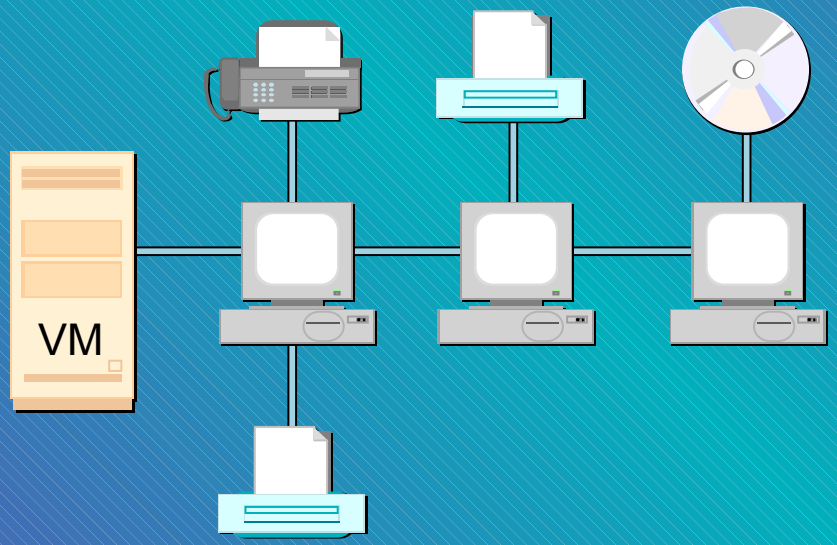
Session 9361 / 9381



VM TCP/IP Advanced Configuration

Alan Altmark
IBM Corporation
Endicott, New York

This presentation provides in-depth information on configuration of the major components of VM TCP/IP FL320.

References to IBM products, programs, or services do not imply that IBM intends to make these available in all countries in which IBM operates. Any reference to an IBM product, program, or service is not intended to state or imply that only IBM's product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe on any of the intellectual property rights of IBM may be used instead. The evaluation and verification of operation in conjunction with other products, except those expressly designed by IBM, are the responsibility of the user.

The following terms are trademarks of the IBM Corporation in the United States or other countries or both: S/390 VM/ESA IBM OS/390

Other company, product, and service names, which may be denoted by double asterisks (**), may be trademarks or service marks of others.

Agenda

- Server configuration architecture review
- Stack configuration
- Application configuration
  - TN3270E
  - FTP
  - SMTP
  - LPR and LPD
  - NFS
  - DNS
- A 2nd TCP/IP stack
- Security
- Common Problems

Defining a Server

- DTCPARMS file

```
:nick.TCPIP     :type.server      :class.stack
                :attach.430-431, 320-321
                :vctc.200 vse 200, 201 vse 201

:nick.FTPSERVE  :type.server      :class.ftp
                :anonymous.yes
                :ESM_Enable.yes

:nick.FTPSERVA  :type.server      :class.ftp
                :anonymous.yes
                :ESM_Enable.yes
```

- *userid*, *nodeid*, SYSTEM

Server Startup Parameters

- Server profile exits
  - Global exit called for all servers, TCPRUNXT EXEC
  - Server-specific exit called via :Exit. tag
  - Returns tags
  - Think of it as a dynamic DTCPARMS file

```
arg calltype class .
select
  when calltype = "SETUP" & class = "NFS" then
   return ":ESM_Enable.YES"
  when calltype = "SETUP" & class = "FTP" then
   return ":ESM_Enable.YES"
end
```

Some Things to Configure

- Stack
- TN3270E
- FTP
- LPR/LPD
- SMTP
- NFS
- Caching DNS server
- A second TCP/IP stack

Stack Basics

- Control block pool sizes
  - Only defines initial size - expansion is dynamic
  - Stack will complain when pool is expanded
  - Watch via NETSTAT POOL
- **Link** and **Device** statements
  - Use the correct port number on the LINK statement
  - OSA has unit address 00-03 unless changed by OSA/SF
  - Don't forget a START statement
- **SysContact** and **SysLocation** used by SNMP

Stack Basics

- **Home** statement defines IP address on each link
  - Be careful about using same IP address on different links
  - Put connected systems in a different subnet
- **Autolog** statement defines servers to start
- **Port** statement gives permission to listen on a low port
  - Listed ports are monitored unless NOAUTOLOG specified
- **AssortedParms**
  - Look at possible settings and decide what works for you
  - Security is affected
  - Variable subnetting and virtual IP addressing controls

Routing

- **Gateway** statement used for static routing
- **BsdRoutingParms** statement used for dynamic routing
  - **Gateway** statement is ignored
  - Use **ETC GATEWAYS** file to add static routes
  - RouteD server needed
  - Can use RIPv1 or RIPv2
  - Virtual IP Addressing (VIPA)
  - VM can broadcast routes for attached guests

Static TN3270e

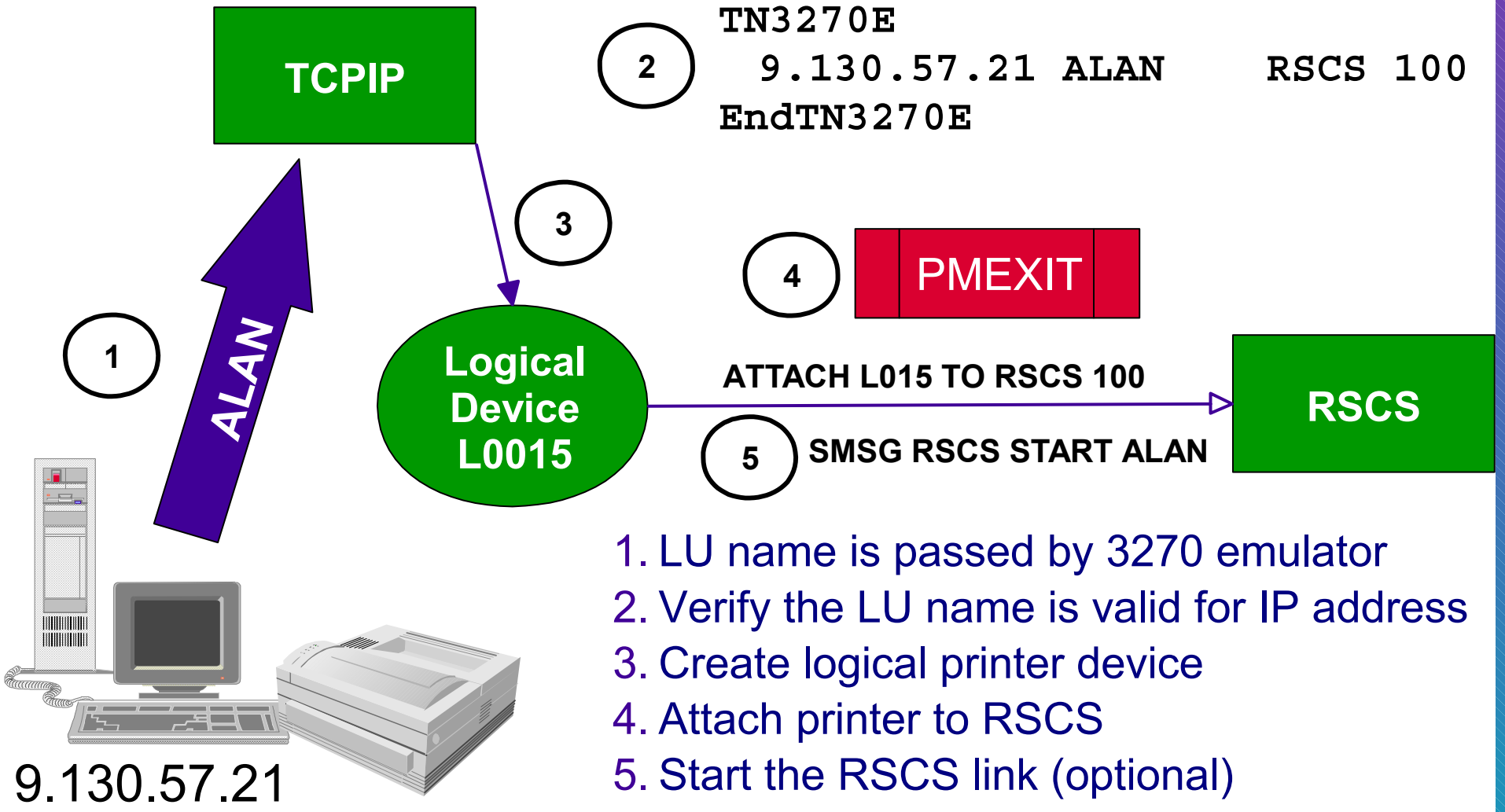
- Define RSCS TN3270E link named **ALAN**
- Update PROFILE TCPIP

```
AssortedParms
   TN3270Eexit PMEXIT
EndAssortedParms

TN3270E
   9.130.57.21 ALAN    RSCS 100
EndTN3270E
```

- Use link name "ALAN" as LU Name in emulator printer configuration

Static TN3270e



1. LU name is passed by 3270 emulator
2. Verify the LU name is valid for IP address
3. Create logical printer device
4. Attach printer to RSCS
5. Start the RSCS link (optional)

Dynamic TN3270e

- Same as for Static TN3270e, except:
  - PMEXIT will not receive target user ID and virtual address
  - Any restriction on IP address-LU name pairs must be implemented by PMEXIT
  - **TN3270E** stanza in PROFILE TCPIP not required
  - Update PMEXIT to scan RSCS config file to locate LINKDEFINE entry with matching LU name and attach ldev to RSCS using found address

FTP Server

- **FTP BANNER** displayed to all clients

```
**********************************
* Hello.  Welcome to my world.   *
* Don't abuse my system. Or else. *
**********************************
```

- **CHKIPADR EXEC** called after client login
  - knows user ID and IP address
  - places directives in program stack
  - initial directory

```
queue 'VMSYSU:'userid'.'
or  queue userid'.191'
```

  - personal banner

```
queue 'BANNER' userid
```

LPD Server

- Use RSCS instead of LPSERVE for LPD
  - no charge
  - LPD link handles many clients
  - Print destination determined by client-specified queue name
    - *userid@nodeid*
    - *linkname*
    - Can be overridden by LPD CONFIG file

- **RSCSTCP CONFIG**

```
LinkDefine LPD type LPD
Parm LPD exit=LPDXMANY
*
LinkDefine LPD2 type LPD
Parm LPD2 exit=LPDXMANY eparm='config=LPD'
```

LPR using RSCS

- Use RSCS to provide asynchronous delivery
  - VM-based print server
  - LPD can redirect to LPR
  - LPR my file a (printer lpt1 host alan.endicott.ibm.com **async**

- **RSCSTCP CONFIG**

```
LinkDefine LPR type LPR ast form *
Parm LPR exit=LPRXONE ito=0 user=yes
*
LinkDefine LPRP type LPR ast form *
Parm LPRP exit=LPRXPSE ito=0 user=yes
```

SMTP Server

- SMTP CONFIG
  - Watch out for DNS that resolves addresses outside of your firewall
  - SMTP will forward mail to **IpMailerAddress** if and only if the domain name cannot be resolved via DNS.
  - Consider private DNS
  - Eliminating DNS means all mail is forwarded to IpMailerAddress

SMTP Server

- SMTP CONFIG
  - May need own TCPIP DATA on another disk
    - Have server exit copy TCPIP DATA from 198 to 191, making the needed changes at each startup
  - Enable **VerifyClient** to ensure identity of network clients
    - Can use exit instead if desired
  - Don't use STANDARD translation table

NFS Server

- VMNFS CONFIG
  - Export - Makes mounting file systems easier for clients

```
export   Your_191   %userid.191,rw,Lines=ext,Trans=ext
export   home       %fsroot%iwdir,rw,Lines=ext,Trans=ext
export   SFS        VMSYSU:%userid.,rw,Lines=ext,Trans=ext
```

    - Client sees exported name, server generates mount string
    - %userid, %fsroot, and %iwdir are substituted based on authentication data and corresponding CP directory entry
  - VMfiletype - defines translation options

```
VMfiletype   *BIN     translate=no   lines=none
```

Caching-only DNS server

- Always run DNS server on VM
  - Improves performance by caching name lookups
  - Easy to do
- NSMAIN DATA

```
CachingOnly MYCACHE DNSINFO
NegativeCaching
```

- MYCACH DNSINFO

```
.                          86400   IN  NS   maindns.company.com
maindns.company.com        86400   IN  A    10.26.43.1
```

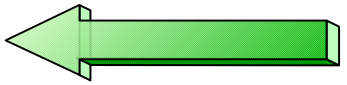
- TCPIP DATA

```
NSINTERADDR   127.0.0.1
```

A Second TCP/IP Stack

- PROFILE TCPIP in 1st stack (TCPIP) with dynamic routing

```
DEVICE   IUCVDEV IUCV 0 0 TCPIP2 A
LINK     TO-SECONDARY IUCV 0 IUCVDEV
HOME
    :
    10.0.0.1      TO-SECONDARY
BsdRoutingParms true
    :
    TO-SECONDARY   4096    0   255.0.0.0   10.0.0.2
START IUCVDEV
```



Note "A"

- ETC GATEWAYS
  - broadcasts route to 2nd stack

```
host 10.0.0.2 gateway = metric 1 permanent
```

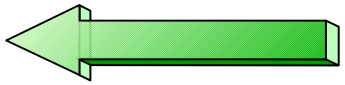
A Second TCP/IP Stack

- PROFILE TCPIP in 2nd stack (TCPIP2) with static routing

```
DEVICE   IUCVDEV IUCV 0 0 TCPIP B
LINK     TO-PRIMARY IUCV 0 IUCVDEV
HOME
    10.0.0.2   TO-PRIMARY

GATEWAY
    10.0.0.1    =           TO-PRIMARY   4096 HOST
    defaultnet 10.0.0.1     TO-PRIMARY   4096 0

START IUCVDEV
```



Note "B"

A Second TCP/IP Stack

- DTCPARMS file

```
:nick.TCPIP2       :type.server      :class.stack

:nick.FTPSERV2     :type.server      :class.ftp
                   :stack.TCPIP2
                   :anonymous.yes
                   :ESM_Enable.yes
```

- :Stack. tag prevents warning message
  - value is compared to TCPIPUSERID in TCPIP DATA
- TCPIP DATA
  - `TCPIPUSERID TCPIP2`

Translation Tables

- Over 200 translations to choose from
  - The one to choose depends on code page used on VM and on client
- TCPXLBIN files on TCPMAINT 592
  - A few file names:. 10470819, 09240923, 00371252
- FTP and NFS clients may select the translation to be used
  - `quote site xlate 10470819`
  - `mount /usr/alan vmtest.ibm.com:alan.191,xlate=10470819`
- Other clients will use default translation selected by you

Translation Tables

- Clients and servers have a default, *preferred*, translation table
  - Name is different for each client and server
- If preferred table not found, STANDARD is loaded
  - Consider replacing STANDARD with your preferred table
  - Don't use STANDARD
  - Don't ignore the euro - it affects the United States, too!
- SMTP server uses two translation tables
  1. mail supposedly restricted to standard 7-bit ASCII characters
  2. mail that indicates it contains 8-bit MIME encodings
  - Suggestion: Make both tables the same

Translation Tables

- Non-reversible 7-bit ASCII (0x00-0x7F only!) is the default, a.k.a STANDARD
- See **http://www.ibm.com/vm/euro** for a complete discussion of code pages
- See "Using Translation Tables" on page 505 of the TCP/IP FL320 Planning and Administration guide

Security

- **AssortedParms**
  - **RestrictLowPorts** - Control use of well-known ports
  - **PermittedUsersOnly** - Control access to stack by VM users
  - **IgnoreRedirect** - Do not permit hosts to tell you to use a different router
- **Obey** list
  - Can issue privileged server functions
  - Can issue privileged NETSTAT commands, including CP
  - Can create own IP packets ("raw")
  - Can issue TRACERTE command (uses raw sockets!)

Security

- SMTP server exits
  - What to do when IP address and domain name don't match
  - Whether or not to act as a mail relay
  - Protocol monitor and control
  - Sample calls Rexx exec
- FTP server exits
  - Auditing, logging, or accounting
  - Protocol monitor and control
  - Limit user access (e.g. CD, PUT, GET)
  - Sample calls Rexx exec

Security

- Telnet server exits
  - Session Connection Exit (SCEXIT)
    - Limit or audit connections
    - Automatically DIAL a guest
    - Can "hide" VM logo
  - Printer Management Exit (PMEXIT)
    - Controls TN3270E printer setup
  - Samples call Rexx exec (surprise!)

Security

- NFS
  - EXPORTONLY YES - limits mounts to export list
    DUMPMOUNT NO - prevents listing of mounts
  - VMNFSMON EXEC
    Limits what can be mounted and by whom
  - VMNFSMSG EXEC
    Limits who can issue SMSG command
  - VMNFSCMS EXEC
    Enables use of SMSG CMS subcommand

External Security Mangers

- Need :ESM_Enable.YES in DTCPARMS file or exit
- Called by all servers that check passwords
- FTP and NFS servers also verify minidisk permissions
- Check vendor recommendations
  - RACF requirements documented in VM TCP/IP Planning and Administration
- Servers act on behalf of clients, but they are *not* batch machines
  - different security policy

Common Hardware-Related Errors

- Forgot to attach all addresses for a particular adapter
- Wrong device type on DEVICE statement
- Wrong adapter number on LINK statement
  - Identifies which port on a multiport device
  - '0' and '1' on CTC (or cross-couple, instead)
- Adapter configured for full duplex
  - on shared LAN segment
  - when not supported by hub or switch

Common Routing Errors

- Incorrect MTU size in routing configuration statements
  - Consult hardware documentation
  - Cannot be larger than smallest MTU used on LAN segment
- Using Gateway statement with RouteD
  - Need BsdRoutingParms instead
- Wrong subnet masks or values (do the math!)
- Subnet vs. Host
- Trying to put guest in same subnet as VM

Common Problems

- FTP, NFS
  - Not an SFS administrator
  - No ESM authorization to act for users (surrogate)
- Missing ESM or CP authorizations
- Outdated CP directory entry (they change!)
- Sample config files may not be optimal

The #1 Problem: Incorrect TCPIP DATA file

- Copy on user's A-disk
- Copy on server's A-disk
- Copy on TCPMAINT 198
- Incorrect NSINTERADDR value
  - Ignorance of network changes is no excuse! Get in the loop!
- TCPIPUSERID pointing to wrong TCP/IP stack v.m.

Summary

- Create a 2nd stack to play with late at night
- Read the manual and follow instructions
- Read RFCs

Read More About It

- *TCP/IP Planning and Customization*, SC24-5847
- *TCP/IP Solutions for VM/ESA*, SG24-5459
  - IBM redbooks at http://www.redbooks.ibm.com
- IETF RFCs http://www.rfc-editor.org/rfcsearch.html
- *Internetworking with TCP/IP*, Comer,
  Prentice Hall, ISBN 0-13-216987-8
- *TCP/IP Illustrated, Vol. 1*, Stevens,
  Addison Wesley, ISBN 0-201-63346-9

Contact Information

- By e-mail: Alan_Altmark@us.ibm.com
- In person: USA 607.752.6027
- On the Web: http://www.ibm.com/vm/devpages/altmarka
- Mailing lists: IBMTCP-L@vm.marist.edu
  VMESA-L@listserv.uark.edu
- On TalkLink: TCPIP CFORUM