Next Generation Cyber Testing

in a Low Cost Emulation of a Target Network

Deepinder Sidhu and Chuck Burdick

TeleniX Corporation

Tel: 410-772-3275

POC Email: dsidhu@telenix.com

NDIA Test & Evaluation Conference 21-23 July, 2014

Chuck Burdick is an Innovative Decisions, Inc. subcontractor

Realistic, Repeatable, Flexible, Inexpensive, Cyber Testing

Agenda

- What is the TeleniX Virtual Emulation Environment (VEE) and what does it do?
- How can VEE Support Cyber Testing?
- Questions

Cyber Testing Headlines

- DARPA builds Multi-million National Cyber Range (NCR) with 100s of high-end servers and a dedicated testing facility.
- NCR 5 year support contract awarded sole-source.

Bottom Line Up Front

Cyber and IA testing on realistic networks is critical, but ranges can be very costly and real networks risky.

- But what if you could use actual internet software and protocols of the real network without all the hardware and software costs?
  - And create actual network configurations in a low-cost virtual emulation – a network clone?
  - And provide the identical network responses to cyber attack as the real network environment?
- And do it running on low-cost computers using actual internet code with bit-level fidelity - essentially duplicating a cyber range on a laptop

Such a realistic network emulation system already exists in the Intelligence Community and is being offered to others

- **TeleniX Virtual Emulation Environment (VEE)**

VEE Uses actual code for all protocols powering the Global Internet

Virtual Emulation Environment (VEE)

Clone a network in VEE using:

- Automated Reverse Engineering Techniques
- Actual protocol implementations & network configurations with 100’s of servers, 100K devices
- With complete interchangeability of code between the real and virtual environments

Emulate the network clone in VEE

- Conduct full-fidelity network operations under real- world configurations and operational scenarios
- Produce behaviors that are indistinguishable from the behavior of its real counterpart (confirmed by IC Red Teams)
  - Packet encapsulations, route tables, link bandwidth utilization, …

VEE on a laptop/server

- Avoid the expense of large-scale hardware and software maintenance/refresh costs, or power, space, & cooling (PSC)
- With minimal personnel support costs
- With rapid reconfigurability and easy portability

VEE

Internet-in-a-Box

VEE Test Advantages

- Realistic Fidelity
- Repeatability
- Low Cost Test HW
- Fast Reconfiguration
- Full Data Collection

- **Standard Commercial Laptop Contains All Necessary Software**
- **No External Connections Required**

VEE uses actual code for all protocols powering the Global Internet

VEE: Configuring Realistic Networks

Former DoD CIO Teri Takai, speaking at Intel's April 2, 2014 "Security Through Innovation Summit":

"The way that we're configured and constructed today…it is enormously difficult for [U.S. Cyber Command] to actually do their job, to actually be able to see into the networks, understand what is in all of the networks and actually be able to defend those networks."

With VEE you can realistically:

Configure network infrastructure

- SDH, GigEther, LANs, MANs, WANs, IPv4/IPv6, RIP, OSPF, BGP, LDP, MPLS, DNS, DHCP, Clients, Servers, …
- SS7, WDM, CDMA, GSM, P2P, VoIP, …

Configure network security

- Firewalls, ACLs, IPSec, IKE/ISAKMP, VPNs, HAIPE, vulnerabilities, malware, NVD, DISA STIGs, …

Configure wireless/mobility devices

- IEEE 802.11, Mobile-IP, MANETs, …

Use realistic data sets

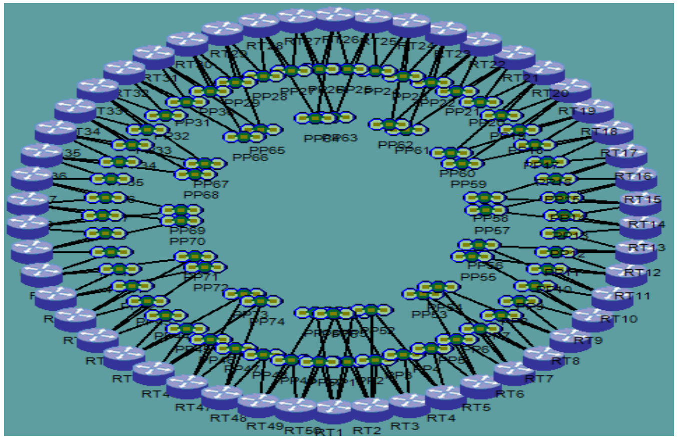
- Sufficient size, proper encapsulations, free from legal issues such as USSID 18
- Have created a 20 million persona data base

Reverse engineer networks from data collected on them to see into the network, understand what is in all of the networks and actually be able to defend those networks

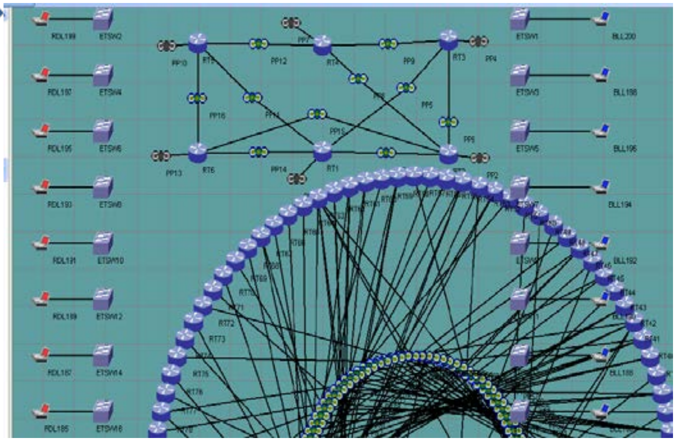
VEE: Network Construction Options

1. **Manually – Drag/Drop/Connect**
   - Library of pre-config. components
     - Hosts, Routers, switches, …

2. **Automatically Generate Notional Networks**
   - # nodes - 50
   - Aver. node degree = 3



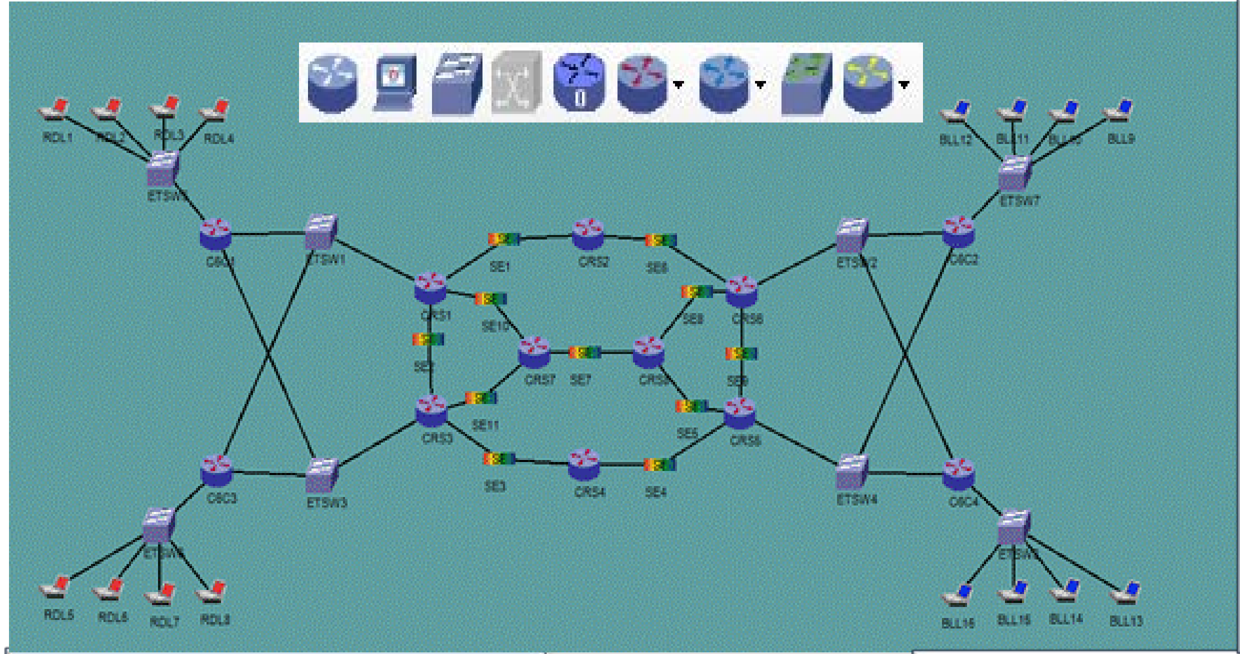
3. **Reverse Engineer from Network Data Collection**
   - Three data feeds:
     - Full capture (top middle rectangle)
     - Router configs (big circle)
     - Netflow (left and right vertical)



Note: Pre-configured components are clones of vendors networking products. They are created based on publically available information about these products.

VEE: Creating a Cyber Range - On a Laptop

In addition to automated cloning of actual networks, Testers can build networks that are still in the design stage to evaluate expected network responses and do so with all the fidelity of the implemented network



VEE Provides Unprecedented Insight and Visibility into Target Network Operations to Cyber Mission Planners and Decision-Makers Before, During and After Operation

Reverse-Engineer Network to Create Network/Cyber Situational Awareness

Clone & Emulate Network with Full-Fidelity

Emulate Cyberspace Operations: CND, CNA, CNE

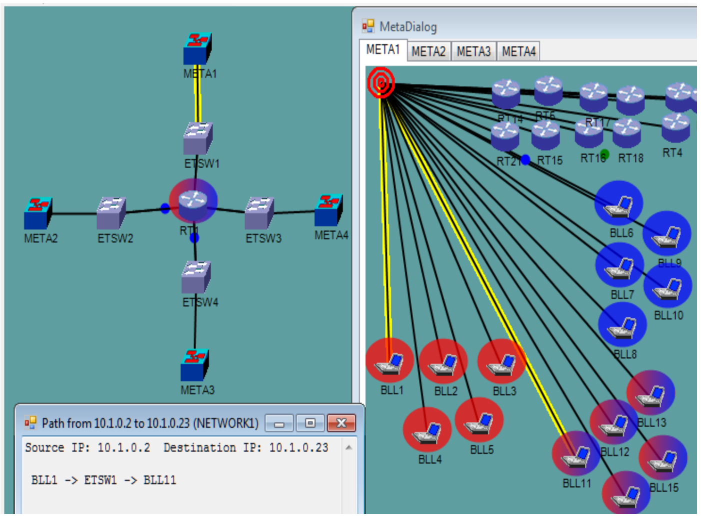
Emulate Cyber Command & Control (C2)

Emulate joint, alliance, CMF Training

Test network responses to cyber attacks on a laptop

Emulating multiple concurrent cyber teams operating on a common cloned network in VEE

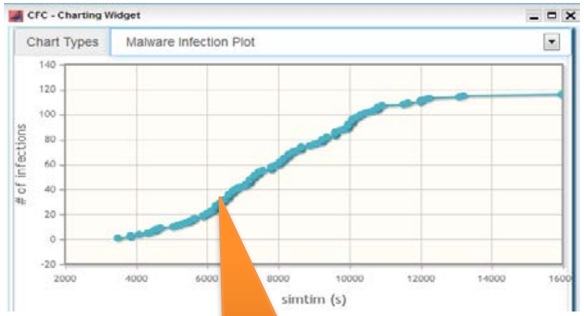
Role-Based Multi-Party Web Interface for Simultaneous Red and Blue Teams Operating within the Same Cloned Network



Path from 10.1.0.2 to 10.1.0.23 (NETWORK1)

```
Source IP: 10.1.0.2  Destination IP: 10.1.0.23

 BLL1 -> ETSW1 -> BLL11
```



Graphing Engine – Force Directed Layout Algorithm

Ozone Widgets	Category
VEE VEE VEE	Summary
VEE VEE	Infection graphs
VEE	Activity graphs
VEE VEE VEE VEE VEE	Detailed Logs
VEE	Network Topology
VEE	Malware Topology
VEE VEE	Terrestrial Topology
VEE	Report Generation
VEE	Event Insertion

Comparison of Cyber Testing Solutions

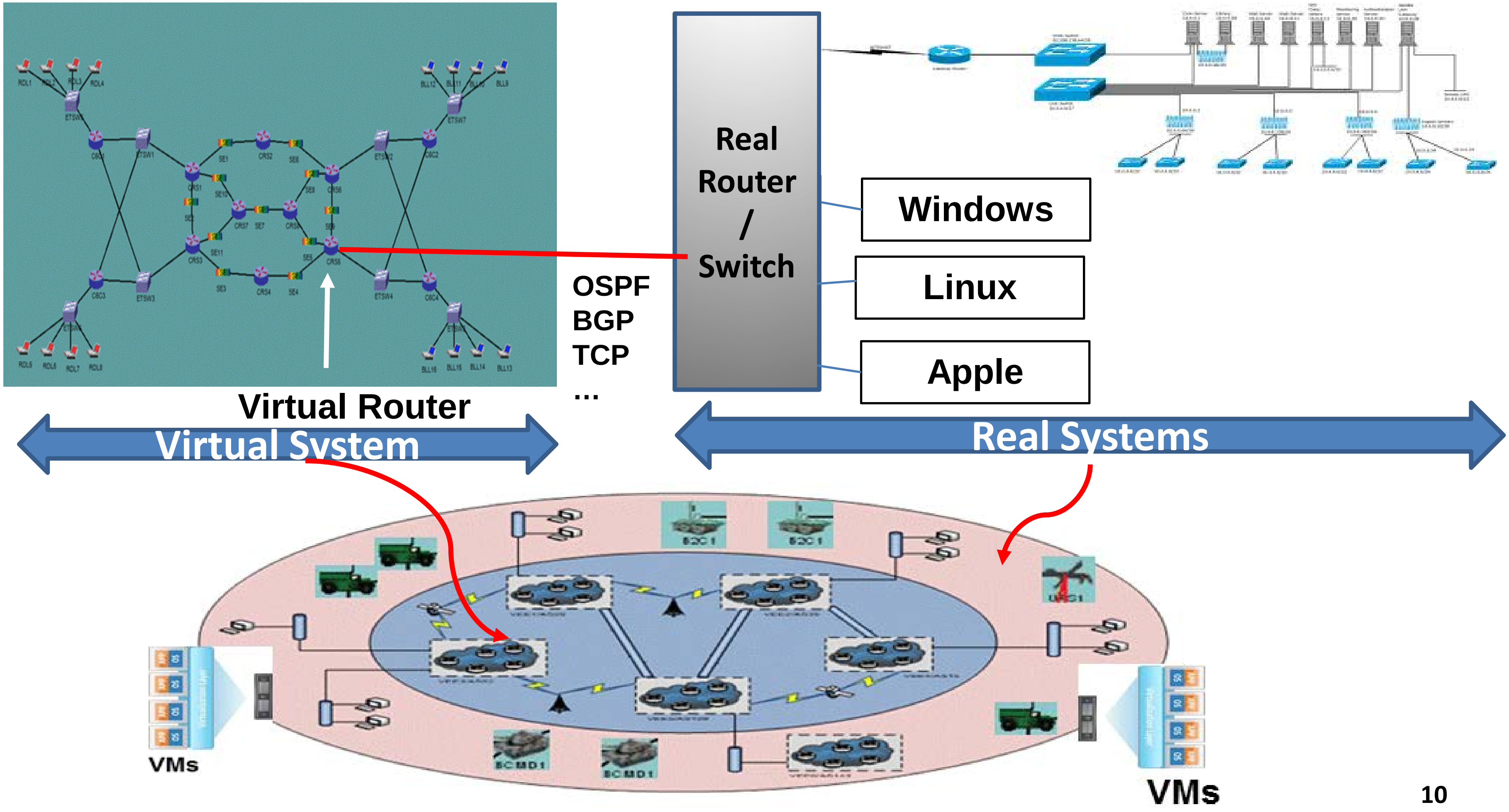
Problems

- Non-agile hardware-based solutions
- High expense of cyber ranges (100's servers)
- Challenge of rapid reconfiguration of large computer facilities within a Cyber Range

Areas of Concern	Cyber Farm High Fidelity Approaches	VEE High Fidelity Approach
Basis of Test Environment	Custom Hardware/Software	Low-cost laptop to server class multi-core class machine (s)
Expense ($) of Cyber Farm	Millions to tens of Millions	A few Thousands
Scalability	Limited – adding custom HW/SW upgrade is expensive	Inexpensive – adding commodity machine and/or added functionality is low cost
Space needed	Dedicated room and rack(s)	Essentially none
Power/AC to run	Significant for large configurations	Insignificant
Resources to operate & manage	Dedicated team of administrators and network engineers	User operates and manages his own progression on his own laptop
Access to Classified Environments	Dedicated SCIF with Electromagnetic Controls surrounding the range	Any SCIF and a small Faraday Cage
User control over cyber testing	Limited – may require strict scheduling of times for use	Unlimited – Cyber Testing anywhere and anytime

VEE: Live-Virtual Systems Integration

- Link VEE to networked servers/cyber farms, actual networks, and mobile devices to extend Cyber ranges at minimal cost
- Link cloned networks & test Systems of Systems at minimal cost.



Real Router / Switch

Windows

Linux

Apple

OSPF
BGP
TCP
…

Virtual Router

Virtual System

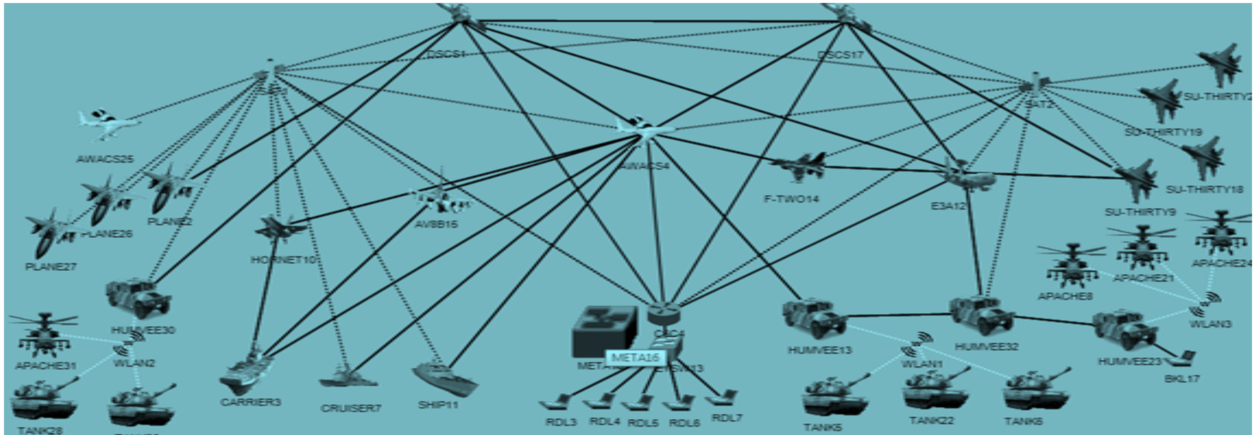
Real Systems

VMs

VMs

What Can VEE do for Cyber Testing?

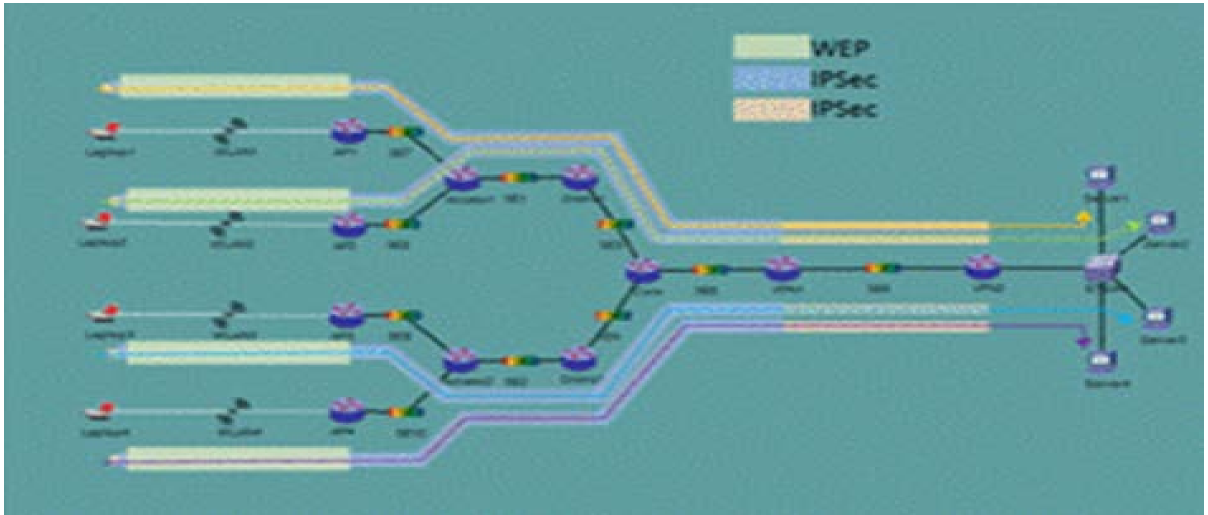
- Provide a documented path to a network's actual configuration and rapidly build a specific network from real-world software components and configurations
- Significantly reduce the cost of realistic network tests by performing them on a low-cost computer. Perform many tests simultaneously on separate laptops and demonstrate their repeatability
- Expand testing by linking cloned networks with real networks and/or cyber farms to create systems of systems, especially for joint and allied interface testing.



- New low-cost opportunities to greatly increase the scope and number of high-fidelity network tests conducted

What Can VEE do for Cyber Testing?

- Rapidly reconfigure by wiping a single machine. Use automated reports to begin analysis almost immediately
- If planning to reuse a network, save and store the network configuration and rapidly reload it on another laptop
- House the network test in a normal office environment. Or take a whole network into a SCIF on a laptop
- Easily swap cloned networks among test organizations



New efficiencies in cyber facilities, support, test conduct, and post-test analysis

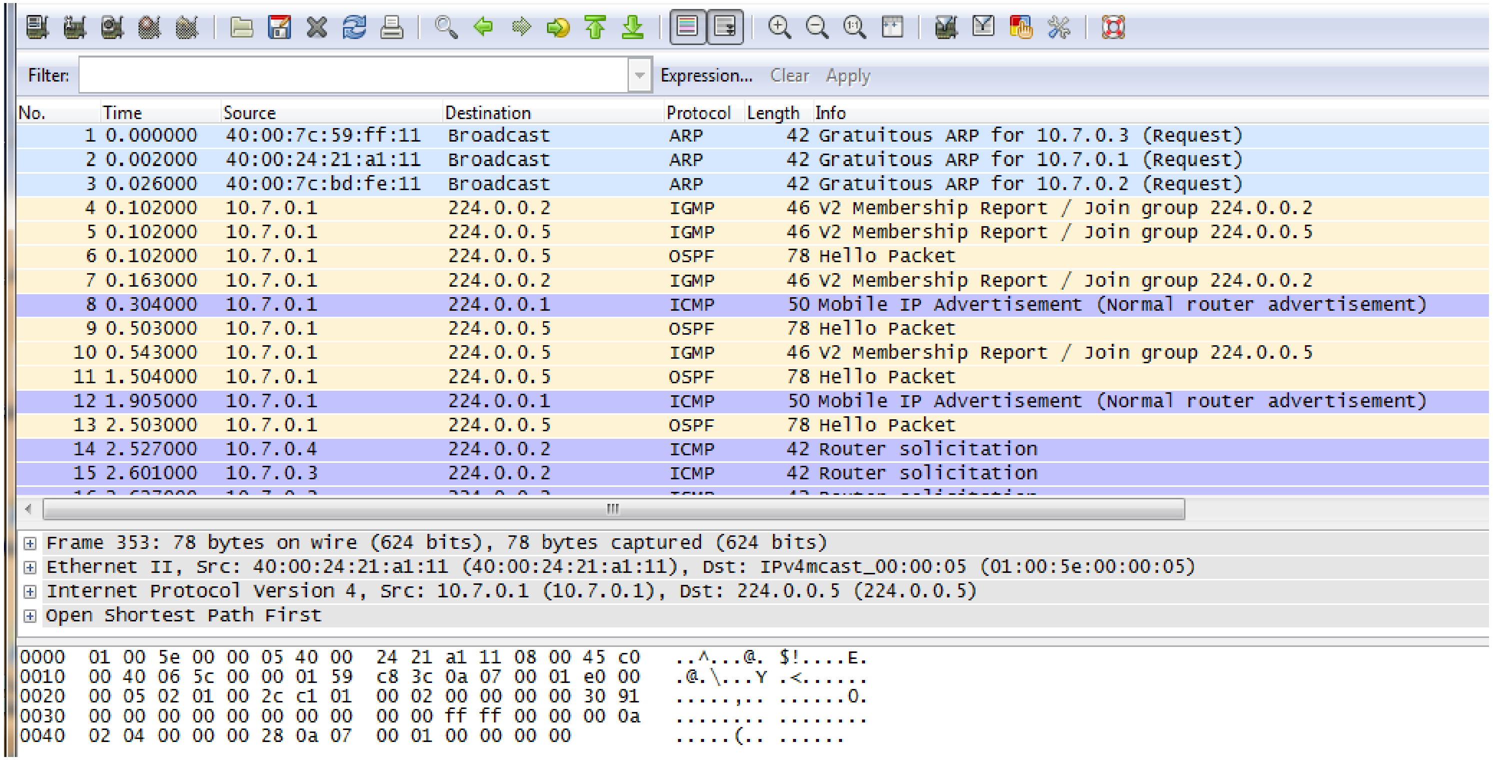
VEE Test Support Summary

- Networks Reverse-Engineered from Net Data
- Realistic Responses down to the bit level
- Extensively Instrumented with Network Tools
- Agile, Quickly Reconfigured, Repeatable
- Inexpensive Hardware that's Easily Expanded
- Interfaces to live systems/devices and actual networks are currently being demonstrated
- Available under license to Government Agencies & Government authorized contractors

Low-Cost, High Fidelity Cyber Testing Using VEE

VEE Demonstrations Available

- **Live, unclassified VEE demonstrations are available and can be arranged for Government Agencies & Government authorized contractors.**
- **POCs for VEE users in the IC community can be provided.**



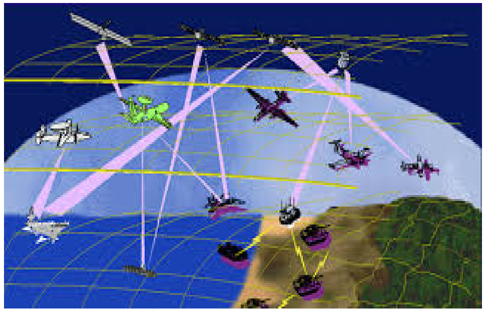
```
No.    Time       Source              Destination      Protocol Length Info
     1 0.000000   40:00:7c:59:ff:11   Broadcast        ARP         42 Gratuitous ARP for 10.7.0.3 (Request)
     2 0.002000   40:00:24:21:a1:11   Broadcast        ARP         42 Gratuitous ARP for 10.7.0.1 (Request)
     3 0.026000   40:00:7c:bd:fe:11   Broadcast        ARP         42 Gratuitous ARP for 10.7.0.2 (Request)
     4 0.102000   10.7.0.1            224.0.0.2        IGMP        46 V2 Membership Report / Join group 224.0.0.2
     5 0.102000   10.7.0.1            224.0.0.5        IGMP        46 V2 Membership Report / Join group 224.0.0.5
     6 0.102000   10.7.0.1            224.0.0.5        OSPF        78 Hello Packet
     7 0.163000   10.7.0.1            224.0.0.2        IGMP        46 V2 Membership Report / Join group 224.0.0.2
     8 0.304000   10.7.0.1            224.0.0.1        ICMP        50 Mobile IP Advertisement (Normal router advertisement)
     9 0.503000   10.7.0.1            224.0.0.5        OSPF        78 Hello Packet
    10 0.543000   10.7.0.1            224.0.0.5        IGMP        46 V2 Membership Report / Join group 224.0.0.5
    11 1.504000   10.7.0.1            224.0.0.5        OSPF        78 Hello Packet
    12 1.905000   10.7.0.1            224.0.0.1        ICMP        50 Mobile IP Advertisement (Normal router advertisement)
    13 2.503000   10.7.0.1            224.0.0.5        OSPF        78 Hello Packet
    14 2.527000   10.7.0.4            224.0.0.2        ICMP        42 Router solicitation
    15 2.601000   10.7.0.3            224.0.0.2        ICMP        42 Router solicitation
```

```
⊞ Frame 353: 78 bytes on wire (624 bits), 78 bytes captured (624 bits)
⊞ Ethernet II, Src: 40:00:24:21:a1:11 (40:00:24:21:a1:11), Dst: IPv4mcast_00:00:05 (01:00:5e:00:00:05)
⊞ Internet Protocol Version 4, Src: 10.7.0.1 (10.7.0.1), Dst: 224.0.0.5 (224.0.0.5)
⊞ Open Shortest Path First
```

```
0000  01 00 5e 00 00 05 40 00  24 21 a1 11 08 00 45 c0   ..^...@. $!....E.
0010  00 40 06 5c 00 00 01 59  c8 3c 0a 07 00 01 e0 00   .@.\...Y .<......
0020  00 05 02 01 00 2c c1 01  00 02 00 00 00 00 30 91   .....,.. ......0.
0030  00 00 00 00 00 00 00 00  00 00 ff ff 00 00 00 0a   ........ ........
0040  02 04 00 00 00 28 0a 07  00 01 00 00 00 00         .....(.. ......
```

- **Wireshark$_{tm}$ successfully decodes pcap data captured in VEE into packets. Most network tools work as on real nets.**

Questions?



Capture Sufficient Data from Any Net to Build a Clone

POC:

Dr. Deepinder Sidhu
Chief technologist
TeleniX Corporation
dsidhu@telenix.com
410-772-3275

Emulate Realistic Networks for Low-Cost Cyber Testing on a laptop

Low-Cost, High Fidelity Cyber Testing Using VEE

Network Cloning

- Clone behavior is indistinguishable from the real network
- Clone requires no validation since it is identical to its real counterpart
- All decisions in clone made by actual code and network state – no randomness
- Clone evolves to actual system
- Clone answers any/all questions about net over its life-cycle
- Virtual host/routers in network clone run complete TCP/IP stack under FreeBSD kernel as in real net
- Clone uses identical code and configurations of a real network
- Clone can be used to diagnose and solve operational problems such as routing
- Clone uses 100% of actual code

Network Modeling

- No mathematical basis for the model to behave like a real system
- Virtually impossible to validate a model-based network
- Many decisions in network model made by calling random numbers
- Models often thrown away after use
- Often build new models to answer new questions
- Model has no OS kernel in model nodes, mimics TCP/IP using small amount of code in nodes, runs as app
- No model has ever become reference implementation of any Internet protocol
- Model “mimics” some limited aspect of a network with small amount of code
- Typically uses <20% code with abstractions