hp TCP/IP Services for OpenVMS Technical Update and Strategy

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

October 2006

Agenda

- Support Matrix
- Current TCP/IP Services V5.4/V5.5 ECO Levels
- Focus on Quality Improvements
- New Features in TCP/IP Services V5.6
- IPSEC overview
- High Availability overview
- TCP/IP Services Strategy and Proposed Roadmap

Supported Versions & ECO's

OpenVMS VAX V7.3	TCPIP V5.3 ECO 4
OpenVMS Alpha V7.3-2	TCPIP V5.4 ECO 6
OpenVMS Alpha V8.2 OpenVMS Integrity V8.2-1	TCPIP V5.5 ECO 1 or TCPIP V5.6
OpenVMS V8.3 (Alpha and Integrity)	TCPIP V5.6 (TCPIP V5.5 unsupported)

TCP/IP Services ECO kits

TCP/IP V5.4 ECO 6 & V5.5 ECO 1

- TCP/IP V5.4 ECO 6 shipped in August ’06
  - Contains over 100 fixes across many components

- TCP/IP V5.5 ECO 1 shipped in October ’05
  - ECO 2 expected by H1 ’07

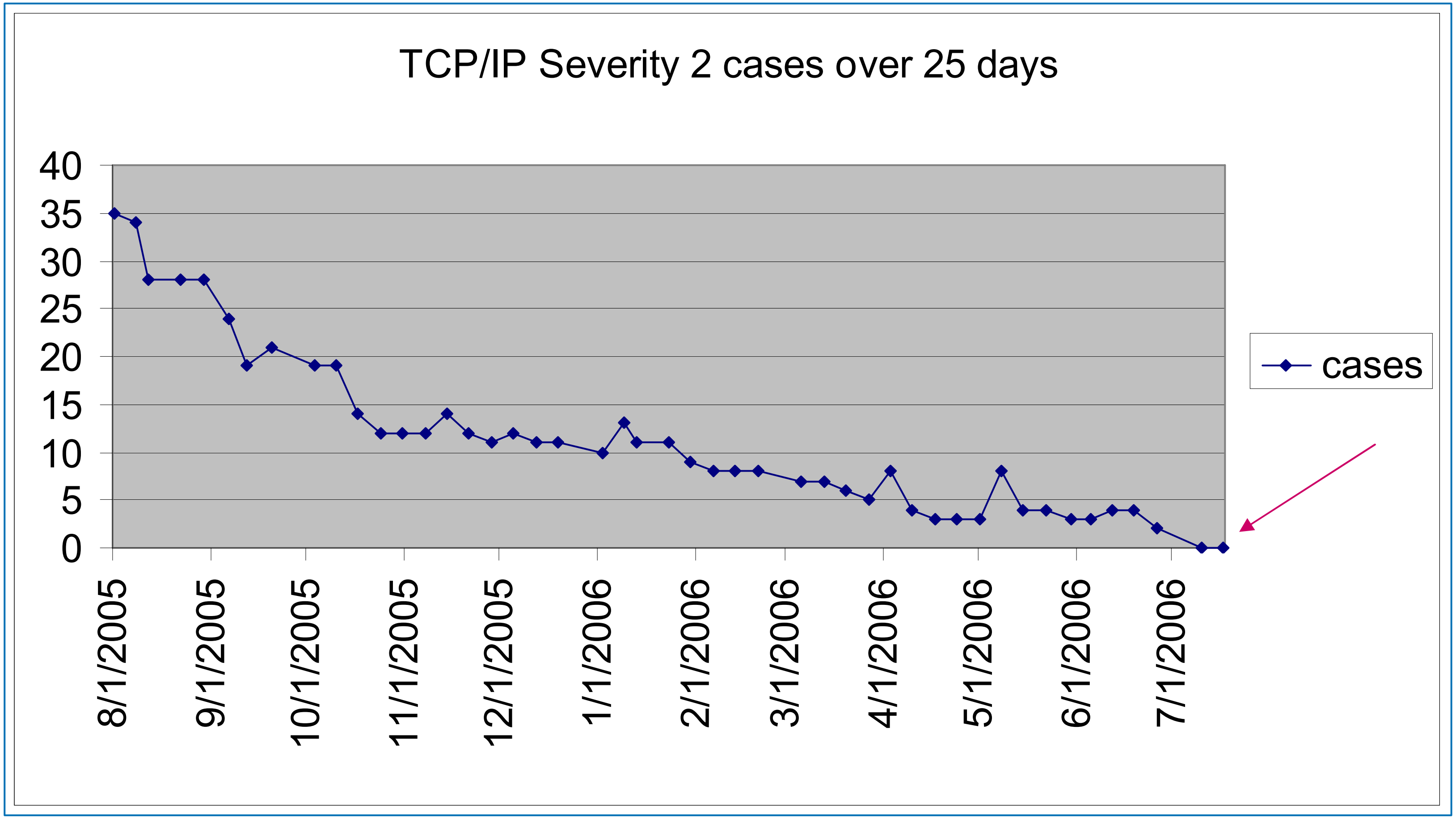
- New version of SSH introduced in V5.4 ECO 5 and V5.5
  - Security fixes, IPv6 support, and more
  - SSH Configuration files must be updated

NOTE: Please review release notes prior to upgrade

Focus on Quality Improvements

- SWAT team
- Areas of prime focus - NFS, SSH, Kernel
- Solved 188 customer cases over the past 12 months
- Eliminated the backlog of major severity customer cases
- Enhanced test suite
- Favorable feedback from customers and field
- Continue to place high priority on quality

TCP/ IP Backlog – Major Severity



TCP/IP Services V5.6

TCP/IP Version 5.6

- Shipped with OpenVMS 8.3
- OpenVMS Alpha and Integrity
- NFS server returns on Integrity
- NFS client TCP transport
- DNS/BIND 9 resolver and v9.3 server
- DNSsec
- NFS symbolic links
- NTP security update including SSL, AutoKey
- SMTP multi-domain zone
- SSH upgrade with Kerberos
- IPv6 support for printing
- FTP performance boost for VMS Plus
- Updates to TCPIP$CONFIG (Interface menu)
- Improved management utilities (such as ifconfig)
- PPP serial-line support returns

Please read the V5.6 release notes for FULL details

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() and getnameinfo()
- BIND server
  - Includes critical updates to DNSSEC (signed zones)
  - Aligns DNSSEC with current RFCs and industry practice

NFS Client TCP Support

- TCP transport for NFS (previously server-only)
  - Important for WAN access (mounting file systems)
  - Offers robust flow control and retransmission behavior
  - Friendly to tunneling and port forwarding

NFS Symlink (symbolic link) Support

- A symbolic link is simply a link to another file
- When accessed, the target file is used automatically
- Deletion of the link has no effect on target file
- Links can span disks and even 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
- Shipped with OpenVMS V8.3
    - More updates and refinements already underway

NTP Security Update

- Security updates from University of Delaware (UDel) NTPv4 (Version 4.2.0)
- NTP 4.2 AutoKey cryptography, using SSL
  - AutoKey is based on public key cryptography
  - Provides for secure server authentication, packet integrity, resistance against clogging and replay attacks, spoofing, and protection against masquerade.
  - Uses the OpenSSL crypto library
  - Detailed configuration steps in an Appendix of the Release Notes
  - Existing private key mechanism with MD5 remains available

SSH Upgrade with Kerberos Support

- Kerberos support is enabled for V5.6
  - Password Authentication mode
  - Checks Kerberos for password before the SYSUAF
- DCL help for SSH commands
- SFTP/SCP
  - Improved support for additional VMS file types
    - Most popular structures are now supported
    - No support yet for RMS Indexed files
      - (You can encapsulate them in a saveset or ZIP file)

TELNET Server Device Limit

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

IPv6 Support for LPD and TELNETSYM

- Allows printer communication to use IPv6
- Needed for deployment of a mostly-IPv6 network

- Note: HP enterprise printers now support IPv6

Updated TCPIP$CONFIG (Interface Menu)

- Previous TCPIP$CONFIG.COM used outdated notion of cluster interfaces and one IP address per interface
- Improved configuration of multiple addresses
- Simplifies common task of changing IP address and/or hostname
- Additional information displayed to the user
- Manages both permanent database and active system
- Pseudo-interfaces continue to be stored internally

New Look of Interface & Address Menu

```
HP TCP/IP Services for OpenVMS Interface & Address Configuration Menu

Hostname Details:   Configured hostname=gryffindor-e0,  Active=gryffindor-e0

Configuration options:

  1  -  WE0 Menu (EWA0: Multimode 1000mbps)
  2  -  10.0.0.1/16      gryffindor-g0         Configured,Active

  3  -  BE0 Menu (EBA0: Unspecified 30000mbps)
  4  -  1.2.3.4/8        *noname*              Configured,Active

  5  -  IE0 Menu (EIA0: TwistedPair 100mbps)
  6  -  10.1.1.10/23     gryffindor-e0         Configured,Active

  7  -  IE1 Menu (EIB0: TwistedPair 100mbps)
  8  -  10.1.1.11/23     gryffindor-e1         Configured,Active
  9  -  10.1.1.10/23     gryffindor-e0         Configured,Active-Standby

  I  -  Information about your configuration

 [E] -  Exit menu
```

Interface Menu

```
HP TCP/IP Services for OpenVMS Interface WE0 Configuration Menu
Configuration options:

        1  - Add a primary address on WE0
        2  - Add an alias address on WE0
        3  - Enable DHCP client to manage address on WE0

       [E] - Exit menu

Enter configuration option:
```

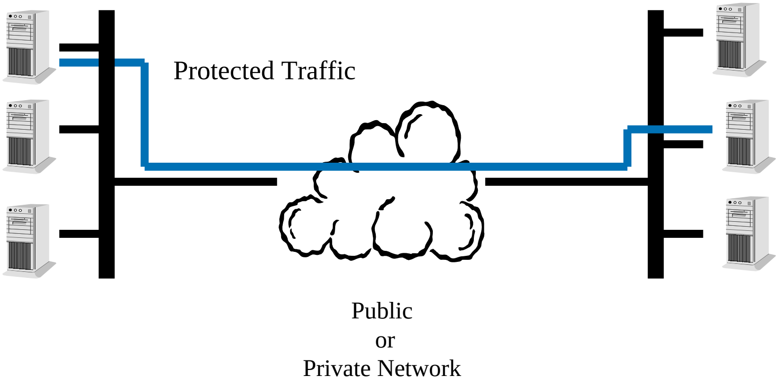
Address Menu

```
HP TCP/IP Services for OpenVMS Address Configuration Menu

     WE0 10.0.0.1/16 gryffindor-g0 Configured,Active WE0

Configuration options:

        1  - Change address
        2  - Set “gryffindor-e0” as the default hostname
        3  - Delete from configuration database
        4  - Remove from live system
        5  - Add standby aliases to config database (for failSAFE IP)

       [E] - Exit menu

Enter configuration option:
```

What is IPsec?

- Set of protocols developed by the IETF
- Provides security at the IP layer
- Strong security that can be applied to all traffic
- Transparent to applications and end users
  - No need to train users on security mechanisms
- Protects all upper layer protocols
- Secures traffic between any two IP systems
  - Can be used end-to-end, router-to-router, or host-to-router
- Extensions to the IP protocol suite
  - Applies to IPv4 and IPv6
- Encryption and Authentication
- Key management and Security Association creation and management

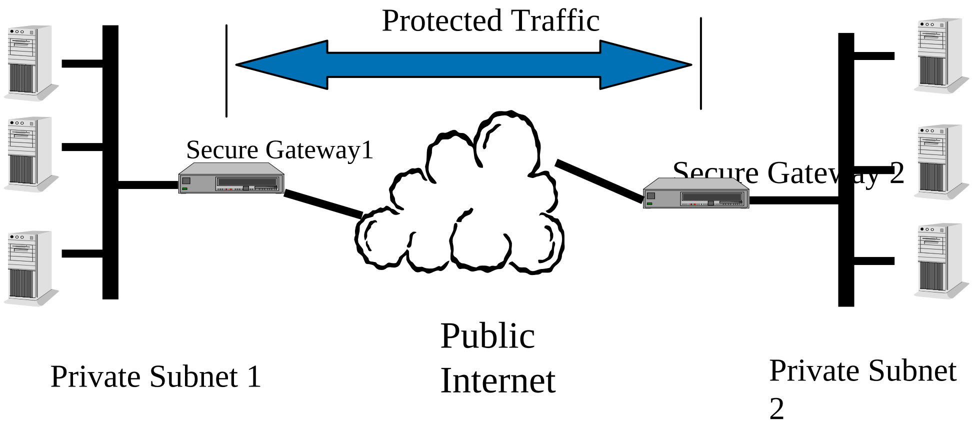
IPsec Security



Protected Traffic

Public
or
Private Network

IPsec for Host-to-Host



Protected Traffic

Secure Gateway1

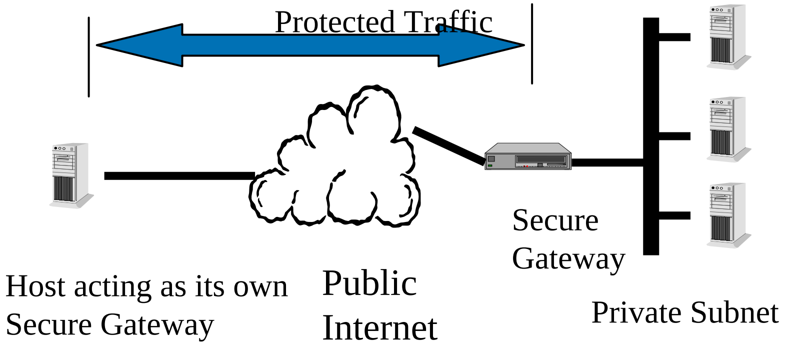
Secure Gateway 2

Private Subnet 1

Public
Internet

Private Subnet
2

IPsec for Virtual Private Networks



Protected Traffic

Host acting as its own
Secure Gateway

Public
Internet

Secure
Gateway

Private Subnet

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

High Availability

- **failSAFE IP**
  - failSAFE service needs to be enabled
  - Interface configured on all nodes
  - Moves an IP address to a different interface within a VMScluster upon detecting a link failure (ie. NIC, switch, software)
- **LAN Failover** (LLDRVER)
  - Multiple interfaces form a LAN failover set
  - One is active while the others remain idle (standby)
  - Operates at the LAN layer, pairing two or more adapters on the same node and the same LAN so as to quickly and automatically select a working one
- **Load Broker and Metric Daemon**
  - Protection and Load Sharing for the DNS Alias
  - Provides load balancing at the hostname-to-address level, returning addresses of cluster members that are up and least heavily loaded at the time of a query

LAN Failover and failSAFE IP

Feature	LAN Failover	failSAFE IP
Interface Usage	One active interface, others are standby	All interfaces active, load balancing & sharing
Devices Supported	DEGXA, DEGPA, DE600, DE500-BA, All integrity devices	Independent of device types
Protocols	LAN client protocols	IP client protocols
Failover Time	Typically milliseconds	Typically a few seconds
Complexity	Simple	Simple to Moderate

failSAFE IP can operate over LL driver – so you get combination of features

TCP/IP Services Strategy and Roadmap

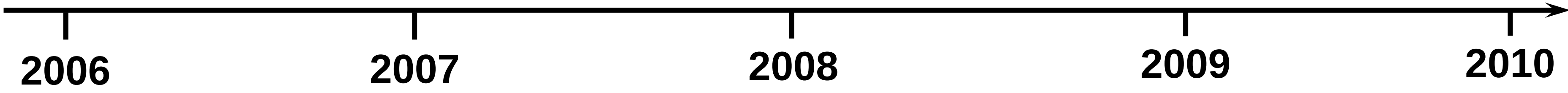
TCP/ IP Strategy

- 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 is important and key TCP/IP applications
- Improve scalability in complex environments with more and faster CPU's
- Support critical emerging network related technology as required
- Provide network functionality that meets our customers requirements
- 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.
- Internet Systems Consortium (ISC) BIND
- SSL
- Kerberos
- HP-UX TCP/IP applications

TCP/IP Services for OpenVMS - Proposed



TCP/IP V5.6 August 2006 - 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 update
- Improved Mgt utilities (ifconfig)

TCP/IP (Next)

- *Continued focus on* Networking enhancements to support interoperability, connectivity, discovery, and security
-IPSec
-Clusters over IP
-Packet Processing Engine (PPE) for more scaling
-NFS enhancements
-FTP enhancements
-LPD port configurability

IPsec EAK available post OpenVMS V8.3 & TCP/IP V5.6

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 this TCP/IP presentation

TCP/IP Services V5.5

TCP/IP V5.5 with OpenVMS V8.2 (shipped January 2005)

- Both Alpha and Integrity
- SSH upgrade to version 3.2
- Secure IMAP (SSL)
- IPv6 updates and enhancements
- failSAFE IP and PWIP 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

- Lacked NFS server on Integrity and PPP support

SSH

- 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

- Maximum file size for SSH file copy operations has been increased from 4 megabytes to 4 gigabytes. The speed of file transfers was improved 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
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 no SSL software is installed, IMAP runs in non-SSL mode
  - OpenVMS 8.3 shipped with SSL
- SSL startup procedure should run before TCPIP$STARTUP.COM
- The secure IMAP configuration is controlled by the configuration file SYS$SYSDEVICE:[TCPIP$IMAP]TCPIP$IMAP.CONF

IPv6 Updates and Enhancements (1 of 2)

- 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 updated to RFC 3152 and can send dynamic updates for the forward and 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 of 2)

- Several programming functions provided in earlier Early Adopter Kits (EAKs) were deprecated. These functions are no longer 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$COMMON:[SYSHLP.EXAMPLES.TCPIP] were ported to IPv6.
- The IPv6 example database and configuration files in SYS$COMMON:[SYSHLP.EXAMPLES.TCPIP.IPV6.BIND] were updated to reflect current practice

failSAFE and PWIP Support for IPv6

- failSAFE IP was upgraded to support IPv6
- failSAFE IP enhancements
  - Avoiding failSAFE IP phantom failures
  - 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

failSAFE IP (since hp TCP/IP Services for OpenVMS V5.4)

Protecting the IP Address

failSAFE IP Features

- failSAFE IP
    - Failover of IP addresses and static routes across interfaces
    - Removes interface as SPOF
- Configuration Requirements
    - Address configured across multiple interfaces (within a node or across a cluster)
        - Only one instance of the address is active, others are standby
    - failSAFE service enabled (monitors health of interfaces)
  - Failures Detected (if service enabled)
    - Interface’s Bytes Received counter stops changing
        - Cable disconnect, interface failure, switch failure, etc.

failSAFE IP – Failure and Recovery

- Upon interface failure
  - IP address and static routes on failed interface are removed
  - Standby IP address becomes active
  - Static routes created on any interface where the route is reachable
  - Existing connections are seamlessly maintained if failover to interface on same node
  - IP addresses preferentially failover to an interface on the same node in an effort to maintain existing connections
- Upon interface Recovery
  - IP addresses may be returned to the *home* interface
  - IP addresses will not return to a home interface if it means connections will be lost

LAN Failover – LLDRIVER

(Added in OpenVMS V7.3-2)

LAN Failover Features

- Multiple interfaces form a LAN Failover Set
- One interface is active others remain idle
- In event of failure, the MAC address migrates to standby interface
- Must be connected on same LAN
- Supports all LAN client protocols
- Support for DEGPA, DEGXA (GbE), DE600, DE500-BA (FastEthernet)
- Failover time is typically milliseconds for link disconnects

LAN Failover Restrictions

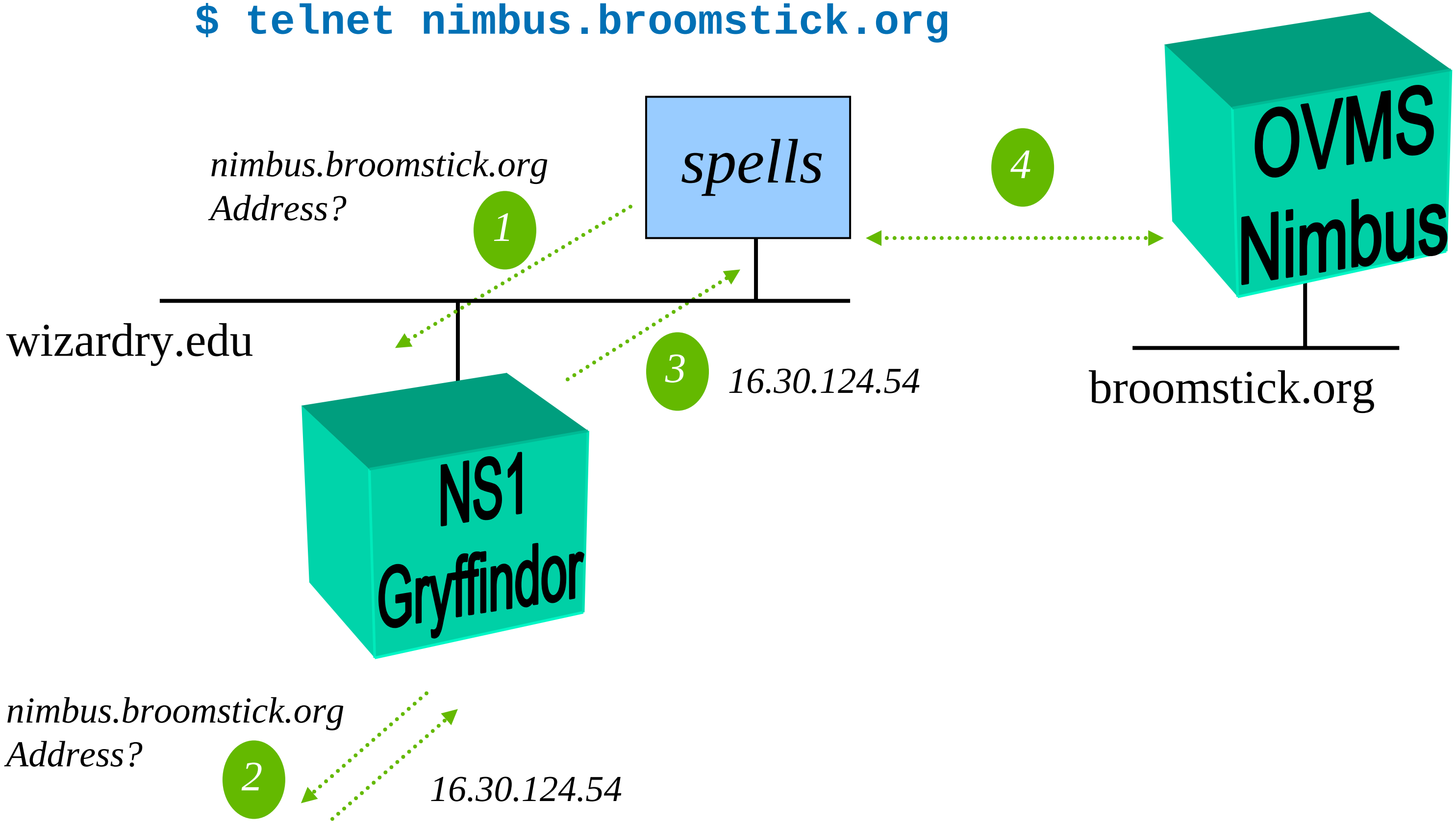
- Standby interfaces cannot be used
- Maximum of 8 interfaces per failover set
- Interfaces cannot be connected point-to-point

DNS/BIND

Name & Address Mapping

DNS/BIND Server

```
$ telnet nimbus.broomstick.org
```



Configuring DNS/BIND

- Configure one Master and multiple Slaves
- TCPIP$CONFIG.COM enables service
  - Creates directory, template & more
    - SYS$SPECIFIC:[TCPIP$BIND]
    - TCPIP$BIND_CONF.TEMPLATE
- Create BIND Databases
  - Convert from old configuration
    - During first time run of TCPIP$CONFIG
    - TCPIP CONVERT /CONFIG BIND
  - TCPIP$BINDSETUP.COM

TCPIP$BIND.CONF (/etc/named.conf)

```
options { directory “sys$specific:[tcpip$bind]”; };
zone “0.0.127.in-addr.arpa” in {
                type master;
                file “127_0_0.DB”;
    };
zone “wizardry.edu” in {
                type master;
    allow-update {130.25.41.85;};
    file “WIZARDRY_EDU.DB”;
    };
zone “25.130.in-addr.arpa” in {
                type master;
                allow-update {130.25.41.85;};
                file “25_130_in-addr_arpa.db”;
    };
zone “.” in {
                type hint;
                file “root.hint”;
    };
```

Load Broker & Metric Server

Protection and Load Sharing for the
DNS Alias

BIND/DNS Load Balancing

- “Load Balancing” comprised of two components
  - Metric server on each cluster member tells Load Broker its “metric” - how busy it is.
    - Algorithm to calculate metric same as LAT
  - Load Broker makes list of IP addresses based on member load
    - Sends dynamic DNS update to name server
- BIND server must support dynamic updates (e.g. DNS/BIND V8.1)

Load Broker Configuration & Operation

```
SYS$SYSDEVICE:[TCPIP$LD_BKR]TCPIP$LBROKER.CONF

cluster “hogwarts.wizardry.edu” {
    dns-ttl          45 ;
    dns-refresh      30 ;
    masters { 130.25.36.1 } ;
    polling-interval 9 ;
    max-members      6 ;
    members {
       130.25.36.1 ;  130.25.36.5 ;
       130.25.36.2 ;  130.25.36.6 ;
       130.25.36.3 ;  130.25.36.7 ;
       130.25.36.4 ;  130.26.37.8 ;    } ;
   failover 130.25.41.85 ;
 } ;
```

SSH since V5.4 ECO 5 & V5.5 ECO 1

- V5.4 ECO 5 and V5.5 ECO 1
  - Improved file transfer speed (sftp server)
  - Support for <CTRL/C> and non-STREAM_LF files
  - 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