IP Networking Architecture Best Practices

Wayne M. Pecena, CPBE, CBNE
Texas A&M University
Office of Information Technology
Educational Broadcast Services
My Agenda

• Introduction
• Conceptual Network Designs
• The Building Blocks
• Building the Network
• Securing & Accessing the Network
• Reference Documents
• Best Practices Summary / Q & A
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 Design Considerations

- Performance
- Reliability / Redundancy
- Security
- Scalability
- Flexibility
- Manageability
- Affordability
The Design Process

Value Engineering vs Cost Cutting
The Basic Network
Adding Redundant ISP’s
Layered Network Design

- Separate Network in “Layers” or Zones
  - External or Public Network
  - “DMZ” or Demilitarized or Perimeter Zone
  - Create Internal or Private Network(s)
Standards

- OSI Model & IETF RFC’s
- Your Internal Standards:
  - Device Naming Scheme
    - Device Type
    - Device Number
    - Device Location
  - IP Addressing Scheme
    - Public
    - Private
  - VLAN Naming Scheme
  - Wiring Schemes
  - Documentation
IP Focused – DOD or TCP/IP Models

<table>
<thead>
<tr>
<th>OSI Model</th>
<th>DoD Model</th>
<th>TCP/IP Model</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>Application</td>
<td>Application</td>
</tr>
<tr>
<td>Presentation</td>
<td>Host to Host</td>
<td>Transport</td>
</tr>
<tr>
<td>Session</td>
<td>Internet</td>
<td>Internet</td>
</tr>
<tr>
<td>Transport</td>
<td>Network</td>
<td>Network Interface</td>
</tr>
<tr>
<td>Network</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Link</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

IP Focused
Reference Hardware & Services

“Building Blocks”

- Physical Medium(s)  L1
- Switches            L2
- Routers             L3
- Firewalls
- VLAN(s)
- VPN(s)
Managed vs Un-Managed Ethernet Switches

• Managed Switch
  – User Configurable
  – Control & Monitor Host Communications
  – Individual Port Configuration
  – VLAN Implementation
  – Redundancy Supported (STP)
  – QoS Implementation
  – Port Mirroring

• Un-Managed Switch
  – Fixed Configuration
  – “Plug & Play”
  – Provides Basic Host Communications
  – Cheaper
Addressing
Physical & Virtual Addressing

- Each Host on an Ethernet Based IP Network Has:
  - An **Unique MAC Address**
    - Layer 2 **Physical Address** (local network segment)
  - An **Unique IP Address**
    - Layer 3 **Logical Address** (global routed)
Encapsulation – De-Encapsulation

Model Provides Modularity – Flexibility - Abstraction

Encapsulation

De-Encapsulation or De-Mux

Layer 1
Layer 2
Layer 3
Layer 4
Layer 7

Get HTTP

TCP

IP

MAC

The “Wire”
IP Address Plan Considerations

- Design by Required Space vs Available Space
- Do I Subnet?
- Private Addresses – RFC 1918
- “Public” Addresses
- Static Assignment
- Dynamic Assignment
The IP Address Subnet Mask

“VLSM” - Each IP Address Must Have a Subnet Mask to Define the Network and the Host

32 Bit Address & Subnet Mask Format
Expressed in Decimal as (4) 8-bit Octets using “Dotted Decimal Notation”

IP Address: 192.168.1.100 /26

192.168.1.100 /26 or 255.255.255.192

11000000.10101000.00000001.01100100

11111111.11111111.11111111.11000000

Network | Host
IP Address Subnetting

• **What is a Subnet?**
  – Logical Subdivision of a Larger Network
  – Creates New Smaller Network(s) from a Larger Network
  – Created by Stealing Host Bits!

• **Why Do We Subnet?**
  – Efficient Use of IP Address Space - “Right Size”
  – Increase Performance (smaller Broadcast Domain)
  – Network Management Policy
  – Segmentation (function, ownership, geo location)
  – Job Security for the Network Engineers!
Subnet Example

<table>
<thead>
<tr>
<th>Network</th>
<th>Existing Hosts</th>
<th>Design Host (12%)</th>
<th>Required Subnet Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>A – Admn</td>
<td>35</td>
<td>40</td>
<td>64</td>
</tr>
<tr>
<td>B – Eng</td>
<td>17</td>
<td>20</td>
<td>32</td>
</tr>
<tr>
<td>C – Prod</td>
<td>27</td>
<td>30</td>
<td>32</td>
</tr>
</tbody>
</table>

Remember the Powers of 2:

```
128  64  32  16  8  4  2  1
```
# IP Subnet “ Helpers ”

## VLSM

<table>
<thead>
<tr>
<th>Mask</th>
<th>Block Size</th>
<th>CIDR 4th Octect</th>
</tr>
</thead>
<tbody>
<tr>
<td>/25</td>
<td>/25</td>
<td>/25</td>
</tr>
<tr>
<td>/26</td>
<td>/26</td>
<td>/26</td>
</tr>
<tr>
<td>/27</td>
<td>/27</td>
<td>/27</td>
</tr>
<tr>
<td>/28</td>
<td>/28</td>
<td>/28</td>
</tr>
<tr>
<td>/29</td>
<td>/29</td>
<td>/29</td>
</tr>
<tr>
<td>/30</td>
<td>/30</td>
<td>/30</td>
</tr>
<tr>
<td>/31</td>
<td>/31</td>
<td>/31</td>
</tr>
<tr>
<td>/32</td>
<td>/32</td>
<td>/32</td>
</tr>
</tbody>
</table>

## CIDR Proportion

<table>
<thead>
<tr>
<th>Classful Ranges</th>
<th>Subnet Proportion</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>0.0.0.0 - 127.255.255.255</td>
</tr>
<tr>
<td>B</td>
<td>128.0.0 - 191.255.255.255</td>
</tr>
<tr>
<td>C</td>
<td>192.0.0 - 223.255.255.255</td>
</tr>
<tr>
<td>D</td>
<td>224.0.0 - 239.255.255.255</td>
</tr>
<tr>
<td>E</td>
<td>240.0.0 - 247.255.255.255</td>
</tr>
<tr>
<td>RFC1918</td>
<td>192.0.0 - 192.0.0.255</td>
</tr>
<tr>
<td>LocalHost</td>
<td>127.0.0.0 - 127.255.255.255</td>
</tr>
</tbody>
</table>

## CIDR Terminology

CIDR: Classless inter-domain routing was developed to VLSM. Variable length subnet masks are an arbitrary length prefix; more granularity than regular classful addressing (between 0 and 32 bits). CIDR relies on VLSM to define masks. Masks expressed in the form /32 and in CIDR notation.

by Jeremy Strobel

v1.0
Network Address Translation – NAT

RFC 1631

• Maps Internal (private) Address Space to External (public) Address Space
  – Allows Internal IP Addresses to be Hid (Security)
  – Can Conserve IP Public Address Space
Let’s Hook Some Stuff Up!

- Layered Network Design
- Switching
  - Managed Switch(s)
  - VLAN(s)
- Routing
- Access Control
  - Firewall
  - VPN Tunnel
Switching and Routing

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

• Legacy Ethernet Used Hubs

• 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”
  – Receiving Port to a Destination Port
VLAN’S Are Your Friend!

- Virtual Local Area Network – VLAN
  - Logical Network of a Physical Network
- Allows Separation of Networks Across a Common Physical Media
  - Each Port is a Collision Domain (eliminates collisions)
  - Each VLAN is a Broadcast Domain (minimizes size)
  - Architecture Flexibility
  - Security
- Static Port Based VLAN(s)
  - Most Popular - Manual Configuration
- Dynamic Port Based
  - MAC-Based VLAN(s)
  - Protocol-Based VLAN(s)
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
Interface Configuration

Interface Config:
- TRUNK
- Blue VLAN
- Green VLAN

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

Switch 1

Switch 2

Switch 3

28
Add Connectivity Between Broadcast Domains

Unique IP Address Range

Blue VLAN

Unique IP Address Range

Green VLAN

Unique IP Address Range

Red VLAN
Routing

• Routing is Simply the Moving of Data Between Networks
• OSI Model Layer 3 Process
• Routing Involves Two Processes:
  – Determining the Best Path  The Hard Part
  – Actually Sending of the Data  The Easy Part
• Static Routing
  – Fixed Path or Stub Routing
• Dynamic Routing
  – Path is Automatically Determined
Routing Types:

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

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

## Narrow Down the 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>IGP v6</td>
<td>RIPng</td>
<td>EIGRP v6</td>
<td>OSPF v3</td>
</tr>
<tr>
<td>IPv6</td>
<td></td>
<td></td>
<td>IS-IS v6</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>BGP v4</td>
</tr>
</tbody>
</table>
Routing Protocols: Which One is Best?

“It Depends”
## Practical Routing Protocol Choices

### “Common” IGP Protocols

<table>
<thead>
<tr>
<th></th>
<th>RIP v2</th>
<th>EIGRP (Cisco)</th>
<th>OSPF v2</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type:</strong></td>
<td>Distance Vector</td>
<td>Hybrid</td>
<td>Link-State</td>
</tr>
<tr>
<td><strong>Metric:</strong></td>
<td>Hop Count</td>
<td>Bandwidth/Delay</td>
<td>Cost</td>
</tr>
<tr>
<td><strong>Administrative Distance:</strong></td>
<td>120</td>
<td>90</td>
<td>110</td>
</tr>
<tr>
<td><strong>Hop Count Limit:</strong></td>
<td>15</td>
<td>224</td>
<td>None</td>
</tr>
<tr>
<td><strong>Convergence:</strong></td>
<td>Slow</td>
<td>Fast</td>
<td>Fast</td>
</tr>
<tr>
<td><strong>Updates:</strong></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><strong>RFC Reference:</strong></td>
<td>RFC 1388</td>
<td>N/A</td>
<td>RFC 2328</td>
</tr>
</tbody>
</table>
Which Routing Protocol?

Static Routing
- EGP
  - BGP
- IGP
  - Distance Vector Protocol: RIP
  - Link State Protocol: OSPF
- Hybrid Protocol: EIGRP

Dynamic Routing
- IGP
  - Link State Protocol: IS-IS
Routing & Switching Summary

Route Between Networks
(Control Broadcast Domains)
Switch to Eliminate a Collision Domain Within a Broadcast Domain
What Is A “Layer 3” Switch?

• “Marketing Terminology” Applied to a One Box Solution:
  – Switching is a Layer 2 Function
  – Routing is a Layer 3 Function

• Layer 3 Switch Performs Both Functions

• 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
How Many Networks Are Shown?

What About Security?

You Can Implement Stateless Packet Filtering via ACL
Implements “Stateful” Packet Filtering
The Security Challenge

PERFORMANCE
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”
Network Infrastructure Threats

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

• **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 do anything?

• **First Step:**
  – Lock down all LAN switch ports
  – Require Users & Devices to Authenticate
Switch Port Security

• Avoid Using VLAN 1

• Port Security Aspects:
  – One MAC Address Per Port
    • Dynamic
    • Fixed
  – MAC Violation Actions (Cisco example)
    • Protect
    • Restrict
    • Shutdown
  – Disable Unused Ports
Network Security Tools

• **Firewall**
  – Defines Traffic That Can Enter or Exit a Network
  – Used to Create a “Trusted” Network Segment(s)
  – Types of Firewalls:
    – Stateless
    – Stateful

• **Detection Tools**
  – Intrusion Detection Systems (IDS)
    • Signature Based
    • Anomaly Based
  – Intrusion Prevention Systems (IPS)
Firewall Types:

Packet Filtering - “Stateless”

Packet Filtering - “Stateful”

HTTP Request

HTTP Reply

Blocked X

HTTP Request

HTTP Reply

Blocked X

Telnet Session
Firewall Implementation

“The 3-Armed Firewall”
VPN Implementation

“Virtual Private Network”
Don Not Confuse VLAN’s and VPN’s
A VPN is a SecureTunnel Through a Network Infrastructure

Virtual Private Network – VPN Protocols
- IPsec with Encryption
- L2TP inside of IPsec
- SSL with Encryption
Can You Balance Your Network Infrastructure Security?

“DoS” Attack
Spoofing
Hijacking
“Back Door” Access
Physical Access
Social Engineering
Phishing
And more …..

USEABILITY

The Goal – “Create a Secure But Useable Network”
Some Best Practices to Consider

- Adopt a Layered Design Approach
- Disable Services Not Required
- Disable Switch Ports Not Used
- Recognize Physical Security
- Change Default Logins
- Segregate Network(s)
- Subnet by Function or Policy
- Transport Separate Networks via VLANS
- Implement Switch Port Security
- Utilize Filtering in Network Devices
- Do Not Overlook Network Egress Traffic
- Deny All Traffic – Then Permit Only What Is Required

- Keep Up With Equipment “Patches”
- Utilize Access Logging on Key Network Devices
- Use Encrypted Logins
- Utilize Session Timeout Features
- Restrict Remote Access Source if Possible
- Understand & Know Your Network Baseline
- Actively Monitor Your Network & Look for Abnormalities
- Limit Network Internal Details to a “Need-to-Know” Basis
- Document What You Do!
Document What You Do!
Web Reference Sources:

IETF RFC Documents:
www.rfc-editor.org

Learn More About the OSI Model:
http://www.9tut.com/osi-model-tutorial

Learn More About Switching:

Learn More About Routing:

Learn More About Layer 3 Switching:
http://happyrouter.com/layer-3-switches-explained

Learn More About IP Addressing:
https://learningnetwork.cisco.com/docs/DOC-5893
# Real – World OSI Model

## Important to Recognize During Troubleshooting

<table>
<thead>
<tr>
<th>Protocol Layer</th>
<th>ID10T Errors</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>

Reference:
- RFC 2321
- RITA - The Reliable Internetwork Troubleshooting Agent
There's more to networking than just hooking things up.
Thank You for Attending!

Wayne M. Pecena, CPBE, CBNE
Texas A&M University
Office of Information Technology
Educational Broadcast Services

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

979.845.5662