hp TCP/IP Services for OpenVMS Technical Update and Strategy

Jim Lanciani - Manager
OpenVMS Security, Application Integration and Network Labs

September 27th 2005

Agenda

- TCP/IP Services ECO’s
- TCP/IP Services V5.5 Features List
- TCP/IP Services V5.6 Proposed Features List
- TCP/IP Services Strategy and Roadmap
- IPsec Overview

TCP/IP V5.4 ECO5/V5.5 ECO1

- TCP/IP V5.4 ECO5 shipped in June ‘05
- TCP/IP V5.5 ECO1 expected in October ‘05
- Completely new version of SSH
  - Upgrade to V3.2 (V5.4 ECO5 and V5.5)
  - Security fixes
  - SSH Now supports IPv6
  - SSH Configuration files must be updated (V5.4 ECO5 and V5.5)
- Many CERT updates addressed in ECO5 (see release notes)
- IPv6 documentation updates (see release notes)
- NFS bug fixes
  - Handling of mode, uid, gid, size, atime, mtime
  - Support for CASE_SENSITIVE options for ODS-5
  - chmod operation from a Unix client results in an invalid date
- Improved FTP copies of large (multi-gigabyte) files to a disk with high-water marking
- Support for 'filter' command with ifconfig to perform filtering of IP addresses
- NTP - Clock synchronization algorithm delays fixed

NOTE: Please review release notes prior to upgrade

TCPIP V5.5 for OpenVMS V8.2 Features List

- TCP/IP Services V5.5 FCS January 2005 on OpenVMS Version 8.2 or higher
- Supported on both OpenVMS Alpha and OpenVMS Industry Standard 64 (I64) systems with the same functionality unless otherwise noted
  - No NFS server on IA64 yet
  - No PPP on IA64 and Alpha yet
- On VAX systems, use TCP/IP Services V5.3

- New features
  - SSH upgrade to Version 3.2
  - Secure IMAP
  - IPv6 Updates and Enhancements
    - SSH support for IPv6
    - failSAFE IP Support for IPv6
  - NTP Network Time Protocol upgrade to Version 4.2
  - TCPDUMP upgrade to Version 3.8.3 and libpcap API
  - Updated Header Files in TCPIP$EXAMPLES
  - See Release Notes for more New Features

TCPIP V5.6 for OpenVMS V8.3 Proposed Features List

- Supported on both OpenVMS Alpha and OpenVMS Industry Standard 64 (I64) systems
- DNS/BIND 9 Resolver and v9.3 Server
- DNSSEC
- IPv6 Compliance Testing
- NFS Client TCP Support
- NFS Server Support for I64
- NFS Symlink Support
- NTP Security Update (SSL), NTP AutoKey
- SMTP Multi-Domain Zone
- SSH Upgrade with Kerberos
- TELNET Upgrade with Kerberos Support
- TELNET Server Device Limit
- IPv6 support for LPD and TELNETSYM
- FTP Performance Boost for VMS Plus Mode
- Updates to TCPIP$CONFIG (failSAFE IP)
- Improved Management Utilities (ifconfig etc.)
- ***IPsec Support (post 5.6)***

TCP/IP Services Strategy and Roadmap

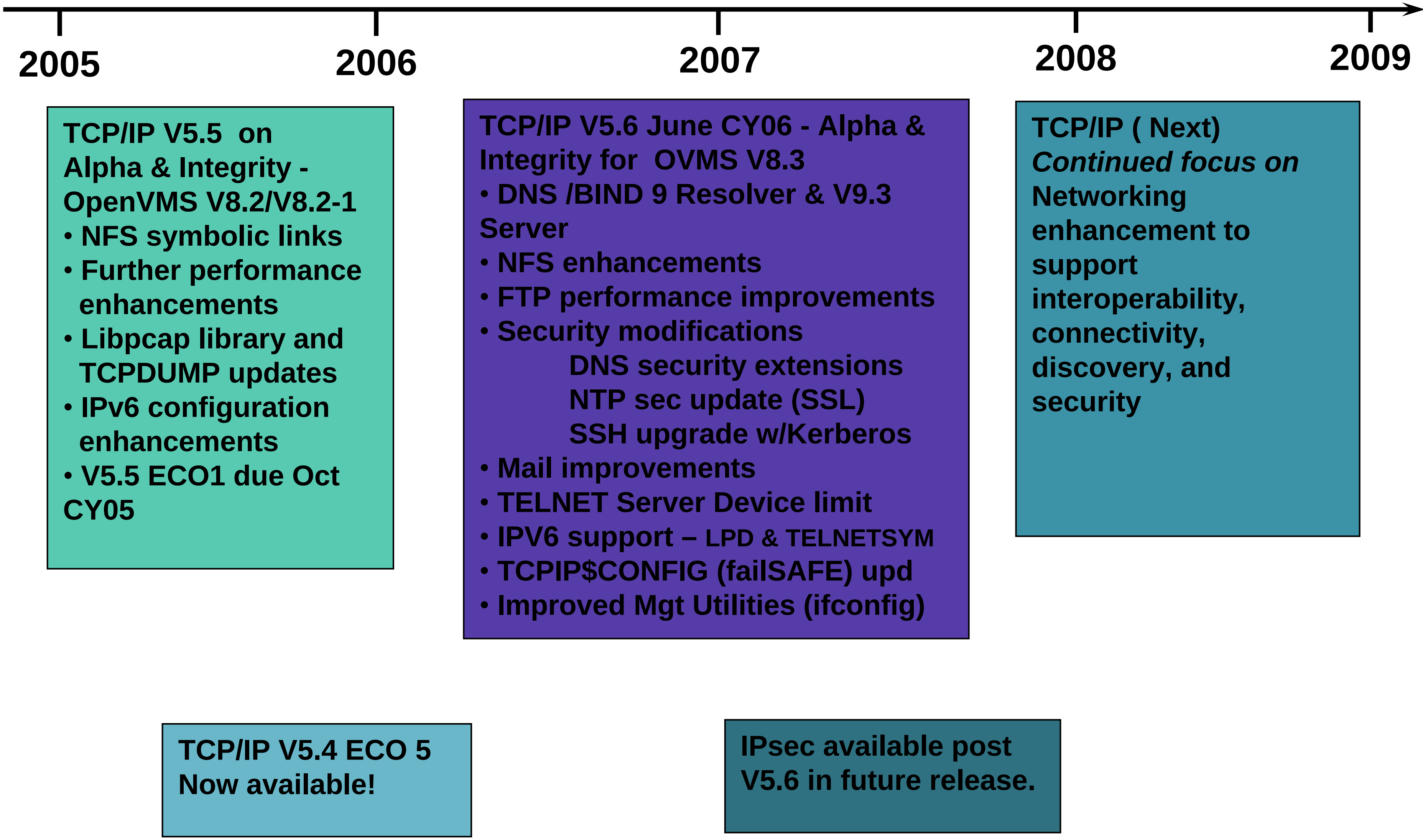
TCP/IP Strategy

- Networking is more strategic than ever in today's enterprise
  - Vital component in all customer's environment
  - Customers expect Networking to "just work" and to be ubiquitous
- Networking must continue to support interoperability, connectivity, discovery, and security for OpenVMS
  - Current Standards-based network environment
  - Remain current with network changes in industry
  - Meet evolving Internet Security requirements
- Continuing performance improvements in important and key TCP/IP applications
- Continue to improve scalability in complex environments with more and faster CPU's
- Continue to monitor and support critical emerging network related technology as required
- Continue to provide network functionality that meets our customers requirements
- Continue to provide Secure networks

TCP/IP Staying Current with Internet Technology Changes

- Participation in ESS/BCS Network Forum
- Participation in IETF
- Leveraging Public Domain BSD
- Leveraging from Third Party Partners
- SafeNet Inc.
- ISC BIND Consortia
- SSL
- Kerberos
- HP-UX TCP/IP applications

TCP/IP Services for OpenVMS



TCP/IP V5.5 on Alpha & Integrity - OpenVMS V8.2/V8.2-1

- **NFS symbolic links**
- **Further performance enhancements**
- **Libpcap library and TCPDUMP updates**
- **IPv6 configuration enhancements**
- **V5.5 ECO1 due Oct CY05**

TCP/IP V5.6 June CY06 - Alpha & Integrity for OVMS V8.3

- **DNS /BIND 9 Resolver & V9.3 Server**
- **NFS enhancements**
- **FTP performance improvements**
- **Security modifications**
  - **DNS security extensions**
  - **NTP sec update (SSL)**
  - **SSH upgrade w/Kerberos**
- **Mail improvements**
- **TELNET Server Device limit**
- **IPV6 support – LPD & TELNETSYM**
- **TCPIP$CONFIG (failSAFE) upd**
- **Improved Mgt Utilities (ifconfig)**

TCP/IP (Next)
Continued focus on
Networking enhancement to support interoperability, connectivity, discovery, and security

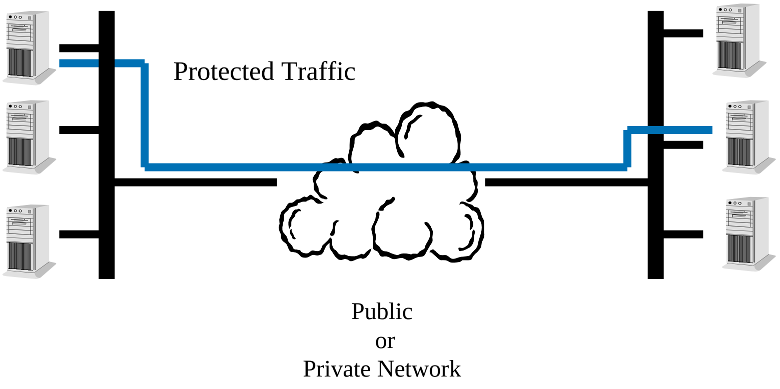
TCP/IP V5.4 ECO 5
Now available!

IPsec available post V5.6 in future release.

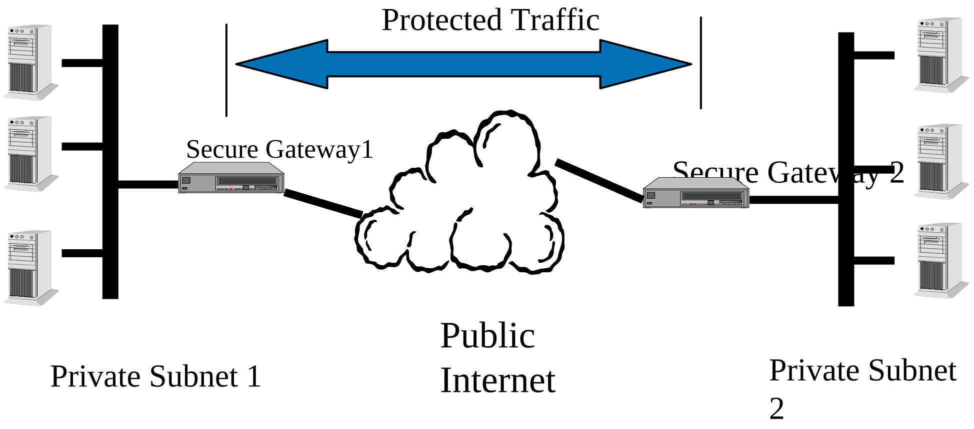
What is IPsec?

- Provides IP Security at the IP layer not the application layer
- Strong security that can be applied to all traffic
- Transparent to applications and end users
  - There is no need to train users on security mechanisms
  - Security/System Administrator
- Protects all upper layer protocols
- Secures traffic between any two IP systems
  - Both end-to-end and router-to-router ("secure gateway")
- Extensions to the IP protocol suite
  - Applies to IPv4 and IPv6
- Encryption and Authentication
- Key Management and Security Association creation and management

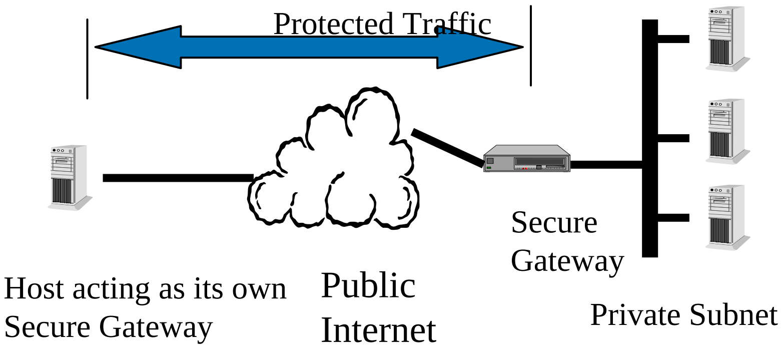
IPsec Security



IPsec for Host-to-Host



IPsec for Virtual Private Networks



IPsec for Remote Access

IPsec Support

- Based on the IPsec implementation from SafeNet Inc. http://www.safenet-inc.com/ called "QuickSec"
- IPsec consists of
  - Interceptor - a platform-specific module that provides the interface between OpenVMS IP kernel and IPsec Engine module
  - Engine – a Loadable IPsec kernel module which provides crypto-processing of packets
  - Policy Manager/IKE - an application which provides processing of security policies formulated by the system manager and exchanges security policies information with remote hosts
  - Management – a set of management utilities (such as key generation, etc.)
  - Configuration tool – a basic IPsec configuration tool which processes security policies formulated by a system manager

TCP/IP Services for OpenVMS Pointers and Contacts

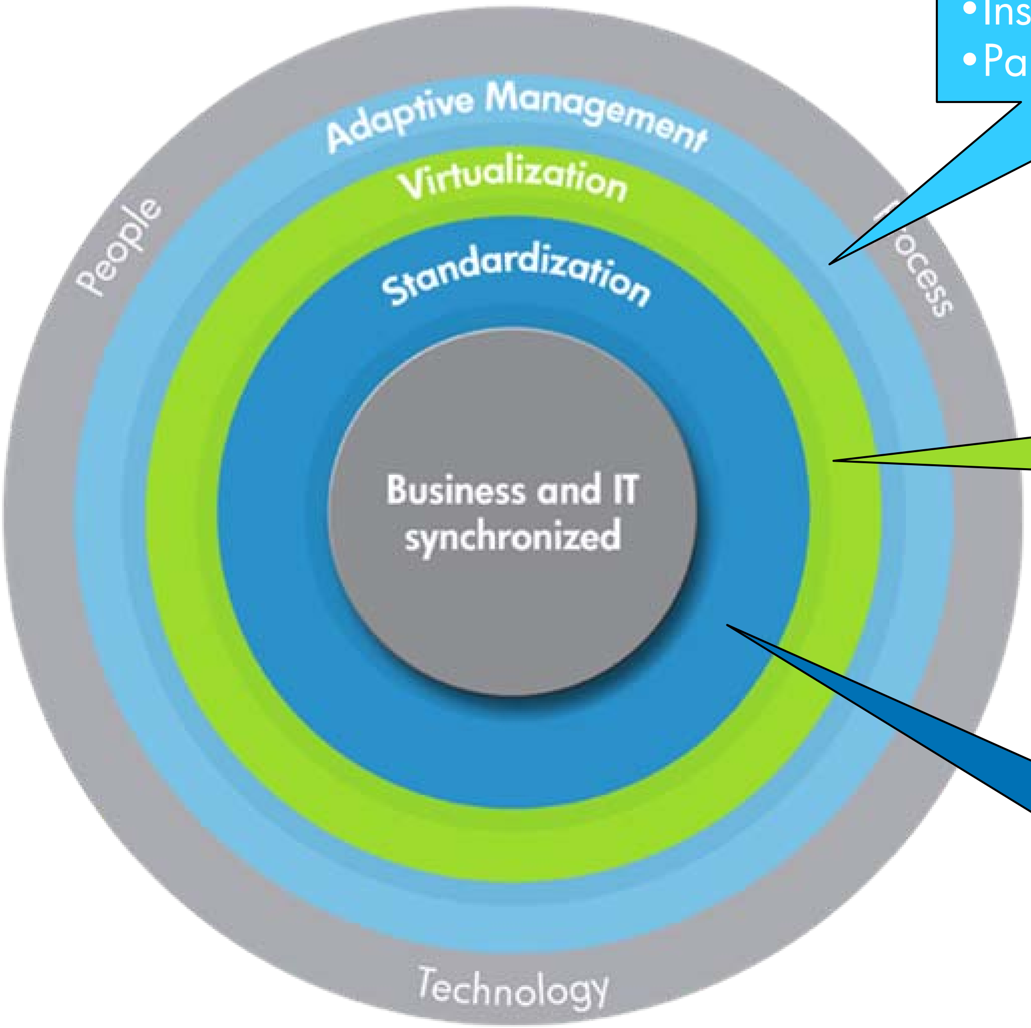
- HP OpenVMS Network Transports Home Page:
  - http://www.hp.com/products/OpenVMS
- Contacts:
  - Product Management
    Lawrence.Woodcome@hp.com
  - Engineering Management
    Jim.Lanciani@hp.com

Thank you !!!

invent

Following are slides that provide details not covered in the abbreviated TCP/IP presentation

OpenVMS in the Adaptive Enterprise



- OpenView
- Insight Manager
- Partner solutions

Key technology in Adaptive Enterprise

- Storage
- Itanium
- Integration
- Open Source
- TCP/IP

ISVs

TCP/IP V5.4 ECO5/V5.5 ECO1 (more improvements for SSH)

- Improved file transfer speed (sftp server)
- Support for <CTRL/C> and non-stream_lf files (OpenVMS server side only)
- RSA keys work for server to client authentication
- Remote client information available in SYS$REM_* logicals
- Local username available on intrusion records for non-OpenVMS client
- Upgrade Notes:
  - Beware re-creation of hostkey.* key files
  - Default for keys created by $SSH_KEYGEN now 2048 bits
  - New format for SSH*_CONFIG. Files
  - New location of SHOSTS.EQUIV
  - File transfer
    - See Release Notes for limitation. In general limited to OpenVMS files with stream_lf and fixed-length 512-byte record formats
    - Consider SSH FTP port forwarding as an alternative

TCP/IP V5.5 for OpenVMS 8.2 features

SSH (1)

- Upgrade to SSH2 Version 3.2.0
  - Introduces changes to the SSH utilities
  - SSH client and server on this version of TCP/IP Services cannot use configuration files from previous versions of SSH
- SSH Supports IPv6
  - SSH service must be set to IPv6
    - TCPIP> SET SERVICE SSH /FLAG=IPV6
- SSH X11 Port Forwarding
  - To use X11 forwarding in native mode, the system must be running DECwindows MOTIF Version 1.3 or higher. The X Authority utility (xauth) is also required

SSH (2)

- Maximum file size for SSH file copy operations has been increased from 4 megabytes to 4 gigabytes. The speed of file transfers has increased significantly.
- Can use SSH commands in batch jobs
- SCP and SFTP commands from the following Windows clients have been tested and interoperate correctly with the OpenVMS SSH server:
  - PuTTY
  - SSH Communications

Secure IMAP over the Secure Sockets Layer (SSL)

- Accepts connections on port 993 (by default) and encrypts passwords, data, and IMAP commands
- Compatible with clients that use SSL, such as Outlook Express, Netscape, and Mozilla
- Must install HP SSL kit from the HP OpenVMS Security web site: http://h71000.www7.hp.com/openvms/security.html
  - If the HP SSL software is not installed, the IMAP server will communicate in non-SSL mode.
- If you have IMAP configured to use SSL logical names for locating the certificate and key files
  - You must ensure that the SSL startup procedure is run before the TCP/IP Services startup procedure
- The secure IMAP configuration is controlled by the configuration file SYS$SYSDEVICE:[TCPIP$IMAP]TCPIP$IMAP.CONF

IPv6 Updates and Enhancements (1)

- IPv6 Configuration Enhancements and fixes
  - Can successfully configure 6to4 tunnels, all routes required for a 6to4 relay router, automatic tunnels, IPv6 over IPv6 manual tunnels, and manual routes
- ifconfig now documents how to manipulate IPv6 addresses
- IPv6 Neighbor Discovery process now supports RFC 3152 and can be configured to send Dynamic Update Requests for the forward and ip6.arpa DNS Reverse Zone
  - If you still need to support delegations based on the ip6.int zone you can use DNAME to rename ip6.int
  - For more information, refer to Section 3.1.3,of the HP TCP/IP Services for OpenVMS Guide to IPv6

IPv6 Updates and Enhancements (2)

- Several programming functions provided in earlier Early Adopter Kits (EAKs) were deprecated. These programming functions will no longer be supported after V5.5.
  - The following table lists the functions and their replacements:

Deprecated Function	Replacement Function
getipnodebyname	getaddrinfo
getipnodebyaddr	getnameinfo
freehostent	freeaddrinfo

- IPv4 TCP and UDP client and server C socket programming example programs in SYS$COMMON:[SYSHLP.EXAMPLES.TCPIP] have been ported to IPv6.
- The IPv6 example database and configuration files in SYS$COMMON:[SYSHLP.EXAMPLES.TCPIP.IPV6.BIND] have been updated to reflect current practice

failSAFE and PWIP Support for IPv6

- failSAFE IP has been upgraded to support IPv6
- failSAFE IP enhancements
  - failSAFE IP Phantom Failures
  - Change of the Location for the failSAFE IP Log File
  - SHOW INTERFACE Command Does Not Display Pseudointerface Addresses
- PWIP driver has been upgraded to operate in an IPv6 environment.
  - PWIP driver is used by DECnet, PATHWORKS
- Work on the DECnet side has started, please refer to the DECnet-Plus schedule

NTP V4.2

- Upgrade to NTP V4.2 from University of Delaware
- Support for NTP V1 has been removed because of security vulnerabilities
- Supports authentication using symmetric key cryptography
- Support for IPv6
  - Both IPv4 and IPv6 can be used at the same time
  - Versions of NTPDC provided prior to this release of TCP/IP Services are not IPv6-capable and will only show IPv4 associations
  - Versions of NTPQ provided prior to this release of TCP/IP Services are not IPv6-capable and will show 0.0.0.0 for IPv6 associations
  - NTPTRACE utility has not been updated to NTP Version 4.2.0 and works with the IPv4 address family only

TCPDUMP and libpcap

- TCPDUMP has been upgraded to V3.8.2
- For more information about the changes in the new version of TCPDUMP, see the www.tcpdump.org web site
- libpcap API is provided for Early Adopters
  - An example program is included in the directory pointed to by the logical name TCPIP$LIBPCAP_EXAMPLES
  - The libpcap object library resides in the directory pointed to by the logical name TCPIP$LIBPCAP
    - The directory pointed to by the logical name SYS$SHARE contains an executable file

NFS Server
Case-Sensitive Lookups

- The management ADD EXPORT command has two new options, CASE_BLIND and CASE_SENSITIVE
  - CASE_SENSITIVE enables UNIX-like case sensitivity for NFS server file lookups.
    - For example, NFS would preserve the case in the file names AaBBc.TXT and AABBC.TXT, regarding them as two different files
  - For UNIX clients lookup case-sensitivity is determined by the current ADD EXPORT/OPTION
  - For OpenVMS-to-OpenVMS mode
    - If running TCP/IP v5.5 or later, lookup case-sensitivity is determined by the OpenVMS DCL SET PROCESS/CASE_LOOKUP setting
    - If older version lookup case-sensitivity is determined by the setting of the ADD EXPORT/OPTIONS

TCP/IP kernel

- Scalable Kernel, which was optional in V5.4, now replaces the standard kernel
- The logical name TCPIP$STARTUP_CPU_IMAGES, which was used to select the alternate Symmetric MultiProcessing (SMP) images, is now ignored
  - Remove the local definition of that logical name

Configuration - Join an OpenVMS Cluster as a TCP/IP Host

- TCP/IP Services Version 5.5 creates OpenVMS accounts using larger system parameter values than in previous versions
  - These values are useful on OpenVMS Alpha systems but essential on OpenVMS I64 systems
- To join an OpenVMS Cluster as a TCP/IP host it is strongly suggested that you add the system to the cluster before you configure TCP/IP Services
  - If you configure TCP/IP Services before you add the system to a cluster, when you add the system to the cluster the owning UIC for each of the TCP/IP service SYS$LOGIN directories may be incorrect
- If TCP/IP Services has previously been installed on the cluster and you encounter problems running a TCP/IP component on the system, modify SYSUAF to raise the parameter values for the account used by the affected component

TCP/IP V5.6 for OpenVMS 8.3 proposed features

BIND 9 Resolver and Server

- BIND 9.3.1 for Resolver and server
  - Resolver in TCPIP V5.5 was based on BIND 8
  - Server in TCPIP V5.5 was based on BIND 9.2.1
- BIND Resolver
  - lookups over IPv6
  - New ASCII configuration file (supplements existing one)
  - Improved thread support in getaddrinfo()/getnameinfo()
- BIND Server
  - Includes critical updates to DNSSEC (signed zones)
  - Aligns DNSSEC with current RFCs and industry practice

NFS Client TCP Support

- NFS client TCP support
  - Important for WAN access
  - Offers robust flow control and retransmission behavior
  - Friendly to tunneling and port forwarding

NFS Symlink (symbolic link) Support

- Symbolic links are files that contain a link to another file or directory. When accessed the target file is accessed and deletion of the link has no effect on target file. Links can span disks and can span systems with NFS support
- Requires changes in CRTL, RMS and NFS
- NFS server must be able to create and recognize links
- NFS client must properly create, detect and follow links
- Will be included in symlink SDK

NTP Security Update

- Enable NTP 4.2 Autokey cryptography which will require use of SSL

SSH PKI Support and Upgrade with Kerberos Support

- Enable support for X.509 certificates
  - PKI is an alternative to SSH public keys or Kerberos
  - Also has provision to fetch certificates via LDAP
- Kerberos support will be enabled for V5.6
- DCL Help for SSH Commands

TELNET Server Device Limit

- OpenVMS now supports large unit numbers
- Previous version of TCPIP V5.5 allowed units beyond 9999 for BG devices
- For V5.6, we will add this support for TN devices

IPv6 Compliance

- IPv6 Phase II Logo testing at UNH IOL
- Note: Logo will be tested separately for IPv6 Phase II Logo

IPv6 Support for LPD and TELNETSYM

- Supports for printing over IPv6
- Note: HP enterprise printers are being released with IPv6 support
  - They have even done Phase II Logo testing
  - IPsec support is being added to printer firmware

Updated TCPIP$CONFIG (failSAFE IP)

- Existing TCPIP$CONFIG.COM used outdated notion of cluster interfaces and one IP address per interface
- Update provides failSAFE IP support
- Also allows configuration of multiple addresses
- Simplifies common task of changing name or address
- Pseudo-interfaces continue to be stored internally

TCP/IP – Kernel Roadmap

- Enhancements to Kernel Scalability and Performance
- Quality improvements
- Keep up with network standards TCP/IP, IPv6
- failSAFE IP Multicast
- IPsec Interceptor
- Defer Mobile IP support
  - Keep eyes on industry and deliver as required
- Track SCTP industry direction
  - Modify roadmap as required
- Support new IO technology products such as 10GigE and iSCSI
- BCS Network Strategy
- Track new network offload technologies
  - TOE, RDMA, security…etc.
- OTHER?
  - Next Generation Telco Protocols
  - IP QoS Multimedia
  - IPv6 Routing (GateD v9)
  - DHCPv6
  - Further tcpdump and libpcap improvements

TCP/IP – Security Roadmap

- Quality improvements
- CERT compliance
- IPSEC enhancements and maintenance
- IKEv2
- SSH enhancements and maintenance
- Support SSL upgrades
- Support Kerberos upgrade
- Kerberos authentication support for SSH
- FTP Kerberos support
- Further performance improvements
- Packetfilter and IPfilter support
- BCS Security strategy
- OTHER?

TCP/IP – NFS Roadmap

- NFS quality and performance enhancements
- Track NFS requirements to ensure seamless connections with HP-UX and LINUX
- OTHERS?
  - Multifile version support
  - NFS over IPv6
  - RDMA for NFS
  - NFS v3 client
  - NFS v4 server and client

TCP/IP – Management Roadmap

- IOCTLs
- IPSEC management ala HP-UX
- Track OpenView/OpenVMS integration
- OTHER?
  - SNMP/MIBs
  - SNMPv3
  - Integrated IPSEC configuration tool
  - Integrated IPv6 configuration tool
  - Usability improvements
  - Enhancements to TCPIP C L I
  - Health-Check procedures

TCP/IP – Application Roadmap

- Keep BIND server and Resolver current with releases from ISC
- FTP performance improvements
- OTHERS?
  - SMTP Anti-spam enhancements
  - SMTP persistent server performance enhancements
  - Any additional TCP/IP application IPv6 enablement
  - DNS/BIND server support for dynamic updates with multiple masters
  - Callable FTP and Callable Telnet
  - Long list of Customer Requests

- Note: Available unsupported VMS port of Spamassassin
  - Kit available to send email to majordomo@vms.zko.hp.com. In the body say:

    get vms-spama [.2_55_T2]SPAMA_README.TXT

    get vms-spama [.2_55_T2]SPAMA_ZIP.UUENCODED get vms-spama [.PIPE_MAILSHR.V2_0]PIPE_MAILSHR_KIT_README.TXT

    get vms-spama [.PIPE_MAILSHR.V2_0]PIPE_MAILSHR_V2_0_ZIP_AXPEXE.UUENCODED