“IP Networking Fundamentals and Advanced Practice”

Wayne M. Pecena, CPBE, CBNE
Texas A&M University
Educational Broadcast Services – KAMU FM-TV
“IP Networking Fundamentals and Advanced Practice”

Advertised Presentation Scope

Tutorial Overview

IP networks are an integral component of the broadcast technical plant today. Integration with the legacy broadcast infrastructure can range from minimal system control functions to an end-to-end IP based content transport infrastructure. Regardless of the integration level or complexity, knowledge of IP networking is essential for the broadcast engineer and cybersecurity must be a top-of-mind concern. This tutorial presentation will seek to provide an understanding of IP network fundamentals, an awareness of advanced features, and practical steps to implement network security best practices in the design and support of a broadcast IP network.
“IP Networking Fundamentals and Advanced Practice”
Outline

• Introduction to Networking Standards & Models
• Beyond the Fundamentals
• Structured Cybersecurity Implementation
• Thinking Like a “Hacker”
• Best Practices, References, & Takeaways
Introduction to Networking Standards & Models
Networking Standards

• **IEEE** - Institute of Electrical & Electronic Engineers
  - Project 802 Ethernet Standards:
    - 802.1 Bridging
    - 802.3 Ethernet
    - 802.11 Wireless

• **IETF** – Internet Engineering Task Force
  - Request for Comments – RFC xxxx
    - The “Standards Bible” of the Internet
    - **Requirement Levels:**
      • Required
      • Recommended
      • Elective
      • Limited Use / Not Recommended / Depreciated

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

www.rfc-editor.org/rfc.html
The OSI Model

Open Systems Interconnection Model

Conceptual Model – Abstract in Nature – Modular in Structure
Defines How Data Traverses From An Application to the Network

Application Layers

Networking Focus

Data Flow Layers

- Physical
- Data Link
- Network
- Transport
- Session
- Presentation
- Application

Levels:

1. Physical
2. Data Link
3. Network
4. Transport
5. Session
6. Presentation
7. Application
The OSI Model Expanded

<table>
<thead>
<tr>
<th>Layer</th>
<th>PDU</th>
<th>Addressing</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>Application</td>
<td>SESSION ID</td>
</tr>
<tr>
<td>6</td>
<td>Presentation</td>
<td>PORT</td>
</tr>
<tr>
<td>5</td>
<td>Session</td>
<td>IP ADDRESS</td>
</tr>
<tr>
<td>4</td>
<td>Transport</td>
<td>MAC ADDRESS</td>
</tr>
<tr>
<td>3</td>
<td>Network</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Data Link</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Physical</td>
<td></td>
</tr>
</tbody>
</table>

- DATA STREAM: BITS
- DATAGRAM: PACKET (Datagram)
- DATA FRAME: FRAME
- DATA BIT: BITS (data stream)
TCP/IP Focused Models

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
Yet Another Model to Consider Soon!

ATSC 3 / NextGen TV
Beyond the Fundamentals
Is The Broadcast Network Special?

It Depends!

• The “Broadcast” or “Media” Network:
  – Low Latency / Constant Bit Rate
  – Can Require High Bandwidth
  – Advanced Features Utilized:
    • Multicast
    • QoS
    • PTP (IEEE-1588)
    • IETF Real Time Protocol(s)

Design for Performance

Design for Cybersecurity
Layered Network
Segmented Network Architecture

DMZ – email / web Zone 4

Office / Admin Zone 3

Engineering / Control Zone 2

Broadcast Content/Transmission Zone 1

The “Onion” Network
Ethernet Switch Functions

- Learn MAC Addresses – Build “Table”
- Filter / Forward Ethernet Frames
- Flood Ethernet Frames
- Provide Loop Avoidance - Redundancy
- Provide Security Features
- Provide Multicast Support
Managed & 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

Netgear GS105Ev2 “Web Managed” Switch
GigE, Port Mirror, VLAN, Cable Check
The Layer 2 Ethernet Frame

### An Ethernet II (DIX) Frame

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

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

*Note – Preamble Not Used in Frame Length Calculation*

<table>
<thead>
<tr>
<th>Destination Address</th>
<th>Source Address</th>
<th>Type</th>
<th>Data</th>
<th>CRC</th>
</tr>
</thead>
<tbody>
<tr>
<td>64 Byte Minimum</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Data-Link Layer Physical Addressing

- **MAC Address** – 6 Bytes – Hexadecimal Notation - **00:12:3F:8D:4D:A7**
  - Layer 2 **Physical Address**
  - Fixed “**Burned-in-Address**” – Assigned by NIC Mfg.
  - **Local in Scope**
The Ethernet MAC Address
Always 48 Bits – Expressed as Hexadecimal

Can Be Represented in Several Formats:

00:A0:C9:14:C8:29
00-A0-C9-14-C8-29
00A0.C914.C829
Virtual Local Area Network – VLAN

- Allows Separation or Segmentation of Networks Across a Common Physical Media
  - Creates Subset of Larger Network
  - VLAN Controls Broadcast Domain Reach – Each VLAN is a Broadcast Domain
  - Architecture Flexibility
  - Security
- Static Port Based VLAN(s)
  - Most Popular
  - Manual Configuration
  - Switch Port Security Features
- Dynamic Port Based
  - MAC-Based VLAN(s)
    - Assignment Based Upon MAC Address
  - Protocol-Based VLAN(s)
    - Assignment Based Upon Protocol

What Happens in the VLAN, Stays in the VLAN
Virtual Local Area Network - VLAN

- Group of Host Devices That Communicate Via Isolated Networks (subnets, broadcast domains) on the Same Network Infrastructure
- Logical Connection Based
- Ethernet Switch Port Mode:
  - Trunk (Tagged Port)
  - Access (Non-Tagged Port)
Adding the VLAN Tag

**ETHERNET FRAME**

| PREAMBLE | DESTINATION MAC ADDRESS | SOURCE MAC ADDRESS | TYPE | DATA | CRC |

**802.1Q ETHERNET FRAME**

| PREAMBLE | DESTINATION MAC ADDRESS | SOURCE MAC ADDRESS | TAG | TYPE | DATA | CRC |

TPID “0X8100”

PRI

CFI

VLAN ID

802.1Q TAG

Double & Triple Tagging Can Occur
The 802.1Q Tag in Detail

TPID

PRI

DEI

VID

TPID

Tag Protocol ID “0x8100” 16 bits

PRI

Priority 3 bits

DEI (CFI)

Drop Eligible Indicator

Canonical Format ID 1 bit

VID

VLAN Identifier 12 bits

TAG CONTROL INFO

2 bytes

2 bytes

32 bits or 4 bytes

Be Aware – Proprietary VLAN Tags Exist (ie Cisco “VTP & ISL”)
VLAN Example – Redundant Links

Added Link Between Switch 1 and Switch 3:
Provides Redundant Architecture – “Ring” Topology
But, Creates “Loop”
Redundant Links & Spanning Tree

Link Aggregation – “LAG”
IEEE 802.3ad

Expand Link Capacity by Bundling Multiple Ports
+ Redundancy
Frame or Forwarding Loops
LAG Implementation
Can Have Many Names!

- Also Known As:
  - Port Trucking
  - Port Teaming
  - Ethernet Trucking
  - Link Bundling
  - Cisco “EtherChannel”
  - Juniper's “Aggregated Ethernet”
  - AVAYA “Multi-Link Trunking”
  - NIC Bonding / Teaming
Network Layer
IP Virtual Addressing

- **IPv4 Address** – 4 Bytes – Doted Decimal Notation - **172.15.1.1**
  - Layer 3 **Logical Address**
  - Can Change – **Determined by Network** - Assigned by User
  - Global in Scope

![Simplified Representation of IP Packet and Ethernet Frame]
The IP Addressing “Rules”

- Each Network MUST Have a **Unique Network ID**
- Each Host MUST Have a **Unique Host ID**
- Every IP Address MUST Have a **Subnet Mask**
  - Implied for a Classful Network (A,B,C,D,E)
  - Explicit Stated for Classless Network (255.255.255.0 or /24)
- An IP Address Must Be **Unique Globally** If Host on the Public Internet
- The **First** & **Last** IP Address Of a Network is **Not Assignable**!
  - First Address = Network Address or “Wire” Address
  - Last Address = Broadcast Address
Structured Cybersecurity Implementation
Why Be Concerned?

Ransomware attack puts KQED in low-tech mode

By Marissa Lang | July 18, 2017 | Updated: July 26, 2017 4:17pm

Another Ransomware Attack Ravages A Radio Cluster

By Adam Jacobson - October 26, 2019

PORTLAND, ORE. — Travel two hours to the east of the ever-changing Woodlawn neighborhood in Northeast Portland, and you’ll find yourself in one of the most beautiful locales of the Pacific Northwest: the Columbia River Gorge.

Unfortunately, there’s an ugly situation going on in this picturesque corner of the U.S. And, it’s due to another ransomware attack at a group of radio

French Broadcaster M6 Recovering From Ransomware Attack

Television and Radio Stations Continued to Operate Without Interruption

Cyber attack hits Spanish companies including radio network

By Reuters - last updated: 04/11/2019 - 19:04
The Broadcast & Media Technical Plant Has Changed

- Transition to IP Based Plant
- “Cloud” Based Services
- Service Based Architectures:
  - IaaS, PaaS, SaaS, CaaS
IT Security Principals

• CIA Triad
• Defense-in-Depth
• Least - Privilege
• Risk-Based Analysis
• NIST Practices

Generalized Action Steps:
– Minimize attack area(s)
– Adopt “separation of duties” in network design
– Coordinate security precautions
– Perform weakest link analysis
– Identify “single points of takeover”
– Simplify implementation
The “CIA” Triad

A Fundamental Principal of IT Security

Also Known as “AIC” Triad
Defense in Depth – “DiD”

Principal Based Upon Multiple Layers of Protection

- NSA developed approach based upon coordinated “multiple layered” security protections
  - Based upon redundancy of protection mechanisms
  - If a layer is breached – another layer is encountered
  - Possible layers of protection:

<table>
<thead>
<tr>
<th>Physical Access</th>
<th>Access Control Tools</th>
<th>Administrative Tools/Policies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication</td>
<td>2-Factor Authentication</td>
<td>Anti-Virus Software</td>
</tr>
<tr>
<td>Firewalls</td>
<td>Packet Filtering</td>
<td>Malware Detection Software</td>
</tr>
<tr>
<td>Data Encryption</td>
<td>Segmented Networks</td>
<td>Intrusion Detection Technology</td>
</tr>
</tbody>
</table>
“DiD” Implementation

“Castle Approach”
The Security Policy

• Security Implementation Begins With a **Security Policy**
• This is Your Implementation **Roadmap**
• Apply to "**Anyone / Anything**" With Network Access!
  – Company / Regulatory Policy Objectives
  – System Business Standards /Requirements
  – User Practices
  – Specific Procedures
Attributes of a Secure Network

• **Established Security Policy**
  – The Organizations Security “Rule Set”
  – What Must Be Secured & How Identified
  – How It Is SecuredOutlined

• **Complies With “CIA” Triad Objectives**
  – Confidentiality, Integrity, Availability

• **Layered Design Approach (“Defense in Depth”)**
  – Segmentation of Network Into Workgroup Areas or Groups
  – Different Security Controls Within Areas / Groups

• **Privileges Limited:**
  – Limit “Privileged” Users
  – Restrict to “Need – To – Access”
  – “Deny by Default”

• **Access Controlled**
  – Restrict by Firewalls, Proxies, etc.

• **Active Support, Monitoring, & Logging**
  – Patch Maintenance
  – Establish Accountability Trail
  – Activity Logging / Tracking / Monitoring
Structured Implementation Plan

Layer 1 – Physical Access

Layer 2 – Ethernet Switch Security

Layer 3 – Packet Filtering

Layer 4 and above – Encryption & Authentication
Layer 1 - Physical Access

• Restricted Physical Access to Network Infrastructure

• Controlled Access:
  – Access Badges
  – Cyber-Locks
  – Bio-Recognition

• Monitor Access
  – Access Logs
  – Surveillance Cameras
Layer 2 - Switch Port Security

• Port Security Options:
  – Prevent Foreign Host Network Connection
  – Permit Specific MAC Address / Port
  – Limit # MAC Addresses / Port

• Violation Actions:
  – Discard Frame
  – Shutdown Port
  – Notification

Prevents CAM Table Overflow Attacks
Limits DoS & DDoS Attack Impact
L3 Network Security Tools

• **Packet Filtering & Firewalls**
  – Used to Create a “Trusted” Network Segment by Filtering Network Packets
    • Permit
    • Deny
  – Types of Firewalls:
    • Stateless Packet Filtering – Single Packet Inspection Based
    • Stateful Packet Filtering – Flow or Conversation Inspection Based

• **Proxy**
  – Intermediary Host or Software Ap
  – Access Control Mechanism

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

• Provides “Basic” Packet **Filter** Network Access Security Buffer

• **Filter** IP Network Packets:
  – Forwarded @ Egress Interface
  – Blocked @ Ingress Interface

• **Standard** Access List – Layer 3 Header Info
  – Can Only Permit or Deny The Source Host IP Address
  – **Placed Closest to Destination Host**

• **Extended** Access List – Layer 3 & 4 Header Info
  – Can Permit or Deny Based Upon:
    • Source IP Address
    • Destination IP Address
    • TCP Port #
    • UDP Port #
    • TCP/IP Protocol
  – **Placed Closest to Source Network**
Implementing an Access Control List

One ACL per:
- Interface
- Direction
- Protocol

Permit or Deny:
- Source IP Address (standard)
- Destination IP Address
- ICMP
- TCP/UDP Source Port
- TCP/UDP Destination Port

Create
Access Control List

Apply
Access Control List
Access Control List (ACL) - Example

Block External Users From “Pinging” Inside Network Hosts

Create Access List on Router 1:
access list 100 deny icmp any any
access-list 100 permit ip any any

Apply Access List to Interface:
interface ethernet1
ip access-group 100 in

Configuration Disclaimer:
Exact configuration commands may vary based upon specific equipment models and software version. Generic “Cisco” commands utilized for illustration purposes.
Firewall Types

- Packet Filtering (stateless)
- Packet Filtering (stateful inspection)
- Application Gateway (proxy)
- Circuit Gateway (NAT)  
  - Hides Internal Host IP Address
- Next-Gen Firewall  
  - Traditional Stateless / Stateful Firewall  
    + Application Deep Packet Inspection (DPI)  
    + Intrusion Prevention System (IPS)
A “State”

- A dynamic rule created by the firewall based upon a host-host source destination address-port combination
Stateful Firewall

Aware of connections between protected network host & un-protected host. Maintains connection “state table” to implement security policy

Filtering Parameters:
- IP Source Address
- IP Destination Address
- Protocol
- Connection Status
- Source Port Number
- Destination Port Number
Stateless Firewall

In Addition to TCP/IP Header Checks, A Stateless Firewall Can Detect Packet Anomalies:

- IP Packet Header Makeup
- IP Addressing Non-Compliance
- IP Fragmentation Errors
- TCP Flow Sequencing
- UDP Flow Sequencing
- Anomalies Associated with Packet Flows:
  - SYN-ACK Sequence Not Compliant
  - ICMP Errors
Proxy Firewall

- Hides “Internal” Network Hosts
- External Hosts Only Sees Proxy Address
- Limits Network Access to Application Protocols
- Client – Server Relationship
- Can Be Implemented Within Firewall
- Can Be Implemented Within Server
- Can Filter Content
Recognize IP Is **NOT** Secure

- Security Was **NOT** of Concern When Developed

**Potential Issues:**
- Maintaining Confidentiality
- Privacy (Examination)
- Packet Replay (Unauthorized)
- Spoofing (Identity)

**What is Needed?**
- Verify IP Source
- Prevent Packet Replay
- Protect Confidentiality
Internet Protocol Security “IPSec”

• **Provides:**
  – Data Confidentiality (via encryption)
  – Data Integrity (via hashing algorithm)
  – Authentication (identity key)
  – Also prevents “packet replay” (integrated sequence numbering)

• **Encryption & Authentication Keys**
  – More Bits = More Secure (768, 1024, or 2048 bit)
  – Symmetric Keys – Must Be Pre-Installed
  – Asymmetric Keys – Keys Are Exchanged via D-H Key Exchange
    • DES, 3DES, AES, Blowfish
IPSec Modes

• Transport Mode:
  – Original IP Header Not Touched
  – ESP & AH Inserted
  – Authenticated

• Tunnel Mode:
  – New IP Header Created
  – Entire Packet is Encrypted
  – Temporary IP Header Added
Virtual Private Network “VPN”

Providing Remote Access

- **VPN:**
  - Establishes a Private Network Across A Public or Shared Network Infrastructure
- **Virtual:**
  - Not Physically Distinct Network Infrastructure
- **Private:**
  - Encrypted Tunnel Between Hosts
- **Application:**
  - Remote Client VPN
  - Site – Site VPN
- **VPN Protocols:**
  - IPSec – Internet Protocol Security
  - L2TP – Layer 2 Tunneling Protocol
  - TLS – Transport Layer Security
  - SSL – Secure Sockets Layer
  - SSH – Secure Shell
Hardening Host Devices

• Hardening is a process to reduce the attack surface of a host device operating system
• Implementation activities typically include:
  – Changing default passwords
  – Removing un-used applications / services (debloating)
  – Deleting un-used accounts
  – Adjusting / changing default configurations
  – Strong password management
  – Keeping updates & patches up-to-date
  – Closing network “back doors”
Linux vs Windows

• Keep in mind:
  – Windows in a closed system (limited configurability)
  – Linux is an open-source system (totally configurable)

• Which is considered more secure?
  – No operating system is totally secure and can be compromised
  – In general, Linux is considered “more” secure due to the design of the operating system (kernel)
  – Windows utilizes a monolithic (micro) kernel (NT kernel)
  – Linux utilizes a modular kernel - does not allow autonomous processes to be executed IE malware to be installed – must be installed by “root” supervisor
  – Linux vulnerabilities are generally based upon mis-configuration
  – Windows 10 is considered to be “secure” with add-on 3rd party anti-virus, anti-malware, etc
Windows Op System

- Separate user and admin account(s)
- Obfuscate local admin account (rename)
- Disable “guest” account(s)
- Disable LAN Manager
- Use “strong” password management
- Utilize data encryption
- Insure “drivers” are patched up-to-date
- Insure “bundled” applications are up-to-date OR remove
- Disable “un-needed” services
- Utilize “domain controller” to administer multiple hosts
Linux Op System

- Password protect the host BIOS
- Enable disk encryption
- Lock boot directory (read-only)
- Disable USB storage
- Maintain system (kernel) updates & patches
- Disable / remove any un-used services (ie telnet, tftp, etc)
- Check for open ports (pen test)
- Secure SSH (change port, disable root login)
- Utilize SELinux (Security Enhanced Linux)
- Disable network parameters:
  - IP Forwarding
  - ICMP Re-Directs
  - Send Packet Re-Directs
- Set a “strong” password hashing algorithm (SHA512)
- Lock accounts after x failed login attempts (3-5)
- Insure permissions are valid
Thinking Like a “Hacker”
The “Hacker” Culture

- **“White Hat” Hacker**
  - Intent is to protect IT systems
- **“Black Hat” Hacker**
  - Intent is to harm IT systems
- **“Gray Hat” Hacker**
  - Intent is the challenge
Network Reconnaissance

What Can You Learn?

- IP Address Discovered
- Operating System ID
- Active Ports ID
- Services / Apps Available
- What Version?

Insight to Compromise Host

Vulnerability?

Default login?
Tools of the “Hacker”

https://www.concise-courses.com/hacking-tools/
Tools of the “Hacker”

10 Most Popular

• nmap
• metasploit
• John The Ripper
• THC Hydra
• OWASP Zed
• Wireshark
• Aircrack-ng
• Maltego
• Cain and Abel Hacking Too
• Nikto Website Vulnerability Scanner
SHODAN

https://www.shodan.io

The search engine for the Internet of Things
Shodan is the world's first search engine for Internet-connected devices.

Explore the Internet of Things
Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.

See the Big Picture
Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!
SHODAN
https://www.shodan.io
SHODAN

https://www.shodan.io
Best Practices, References, & Takeaways
Do These 10 Things
(first 4 if nothing else)

• Change default logins
• Use strong passwords (paraphrases)
• Separate Admin & User accounts on hosts (WIN)
• Segment your network (VLAN) – create multi-layer security zones
• Use packet filtering to control host access (ACL and/or firewall)
• Disable un-used services – close ports not used
• Monitor you network – know what is normal
• Use secure access (SSH not telnet)
• Use VPN for off-site access
• Don’t be a social engineering victim – educate users
NIST Cybersecurity Framework

https://www.nist.gov/cyberframework/framework

<table>
<thead>
<tr>
<th>Process (PR.IP)</th>
<th>Reference</th>
</tr>
</thead>
</table>
| PR.IP-4: Backups of information are conducted, maintained, and tested          | - CIS CSC 10  
- COBIT 5 APO13.01, DSS01.01, DSS04.07  
- ISA 62443-2-1:2009 4.3.4.3.9  
- ISA 62443-3-3:2013 SR 7.3, SR 7.4  
- NIST SP 800-53 Rev. 4 CP-4, CP-5, CP-9 |
| PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met | - COBIT 5 DSS01.04, DSS05.05  
- ISA 62443-2-1:2009 4.3.3.3.1, 4.3.3.3.2, 4.3.3.3.3, 4.3.3.3.5, 4.3.3.3.6  
- NIST SP 800-53 Rev. 4 PE-10, PE-12, PE-13, PE-14, PE-15, PE-18 |
| PR.IP-6: Data is destroyed according to policy                                | - COBIT 5 BA109.03, DSS05.06  
- ISA 62443-2-1:2009 4.3.4.4.4  
- ISA 62443-3-3:2013 SR 4.2  
- ISO/IEC 27001:2013 A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7  
- NIST SP 800-53 Rev. 4 MP-6 |
| PR.IP-7: Protection processes are improved                                     | - COBIT 5 APO11.06, APO12.06, DSS04.05  
- ISA 62443-2-1:2009 4.4.3.1, 4.4.3.2, 4.4.3.3, 4.4.3.4, 4.4.3.5, 4.4.3.6, 4.4.3.7, 4.4.3.8  
- ISO/IEC 27001:2013 A.16.1.6, Clause 9, Clause 10  
- NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR-8, PL-2, PM-6 |
| PR.IP-8: Effectiveness of protection technologies is shared                    | - COBIT 5 BA108.04, DSS03.04  
- ISO/IEC 27001:2013 A.16.1.6  
- NIST SP 800-53 Rev. 4 AC-21, CA-7, SI-4 |
FCC Working Group 4

CSRIC IV Working Group 4 (WG4) was given the task of developing voluntary mechanisms that give the Federal Communications Commission (FCC) and the public assurance that communication providers are taking the necessary measures to manage cybersecurity risks across the enterprise.\(^1\) WG4 also was charged with providing implementation guidance to help communication providers use and adapt the voluntary NIST Cybersecurity Framework\(^2\) (hereinafter “NIST CSF”).

The Communications Security, Reliability and Interoperability Council IV
Final Report

9.1 BROADCAST SEGMENT
CYBERSECURITY RISK MANAGEMENT AND BEST PRACTICES
WORKING GROUP 4
March 2015

Fundamentals of IP Networking Series

Length: 1 h
Presenter: Wayne Pecena, CPBE, 8-VSB, AMD, DRB, CBNE
Part 1 serves as an introduction for the remaining series parts and will focus on standards found today in an Ethernet-based IP network. Physical layer topics include integration of the various Ethernet standards. Presented by Wayne Pecena, this series focuses on understanding underlying technology, standards and protocols used in IP networks in the broadcast and technical plant.

SBE ATSC 3.0 Networking

ATSC 3.0 Networking: Module 1: Standards and the Physical Layer
Wayne Pecena, CPBE, 8-VSB, AMD, DRB
In networking technology utilized in an ATSC broadcast industry with integration of traditional standards, the ATSC 3.0 standard is the core transport protocol that provides the need to transport data over the air (OTA) signals and broadband delivered IP content.

ATSC 3.0 Networking: Module 2: \nWayne Pecena, CPBE, 8-VSB, AMD, DRB
A foundation in networking technology utilized in a network architecture design for performance and scalability. Use of VLANs to provide network traffic isolation. ATSC 3.0 promises to revolutionize the broadcast industry with integration of traditional over-the-air (OTA) signals and broadband delivered IP content.

ATSC 3.0 Networking: Module 3: IP Routing
Module 3 completes the ATSC 3.0 Networking Series presented by Wayne Pecena, CPBE, 8-VSB, AMD, DRB, CBNE. In the final module, IP Routing, secure remote access and security best practices to ensure reliable system operation and ongoing support capabilities are discussed. ATSC 3.0 promises to revolutionize the broadcast industry with integration of traditional over-the-air (OTA) signals and broadband delivered IP content.

Cybersecurity

Broadcast Infrastructure Cybersecurity Webinar Series Module 1: Introduction & Network Security Principals
Length 1 hour, 23 minutes
This is the first presentation of a four-part series on Cybersecurity presented by Wayne Pecena, CPBE, 8-VSB, AMD, DRB, CBNE. In this session, you receive an introduction to cybersecurity in the broadcast plant as well as an overview of the security policy. The course also covers the structured security implementation and hardening the broadcast IP Network.

Broadcast Infrastructure Cybersecurity Webinar Module 2: Understanding the Firewall
Length 1 hour, 28 minutes
In this second part of the Cybersecurity Series, Presenter Wayne Pecena, CPBE, 8-VSB, AMD, DRB, CBNE, discusses the access control list (ACL) and the firewall. He reviews “Firewall Implementation & Ruleset Configuration” as well as applying the security policy through the firewall ruleset.

Module 3: Understanding Secured Remote Access
Length 1 hour, 9 minutes
In this third presentation in the series, secured remote access and establishing secured remote access are discussed. This session also reviews VPN implementation and configuration.

Module 4: Security Verification Through Penetration Testing
Length 1 hour, 10 minutes
In this final presentation of the series, proactive security monitoring is discussed. Wayne Pecena, CPBE, 8-VSB, AMD, DRB, CBNE, also provides an overview of network penetration testing and network presentation testing tools. Examples are included in the discussion.
Reference Texts:

2. Gary A. Donabue, "Network Warrior: Everything You Need to Know That Wasn't on the CCNA Exam, 2nd Edition"
The “Real World” OSI Model

<table>
<thead>
<tr>
<th>Layer</th>
<th>Number</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

Phishing & Social Engineering Exploits
Social Engineering

What is Social Engineering?

*The use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes.*

Preparing the ground for the attack:
- Identifying the victim(s).
- Gathering background information.
- Selecting attack method(s).

Closing the interaction, ideally without arousing suspicion:
- Removing all traces of malware.
- Covering tracks.
- Bringing the charade to a natural end.

Deceiving the victim(s) to gain a foothold:
- Engaging the target.
- Spinning a story.
- Taking control of the interaction.

Obtaining the information over a period of time:
- Expanding foothold.
- Executing the attack.
- Disrupting business or/siphoning data.
Thank You for Your Time This Evening!

Wayne M. Pecena
Texas A&M University
w-pecena@tamu.edu
wpecena@sbe.org
979.845.5662

Distinguished Lecturer

There's more to networking than just hooking things up.