>
<td>[RFC1393]</td>
</tr>
<tr>
<td>31</td>
<td>Datagram Conversion Error</td>
<td>[RFC1476]</td>
</tr>
<tr>
<td>32</td>
<td>Mobile Host Redirect</td>
<td>[David Johnson]</td>
</tr>
<tr>
<td>33</td>
<td>IPv6 Where-Are-You</td>
<td>[Simpson]</td>
</tr>
<tr>
<td>34</td>
<td>IPv6 I-Am-Here</td>
<td>[Simpson]</td>
</tr>
<tr>
<td>35</td>
<td>Mobile Registration Request</td>
<td>[Simpson]</td>
</tr>
<tr>
<td>36</td>
<td>Mobile Registration Reply</td>
<td>[Simpson]</td>
</tr>
<tr>
<td>37</td>
<td>Domain Name Request</td>
<td>[RFC1788]</td>
</tr>
<tr>
<td>38</td>
<td>Domain Name Reply</td>
<td>[RFC1788]</td>
</tr>
<tr>
<td>39</td>
<td>SKIP</td>
<td>[Markson]</td>
</tr>
<tr>
<td>40</td>
<td>Photuris</td>
<td>[RFC2521]</td>
</tr>
<tr>
<td>41</td>
<td>ICMP messages utilized by experimental mobility protocols such as Seamoby</td>
<td>[RFC4065]</td>
</tr>
<tr>
<td>42-255</td>
<td>Reserved</td>
<td>[JBP]</td>
</tr>
</tbody>
</table>
Noteworthy TCP/IP System Protocols:

- FTP “File Transfer Protocol”
- TELNET
- HTTP
- POP3 “Post Office Protocol”
- NTP “Network Time Protocol”
- SNMP “Simple Network Management”
- HTTPS
5. TCP and UDP Fundamentals

TCP Fundamentals & Operation
UDP Fundamentals & Operation
TCP vs UDP Comparision
Unicast & Multicast
TCP / UDP

TCP - RFC 793
• Referred to as a "Connection – Oriented" Protocol
• Guaranteed Or Reliable Data Delivery
  – Acknowledgment of Packet Receipt
  – Retransmission Occurs if Packet Not Received or Error Occurs
• High Overhead thus Slow
• A TCP Conversation Requires Establishment of a 2-Way “Session” Between Hosts

UDP - RFC 768
• A “Simple” Protocol or “Lightweight”
• Low Overhead = Fast
• “Best Effort” – Non-Guaranteed Data Delivery
• Why Use?
  – Required for Real-Time Applications - VoIP or Video Transmission”
  – Latency More Detrimental Than Data Loss
TCP Handshake / UDP Data Flow

TCP

Send Host

SYNCHRONIZE – Establish Connection
SYNCHRONIZE & ACKNOWLEDGE
ACKNOWLEDGE – Send Data

Receive Host

UDP

Send Host

SYNCHRONIZE – Establish Connection
SYNCHRONIZE & ACKNOWLEDGE
ACKNOWLEDGE – Send Data
Send Data
Send Data
Send Data

Receive Host
## TCP vs UDP

<table>
<thead>
<tr>
<th>TCP HEADER</th>
<th>UDP HEADER</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Port</td>
<td>Source Port</td>
</tr>
<tr>
<td>Destination Port</td>
<td>Destination Port</td>
</tr>
<tr>
<td>Sequence Number</td>
<td>Length</td>
</tr>
<tr>
<td>Acknowledgment Number</td>
<td>Checksum</td>
</tr>
<tr>
<td>Flags</td>
<td>Window Size</td>
</tr>
<tr>
<td>Checksum</td>
<td>Urgent</td>
</tr>
<tr>
<td>Options</td>
<td></td>
</tr>
</tbody>
</table>
TCP Basics
RFC 793

- Referred to as a **“Connection – Oriented”** Protocol
- **Guaranteed** Or Reliable Data Delivery
  - Acknowledgment of Packet Receipt
  - Retransmission Occurs if Packet Not Received or Error Occurs
- High Overhead thus Slow
- A TCP Conversation Requires Establishment of a 2-Way “Session” Between Hosts

- **TCP Windowing**
  - Segment Acknowledgement
  - Dynamic Window Sizing
  - “Slow-Start”
TCP Session

3-Way Handshake

SYN
SYN / ACK
ACK

Segment Acknowledgment

Request
Data
Data
ACK
Data
ACK
FIN

TCP Connection Established
TCP 3-Way Handshake

Send Host:
- I Want to Connect. My Sequence Number is 100
  - SEQ = 100
  - CONTROL = SYN

Receive Host:
- SEQ = 100
  - CONTROL = SYN

Send Host:
- I Received Your Sequence 100! My Sequence Number is 1 & Ready for 101
  - SEQ = 1
  - ACK=100
  - CONTROL = SYN, ACK

Receive Host:
- I Received Your Sequence 1 & Ready for Sequence 2
  - SEQ = 101
  - ACK=2
  - CONTROL = ACK
Handshake in More Detail:

- **SYN** – SEQ=0
  - Source Port = 1068 / Destination Port = 80

- **SYN, ACK** – SEQ=0 ACK=1
  - Source Port = 1068 / Destination Port = 80

- **ACK** – SEQ=1, ACK=1
  - Source Port = 80 / Destination Port = 1068

Connection Established
TCP Dynamic Window

Send Host

17 16 15 14 13 12 11 10

SEQ = 200
ACK=13
Window Size = 3

Window Size = 3
All Packets Dropped Past 12

Receive Host

17 16 15 14 13

Window=8

Window=8
TCP “Slow-Start”
RFC 1122

- Determines How Reliable a Connection Path is Between Two Hosts
- Transmit Larger and Larger Blocks of Data Until Path is Deemed “Reliable” or Receiver Window Size is Reached
- Window Size is Usually Based Upon Network Connection Bandwidth
  - Windows XP Default:
    - < 1 Mbps: 8 Kb
    - <100 Mbps: 17 Kb
    - >100 Mbps: 64 Kb
UDP Basics
RFC 768

• A “Simple” Protocol or “Lightweight”
• Low Overhead = Fast
• “Best Effort” – Non-Guaranteed Data Delivery
• Why Use?
  – Required for Real-Time Applications - VoIP or Video Transmission”
  – Latency More Detrimental Than Data Loss
• Used By:
  – DNS
  – SNMP
  – DHCP
  – TFTP
  – And others .....
UDP Session
Practical Protocol Analysis

“Visualization of Network Activity”

http://www.wiresharktraining.com/

www.wireshark.org
6. IP Addressing (IPv4)

Classful IP Addressing
Classless IP Addressing
Private vs Public IP Addresses
Private – Public Address Integration
IP Subnetting
Subnetting Basics
The Subnet Calculation Process
IP Address Classes

- **Class A** – 126 Networks / 16,777,214 Hosts
  - 1.0.0.0 to 126.0.0.0
- **Class B** – 16,384 Networks / 65,534 Hosts
  - 128.0.0.0 to 191.255.0.0
- **Class C** – 2,097,152 Networks / 254 Hosts
  - 192.0.0.0 to 192.255.255.0
- **Class D** – Multicast
  - 224.0.0.0 to 239.255.255.255
- **Class E** – Reserved
  - 240.0.0.0 to 255.255.255.255
IP Address Classes

“Classful” Public & Private

- **Class A** – 126 Networks / 16,777,214 Hosts
  - 1.0.0.0 to 126.0.0.0
  - PRIVATE - 10.0.0.0 to 10.255.255.255

- **Class B** – 16,384 Networks / 65,534 Hosts
  - 128.0.0.0 to 191.255.0.0
  - PRIVATE - 172.16.0.0 to 172.31.255.255

- **Class C** – 2,097,152 Networks / 254 Hosts
  - 192.0.0.0 to 192.255.255.0
  - PRIVATE - 192.168.0.0 to 192.168.255.255
IP Address Classes

“32 Bit Dotted Decimal Notation”
IPv4 Provides $2^{32}$ or 4,294,967,296 IP Addresses

XXX.XXX.XXX.XXX

Class A
- NET ID: 8 Bits
- HOST ID: 24 Bits

Class B
- NET ID: 16 Bits
- HOST ID: 16 Bits

Class C
- NET ID: 24 Bits
- HOST ID: 8 Bits
Classful vs Classless IP Address Subnetting

• **Classful Environment IP Address Allocation:**
  – /8 address blocks
  – /16 address blocks
  – /24 address blocks

• **Classless Environment IP Address Allocation:**
  – Can Be Customized to Fit Environment

• **Benefits:**
  – Flexible Network Design
  – Allow Room For Growth
  – Efficient Use of Resources
VLSM & CIDR

VLSM
RFC 1009
• Variable Length Subnet Masking (VLSM)
  – Host Addressing & Routing Inside a Routing Domain
  – Allowed “Classless” Subnetting
    • Mask Information is Explicit
  – Allows More Efficient Use of Address Space – Taylor Address Space to Fit Network Needs
  – Allows You to Subnet a Subnet

CIDR
RFC 1517, 1518, 1519, 1520
• Classless Interdomain Routing (CIDR)
  – Class System No Longer Applies
  – Routing Between Routing Domains
  – Allows “Supernets” To Be Created
    • Combining a Group of Class C Addresses Into a Single Block
  – CIDR Notation (slanted notation):
    172.16.1.1 /16

Example:
Classful Addressing 165.95.240.136 Implied Mask 255.255.0.0
VLSM Addressing 165.95.240.136 Explicit Mask 255.255.255.192
CIDR Notation 165.95.240.136/26
VLSM
RFC 1009

• **Variable Length Subnet Masking (VLSM)**
  – Host Addressing & Routing Inside a Routing Domain
  – “*Classful*” Subnetting
    • Mask Was Assumed Based Upon Class
  – “*Classless*” Subnetting
    • Mask Information is Explicit
  – Allows More Efficient Use of Address Space
  – Allows You to Subnet a Subnet
CIDR
RFC 1517, 1518, 1519, 1520

- Classless Interdomain Routing (CIDR)
  - Class System No Longer Applies
  - Routing Between Routing Domains
  - Class A & B IP Address Exhaustion Pressured Class C Address Space
  - Allows “Routing Tables” To Be Reduced by Grouping Contiguous Class C Addresses into One Network
  - Allows “Supernets” To Be Created
    - Combining a Group of Class C Addresses Into a Single Block
  - **CIDR Notation (slanted notation):** 172.16.1.1 /16
IP Address Formats

Classful Addressing:
165.95.240.136
(Implied Mask 255.255.0.0)

VLSM Addressing:
165.95.240.136 255.255.255.192
(Explicit Mask 255.255.255.192)

CIDR Notation:
165.95.240.136/26
Private vs Public IP Addresses

- **RFC 1918 Established “Private” Address Space**
  - Class A: 10.0.0.0 to 10.255.255.255
  - Class B: 172.16.0.0 to 172.31.255.255
  - Class C: 192.168.0.0 to 192.168.255.255

- **Key Points:**
  - Private IP Addresses Are NOT Routable Outside the Local Network
  - Widely Used in Home & Industry Networks
  - May Be Translated With NAT At An Edge Router
    - Map Private Address Space to Public Address Space
NAT & PAT

NAT
• Translates IP Addresses
  – Limited IP Address Space
  – Security
• Static NAT
  – 1 to 1 Translation
  – Hides Real Host IP Address
• Dynamic NAT (PAT)
  – 1 to Many Translation

PAT
• Always Used with NAT
• Allows 65,536 “Inside” Hosts To Be Identified by a Socket Address
Network Address Translation – NAT

RFC 1631

- Allows Mapping Internal (private) Address Space to External (public) Address Space
  - Allows Internal IP Addresses to be Hidden (Security)
  - Can Conserve IP Address Space
Port-Based Network Address Translation – PAT
or “NAT Overload”

- Allows Mapping Internal (private) Address Space to a Single External (public) Address or Small Address Pool
  - Allows Multiple Internal Addresses to Share a Single Public Address
  - Translation In Place for Duration of Connection
  - Outside Users CANNOT Establish A Connection to an Internal Host

Static Mapping Example:
10.0.0.1 128.194.247.2:16529
10.0.0.2 128.194.247.2:16550
10.0.0.3 128.194.247.2:16888
and so forth...
Why Do We Subnet?

• Exact Reason Varies Based Upon Deployment:
  – Efficient Use of IP Address Space
    • Dividing Networks Into the “Right” Size
  – Performance
    • Create Broadcast Domains
  – Enhance Routing Efficiency – Reduce Routing Table Size
  – Network Management Policy and Segmentation
    • Grouping Hosts by Function or Purpose
    • Grouping Hosts by Ownership
    • Grouping Hosts Geographically
  – Job Security for Network Engineers!
Subnetting

• **What is a Subnet?**
  – Logical Subdivision of a Larger Network

• **Why Do We Subnet?**
  • Efficient Use of IP Address Space
  • Enhance Routing Efficiency – Reduce Routing Table Size
  • Network Management Policy and Segmentation
  • Job Security for Network Engineers!
Classful IP Address Subnetting

Provided IP Address Space: 200.25.0.0/16
Represents 4,096 IP Addresses
Or 256 /24 Class “C” Blocks

Goal:
Allocate Smaller Address Blocks Across Organization
Classful Environment Yields 16 Class “C” Blocks

Diagram:
- 200.25.31.0/24
- 200.25.30.0/24
- 200.25.29.0/24
- 200.25.28.0/24
- 200.25.27.0/24
- 200.25.26.0/24
- 200.25.25.0/24
- 200.25.24.0/24
- 200.25.23.0/24
- 200.25.22.0/24
- 200.25.21.0/24
- 200.25.20.0/24
- 200.25.19.0/24
- 200.25.18.0/24
- 200.25.17.0/24
- 200.25.16.0/24
- 200.25.15.0/24
- 200.25.14.0/24
- 200.25.13.0/24
- 200.25.12.0/24
- 200.25.11.0/24
- 200.25.10.0/24
- 200.25.9.0/24
- 200.25.8.0/24
- 200.25.7.0/24
- 200.25.6.0/24
- 200.25.5.0/24
- 200.25.4.0/24
- 200.25.3.0/24
- 200.25.2.0/24
- 200.25.1.0/24
- 200.25.0.0/8
Classless IP Address Subnetting

Provided IP Address Space: 200.25.0.0./16
Represents 4,096 IP Addresses

Goal:
Allocate Smaller Address Blocks Across Organization
To Suite Environment

200.25.16.0/21
200.25.24.0/22
200.25.28.0/23
200.25.30.0/23
Subnetting Basics

- Identifies the Boundary Between Network and Hosts
- “Subnetting” Simply Moves the Boundary!
  - Moves Boundary to the Right
  - IP Address Subnetting Applies to All Classes
  - Boundary Position Determined by the Subnet “Netmask”

- Expressed in Several Forms:
  - Doted Decimal Notation (same as IP address)
  - Slash Notation (also known as CIDR notation)

**IP Address 165.95.240.100 with Netmask of 255.255.255.0**

**OR**

**165.95.240.100 /24**
IP Subnetting Example

192.168.1.0/24

/24 = 254 hosts
/27 = 30 hosts
/28 = 14 hosts
Required Host IP Configuration Information

- IP Address
- Address Mask
- Gateway Address
- DNS Server Address(s)

Where Do We Get This Information?
<table>
<thead>
<tr>
<th>IP Address</th>
<th>Class A</th>
<th>Class B</th>
<th>Class C</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1.1.100</td>
<td>Class A</td>
<td>Class B</td>
<td>Class C ?</td>
</tr>
<tr>
<td>191.18.10.1</td>
<td>Class A</td>
<td>Class B</td>
<td>Class C ?</td>
</tr>
<tr>
<td>128.194.247.55</td>
<td>Class A</td>
<td>Class B</td>
<td>Class C ?</td>
</tr>
<tr>
<td>192.95.240.135</td>
<td>Class A</td>
<td>Class B</td>
<td>Class C ?</td>
</tr>
<tr>
<td>100.100.100.100</td>
<td>Class A</td>
<td>Class B</td>
<td>Class C ?</td>
</tr>
</tbody>
</table>
Decimal to Binary Conversion

255.255.192.0
Expressed in Binary

11111111.11111111.11000000.000000

<table>
<thead>
<tr>
<th>Power of 2</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>$2^8$</td>
<td>1</td>
</tr>
<tr>
<td>$2^7$</td>
<td>2</td>
</tr>
<tr>
<td>$2^6$</td>
<td>4</td>
</tr>
<tr>
<td>$2^5$</td>
<td>8</td>
</tr>
<tr>
<td>$2^4$</td>
<td>16</td>
</tr>
<tr>
<td>$2^3$</td>
<td>32</td>
</tr>
<tr>
<td>$2^2$</td>
<td>64</td>
</tr>
<tr>
<td>$2^1$</td>
<td>128</td>
</tr>
</tbody>
</table>
What Must Be Known About a Subnet?

**IP Address and Mask**

Provides:

First Network Address
First Network Address Assignable to a Host
Last Network Address Assignable to a Host
Broadcast Address

**192.0.0.0 /24**

Provides: 254 useable IP addresses

Mask: 255.255.255.0

Network Address (Wire Address) 192.0.0.0
First Network Address Assignable to a Host 192.0.0.1
Last Network Address Assignable to a Host 192.0.0.254
Broadcast Address 192.0.0.255
Subnet Calculation Examples

**192.0.0.0 /20**

Provides: **4094 useable IP addresses**  
Mask: 255.255.240.0

| Network Address (Wire Address) | 192.0.0.0 |
| First Network Address Assignable to a Host | 192.0.0.1 |
| Last Network Address Assignable to a Host | 192.0.15.254 |
| Broadcast Address | 192.0.15.255 |

**192.168.1.0 /28**

Provides: **14 useable IP addresses**  
Mask: 255.255.255.240

| Network Address (Wire Address) | 192.168.1.0 |
| First Network Address Assignable to a Host | 192.168.1.1 |
| Last Network Address Assignable to a Host | 192.168.1.14 |
| Broadcast Address | 192.168.1.15 |
IP Addressing Reverse Engineering
“A Useful Troubleshooting Tool”

• Verifying Proper Subnet Configuration When Given an IP Address and Subnet Mask
  – Determine Subnet Address Range
  – Determine “Assignable” IP Addresses
  – Determine Broadcast Address

• Subnetting When Given A Network Requirement

• Subnetting When Given A Host Requirement

You Are Provided:
IP Address / IP Mask
Subnetting Tutorial
“The Magic Box” Approach

The Complete Tutorial:
https://learningnetwork.cisco.com/docs/DOC-2413#comment-7559
## Exercise #1

<table>
<thead>
<tr>
<th>IP Address:</th>
<th>172.16.0.1</th>
<th>2^{11}01100</th>
<th>00010000</th>
<th>00000000</th>
<th>0000000001</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subnet Mask:</td>
<td>255.255.255.0</td>
<td>11111111111111111111111111111111</td>
<td>00000000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Subnet Number:</td>
<td>172.16.0.0</td>
<td>10101100</td>
<td>00010000</td>
<td>00000000</td>
<td>0000000000</td>
</tr>
<tr>
<td>First IP Address:</td>
<td>172.16.0.1</td>
<td>10101100</td>
<td>00010000</td>
<td>00000000</td>
<td>0000000001</td>
</tr>
<tr>
<td>Broadcast IP Address:</td>
<td>172.16.0.255</td>
<td>10101100</td>
<td>00010000</td>
<td>00000000</td>
<td>1111111111</td>
</tr>
<tr>
<td>Last IP Address:</td>
<td>172.16.0.254</td>
<td>10101100</td>
<td>00010000</td>
<td>00000000</td>
<td>1111111100</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Bit 1</th>
<th>OP</th>
<th>Bit 2</th>
<th>Yields</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>AND</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>AND</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>AND</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>AND</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>
### Exercise #2 & #3

**Exercise 2:** You are provided – **192.168.12.0 Mask 255.255.255.224.**

<table>
<thead>
<tr>
<th>IP Address:</th>
<th>192.168.12.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subnet Mask:</td>
<td>255.255.255.224</td>
</tr>
<tr>
<td>Subnet Number:</td>
<td></td>
</tr>
<tr>
<td>First IP Address:</td>
<td></td>
</tr>
<tr>
<td>Broadcast IP Address:</td>
<td></td>
</tr>
<tr>
<td>Last IP Address:</td>
<td></td>
</tr>
</tbody>
</table>

**Exercise 3:** You are provided – **192.168.100.0 Mask 255.255.254.0**

<table>
<thead>
<tr>
<th>IP Address:</th>
<th>192.168.100.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subnet Mask:</td>
<td>255.255.254.0</td>
</tr>
<tr>
<td>Subnet Number:</td>
<td></td>
</tr>
<tr>
<td>First IP Address:</td>
<td></td>
</tr>
<tr>
<td>Broadcast IP Address:</td>
<td></td>
</tr>
<tr>
<td>Last IP Address:</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Bit 1</th>
<th>OP</th>
<th>Bit 2</th>
<th>Yields</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>AND</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>AND</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>AND</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>AND</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>
Subnet Calculation Tools
### IP Addressing CIDR Conversion Reference

<table>
<thead>
<tr>
<th>CIDR Length</th>
<th>Mask</th>
<th># Networks</th>
<th># Hosts</th>
</tr>
</thead>
<tbody>
<tr>
<td>/1</td>
<td>128.0.0.0</td>
<td>128 A</td>
<td>2,147,483,392</td>
</tr>
<tr>
<td>/2</td>
<td>192.0.0.0</td>
<td>64 A</td>
<td>1,073,741,824</td>
</tr>
<tr>
<td>/3</td>
<td>224.0.0.0</td>
<td>32 A</td>
<td>536,870,912</td>
</tr>
<tr>
<td>/4</td>
<td>240.0.0.0</td>
<td>16 A</td>
<td>268,435,512</td>
</tr>
<tr>
<td>/5</td>
<td>248.0.0.0</td>
<td>8 A</td>
<td>134,217,728</td>
</tr>
<tr>
<td>/6</td>
<td>252.0.0.0</td>
<td>4 A</td>
<td>67,108,864</td>
</tr>
<tr>
<td>/7</td>
<td>254.0.0.0</td>
<td>2 A</td>
<td>33,554,432</td>
</tr>
<tr>
<td>/8</td>
<td>255.0.0.0</td>
<td>1 A</td>
<td>16,777,216</td>
</tr>
<tr>
<td>/9</td>
<td>255.128.0.0</td>
<td>128 B</td>
<td>8,388,608</td>
</tr>
<tr>
<td>/10</td>
<td>255.192.0.0</td>
<td>64 B</td>
<td>4,194,304</td>
</tr>
<tr>
<td>/11</td>
<td>255.224.0.0</td>
<td>32 B</td>
<td>2,097,152</td>
</tr>
<tr>
<td>/12</td>
<td>255.240.0.0</td>
<td>16 B</td>
<td>1,048,576</td>
</tr>
<tr>
<td>/13</td>
<td>255.248.0.0</td>
<td>8 B</td>
<td>524,288</td>
</tr>
<tr>
<td>/14</td>
<td>255.252.0.0</td>
<td>4 B</td>
<td>262,144</td>
</tr>
<tr>
<td>/15</td>
<td>255.254.0.0</td>
<td>2 B</td>
<td>131,072</td>
</tr>
<tr>
<td>/16</td>
<td>255.255.0.0</td>
<td>1 B</td>
<td>65,536</td>
</tr>
<tr>
<td>/17</td>
<td>255.255.128.0</td>
<td>128 C</td>
<td>32,768</td>
</tr>
<tr>
<td>/18</td>
<td>255.255.192.0</td>
<td>64 C</td>
<td>16,384</td>
</tr>
<tr>
<td>/19</td>
<td>255.255.224.0</td>
<td>32 C</td>
<td>8,192</td>
</tr>
<tr>
<td>/20</td>
<td>255.255.240.0</td>
<td>16 C</td>
<td>4,096</td>
</tr>
<tr>
<td>/21</td>
<td>255.255.248.0</td>
<td>8 C</td>
<td>2,048</td>
</tr>
<tr>
<td>/22</td>
<td>255.255.252.0</td>
<td>4 C</td>
<td>1,024</td>
</tr>
<tr>
<td>/23</td>
<td>255.255.254.0</td>
<td>2 C</td>
<td>512</td>
</tr>
<tr>
<td>/24</td>
<td>255.255.255.0</td>
<td>1 C</td>
<td>256</td>
</tr>
<tr>
<td>/25</td>
<td>255.255.255.128</td>
<td>2 subnets</td>
<td>128</td>
</tr>
<tr>
<td>/26</td>
<td>255.255.255.192</td>
<td>4 subnets</td>
<td>64</td>
</tr>
<tr>
<td>/27</td>
<td>255.255.255.224</td>
<td>8 subnets</td>
<td>32</td>
</tr>
<tr>
<td>/28</td>
<td>255.255.255.240</td>
<td>16 subnets</td>
<td>16</td>
</tr>
<tr>
<td>/29</td>
<td>255.255.255.248</td>
<td>32 subnets</td>
<td>8</td>
</tr>
<tr>
<td>/30</td>
<td>255.255.255.252</td>
<td>64 subnets</td>
<td>2</td>
</tr>
<tr>
<td>/31</td>
<td>255.255.255.254</td>
<td>none</td>
<td>none</td>
</tr>
<tr>
<td>/32</td>
<td>255.255.255.255</td>
<td>1/256 C</td>
<td>1</td>
</tr>
</tbody>
</table>
Special Use Address
RFC 5735

- 0.0.0.0/8 Network Address “Wire Address”
- 10.0.0.0/8 Private IP Address Space (RFC 1918)
- 127.0.0.0/8 Loopback Address
- 169.254.0.0/16 IETF Zero Configuration Address Space (RFC 3927)
- 172.16.0.0/16 Private IP Address Space (RFC 1918)
- 192.168.0.0/16 Private IP Address Space (RFC 1918)
- 224.0.0.0/4 Multicast Address Space
- 255.255.255.255/32 Broadcast Address

And many more special use cases..........
IP Address Trivia

• What is Special About **127.0.0.1**?
  – Actually Any Address Works in Range of 127.0.0.1 to 127.255.255.255
• Known as a “**Loop-Back**” Address
• Useful For:
  – Test Local IP Stack and Network Adapter Test
  – May Be Used by Client-Server Ap on Host

C:\Documents and Settings\user>ping 127.255.255.100
Pinging 127.255.255.100 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.255.255.100:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
  Approximately round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\user>
7. IP Addressing (IPv6)

IPv6 Terminology & Fundamentals
Addressing Concepts
IPv4 to IPv6 Migration & Integration Strategies
IP Address Distribution

- Assigned Internationally by “Internet Corporation for Assigned Names and Numbers (ICANN)” to One of 5 Regional Internet Registries (RIR)
- Allocated in North & South America by “American Registry for Internet Numbers (ARIN)”
  - US
  - Canada
  - South America
  - Caribbean
- Most User IP Addresses Obtained from an Internet Service Provider - ISP
  - Exceptions: Large Companies / Organizations, Higher Education, Federal & State Government, etc.
5 Regional Internet Registries (RIR)
ICANN Available IPv4 Space

<table>
<thead>
<tr>
<th>Year</th>
<th>Mar</th>
<th>Jun</th>
<th>Sep</th>
<th>Dec</th>
<th>Mar</th>
<th>Jun</th>
<th>Sep</th>
<th>Dec</th>
<th>Mar</th>
<th>Jun</th>
<th>Sep</th>
<th>Dec</th>
<th>Mar</th>
<th>Jun</th>
<th>Sep</th>
<th>Dec</th>
<th>Feb</th>
</tr>
</thead>
<tbody>
<tr>
<td>'06</td>
<td>62</td>
<td>62</td>
<td>59</td>
<td>55</td>
<td>49</td>
<td>49</td>
<td>44</td>
<td>42</td>
<td>41</td>
<td>39</td>
<td>39</td>
<td>34</td>
<td>32</td>
<td>30</td>
<td>26</td>
<td>26</td>
<td>22</td>
</tr>
<tr>
<td>'07</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>'08</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>'09</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>'10</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>'11</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The chart shows the available IPv4 space available from March 2006 to February 2011.
IPv4 Address Depletion

- Recent Press About IP Address Depletion
- As of February 2011 ALL ICANN IPv4 Address Space Assigned!
- Regional Registries Now Have Their Last Allocation!

IPv6 adoption at critical phase

Montevideo, 3 February 2011 -- The Number Resource Organization (NRO) announced today that the free pool of available IPv4 addresses is now fully depleted. On Monday, January 31, the Internet Assigned Numbers Authority (IANA) allocated two blocks of IPv4 address space to APNIC, the Regional Internet Registry (RIR) for the Asia Pacific region, which triggered a global policy to allocate the remaining IANA pool equally between the five RIRs. Today IANA allocated those blocks. This means that there are no longer any IPv4 addresses available for allocation from the IANA to the five RIRs.

IANA assigns IPv4 addresses to the RIRs in blocks that equal to 1/256th of the entire IPv4 address space. Each block is referred to as a "/16" or "slash-16". A global policy agreed on by all five RIR communities and ratified in 2009 by ICANN, the international body responsible for the IANA function, dictated that when the IANA IPv4 free pool reached five remaining /16 blocks, these blocks were to be simultaneously and equally distributed to the five RIRs.

"This is an historic day in the history of the Internet, and one we have been anticipating for quite some time," states Rod Echeberria, Chairman of the Number Resource Organization (NRO), the official representative of the five RIRs. "The future of the Internet is in IPv6. All Internet stakeholders must now take definitive action to deploy IPv6."
IPv4 Run Down Model

Source: http://www.potaroo.net/tools/ipv4/plotvar.png
IPv6 Address Space
IETF - RFC 2460

IPv6 Provides Expanded IP Address Space
\[ 2^{128} = 340,282,366,920,938,463,463,374,607,431,768,211,456 \]
(three hundred forty UNDECILLION addresses)
\[ 3.4 \times 10^{38} \]

• But, IPv6 is More Than Expanded Address Space:
  – An Opportunity to Re-Engineer IPv4
    • Improved Support for Multicasting, Security, & Mobile Aps
    • Multiple Addresses per Interface
    • Host Auto-Configuration Capability
    • Security Incorporated
    • MTU Discovery Incorporated
    • Traffic Engineering Provisions Incorporate
The IPv6 Address

128-Bit Address Binary Format:
00100110000001111011100000000001111010100000000011010000110101011001100011000100010100011110001

Subdivide Into Eight (8) 16-bit Groups:
0010011000000111 1011100000000000 0001111110101010 0000000000000011
0010000110010101 1001100010000111 1011110001001000 001010001111001

Convert Each 16-bit Group to Hexadecimal:
(separate with a colon)
2607:800:0faa:0003:2195:9887:bc48:28f1
2607:b800:faa:3:2195:9887:bc48:28f1
Address Summarization

128-Bit Address Represented as a 32 Hexadecimal Digits Subdivided Into Eight Groups (Chunks, Quads, Quartets) of Four Hexadecimal Digits (separated by colon)

2001:0000:0000:0000:0DB8:8000:200C:417A
or
2001:0:0:0:DB8:8000:200C:417A
or
2001::DB8:8000:200C:417A
IPv6 Representation

• IPv6 Address in a URL:

In IPv4:  https://192.168.1.1:8080

In IPv6: Address 2001::0DB8:8:200C:417A
Entered in URL within [Brackets] as:
 https://[2001::0DB8:8:200C:417A]:8080
IPv6 Is More Than Address Space

“An Opportunity to Re-Engineer IPv4”

• Improved Authentication and Security
• Host Auto-Configuration
• Mobility Incorporated
IPv6 Header Simplification

Fewer Fields & Fixed Header Size Result in Faster Packet Processing
Providing Enhanced Routing Efficiency
Improved Authentication and Security

• IPsec is Mandatory in IPv6
  – IPv6 Is Not Necessarily More Secure Than IPv4

• Mandatory Implementation Ensures Enhanced Security:
  – Data Integrity
  – Authentication
  – Confidentiality
Host Auto-Configuration

- Simply Saves Network Administrators Work!
- Stateless Auto-Configuration
- Stateful Auto-Configuration
- Auto-Configuration Process:

  Host ID Generated from MAC Address:

  Generated IPv6 Address: 2002:80c2:f737::80c2:f737

  For Host with MAC Address: 80:C2:F7:37
Mobility Incorporated

- Provides Roaming Service Without Interrupting Connectivity
  - Ability to Move Between Networks
  - Maintains Home IP Address Regardless of Location
  - Establishes Care-Of IP Address When In a “Foreign” Network
- Similar in Concept to IPv4 Mobile IP
IPv6 Address Types

- **Unicast** – One-to-One Mapping
  - Global Unicast Address
  - Unique-Local Unicast Address (non-Routable or Private)
  - Link-Local Unicast

- **Multicast** – One-to-Many Mapping
  - Multicast Groups Established

- **Anycast** – One-to-Nearest Mapping
  - Packets Are Delivered to the “Closest, Nearest, or Lowest-Cost” Interface
    - Global Anycast
    - Site-Local Anycast
    - Link-Local Anycast
ARIN IPv6 Address Allocation Policies

• End-User / Enterprise Network
  – Qualify by Meeting IPv4 Qualifications
  – /48 Minimum Allocated
    • 65,536 subnets
    • Qualify for Larger Blocks by Justification of Proposed Use
      – Allocation Guideline – Large Sites: /48
      – Allocation Guideline – Small Sites: /56
IPv6 Address Assignment

- Service Provider: /32 \(2^{32} \) /64 subnets
- Large End User: /48 \(65,536 \) /64 subnets
- Small End User: /56 \(256 \) /64 subnets
- SOHO: /64 \(1 \) /64 subnets

A /64 IPv6 subnet = 18,446,744,073,709,552,000 hosts
Routed vs Host portion

- Every IPv6 Address is Divided Into:
  - Routed Portion
  - Host Portion
- The Block Size To-Be-Routed Specified by the Mask
- The Host Portion is the Interface Identifier

EXAMPLE: Global Unicast Address Format (Aggregatable & Routable)
Address Mask

- Every IPv6 Address is Divided Into Routed Portion & Host Portion
- Mask Specifies the Block Size To-Be-Routed

**EXAMPLE:** Global Unicast Address Format (Aggregatable & Routable)
# IPv4 and IPv6

## Comparison Summary

<table>
<thead>
<tr>
<th>IPv4</th>
<th>IPv6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Developed: 1973-1977</td>
<td>Developed: mid 1990’s</td>
</tr>
<tr>
<td>$2^{32}$ or 4.3 Billion Addresses</td>
<td>$2^{128}$ or 340 Undecillion Addresses</td>
</tr>
<tr>
<td>“More Than Anyone Could Possibly Use”</td>
<td>“More Than Anyone Could Possibly Use”</td>
</tr>
<tr>
<td>Address Based Assignment Unit /32</td>
<td>Network Based Assignment Unit /64</td>
</tr>
</tbody>
</table>
Why Slow IPv6 Implementation?

- FUD Principal
- "Does Not Apply to Me" – I Have adequate IP Address Space
- Another IT Industry “Crying Wolf” Event
- Low Priority – No “ROI” Seen
Where is IPv6 Growth?

• Internationally:
  - Developing Countries
  - Asian-Pacific Region

• In US, Those Needing for Large Quantities of IP Address Space:
  - Broadband Access Providers
  - Wireless Access Providers
Is the Year of IPv6 Here?

• Major Broadband Providers Now Deploying:
  – - Comcast
  – - Time Warner Cable
  – - AT&T

• Consumer Electronics Association predicts emergence of IPv6 enabled TVs, Blu-Ray Players, and related consumer devices in 2013
Migration Strategies

This Can Have Different Impact for:

• Broadband Access Providers
• Internet Service Providers
• **Content Providers (The Broadcaster)**
• Enterprise Customers
• Equipment Vendors
• Government Organizations
Migration

• Call to Action – Content Providers or “Broadcasters”
  
  - Provide “Outward” Facing Services in IPv4 and IPv6
  - Be Reachable By New IPv6 Only Internet Customers
  – - Be Reachable Without Translation Solutions
  – - Provide the “Best Quality” Experience to Content Consumer
Viewing the Network

Your Network
“Content Provider”

“Content Consumer”
IPv6 Implementation Techniques

• Tunnel
• Native
  – - IPv4 and IPv6 “Dual Stack”
• Translation Based
  – - Multiple Layer NAT – CGN
  – - NAT64
  – - NAT44
Migration Techniques

“Tunnel”

IPv4 Packet
IPv6 Header
IPv6 Data

Customer Network
IPv4 / IPv6

IPv4 Transport

IPv6 Transport

Internet Service Provider
IPv4

Internet Service Provider
IPv6
Migration Techniques

“Native or Dual-Stack”

Hosts Run IPv4 and IPv6 Simultaneously, But Independently

Advantages:
- Gradual IPv6 Host Implementation
- No Translation Devices – No Added Latency
Migration Techniques

“Translation”
Translation

But, Translation Is Bad for Real-Time Traffic!
Why IPv6?

• Reduction of Dependency Upon IPv4 Address Space for Growth
• Restores the End-End Communications Path Model of the Global Internet
• Enhances Overall Routing Efficiency
• Improved Security Increases Security and Confidentially
Takeaway Summary

• The Industry is Predominantly IPv4 Based Today
• IPv4 Demand Continues, But IPv4 Availability Pool Decreasing
• IPv6 Adoption is the Solution for Continued Growth
• A Growing IPv6 Only Environment Exists
• As a Content Provider, Focus on the “Content Consumer” to Guide Your Migration
• Focus on Outward Facing Services
• Translation is Not the Solution – Especially With Real-Time Media
• IPv6 Is Still IP, but IPv6 is NOT Backward Compatible With IPv4
• Expect IPv4 and IPv6 To Be Maintained for Many Years to Come
An IPv6 Address You Can Remember

The IPv6 Loopback Address
::1
Summarized from:
0:0:0:0:0:0:0:1

Equivalent of the IPv4 Loopback Address: 127.0.0.1
Learn More:
IPv6 Enable Your Home Network

But, My Provider is Not IPv6 Enabled!

Then “Tunnel” to an IPv6 Provider:

http://www.tunnelbroker.net/
IPv6 Test Sites

When both protocols are available, your browser uses IPv6

IPv6

Your internet connection is IPv6 capable

2607:b800:faa:3:2195:9887:bc48:28f1

American Registry Internet Numbers
Address type is
Global Unicast / Native IPv6

http://ipv6-test.com/

Your internet connection is IPv4 capable

165.95.240.136

r-wp.mv.tamu.edu
Texas A&M University

http://v6.testmyipv6.com/

Excellent!

You are successfully using IPv6 to connect to this server!


www.ARIN.net
World IPv6 Day

June 6, 2012

http://isoc.org/wp/worldipv6day/
“Who the hell knew how much address space we needed for an experiment?”
“Who the hell knew how much address space we needed for an experiment?”
“The experiment has not ended”
“The experiment has not ended”

“Vint” Cerf comments on his & colleagues 1977 decision to use 32-bit IP Numbers
What Happened to Version 5 or IPv5 of the Internet Protocol?

“IPv5 Simply Does Not Exist!

Version 5 was intentionally skipped to avoid confusion, or at least to rectify it. The problem with version 5 relates to an experimental TCP/IP protocol called the Internet Stream Protocol, Version 2, originally defined in RFC 1190. This protocol was originally seen by some as being a peer of IP at the Internet Layer in the TCP/IP architecture and these packets were assigned IP version 5 to differentiate them from “normal” IPv4 packets. This protocol never went anywhere, but to be absolutely sure that there would be no confusion, version 5 was skipped over in favor of version 6.”
8. Switching & Routing Fundamentals

Switching Fundamentals
MAC Addresses
VLANS
Routing Fundamentals
Routing Protocols
Routing Metrics
Which Routing Protocols Do I Use?
Switching vs Routing

When to Switch? -- When to Route?
Switching Fundamentals

• **Legacy Ethernet Used Hubs**
  - An “Ethernet DA” of sorts – All Bits Go to All Ports
  - High Collision Level Due to Shared Media
    - *(40-50% of Bandwidth Consumed by Collision Recovery)*
  - High Collision Level Yields High Latency

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

• **Switches Selectively Forward Individual “Frames”** from a Receiving Port to a Destination Port
Switching Fundamentals

- **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 Broadcast Frame
Ethernet Review
IEEE 802.3

An Ethernet II Frame

<table>
<thead>
<tr>
<th>Preamble</th>
<th>Destination Address</th>
<th>Source Address</th>
<th>Type</th>
<th>Data</th>
<th>CRC</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</td>
<td>4 Bytes</td>
</tr>
</tbody>
</table>

RECOGNIZE – THERE ARE MULTIPLE FRAME TYPES:

Original Ethernet Version 1 (no longer used)
**Most Common** Ethernet Version 2 – Ethernet II – DIX-Frame **Most Common**
Novell 802.3
IEEE 802.x LLC Frame
IEEE 802.x LLC - SNAP Frame

Invalid FRAME Lengths:
< 64 BYTES = “RUNT” FRAME
> 1518 BYTES = “GIANT” FRAME
MAC Addresses

- Layer 2 Media Access Control “MAC” Address

- Unique Hardware Encoded Address
  - Burned In Address
  - Physical Address
  - But Cab Be “Spoofed”

- Hexadecimal Format: 12:3A:4D:66:3A:1C or FF-FF-FF-FF-FF-FF

- Switches “Learn” a Table of MAC Addresses
  - MAC Table –

<table>
<thead>
<tr>
<th>Vlan</th>
<th>Mac Address</th>
<th>Type</th>
<th>Port</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>0100.0000.0000</td>
<td>STATIC</td>
<td>CPU</td>
</tr>
<tr>
<td>A1</td>
<td>0100.0000.0000</td>
<td>STATIC</td>
<td>CPU</td>
</tr>
<tr>
<td>A1</td>
<td>0100.0000.0000</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>Fa0/2</td>
</tr>
<tr>
<td>1</td>
<td>0009.0f0a.6974</td>
<td>DYNAMIC</td>
<td>Fa0/8</td>
</tr>
<tr>
<td>1</td>
<td>000b.db12.a3f9</td>
<td>DYNAMIC</td>
<td>Fa0/12</td>
</tr>
</tbody>
</table>
Ethernet Switch Function

• 5 Basic Functions of an Ethernet Switch:
  – Learning MAC Addresses
  – Aging – How Long is a MAC Address Maintained?
  – Flooding
  – Selective Forwarding
  – Filtering
A Simple MAC Table Example

**MAC Table:**

<table>
<thead>
<tr>
<th>ADDRESS</th>
<th>PORT</th>
</tr>
</thead>
<tbody>
<tr>
<td>00-00-0c-11-11-11</td>
<td>Fa/01</td>
</tr>
<tr>
<td>00-00-0c-22-22-22</td>
<td>Fa/02</td>
</tr>
<tr>
<td>00-00-0c-33-33-33</td>
<td>Fa/03</td>
</tr>
</tbody>
</table>
How is the MAC Table Populated?

Host A
172.15.2.2
00:12:3F:8D:4D:A7

Destination MAC 00:12:3F:8D:4D:A7
Source MAC

Destination IP 172.15.1.1
Source IP

DATA

Ethernet Frame

IP Packet
Simplified Ethernet Switch Internals
Switching Types
“Forwarding Method”

• **Store – and – Forward**
  – Receives the Entire Frame Then Makes Decision
  – Drops Any Errored Frame Based Upon CRC
  – SLOW! (but insures no frame errors)

• **Cut – Through**
  – Look Only @ Destination Address in Header of the Frame
  – FAST! (but no error checking)

• **Fragment Free (modified Cut-Through)**
  – Known as “Runt Free” Switching
VLANS

IEEE 802.1Q

• Virtual Local Area Network – VLAN
  – Logical Network of a Physical Network
• Allows Separation of Networks Across a Common Physical Media
  – Creates Subset of Larger Network
  – Control Broadcast Domains – Each VLAN is a Broadcast Domain
  – Architecture Flexibility
  – Security
• Static Port Based VLAN(s)
  – Most Popular
  – Manual Configuration
• Dynamic Port Based
  – MAC-Based VLAN(s)
    • Assignment Based Upon MAC Address
  – Protocol-Based VLAN(s)
    • Assignment Based Upon Protocol
VLAN Trunking

Sub-Interfaces:
eth0/1.1 VLAN 1
eth0/1.2 VLAN 2
eth0/1.3 VLAN 3

Public Internet

Switch 1
VLAN VLAN VLAN VLAN
1 2 3 4

Switch 2
VLAN VLAN
2 3

Switch 3
VLAN VLAN VLAN VLAN
1 2 3 4

Router

167
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
Spanning Tree Protocol “STP” Prevents a “Broadcast Storm”

**STP Operation:**
1 - Determine Root Bridge
2 - Select Root Port
3 - Select Designated Ports
4 - Block Ports with Loops
1. **Root Bridge Elected:**
   - First Powered On
   - Priority Configuration
   - Lowest MAC Address

2. **Root Ports Identified**
   Based Upon Path Cost

3. **Designated Ports Identified**
   Lowest Path Cost to Root

4. **Port Blocked**
   Designated Port with Highest Cost

**In The End:**
1 Root per Network / 1 Designated Port per Segment / 1 Root Port per Non-Root Switch
Port Mirroring

Analyze “Sniff” Data Flow Between Two Hosts

Port Mirroring Enabled:
Switch 2 Port E1 Frames Mirrored to Port E2
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
Routing

• Routing is Simply the Moving of Data Between Networks
• OSI Model Layer 3 Process
• Routing Involves Two Processes:
  – Determining the Best Path
  – Actually Sending of the Data
• Routing Types:
  – Static Routing
  – Dynamic Routing
• Routing Protocols:
  – Interior Gateway Protocol
    • Distance-Vector
    • Link-State
  – Exterior Gateway Protocols (BGP)
Routing Fundamentals

- Routing is Simply Moving Data From One Network to Another Network

![Routing Diagram]

<table>
<thead>
<tr>
<th>Destination Network</th>
<th>Next Hop Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.16.0.0/24</td>
<td>172.16.1.1/30</td>
</tr>
<tr>
<td>172.16.2.0/24</td>
<td>172.16.7.1/30</td>
</tr>
</tbody>
</table>

**Static Routing**
Table Manually Entered

**Dynamic Routing**
Table Generated by Routing Updates from All Routers

**IP Configuration**
172.16.2.2
255.255.255.0 mask
172.16.2.1 default gateway
Static Routing

• Static Routing Can Be Appropriate:
  – Small Networks – Stable Network
  – When an Isolated Network is Connected to a Single ISP
  – When an Isolated Network is Connected to a Hub-Spoke Network (single exit point)

• Advantages:
  – Absolute Control
  – Minimal Router CPU Demand
  – No Bandwidth Utilized for Router Communications

• Disadvantages:
  – Any Infrastructure Changes Must Be Manually Entered
  – No Fault Tolerance
  – Impossible to Manage in a Large Network Environment
Dynamic Routing
Determine the Best Path

• The “Best” Path Between Networks is Determined By Routing Algorithm Metrics Maintained in a Routing Table.
  – Administrative Distance (AD) – Trustworthiness of the Routing Information

<table>
<thead>
<tr>
<th>Route Source</th>
<th>Administrative Distance (default)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Direct</td>
<td>0</td>
</tr>
<tr>
<td>Static</td>
<td>1</td>
</tr>
<tr>
<td>EIGRP</td>
<td>90</td>
</tr>
<tr>
<td>OSPF</td>
<td>110</td>
</tr>
<tr>
<td>RIP</td>
<td>120</td>
</tr>
<tr>
<td>Unknown</td>
<td>255</td>
</tr>
</tbody>
</table>

Highest Reliability
Routing Metric Factors

- **Hop Count**: The Number of Routers in a Path
- **Bandwidth**: Throughput (bps)
- **Load**: Traffic Flowing Through a Router
- **Delay**: Network Latency (distance or congestion)
- **Reliability**: Amount of Downtime of a Network Path
- **Cost**: Administrator Assigned

Smaller Metrics = Best Route
Routing Type Applications:

• **Static Routing**
  – Appropriate for Small Networks
  – Appropriate for Stable Networks
  – Use in “Stub” Networks
  – Minimal Hardware / Easy Administration

• **Dynamic Routing**
  – Appropriate for Changing Topology Environments
  – Desirable When Multiple Paths Exist
  – More Scalable
  – Less Configuration Error Prone
## Static vs Dynamic Routing

<table>
<thead>
<tr>
<th>Static Routing</th>
<th>Dynamic Routing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Complexity Increases With Network Size</td>
<td>Network Complexity Independent</td>
</tr>
<tr>
<td>Human Intervention Required</td>
<td>Automatically Adapts to Topology</td>
</tr>
<tr>
<td>Simple Topology Suited</td>
<td>Complex Topology Suited</td>
</tr>
<tr>
<td>Secure</td>
<td>Less Secure</td>
</tr>
<tr>
<td>Routing Predictable Topology</td>
<td>Routing Dependant Upon Current Topology</td>
</tr>
<tr>
<td>Less Skill Required</td>
<td>Higher Skill Level Required</td>
</tr>
<tr>
<td>Reduced Hardware Requirements</td>
<td>Increased Hardware Requirements</td>
</tr>
</tbody>
</table>
Routing Protocols:

- Interior Gateway Protocols (IGP)
  - Used With Routers Under the Same Organizational Control
    - Distance-Vector
    - Link-State
- Exterior Gateway Protocol (EGP)
  - The Routing Protocol of the Internet (between ISP’s)

**Interior Gateway Protocol Sample:**
- RIP v1 & RIP v2
- IGRP
- EIGRP
- OSPF

**Exterior Gateway Protocol Sample:**
- IS-IS
- BGP v4 (BGP4)
## Routing Protocol Choices

<table>
<thead>
<tr>
<th></th>
<th>Interior Distance Vector</th>
<th>Interior Link State</th>
<th>Exterior Path Vector</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classful</td>
<td>RIP</td>
<td>IGRP</td>
<td>EGP</td>
</tr>
<tr>
<td>Classless</td>
<td>RIP v2</td>
<td>EIGRP</td>
<td>OSPF v2</td>
</tr>
<tr>
<td>IPv6</td>
<td>RIPng</td>
<td>EIGRP v6</td>
<td>OSPF v3</td>
</tr>
</tbody>
</table>

Our Focus
Distance-Vector Routing Protocols

- "Routing by Rumor" – The Overall Network is Unknown, Only Directly Connected Neighbors Are Known by Each Router
- Routing Decision Based Upon a "Distance" or Metric and "Direction" or Vector to Describe the "Next-Hop"

**Router A Route Table:**

<table>
<thead>
<tr>
<th>Destination</th>
<th>Nexthop</th>
<th>Metric</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router C</td>
<td>Router B</td>
<td>2</td>
</tr>
<tr>
<td>Router D</td>
<td>Router B</td>
<td>2</td>
</tr>
</tbody>
</table>

- Send Packets to Me To Reach Router C or D
- Routing Protocol Update
**Simplified Distance Vector Routing Example:**

After Convergence:

<table>
<thead>
<tr>
<th>Network</th>
<th>Metric</th>
<th>Next Node</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network 1</td>
<td>0</td>
<td>-</td>
</tr>
<tr>
<td>Network 2</td>
<td>0</td>
<td>-</td>
</tr>
<tr>
<td>Network 3</td>
<td>1</td>
<td>B</td>
</tr>
<tr>
<td>Network 4</td>
<td>2</td>
<td>B</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Network</th>
<th>Metric</th>
<th>Next Node</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network 2</td>
<td>0</td>
<td>-</td>
</tr>
<tr>
<td>Network 3</td>
<td>0</td>
<td>-</td>
</tr>
<tr>
<td>Network 4</td>
<td>0</td>
<td>-</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Network</th>
<th>Metric</th>
<th>Next Node</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network 3</td>
<td>0</td>
<td>-</td>
</tr>
<tr>
<td>Network 4</td>
<td>0</td>
<td>-</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Network</th>
<th>Metric</th>
<th>Next Node</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network 2</td>
<td>0</td>
<td>-</td>
</tr>
<tr>
<td>Network 3</td>
<td>0</td>
<td>-</td>
</tr>
<tr>
<td>Network 1</td>
<td>1</td>
<td>A</td>
</tr>
<tr>
<td>Network 4</td>
<td>1</td>
<td>C</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Network</th>
<th>Metric</th>
<th>Next Node</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network 3</td>
<td>0</td>
<td>-</td>
</tr>
<tr>
<td>Network 4</td>
<td>0</td>
<td>-</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Network</th>
<th>Metric</th>
<th>Next Node</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network 2</td>
<td>1</td>
<td>B</td>
</tr>
<tr>
<td>Network 1</td>
<td>2</td>
<td>B</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Network</th>
<th>Metric</th>
<th>Next Node</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network 3</td>
<td>0</td>
<td>-</td>
</tr>
<tr>
<td>Network 4</td>
<td>0</td>
<td>-</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Network</th>
<th>Metric</th>
<th>Next Node</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network 2</td>
<td>1</td>
<td>B</td>
</tr>
<tr>
<td>Network 1</td>
<td>2</td>
<td>B</td>
</tr>
</tbody>
</table>
Link-State Routing Protocols

- Network Topology Information is Flooded Throughout the Network
- Each Router Determines its Own “Best Path”
Link – State Algorithms

• More Efficient for Large Networks
• Maintains Topology of the Entire Network
• Only Forwards Updates When Changes Occur
  (OSPF “Paranoia” Updates Every 30 Minutes)
• Classless IP Addressing Supported
• Metrics More Complex – Thus More CPU Overhead
• Fast Convergence
• No Hop Count Limits
Routing Protocols: Which One is Best?
“*It Depends*”
## “Practical” Routing Protocol Comparison

### “Common” Interior Protocols – VLSM Support

<table>
<thead>
<tr>
<th></th>
<th>RIP v2</th>
<th>EIGRP (Cisco)</th>
<th>OSPF v2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type:</td>
<td>Distance Vector</td>
<td>Hybrid</td>
<td>Link-State</td>
</tr>
<tr>
<td>Metric:</td>
<td>Hop Count</td>
<td>Bandwidth/Delay</td>
<td>Cost</td>
</tr>
<tr>
<td>Administrative</td>
<td>120</td>
<td>90</td>
<td>110</td>
</tr>
<tr>
<td>Distance:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hop Count Limit:</td>
<td>15</td>
<td>224</td>
<td>None</td>
</tr>
<tr>
<td>Convergence:</td>
<td>Slow</td>
<td>Fast</td>
<td>Fast</td>
</tr>
<tr>
<td>Updates:</td>
<td>Full Table Every 30 Seconds</td>
<td>Send Only Changes When Change Occurs</td>
<td>Send Only When Change Occurs, But Refreshed Every 30m</td>
</tr>
<tr>
<td>RFC Reference:</td>
<td>RFC 1388</td>
<td>N/A</td>
<td>RFC 2328</td>
</tr>
</tbody>
</table>
RIP v2
Routing Information Protocol
RFC 1388

• **Advantages:**
  – Simple – Easy to Configure
  – Low Maintenance
  – General Understanding Of

• **Disadvantages:**
  – Higher Router CPU Utilization
  – High Bandwidth Use for Routing Updates
  – No Knowledge of Link Bandwidth
  – Slow Convergence
  – Limited Network Size (hop count = 15)
OSPF v2
Open Shortest Path First
RFC 2328

• **Advantages:**
  – Fast Convergence
  – Routing Updates Are Small
  – Scales to Varying Network Sizes
  – Considers Link Bandwidth Into Metric Calculation

• **Disadvantages:**
  – More Knowledge Required – A lot of Options
  – Complex to Configure
When to Route – When to Switch?

When to ROUTE?
“Breaks the Broadcast Domain”

When to SWITCH?
“Breaks the Collision Domain”
What Is A “Layer 3” Switch?

• “Marketing Terminology” Applied to a One Box Solution:
  – Layer 2 Switching or Forwarding
    • Traditionally Performed in Hardware
  – Layer 3 Routing or Forwarding
    • Traditionally Performed in Software

• Layer 3 Switch Performs Both

• Eliminates Use of VLAN(s) – Each Port Can Be Assigned to a Subnet

• Not for All Environments
  – Typically Found in Workgroup Environment
  – Limited to Ethernet
  – Limited to OSPF and RIP Protocols
Layer 3 “Routing Switch”

• Performs Layer 2 & Layer 3 Functions:
  
  – **Layer 2 Forwarding Performed:**
    • Destination MAC Address is different from the switch MAC Address
  
  – **Layer 3 Forwarding Performed:**
    • Destination MAC Address is the same as the switch MAC Address

• Remember – **No WAN Ports** (Ethernet Only)
Multi-Layer Switch Summary

- Layer 1 Switch = Really Does Not Exist - Often a Simple “Hub”
- Layer 2 Switch = Traditional Data-Link Layer Switching
- Layer 3 Switch = Performs Layer 3 Forwarding Decisions

- Layer 4 Switch = Implements Transport-Layer Flow Decisions
  - Firewall
  - VPN Concentrator
- Layer 7 Switch = Provides Applications Level Functionality
  - Often Based Upon a Uniform Resource Locator (URL):
    - Load Balancing
    - Content Management
9. QOS Basics

Why is QoS Needed?
QoS Fundamentals
Implementing QoS
Quality of Service – “QoS”

• Why QoS?
  – Allows Network Traffic to Be Prioritized Based Upon Application
    • Streaming Media
    • IP Telephony
    • Real-Time Control (automation)
    • Mission Critical Applications
  – Network Factors Impacting Quality:
    • Throughput
    • Dropped Packets
    • Errors
    • Latency
    • Jitter
    • Packet Delivery Out-of-Order
QoS continued…..

- Implementing QoS
  - VLAN Implementation
  - Bandwidth Over Provisioning
  - Traffic Shaping
  - DiffServ Implementation
    - Mark Packets According to Type of Service
    - Assigned to Multiple Queues
  - Queue Scheduling Algorithms:
    - Techniques Raise or Lower Queue Priority
      - WFQ - Weighted Fair Queuing
      - Class Based Weighted Fair Queuing
      - WRR – Weighted Round Robin
      - HFSC – Hierarchical Fair Service Curve
QoS continued…..

- **QoS Implementation Architecture**
  - Packet Identification & Marking
  - Network Element Provisioning
  - End-End Policy Management
Controlling Network Traffic

- Traffic Shaping (packet shaping) is Generally Achieved by Delaying Packets
- Used to Optimize or Guarantee Performance
- Control Volume of Traffic Placed on A Network Segment (ingress)
- Traffic Classification:
  - Sensitive
  - Best-Effort
  - Undesired Traffic
  - File Sharing (P2P Traffic)
Packet Filtering & Shaping

- **Packet Filtering**
  - A Firewall is Used to Create a “Trusted” Network Segment by Permitting or Denying Network Packets
  - Can Be Implemented in Router with Access Control Lists (ACL)
  - Ingress Filtering
  - Egress Filtering
  - Types of Firewalls:
    - Packet Filtering:
      - Stateless – Filters Solely on Packet Info
      - Statefull – Identifies as Packet Stream Component
    - NextGen – Provide Application Awareness

- **Packet Shaping**
  - A Traffic Shaper is Used to Control the Volume of Traffic on a Network Segment
  - Generally Achieved by Delaying Packets
  - Traffic is Classified – Rules Applied Based Upon Classification
10. Controlling Network Traffic & Security
The Challenge

SECURITY    USEABILITY
Goals of Network Security

• **Confidentiality**
  “Keeping Data Private”

• **Integrity**
  “Insuring Data Has Not Been Modified”

• **Availability**
  “Insuring Data is Available to the Intended User”
IT Infrastructure Threats

- Viruses
- Worms
- Trojan Horse
- Spyware & Adware
- Botnets “Zombie Computer”

- Operating Systems
- File System / Media
- Application
  - Web Services
  - Email Services
  - P2P
- Wireless / Mobile Environment
- Social Engineering
- And the list goes on & on.....
Network Infrastructure Threats

• Denial of Service “DoS”
• Spoofing
• Hijacking
• Authentication Bypass or “Back Door” Access
• Physical Access
• And the list goes on & on.....
Network Security – The First Step

• Control Access to the Network
  – Open or Available LAN Switch Ports?
  – Can I get an IP Address?
  – If I get an IP Address, can I get Network Access?

• First Step:
  – Lock down all LAN switch ports
  – Require Users & Devices to Authenticate (802.1xX)
Switch Port Security
“Port Lockdown”

• An Important Feature of Implementing Switch Infrastructure

• Port Security Aspects:
  – One MAC Address Per Port
    • Dynamic
    • Static
  – n MAC Addresses Per Port
  – Unused Ports Disabled
  – MAC Violation Action
  – VLAN Specified Per Port
Network Security Concerns

• Focused on Protecting the Network Infrastructure

• **Common Threats:**
  – DHCP Snooping
  – ARP Spoofing (IP Spoofing)
  – Rogue Routers Advertisements
  – Denial of Service Attacks
  – Application Layer Attacks

• **Implementation Considerations:**
  – Know Your Enemy
  – Cost
  – Human Factors
  – Understand Your Network
  – Limit Scope of Access
  – Don’t Overlook Physical Security
Network Security Tools

• **Firewall**
  – Used to Create a “Trusted” Network Segment by Permitting or Denying Network Packets
  – Types of Firewalls:
    • Packet Filtering
      – Stateless
      – Stateful

• **Detection Tools**
  – Intrusion Detection Systems (IDS)
    • Signature Based
    • Anomaly Based
  – Intrusion Prevention Systems (IPS)
    • Combine Firewall & IDS Functions
Firewalls

**Firewall**
- Defines Traffic Types That Can Enter or Exit a Network
- Can Be Software Based
  - Access Control List “ACL” Applied to Router or Switch Interface – Ingress or Egress Filtering:
    - IP Address Filtering
    - Port Number Filtering
    - MAC Address Filtering
- May Be Hardware Based “Appliance”
Firewall Types:

Packet Filtering - “Stateless”

Packet Filtering - “Stateful”

HTTP Request

Blocked X

HTTP Reply

HTTP Request

HTTP Reply

Blocked X

Telnet Session
Layered Network Design

• Separate Network in “Layers” or Zones
  – External or Public Network
  – “DMZ” or Demilitarized Zone or Perimeter Network
  – Internal or Private Network(s)
Firewall Implementation
VPN Implementation

“Virtual Private Network”
Don Not Confuse VLAN’s and VPN’s

Essence of a VPN is a Tunnel Through a Network Infrastructure

Virtual Private Network – VPN Protocols
- IPsec with Encryption
- L2TP inside of IPsec
- SSL with Encryption
Some Best Practices to Consider

- Recognize Physical Security
- Change Default Logins
- Utilize Strong Passwords
- Disable Services Not Required
- Adopt a Layered Design Approach
- Segregate Network(s)
- Separate Networks via VLANS
- Implement Switch Port Security
- Utilize Packet Filtering in Routers & Firewalls
- Do Not Overlook Egress Traffic
- Deny All Traffic – Then Permit Only Required

- Keep Up With Equipment “Patches”
- Utilize Access Logging on Key Network Devices
- Utilize Session Timeout Features
- Encrypt Any Critical Data
- Restrict Remote Access Source
- Understand & Know Your Network Baseline
- Actively Monitor and Look for Abnormalities
- Limit “Need-to-Know”
- Disable External “ICMP” Access
Can You Balance Your Network Infrastructure?

The Goal – “Create a Secure But Useable Network”

USEABLE
11. Network Design Practical

Refer to Separate Handout Documents
## IP Address Allocation

<table>
<thead>
<tr>
<th>06 (1 subnet bit)</th>
<th>06 (2 subnet bits)</th>
<th>07 (3 subnet bits)</th>
<th>08 (4 subnet bits)</th>
<th>09 (5 subnet bits)</th>
<th>10 (6 subnet bits)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>01</td>
<td>02</td>
<td>03</td>
<td>04</td>
<td>05</td>
</tr>
<tr>
<td>01</td>
<td>02</td>
<td>03</td>
<td>04</td>
<td>05</td>
<td>06</td>
</tr>
<tr>
<td>02</td>
<td>03</td>
<td>04</td>
<td>05</td>
<td>06</td>
<td>07</td>
</tr>
<tr>
<td>03</td>
<td>04</td>
<td>05</td>
<td>06</td>
<td>07</td>
<td>08</td>
</tr>
<tr>
<td>04</td>
<td>05</td>
<td>06</td>
<td>07</td>
<td>08</td>
<td>09</td>
</tr>
<tr>
<td>05</td>
<td>06</td>
<td>07</td>
<td>08</td>
<td>09</td>
<td>10</td>
</tr>
</tbody>
</table>

### 01 (1, 14) Subnets

<table>
<thead>
<tr>
<th>26 (1 subnet bit)</th>
<th>27 (2 subnet bits)</th>
<th>28 (3 subnet bits)</th>
<th>29 (4 subnet bits)</th>
<th>30 (5 subnet bits)</th>
<th>31 (6 subnet bits)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>01</td>
<td>02</td>
<td>03</td>
<td>04</td>
<td>05</td>
</tr>
<tr>
<td>01</td>
<td>02</td>
<td>03</td>
<td>04</td>
<td>05</td>
<td>06</td>
</tr>
<tr>
<td>02</td>
<td>03</td>
<td>04</td>
<td>05</td>
<td>06</td>
<td>07</td>
</tr>
<tr>
<td>03</td>
<td>04</td>
<td>05</td>
<td>06</td>
<td>07</td>
<td>08</td>
</tr>
<tr>
<td>04</td>
<td>05</td>
<td>06</td>
<td>07</td>
<td>08</td>
<td>09</td>
</tr>
<tr>
<td>05</td>
<td>06</td>
<td>07</td>
<td>08</td>
<td>09</td>
<td>10</td>
</tr>
</tbody>
</table>

### 02 (1, 14) Subnets

<table>
<thead>
<tr>
<th>26 (1 subnet bit)</th>
<th>27 (2 subnet bits)</th>
<th>28 (3 subnet bits)</th>
<th>29 (4 subnet bits)</th>
<th>30 (5 subnet bits)</th>
<th>31 (6 subnet bits)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>01</td>
<td>02</td>
<td>03</td>
<td>04</td>
<td>05</td>
</tr>
<tr>
<td>01</td>
<td>02</td>
<td>03</td>
<td>04</td>
<td>05</td>
<td>06</td>
</tr>
<tr>
<td>02</td>
<td>03</td>
<td>04</td>
<td>05</td>
<td>06</td>
<td>07</td>
</tr>
<tr>
<td>03</td>
<td>04</td>
<td>05</td>
<td>06</td>
<td>07</td>
<td>08</td>
</tr>
<tr>
<td>04</td>
<td>05</td>
<td>06</td>
<td>07</td>
<td>08</td>
<td>09</td>
</tr>
<tr>
<td>05</td>
<td>06</td>
<td>07</td>
<td>08</td>
<td>09</td>
<td>10</td>
</tr>
</tbody>
</table>

### 03 (1, 14) Subnets

<table>
<thead>
<tr>
<th>26 (1 subnet bit)</th>
<th>27 (2 subnet bits)</th>
<th>28 (3 subnet bits)</th>
<th>29 (4 subnet bits)</th>
<th>30 (5 subnet bits)</th>
<th>31 (6 subnet bits)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>01</td>
<td>02</td>
<td>03</td>
<td>04</td>
<td>05</td>
</tr>
<tr>
<td>01</td>
<td>02</td>
<td>03</td>
<td>04</td>
<td>05</td>
<td>06</td>
</tr>
<tr>
<td>02</td>
<td>03</td>
<td>04</td>
<td>05</td>
<td>06</td>
<td>07</td>
</tr>
<tr>
<td>03</td>
<td>04</td>
<td>05</td>
<td>06</td>
<td>07</td>
<td>08</td>
</tr>
<tr>
<td>04</td>
<td>05</td>
<td>06</td>
<td>07</td>
<td>08</td>
<td>09</td>
</tr>
<tr>
<td>05</td>
<td>06</td>
<td>07</td>
<td>08</td>
<td>09</td>
<td>10</td>
</tr>
</tbody>
</table>

### 04 (1, 14) Subnets

<table>
<thead>
<tr>
<th>26 (1 subnet bit)</th>
<th>27 (2 subnet bits)</th>
<th>28 (3 subnet bits)</th>
<th>29 (4 subnet bits)</th>
<th>30 (5 subnet bits)</th>
<th>31 (6 subnet bits)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>01</td>
<td>02</td>
<td>03</td>
<td>04</td>
<td>05</td>
</tr>
<tr>
<td>01</td>
<td>02</td>
<td>03</td>
<td>04</td>
<td>05</td>
<td>06</td>
</tr>
<tr>
<td>02</td>
<td>03</td>
<td>04</td>
<td>05</td>
<td>06</td>
<td>07</td>
</tr>
<tr>
<td>03</td>
<td>04</td>
<td>05</td>
<td>06</td>
<td>07</td>
<td>08</td>
</tr>
<tr>
<td>04</td>
<td>05</td>
<td>06</td>
<td>07</td>
<td>08</td>
<td>09</td>
</tr>
<tr>
<td>05</td>
<td>06</td>
<td>07</td>
<td>08</td>
<td>09</td>
<td>10</td>
</tr>
</tbody>
</table>

### 05 (1, 14) Subnets

<table>
<thead>
<tr>
<th>26 (1 subnet bit)</th>
<th>27 (2 subnet bits)</th>
<th>28 (3 subnet bits)</th>
<th>29 (4 subnet bits)</th>
<th>30 (5 subnet bits)</th>
<th>31 (6 subnet bits)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>01</td>
<td>02</td>
<td>03</td>
<td>04</td>
<td>05</td>
</tr>
<tr>
<td>01</td>
<td>02</td>
<td>03</td>
<td>04</td>
<td>05</td>
<td>06</td>
</tr>
<tr>
<td>02</td>
<td>03</td>
<td>04</td>
<td>05</td>
<td>06</td>
<td>07</td>
</tr>
<tr>
<td>03</td>
<td>04</td>
<td>05</td>
<td>06</td>
<td>07</td>
<td>08</td>
</tr>
<tr>
<td>04</td>
<td>05</td>
<td>06</td>
<td>07</td>
<td>08</td>
<td>09</td>
</tr>
<tr>
<td>05</td>
<td>06</td>
<td>07</td>
<td>08</td>
<td>09</td>
<td>10</td>
</tr>
</tbody>
</table>
12. Additional CBNE Topics:

Highlights:
Broadcast Digital Content Management & Workflow
General Server Hardware
Wireless Networking
Broadcast Digital Content Management & Workflow

Acquisition
- Record
- Log
- QC

Production
- Ingest
- Encoder
- Add Metadata
- QC

Asset Management
- Catalog
- Search
- Archive
- Store

Distribution
- Encode
- Transcode
- Digital Rights Mgmt
- Brand
- Stream
- Transfer

Tutorial:
http://www.sbe.org/sections/IPandFileBasedArchitecture.php
Content Management & Workflow

- **Workflow:** The decisions and processes that occur in the broadcast plant when a Media Asset enters the system to the distribution of the Media Asset at the output of the system.

- **Media Asset (SMPTE definition):**

```plaintext
efficiency  metadata
            content  rights
   essence---metadata
   content---rights
      media asset
```

The efficiency metadata
            content  rights
   essence---metadata
   content---rights
      media asset
General Server Hardware

- Hard Disk Interface Types
  - SCSI
  - IDE
  - SATA
  - Fiber Channel (FC)
- RAID Basics
- NAS Fundamentals
- SAN Architecture

www.TomsHardware.com
Hard Disk Interface Types
Data Transfer Rate (maximum)

- SCSI: 160 MBps – 320 MBps
- IDE/ATA: 100 MBps – 133 Mbps
- SATA: 150 MBps – 300 Mbps
- FC: 400 MBps

Reference:
RAID Level Basics
Redundant Array of Independent Disks

• Choosing a RAID Level:
  – Cost
  – Data Availability (protection)
  – Performance (read/write)

• Levels:
  – RAID 0
  – RAID 1
  – RAID 5
  – RAID 10 (RAID 1 + 0)
  – And many more.........
RAID Level Overview:

**RAID Level 0**
- Data Blocks Stripped
- No Redundancy
- High Performance

2 disks minimum
Usable Capacity = 100%

**RAID Level 1**
- Data Blocks Mirrored
- High Redundancy
- Good Performance

2 disks minimum
Usable Capacity = 50%
RAID Level Overview:

**RAID Level 5**
- Data Blocks Stripped + Parity
- Good Redundancy
- Good Performance

“Most Popular Server Configuration”
- 3 – 16 disks
- Usable Capacity = 67 – 94%

**RAID Level 10 or “1 + 0”**
- Data Blocks Mirrored + Striped
- High Redundancy
- High Performance

“Best Configuration – Mission Critical Apps”
- 4 disks minimum
- Usable Capacity = 50%
NAS & SAN Architecture

Similar, But Different!

• **Network Attached Storage**
  NAS – Provides File System & Storage (stand alone)
  Shared Storage Over Shared Network

• **Storage Area Network**
  SAN – Provides Storage Only
  Shared Storage Over Dedicated Network
Wireless Fidelity Networking

• **802.11 Standards**
  - 802.11a 5 Ghz 54 Mbps (maximum)
  - 802.11b 2.4 Ghz 11 Mbps
  - 802.11g 2.4 Ghz 54 Mbps
  - 802.11n 2.4/5 Ghz 600 Mbps

• **Frequency Bands (ISM):**
  - 2.4 Ghz 2.4-2.497 Ghz
  - 5 Ghz 5.15 – 5.875 Ghz

• **Wireless Security**
  - WEP
  - WPA
  - WPA2 (802.11i)

**Tutorial:**
CBNE Recommended Study:
My Favorites:
“The TCP/IP Bible”

For any detail I might have over-looked today or not fully covered, you will find it in 1537 pages! 😊
Web Reference Sources:

• Subnet Calculation Tools:
  – www.subnet-calculator.com
  – iPhone / iPad App: (iTunes Store): The MASK

• RFC Documents:
  – www.rfc-editor.org

• IP Subnetting References:

• IP Address Subnet Block Size Chart:
  – https://www.arin.net/knowledge/cidr.pdf
  – http://img.docstoccdn.com/thumb/orig/14990233.png
Web IPv6 Reference Sources:

• IPv6 Reference Texts:
  – Deploying IPv6 Networks – Ciprian Popoviciu
  – Deploying IPv6 In Broadband Access Networks – Adeel Ahmed & Salman Asadullah
  – IP Address Management Principals & Practice – Timothy Rooney
  – Migrating to IPv6 – Marc Blanchet

• IPv6 Reference Websites:
  – www.getipv6.info
  – www.ipv6forum.com
  – http://www.6diss.org/e-learning/index.html
Internet Cleaning Day

Yearly Internet Maintenance Announcement
It is URGENT that you do not connect to the Internet from March 31st 23:59 GMT (11:59 PM) until 00:01 GMT (12:01 AM) April 2nd

It's that time again. As many of you know, each year the Internet must be closed down for a 24-hour period of time in order to receive maintenance, or a "Tune Up" if you will. Many dead links on the World Wide Web will be removed, as well as FTP links that are no longer used. Lost e-mail will also be removed from the system at this time.

In addition to the normal maintenance to be completed this year, we will also be using new high-pressure information jets to clear out the bottlenecks that have plagued the Internet so greatly this past year. Although the down time for maintenance will be an inconvenience for many people, you will find this will allow for a much more efficient and faster responding Internet. This year, the "Tune Up" will occur from 23:59 GMT (11:59 PM) on March 31st until 00:01 GMT (12:01 AM) on April 2nd. During that 24 hour period, dozens of powerful Internet bots at key locations around the globe will simultaneously scan the Internet and complete the desired maintenance jobs wherever they may be required.

To help protect any valuable data you may have on the Internet from possible corruption, we highly recommend you take the following steps before this 24 hour maintenance period begins:
   Disconnect all terminals and LANs from the Internet.
   Disconnect all Internet servers from the Internet.
   Refrain from connecting any computer, or any other Internet connection device, to the Internet in any way.

Again, we understand the inconvenience this will cause many people. And for that, we apologize. However, the great increase in Internet performance you will experience after this short period of maintenance will far outweigh any problems it will cause.

Thank you in advance for your cooperation.

Mr. Yuben T. Ricked
Global Internet Maintenance Organization
Upcoming Webinars

**TV White Space Devices & Wireless Microphones**
*with Joe Snelson, CPBE, 8-VSB*
May 2 · 2-3 p.m. Eastern

**AM Directional Antenna Modeling**
*with Cris Alexander, CPBE, AMD, DRB*
May 10 · 2-5 p.m. Eastern

**SBE RF Safety Course**
*with Richard Strickland*
May 24 · 2:30-5:45 p.m. Eastern

**IPv6 for Broadcasters**
*with Wayne Pecena, CPBE, 8-VSB, AMD, DRB, CBNT*
July 11 · 2-3:30 p.m. Eastern

www.sbe.org
With these online, self-study courses, you pick the date, time and location to learn. Now that’s convenience! The cost for these courses varies from $65 to $99 for SBE Members.

Once you register, you immediately receive a link to the course where you can access it again and again as your schedule permits.

More Information: www.sbe.org
Preparing you for SBE Certification

More Information: www.sbe.org
Webinars by SBE addresses specific subjects of interest to broadcast engineers.

You can view the webinars live, or choose to view the recording on our website.

More Information: www.sbe.org
The Ennes Workshops, *presented by SBE*, were created in an effort to bring affordable education to members locally. These one-day workshops are presented around the United States. Presentations are non-commercial and focus on technology.

More Information: www.sbe.org
? Questions?

Thank You for Attending!
Wayne M. Pecena
Texas A&M University

w-pecena@tamu.edu
N1WP@tamu.edu

979.845.5662