

CYBER
SPACE

CYBER-WARRIOR
Bilim Teknolojisinin Yer Altı Dünyası

Cyberspace Dominance



Next Generation Network Systems Engineering in a Low Cost Network Emulation

Deepinder Sidhu and Chuck Burdick

TeleniX Corporation

Tel: 410-772-3275

POC Email: dsidhu@telenix.com

NDIA Systems Engineering Conference 27-30 Oct 2014

Presentation 17029

Chuck Burdick is an Innovative Decisions, Inc. subcontractor

Network Systems Development in a Realistic, Repeatable, Flexible, & Inexpensive, Environment

Agenda

- **What is the TeleniX Virtual Emulation Environment (VEE) and what does it do**
- **How VEE can Efficiently Support Network Systems Engineering through its Entire Live Cycle**
- **Summary**
- **Questions?**

Network Headlines

- **DARPA builds Multi-million dollar National Cyber Range (NCR) with 100s of high-end servers.**



Bottom Line Up Front

Building robust and well-protected networks is a critical national endeavor, but network RDT&E can be very costly to emulate in hardware, and simulations cannot predict behavior that has not been seen before

- But what if you could use actual internet software and protocols to create an operational virtual network from design onward?
 - And create actual network configurations with bit-level fidelity in a low-cost, virtual emulation – a network clone.
 - And have the cloned network provide the identical responses to misconfigurations, outages, and cyber attacks as the real network in both current and anticipated environments.

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

- TeleniX Virtual Emulation Environment (VEE)

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, HA/PE, 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

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 based only on the design
- 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 Advantages

- Bit Level Fidelity
- Repeatability
- Low Cost 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 ⁵

VEE: Network Construction Options

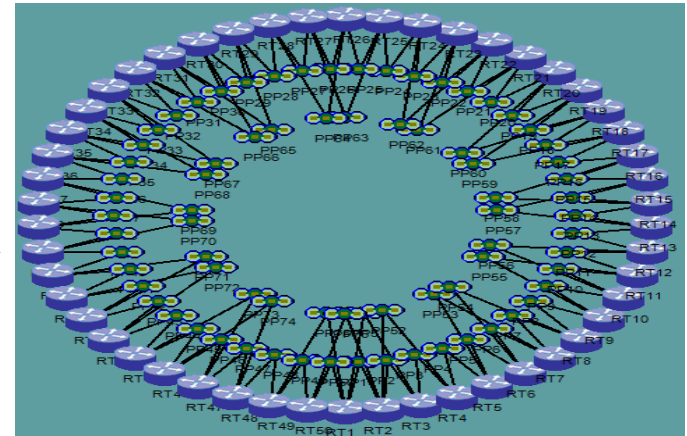
1. Manually – Drag/Drop/Connect

- Library of pre-config. components
 - Hosts, Routers, switches, ...



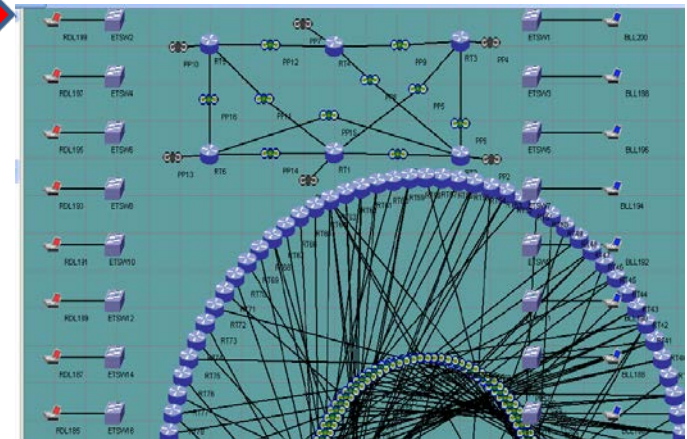
2. Automatically Generate Notional Networks

- # nodes - 50
- Aver. node degree = 3



3. Reverse Engineer from Network Data Collection

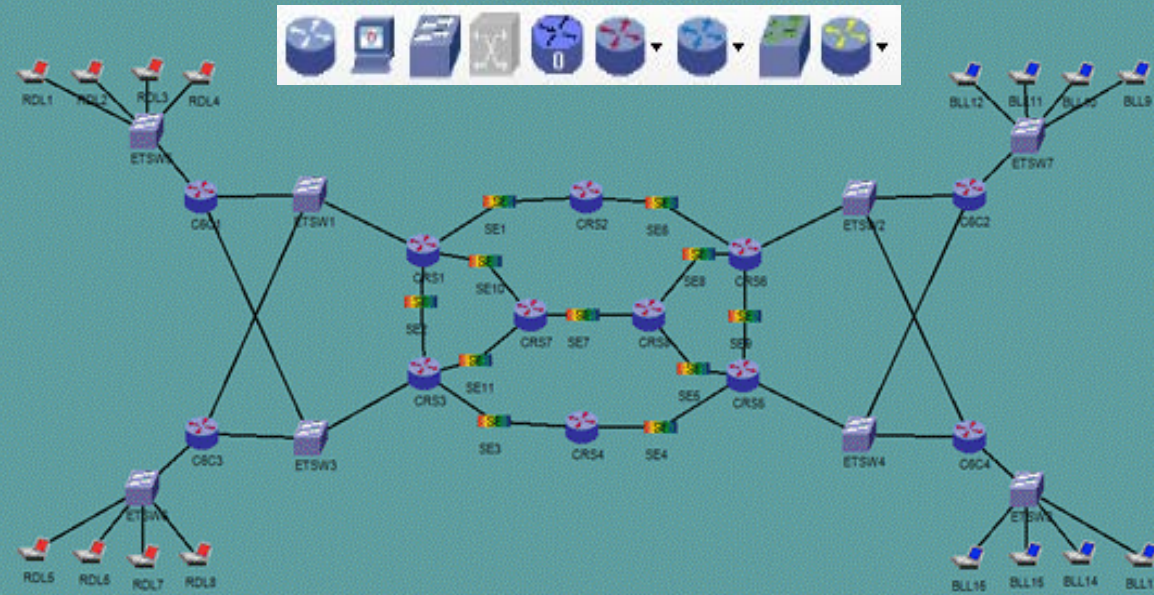
- Three data feeds:
 - Full capture (top middle rectangle)
 - Router configs (big circle)
 - Netflow (left and right vertical)



Note: Pre-configured components are clones of vendor's networking products. They are created based on publically available information about these products and knowledge of the standards they must meet.

VEE: Designing a Network- On a Laptop

Developers can emulate networks that are still in the design stage to evaluate expected network responses such as Emergent Behaviors and do so with all the fidelity of the implemented network



VEE Provides Unprecedented Insight and Visibility into Network Operations to Developers and Decision-Makers

Reverse-Engineer Network to Create Network/Cyber Situational Awareness

Clone & Emulate Network with Full-Fidelity

Emulate Cyberspace Operations: CND, CNA, CNE

Emulate Net/Cyber Command & Control (C2)

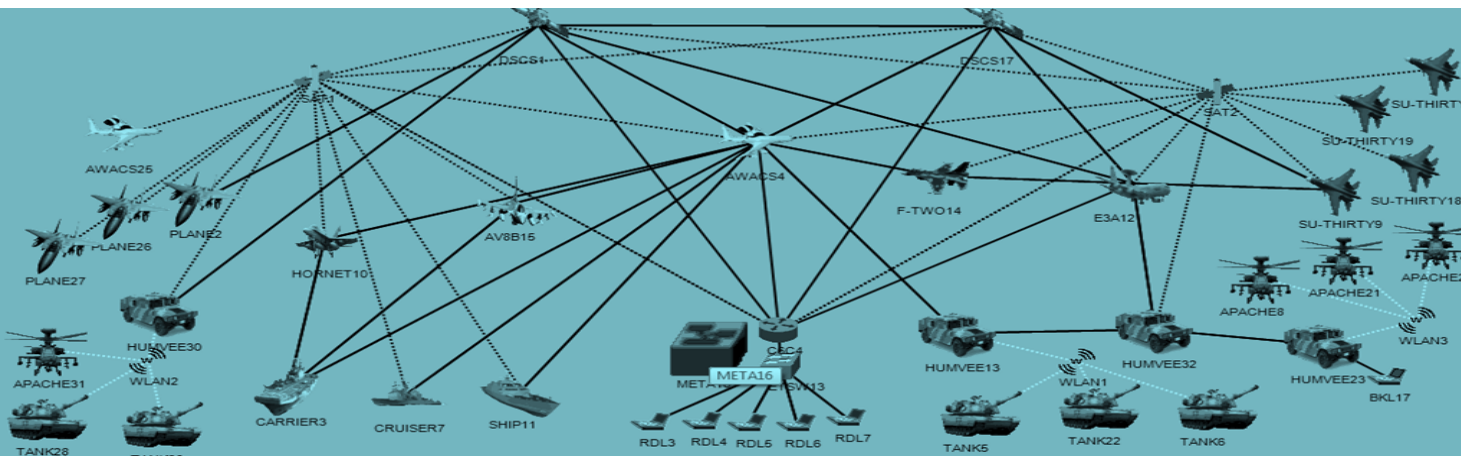
Emulate joint, alliance, CMF Training

Test the network responses at every stage of development

What Can VEE do for Systems Engineering?

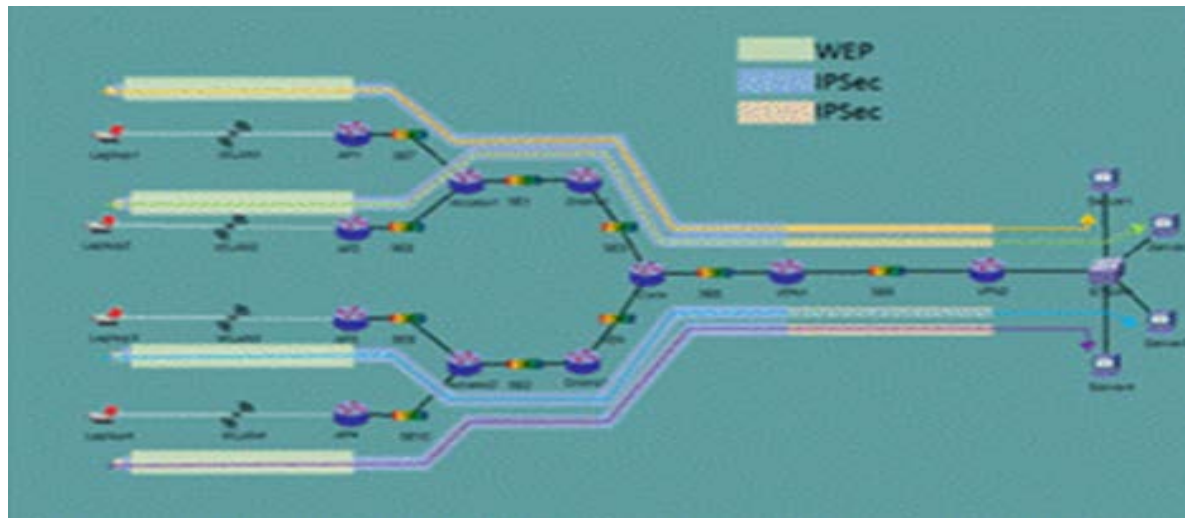
- Rapidly build an operational network from a design using real-world software components and configurations including new capabilities that are just emerging.
- Reduce the cost of realistic network tests by performing them on low-cost computers. Perform many tests simultaneously on separate laptops with perfect repeatability.
- Link cloned networks with real networks and/or cyber farms to create Systems of Systems. This can be used for joint and allied network interface testing long before the new system is built.

Provide low-cost opportunities to conduct early evals of system operations during design & greatly increase the scope and number of high-fidelity tests



What Can VEE do for Systems Engineering 2

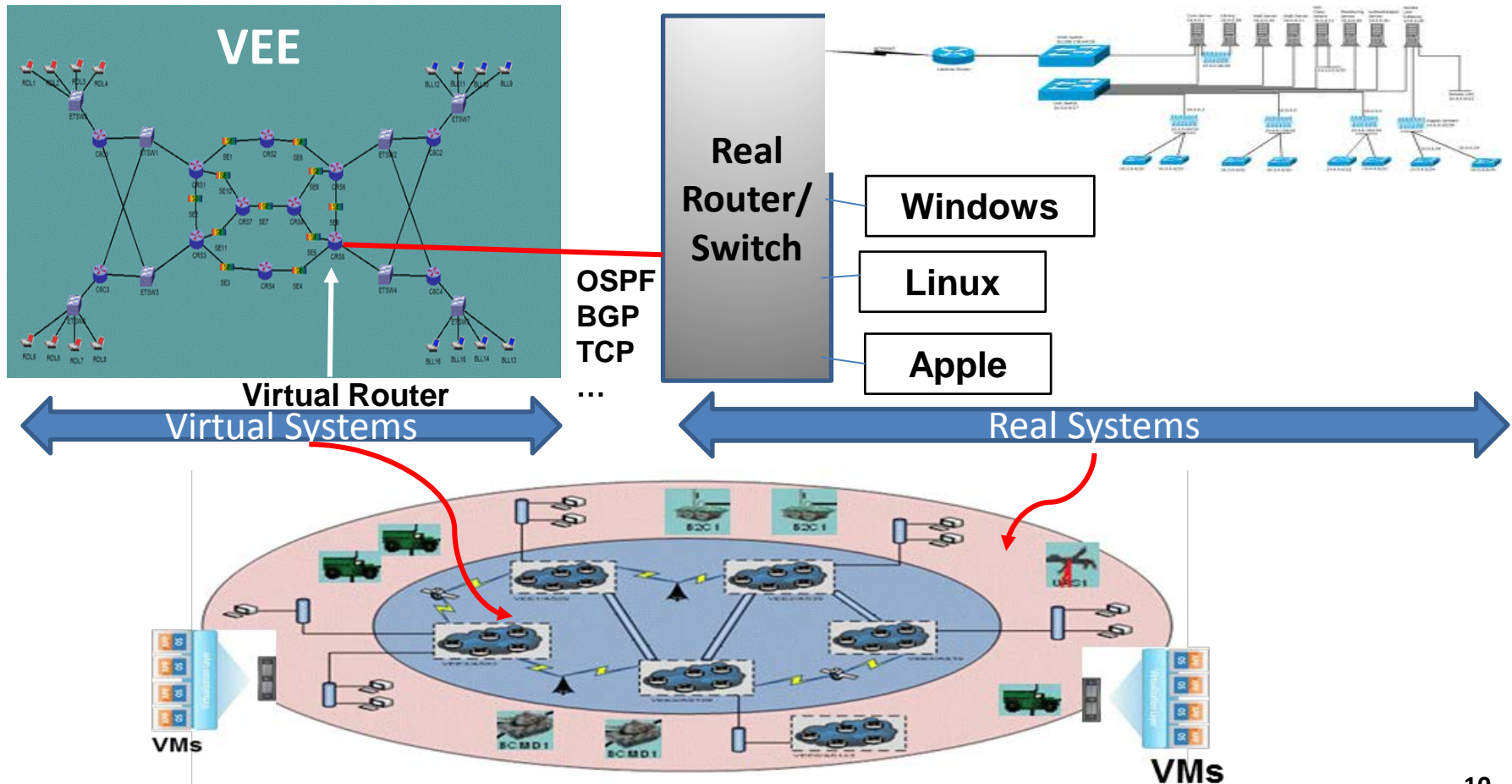
- Solve real-world problems of the operational network using the clone
- Evaluate planned upgrades and patches prior to hosting them on the real network
- Provide Situational Awareness of the deployed network by comparing the clone and the Reverse Engineered state of the actual network
- Support easy swapping of cloned networks among RDT&E organizations



**New
efficiencies
in Systems
Engineering
throughout
the System
Life Cycle**

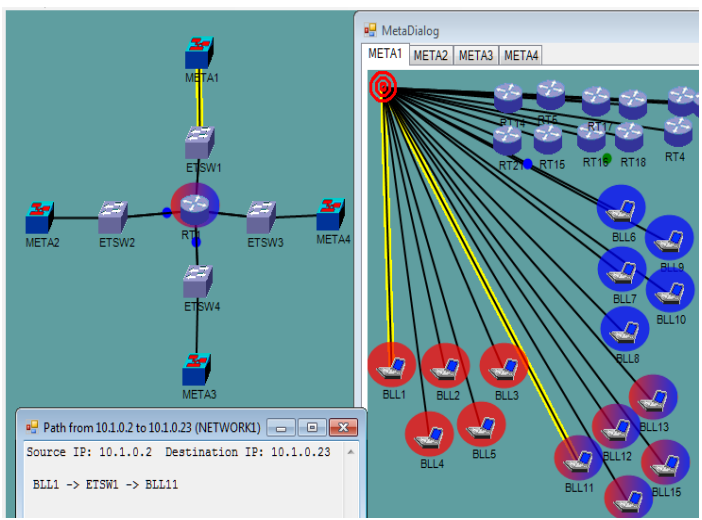
Seamlessly Link Live and Virtual Systems

- Actual networks, networked servers/cyber farms, mobile devices, ...
- Virtual training simulations through HLA (MATREX, ERF, ...), DIS, TENA, and CTIA along with MC systems
- Integrate MC and Live instrumentation systems, Virtual trainers, Constructive Simulations / Stimulations and Gaming capabilities

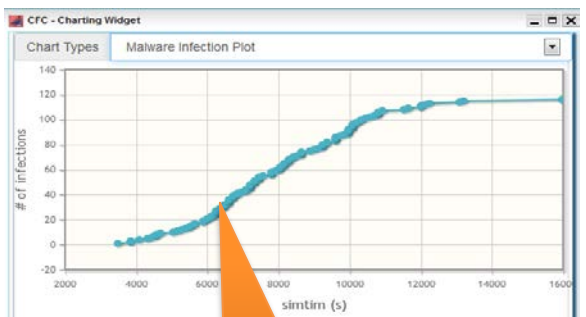


Harden systems by emulating multiple concurrent cyber teams operating on a common cloned network

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



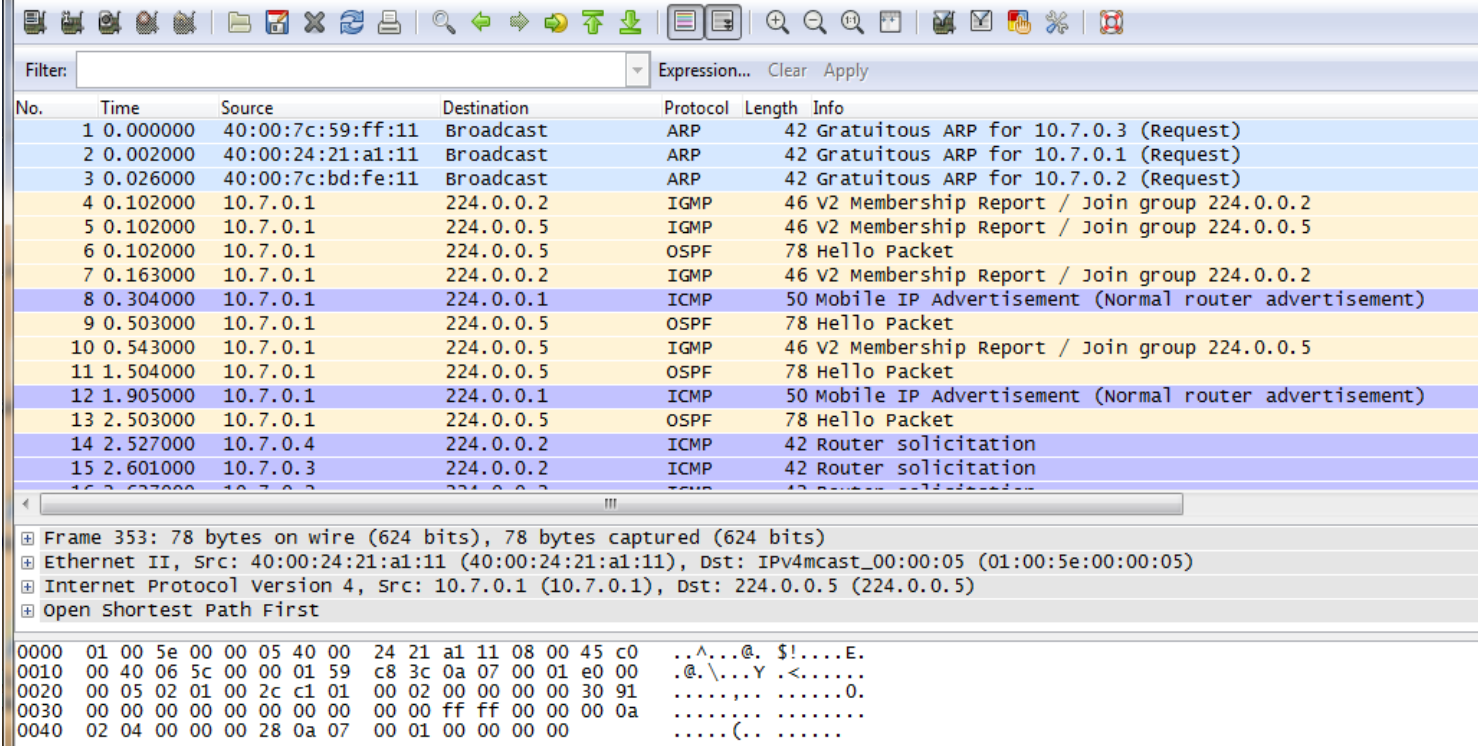
Ozone Widgets	Category
	Summary
	Infection graphs
	Activity graphs
	Detailed Logs
	Network Topology
	Malware Topology
	Terrestrial Topology
	Report Generation
	Event Insertion



Graphing Engine – Force Directed Layout Algorithm

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.



The screenshot shows the Wireshark interface with a list of captured packets. The table below represents the data visible in the packet list pane.

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

Below the packet list, the details pane shows the structure of a selected frame (Frame 353):

- 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

The packet bytes pane shows the raw data in hexadecimal and ASCII:

```
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 00  .....(.. .....
```

- Wiresharktm successfully decodes pcap data captured in VEE into packets. Most network tools work as on real nets.

VEE Network Systems Engineering Summary

- **Emulate Networks that are Still in Design**
 - With Realistic Responses down to the bit level
 - Using Inexpensive Hardware that's Easily Expanded
- **Support Greatly Expanded System Testing**
 - Provide sophisticated test environments at low cost
 - Interface to live systems/devices and actual networks
 - Obtain deep insight into net operations in varied contexts
- **Support System Deployment and Operations**
 - Support Network Defense thru Situational Awareness
 - Test SW patches prior to installation and trouble-shoot problems down to the bit and nanosecond level

Low-Cost, High Fidelity Network Support with VEE is available under license to Government Agencies & Government authorized contractors

Questions?



**Design a Working
Network or
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 IA and Cyber
Operations on a
laptop**

**Low-Cost, High Fidelity Network Systems
Engineering Support throughout the System
Life Cycle Using VEE**

Current SE Solution vs VEE Solution

Network SE Problems

- Non-agile hardware-based solutions
- High expense of cyber ranges (100's servers)
- Challenge of obtaining time on the range and the difficulty 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 RDT&E 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

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

VEE: Cyber Demonstration on Laptop

1. Clone Land/Sea/Air/Space Network

- Packet filtering
- Route changes: Node/Link failures
- Router commands: Route table
- Reporting: Routers configs
- TCP flows
- eBGP

2. Cyber Warriors Training

- Configure CNA/CNE/CND
- VPN tunneling in Mobile architecture
- Reporting: VPN configurations
- Malware propagation
- IDS/Firewall
- Cyber warriors training/certification

3. Network Reverse Engineering

- NetFlow, Router Config , SNMP,
- Cyber Situational awareness
- NVD – overlay vulnerabilities
- Attack vector analysis
- Harden networks

4. Multi-Party Web Interface

- Red/Blue teaming
- Cyber Flag training
- CMF TTPs training

5. Cyber Mission Control

- Data fusion from multiple feeds
- Cyber situational awareness
- Mission support: before, during and after (BDA) operation

6. Live-Virtual Nets Integration

- Extend Cyber/IO ranges
- JLVC Cyber 2020 training

