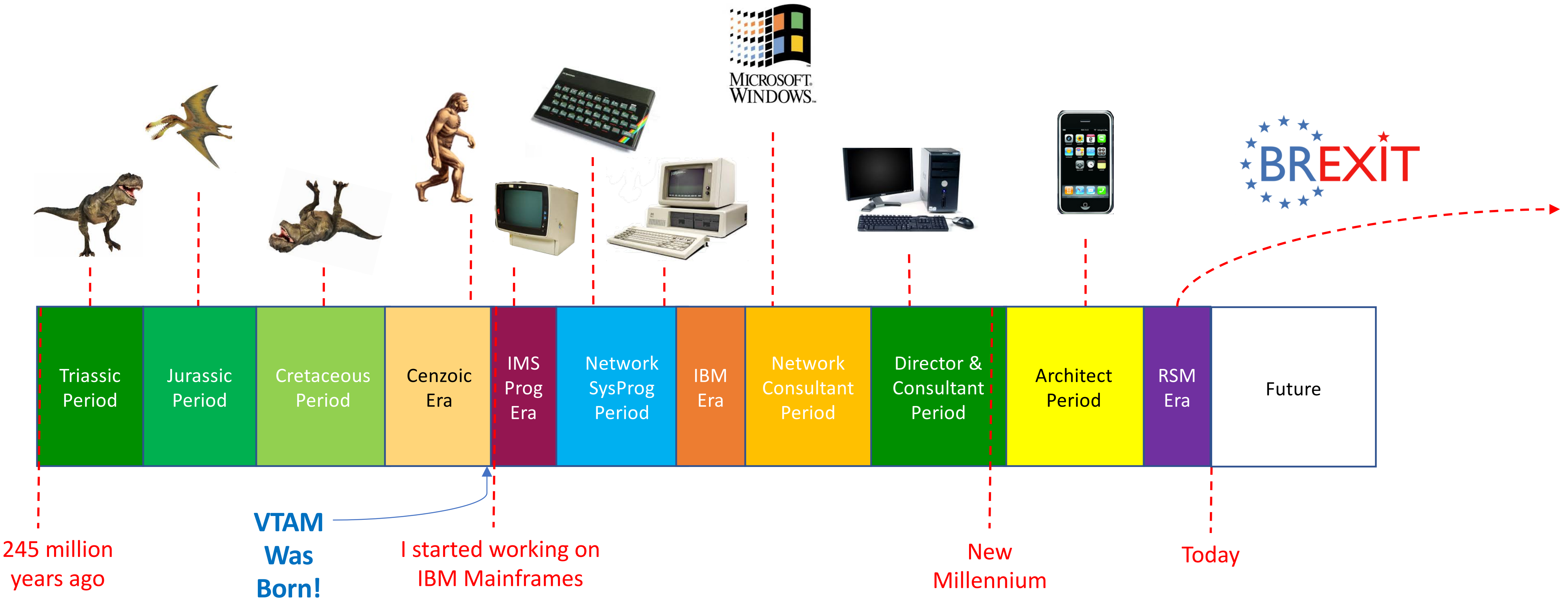
VTAM
Why it is still important

Tony Amies

November 2019

Session EA

Bio timeline



Triassic Period | Jurassic Period | Cretaceous Period | Cenzoic Era | IMS Prog Era | Network SysProg Period | IBM Era | Network Consultant Period | Director & Consultant Period | Architect Period | RSM Era | Future

245 million years ago

VTAM Was Born!

I started working on IBM Mainframes

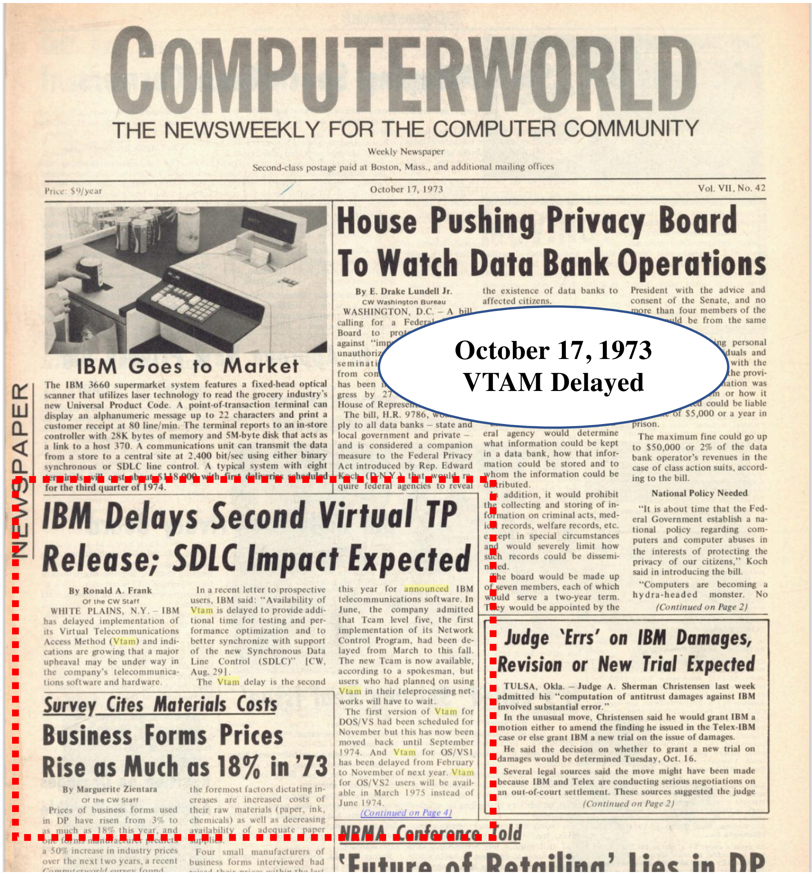
New Millennium

Today

Topics

- VTAM Background
  - What it used to be
- VTAM Today
  - What has changed
  - What is important
- VTAM Security
  - Often overlooked …. but its fully secure. Isn’t it?
- Demo
  - Technology permitting

Anyone remember ?



COMPUTERWORLD

THE NEWSWEEKLY FOR THE COMPUTER COMMUNITY

Weekly Newspaper

Second-class postage paid at Boston, Mass., and additional mailing offices

Price: $9/year October 17, 1973 Vol. VII, No. 42

NEWSPAPER

IBM Goes to Market

The IBM 3660 supermarket system features a fixed-head optical scanner that utilizes laser technology to read the grocery industry's new Universal Product Code. A point-of-transaction terminal can display an alphanumeric message up to 22 characters and print a customer receipt at 80 line/min. The terminal reports to an in-store controller with 28K bytes of memory and 5M-byte disk that acts as a link to a host 370. A communications unit can transmit the data from a store to a central site at 2,400 bit/sec using either binary synchronous or SDLC line control. A typical system with eight terminals will cost about $118,000 with first deliveries scheduled for the third quarter of 1974.

House Pushing Privacy Board To Watch Data Bank Operations

By E. Drake Lundell Jr.
CW Washington Bureau

WASHINGTON, D.C. – A bill calling for a Federal Board to prot against "imp unauthoriz seminati from com has been i gress by 27 House of Represen

The bill, H.R. 9786, wo ply to all data banks – state and local government and private – and is considered a companion measure to the Federal Privacy Act introduced by Rep. Edward Koch (D-N.Y.) that would require federal agencies to reveal the existence of data banks to affected citizens.

eral agency would determine what information could be kept in a data bank, how that information could be stored and to whom the information could be distributed.

In addition, it would prohibit the collecting and storing of information on criminal acts, medical records, welfare records, etc. except in special circumstances and would severely limit how such records could be disseminated.

The board would be made up of seven members, each of which would serve a two-year term. They would be appointed by the President with the advice and consent of the Senate, and no more than four members of the uld be from the same

ing personal duals and with the the provi- nation was m or how it ed could be liable of $5,000 or a year in prison.

The maximum fine could go up to $50,000 or 2% of the data bank operator's revenues in the case of class action suits, according to the bill.

National Policy Needed

"It is about time that the Federal Government establish a national policy regarding computers and computer abuses in the interests of protecting the privacy of our citizens," Koch said in introducing the bill.

"Computers are becoming a hydra-headed monster. No

(Continued on Page 2)

October 17, 1973
VTAM Delayed

IBM Delays Second Virtual TP Release; SDLC Impact Expected

By Ronald A. Frank
Of the CW Staff

WHITE PLAINS, N.Y. – IBM has delayed implementation of its Virtual Telecommunications Access Method (Vtam) and indications are growing that a major upheaval may be under way in the company's telecommunications software and hardware.

In a recent letter to prospective users, IBM said: "Availability of Vtam is delayed to provide additional time for testing and performance optimization and to better synchronize with support of the new Synchronous Data Line Control (SDLC)" [CW, Aug. 29].

The Vtam delay is the second this year for announced IBM telecommunications software. In June, the company admitted that Tcam level five, the first implementation of its Network Control Program, had been delayed from March to this fall. The new Tcam is now available, according to a spokesman, but users who had planned on using Vtam in their teleprocessing networks will have to wait.

The first version of Vtam for DOS/VS had been scheduled for November but this has now been moved back until September 1974. And Vtam for OS/VS1 has been delayed from February to November of next year. Vtam for OS/VS2 users will be available in March 1975 instead of June 1974.

(Continued on Page 4)

Judge 'Errs' on IBM Damages, Revision or New Trial Expected

TULSA, Okla. – Judge A. Sherman Christensen last week admitted his "computation of antitrust damages against IBM involved substantial error."

In the unusual move, Christensen said he would grant IBM a motion either to amend the finding he issued in the Telex-IBM case or else grant IBM a new trial on the issue of damages.

He said the decision on whether to grant a new trial on damages would be determined Tuesday, Oct. 16.

Several legal sources said the move might have been made because IBM and Telex are conducting serious negotiations on an out-of-court settlement. These sources suggested the judge

(Continued on Page 2)

Survey Cites Materials Costs
Business Forms Prices Rise as Much as 18% in '73

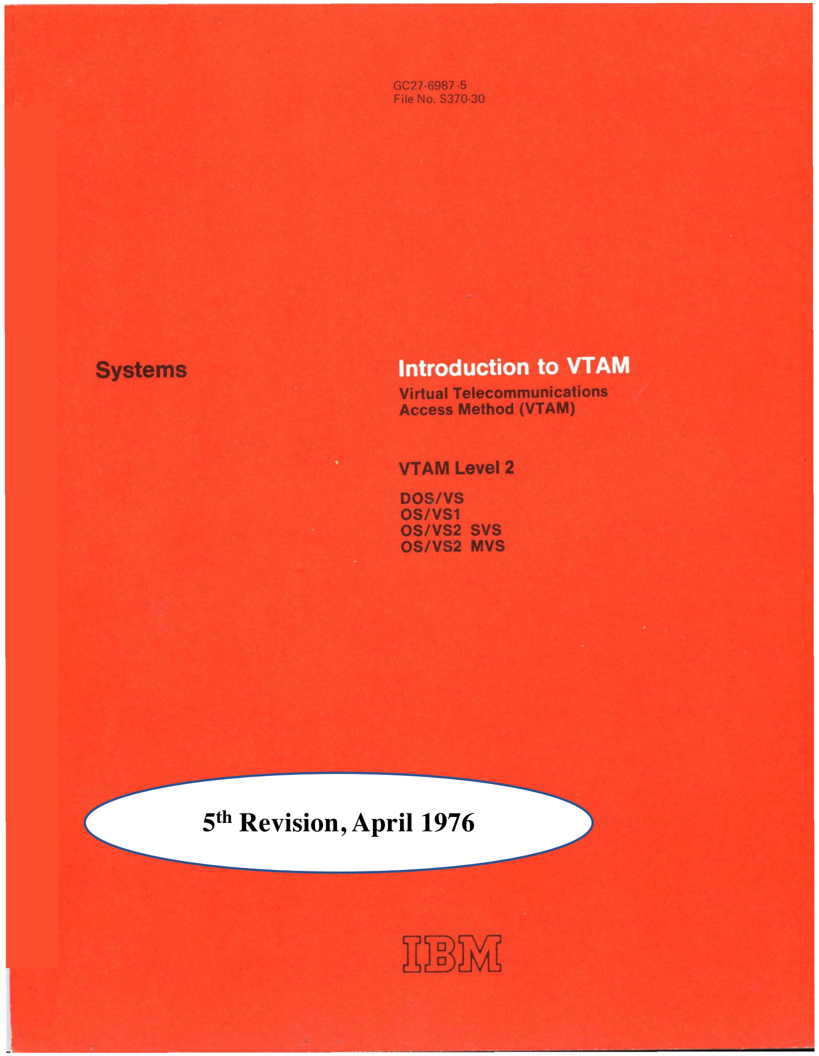
By Marguerite Zientara
Of the CW Staff

Prices of business forms used in DP have risen from 3% to as much as 18% this year, and one forms manufacturer predicts a 50% increase in industry prices over the next two years, a recent *Computerworld* survey found.

the foremost factors dictating increases are increased costs of their raw materials (paper, ink, chemicals) as well as decreasing availability of adequate paper supplies.

Four small manufacturers of business forms interviewed had raised their prices within the last

NRMA Conference Told
'Future of Retailing' Lies in DP



GC27-6987-5
File No. S370-30

Systems

Introduction to VTAM

Virtual Telecommunications Access Method (VTAM)

VTAM Level 2

DOS/VS
OS/VS1
OS/VS2 SVS
OS/VS2 MVS

IBM

5th Revision, April 1976

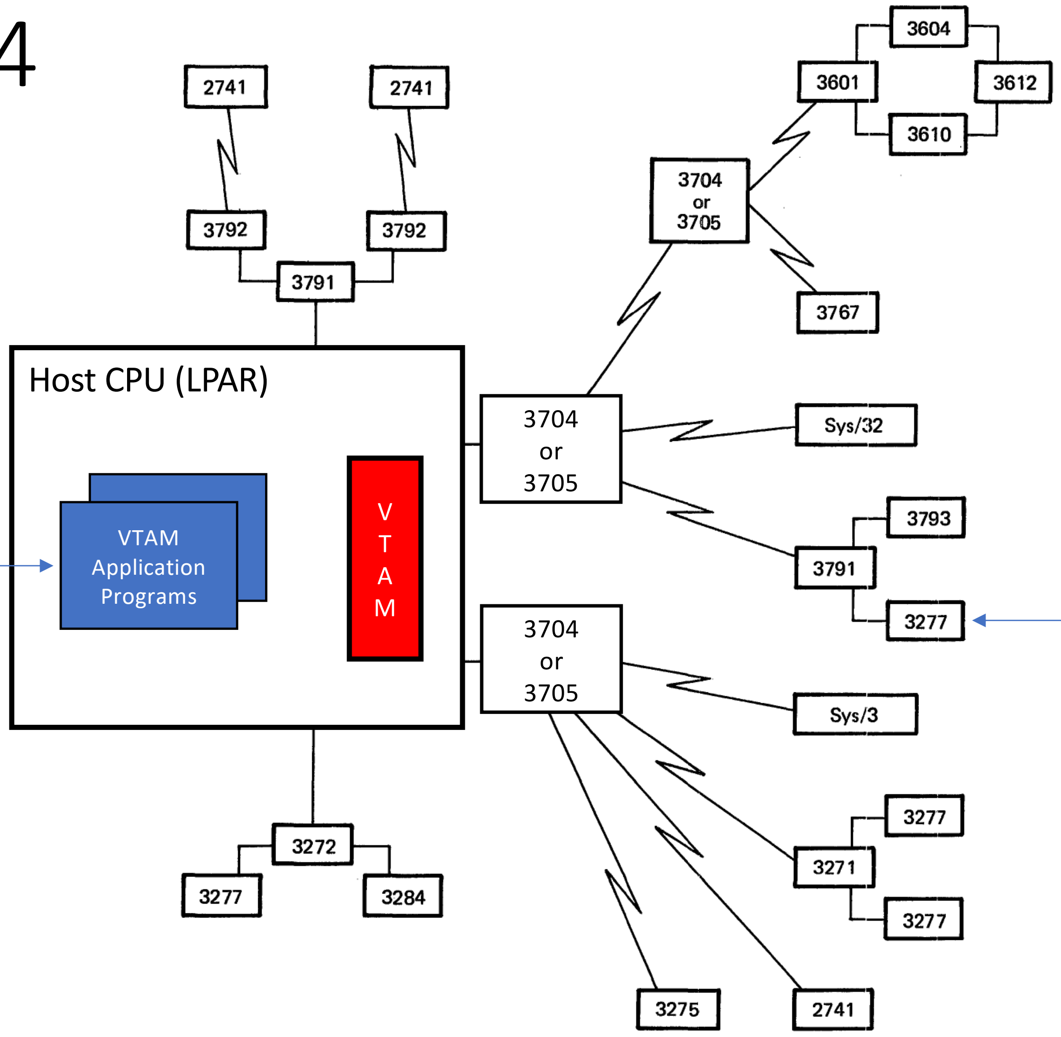
Virtual Telecommunications Access Method

- VTAM has been around for a while now – since circa 1974
- Support for SNA networking for MVS and DOS/VS systems
  - Locally attached devices
  - Network attached devices
  - Devices typically “dumb terminals”
- Support for Front End Processors (FEPs)
  - 3704/5 Network controllers (later 3725s, 3745s)
  - Channel attached or daisy chained
  - Loaded with a Network Control Program (NCP)
  - Supported the network attached devices (SDLC was the crème de la crème).
- Provided an API
  - Applications to communicate with local and network devices
  - Applications to communicate with other applications in network

VTAM in 1974

Early SNA Applications

These would still run today.

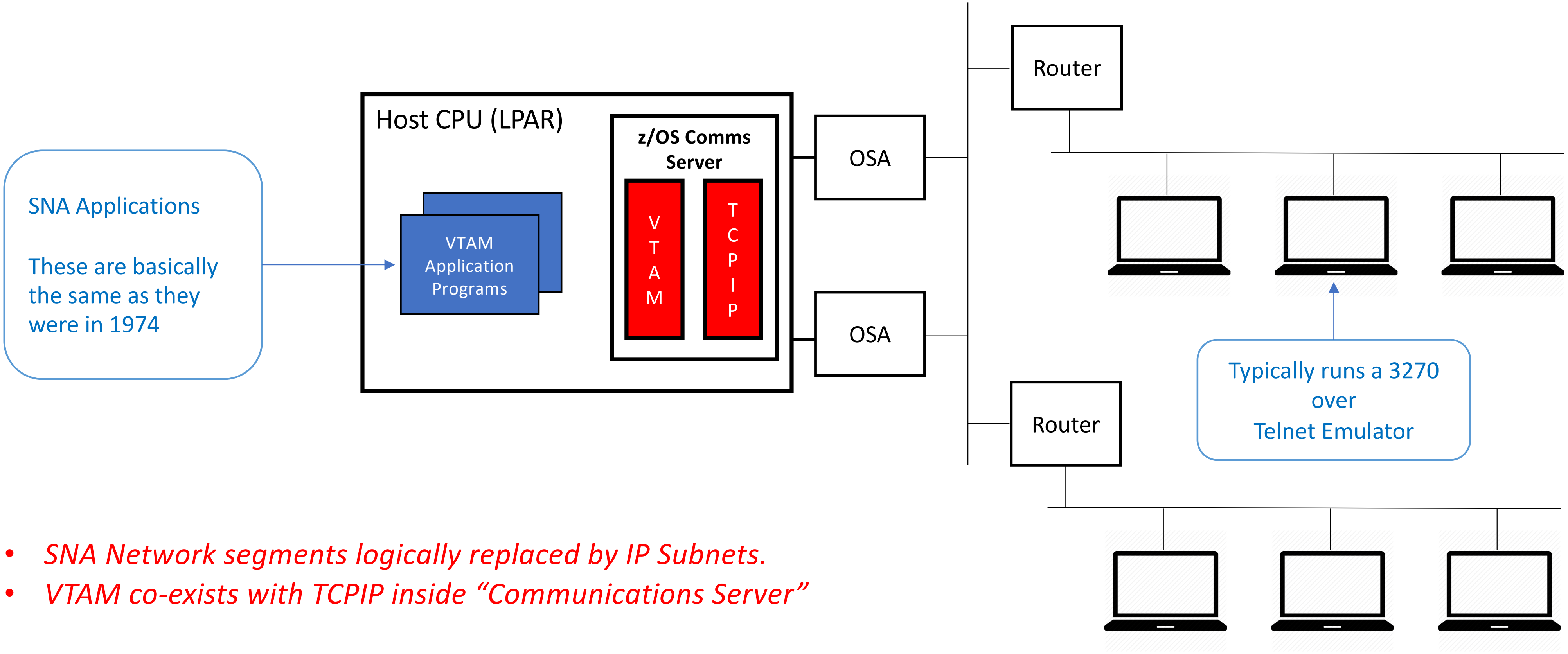


Early 3270 series terminal

Distant relative of today's TN3720 emulator

SNA Network segments called "subareas" : Boundaries at Host and 37x5.

VTAM in 2019


SNA Applications
These are basically the same as they were in 1974
Host CPU (LPAR)
VTAM Application Programs
z/OS Comms Server
VTAM
TCPIP
OSA
OSA
Router
Router
Typically runs a 3270 over Telnet Emulator

- *SNA Network segments logically replaced by IP Subnets.*
- *VTAM co-exists with TCPIP inside “Communications Server”*

VTAM Terminology

VTAM way back when …	VTAM in 2019
Systems Services Control Point (**SSCP**) Manages SNA Subarea Resources	Still exists in Subarea or Interchange Mode
Control Program (**CP**) Manages SNA APPN Resources	Still exists when in APPN or Interchange Mode
Physical Units (**PU**) Hardware or Software based Device Controller	Still exists, but typically in software only.
Logical Units (**LU**) Physical network endpoint device	Still exists, but typically software emulated.
SNA Connections (**Sessions**) LU-LU Sessions for "normal" connections. SSCP-LU, SSCP-PU, SSCP-SSPC for control connections.	Still exist. LU-LU sessions still used for normal connections. Less use of SSCP sessions.

- Many sites still run in subarea or interchange mode
- We still talk about ”sessions” today when referring to connections.
- 21st century, state-of-the-art TN3270 emulators still reference LU names

SNA Evolution

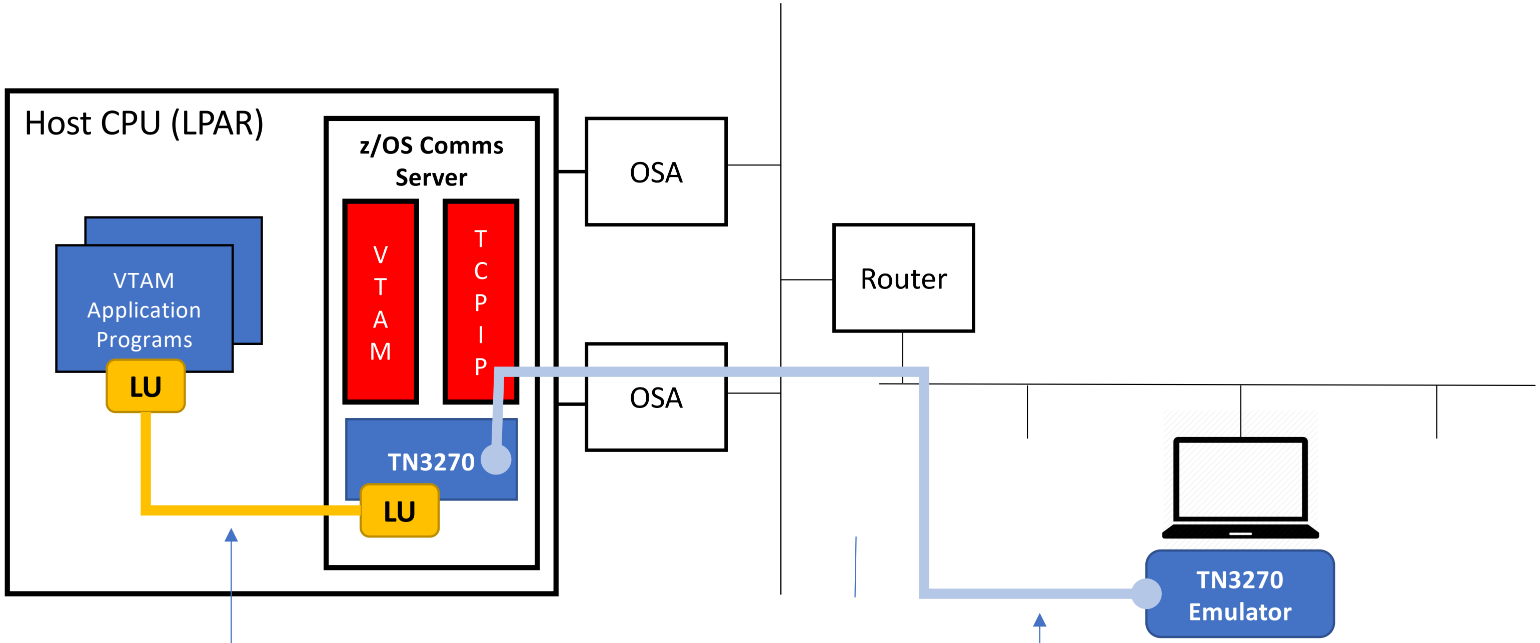
- SNA was originally hierarchical
  - A primary LU (PLU) was normally the application
  - A secondary LU (SLU) was normally the terminal
  - SLU normally initiated connection to PLU : *login applid(appname)*
  - PLU could initiate session with SLU (acquire a session, such a printer)
- Peer-to-peer (more like TCPIP today) introduced
  - Application to application session evolved : LU Types 6.1, 6.2 (APPC)
  - Extensive support in CICS
  - VTAM APIs extended for LU6.2
  - APPC/MVS for simpler, non-assembler applications
- Peer-to-peer networking (even more like TCPIP today) introduced
  - Advanced Peer-to-peer networking (APPN)
  - Self defining and routing, PU Type 2.1 and APPC sessions.

SNA Today

… the death of SNA has been grossly exaggerated (*Mark Twain*, nearly)

- Still predominantly used for 3270 sessions
  - Over TN3270 to TSO, CICS, IMS …
    - Session protocols are identical to those back in 1970s
    - LU-LU sessions between a PLU and an SLU
    - Main difference is the SLU is a software component of the TN3270 Server.
- Application to Application sessions
    - LU-LU sessions between applications (mainly LU6.2 sessions, typically CICS)
    - Applications probably haven’t changed
    - APPC/MVS still in use
- Physical SNA Wide Area Network
  - SNA hardware has (or at least should have) gone
  - Replaced by IP backbone

SNA in 2019 (TN3270)



SNA LU-LU Session

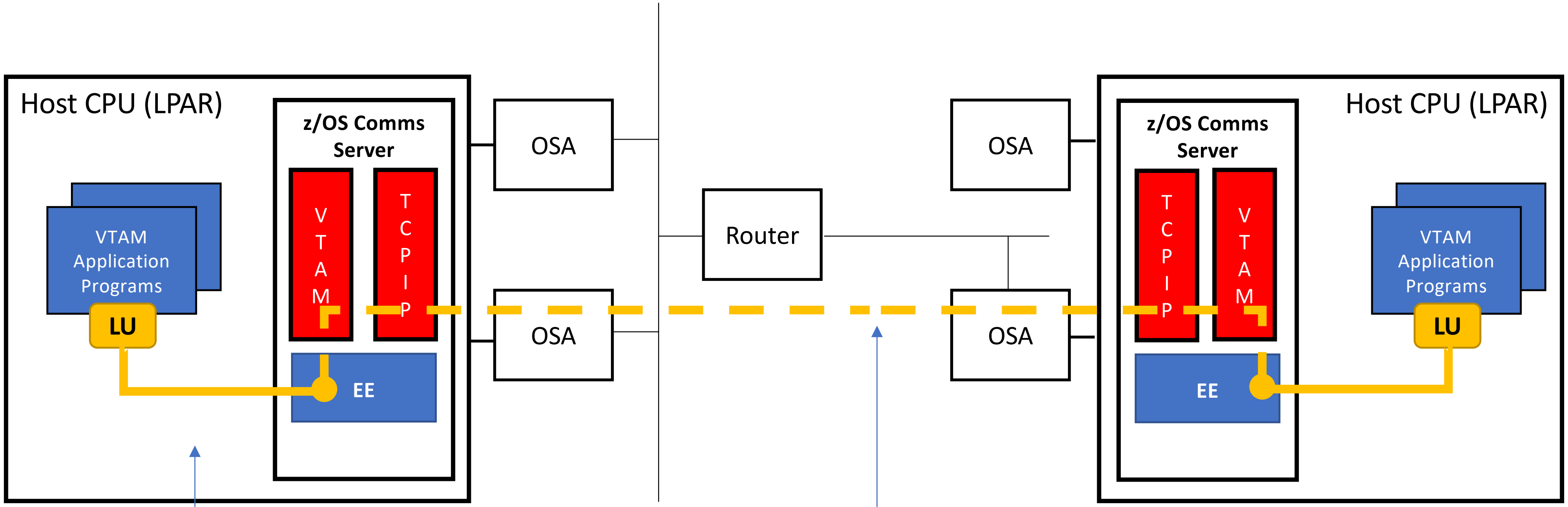
Same as in 1974

TCP/IP Connection

3270 data wrapped in TCP packet

SNA in 2019 (Application to Application)

Exploits Enterprise Connector (EE)



SNA LU-LU Session

Same as in 1974

UDP/IP Packets

SNA data wrapped in UDP packet by EE

VTAM in 2019

Integral component of *z/OS Communications Server*

- Still needed for vanilla SNA
    - Subarea, APPN or Interchange Modes
- Provides Enterprise Extender (EE)
    - Support SNA sessions over IP wide area networks
- Channel Attached Device Support (for SNA and TCPIP)
    - OSA Adaptors
- Sysplex Services (for SNA and TCPIP)
    - MPC, XCF
- Provides Communications Storage Manager
    - High performance storage option – available to any (including TCPIP)

Enterprise Extender (EE)

- Allows SNA transport over IP backbone
  - Widely used within an organisation
  - Frequently used between organisations
- Uses SNA APPN High Performance Routing (HPR)
- SNA Request Headers & Request Units (aka. Data)
  - HPR Headers added
  - Sent over IP using UDP protocol
  - Traffic priority managed by using different UDP Ports (12000-12004)
- Application DOES NOT KNOW SNA Session has been transferred over an IP backbone
  - Application code can be (and probably is) unchanged from pre-TCPIP days
- EE Supported
  - By VTAM for inter-mainframe sessions
  - OEM products Routers, SNA Servers (they still exist), Printers ….

Channel Attached Device Support

- TCP/IP 100% reliant on Network Interface Card (NIC)
- On a mainframe, this is typically
  - One or more OSA Adaptors
  - RoCE Express Adaptor (for RDMA)
- TCPIP has no native support for OSAs
- VTAM owns and controls these devices
  - VTAM can still use the devices for SNA work
  - Co-operative definitions (VTAM TRLEs and TCPIP Profile Interface)
- Multipath Channel I/O (MPC)
  - Protocol Headers and Data handled separately
  - VTAM support allows single device to handle multiple protocols
- VTAM must be configured and active to start TCP/IP devices

Sysplex Services

- Cross Coupling Facility (XCF)
  - Integral part of inter-LPAR communications within a Sysplex
  - XCF is protocol independent (has its own API)
  - TCP/IP can use XCF to communicate between TCP/IP stacks
  - XCF used to manage ephemeral sockets use with DVIPAs
  - All dependent on VTAM
- Hypersockets
  - Can be over XCF (requires VTAM)
  - Can be over a QDIO TRLE (requires VTAM)

Communications Storage Manager

- High performance storage management provided by VTAM
- Buffers shared/move between applications
  - Without physically copying data
- VTAM and TCPIP are typically the biggest user
  - But any authorized application can use CSM buffers
- Buffer Storage Allocated in
  - ECSA, Data spaces, 64 bit CSA
- VTAM Commands supplied to
  - Display CSM Buffer utilization
  - Display CSM Buffer users
  - Monitor CSM Buffers

Anyone doing this?

Communications Storage Manager

```
D NET,CSMUSE
IVT5508I DISPLAY ACCEPTED
IVT5572I PROCESSING DISPLAY CSMUSE COMMAND - OWNERID NOT SPECIFIED 112
IVT5532I ------------------------------------------------------
IVT5575I USAGE SUMMARY - 4KECSA   POOL TOTAL (ALL USERS)  =      164K
IVT5576I    AMOUNT   MONITOR ID    OWNERID     JOBNAME
IVT5577I      144K       21          0025      VTAM
IVT5578I DISPLAY TOTAL FOR 4KECSA   POOL (1 USERS)        =      144K
IVT5532I ------------------------------------------------------
IVT5575I USAGE SUMMARY - 16KECSA  POOL TOTAL (ALL USERS)  =       16K
IVT5576I    AMOUNT   MONITOR ID    OWNERID     JOBNAME
IVT5577I       16K       B1          0042      TCPIP
IVT5578I DISPLAY TOTAL FOR 16KECSA  POOL (1 USERS)        =       16K
IVT5532I ------------------------------------------------------
IVT5575I USAGE SUMMARY - 4KDS64   POOL TOTAL (ALL USERS)  =      896K
IVT5576I    AMOUNT   MONITOR ID    OWNERID     JOBNAME
IVT5577I      896K       21          0025      VTAM
IVT5578I DISPLAY TOTAL FOR 4KDS64   POOL (1 USERS)        =      896K
IVT5532I ------------------------------------------------------
IVT5575I USAGE SUMMARY - 4KHCOM   POOL TOTAL (ALL USERS)  =     4452K
IVT5576I    AMOUNT   MONITOR ID    OWNERID     JOBNAME
IVT5577I     4332K       23          0042      TCPIP
IVT5578I DISPLAY TOTAL FOR 4KHCOM   POOL (1 USERS)        =     4332K
IVT5532I ------------------------------------------------------
IVT5575I USAGE SUMMARY - 16KHCOM  POOL TOTAL (ALL USERS)  =       32K
IVT5576I    AMOUNT   MONITOR ID    OWNERID     JOBNAME
IVT5577I       32K       B1          0042      TCPIP
IVT5578I DISPLAY TOTAL FOR 16KHCOM  POOL (1 USERS)        =       32K
IVT5532I ------------------------------------------------------
IVT5575I USAGE SUMMARY - 32KHCOM  POOL TOTAL (ALL USERS)  =       96K
IVT5576I    AMOUNT   MONITOR ID    OWNERID     JOBNAME
IVT5577I       96K       B1          0042      TCPIP
IVT5578I DISPLAY TOTAL FOR 32KHCOM  POOL (1 USERS)        =       96K
IVT5599I END
```

```
D NET,CSM
IVT5508I DISPLAY ACCEPTED
IVT5529I PROCESSING DISPLAY CSM COMMAND - OWNERID NOT SPECIFIED 118
IVT5530I BUFFER BUFFER
IVT5531I SIZE   SOURCE                INUSE      FREE     TOTAL
IVT5532I ------------------------------------------------------
… lines removed
IVT5535I TOTAL  ECSA                   176K      976K     1152K
IVT5532I ------------------------------------------------------
… lines removed
IVT5535I TOTAL  DATA SPACE 31            0M      256K      256K
IVT5532I ------------------------------------------------------
… lines removed
IVT5535I TOTAL  DATA SPACE 64          896K     1256K     2152K
IVT5532I ------------------------------------------------------
… lines removed
IVT5535I TOTAL  DATA SPACE             896K     1512K     2408K
IVT5532I ------------------------------------------------------
… lines removed
IVT5535I TOTAL  HVCOMM                4496K     2672K        7M
IVT5532I ------------------------------------------------------
IVT5536I TOTAL  ALL SOURCES           5568K     5160K    10728K
IVT5538I FIXED  MAXIMUM =      240M  FIXED  CURRENT =     8637K
IVT5541I FIXED  MAXIMUM USED =     8765K SINCE LAST DISPLAY CSM
IVT5594I FIXED  MAXIMUM USED =     8765K SINCE IPL
IVT5539I ECSA   MAXIMUM =      120M  ECSA   CURRENT =     1475K
IVT5541I ECSA   MAXIMUM USED =     1475K SINCE LAST DISPLAY CSM
IVT5594I ECSA   MAXIMUM USED =     1475K SINCE IPL
IVT5604I HVCOMM MAXIMUM =     2000M  HVCOMM CURRENT =        7M
IVT5541I HVCOMM MAXIMUM USED =        7M SINCE LAST DISPLAY CSM
IVT5594I HVCOMM MAXIMUM USED =        7M SINCE IPL
IVT5559I CSM DATA SPACE 1 NAME: CSM64001
IVT5559I CSM DATA SPACE 2 NAME: CSM31002
IVT5599I END
```

VTAM Security

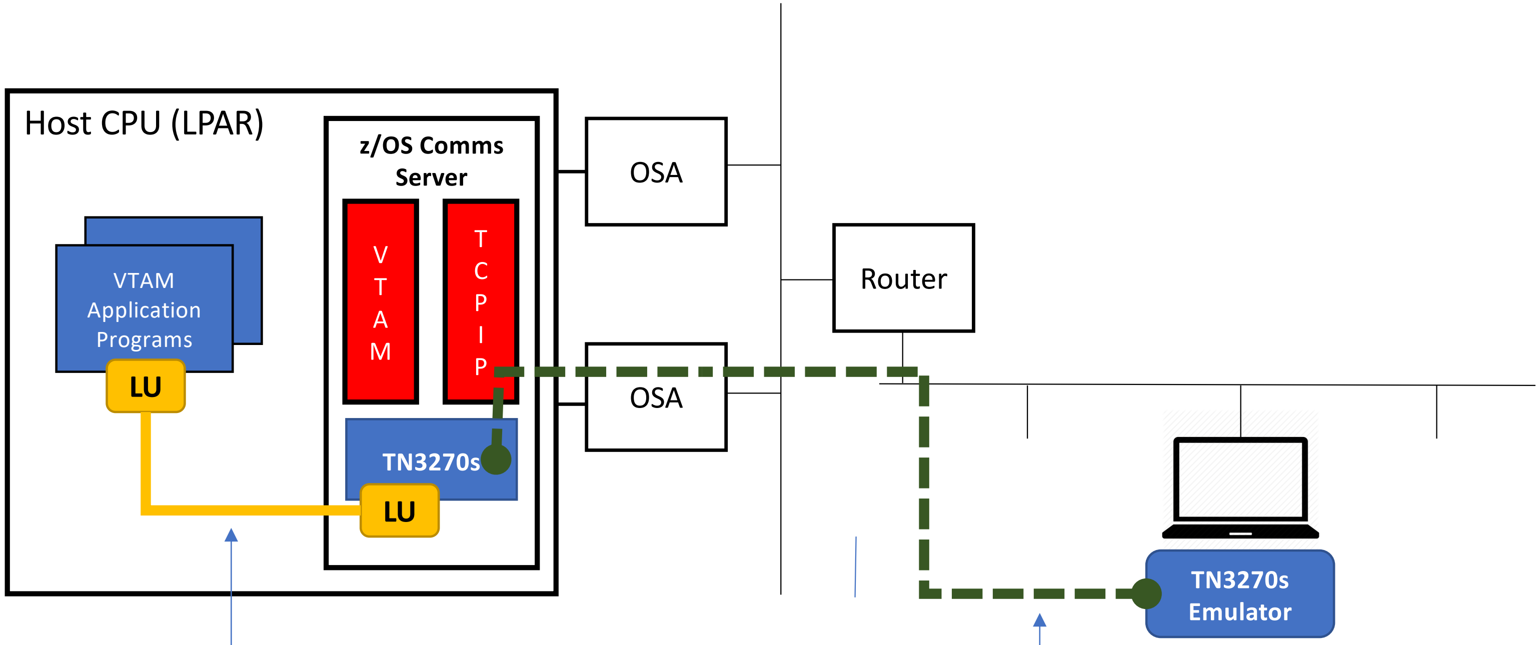
- Security focus is always on TCP/IP
  - Encryption
  - IP Filtering
  - Protected Ports
  - Intrusion Detection Services
  - All powerful and essential features
- SNA and VTAM has always been secure, so why worry?
- Key Issues
  - Integration of TCP/IP and VTAM/SNA has opened some holes
  - Redundancy of old VTAM definitions

Many organizations have a “everything must be encrypted” policy. Is it really being achieved?

TN3270/EE Security

- TN3270 Connections can be encrypted
  - Using TLS/SSL Protocols
  - Supported natively in TN3270 Server or via AT-TLS
  - Secure TN3270 client needed in PC
  - Server certificate and optionally client certificate required
  - Nobody can view the data in flight
  - So company policies are fully met? … well, maybe.
- EE Connections
  - Go over UDP – cannot be protected by TLS/SSL or AT-TLS
  - IPSec typically the preferred option
  - At least one OEM solution available ☺

Encrypted TN3270 (Meeting Policy)



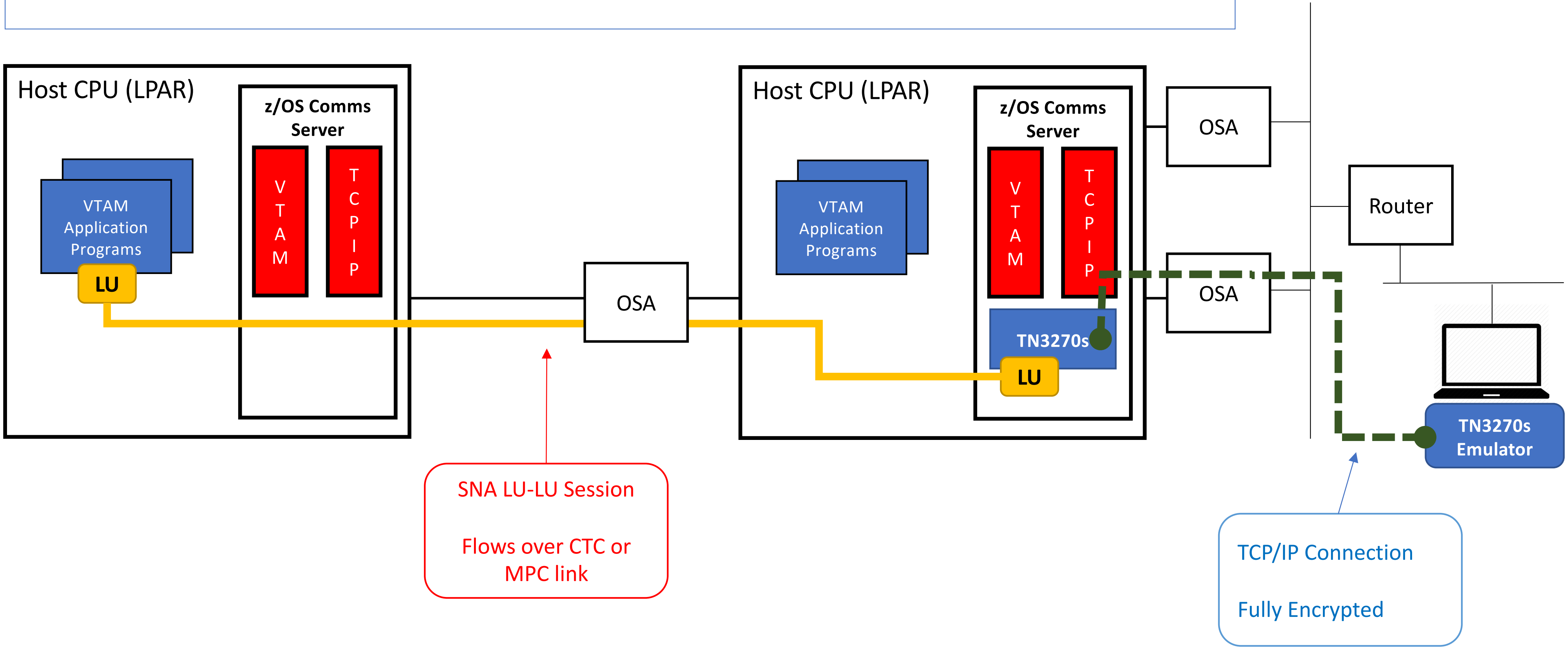
SNA LU-LU Session

Not encrypted, but doesn't leave LPAR.

TCP/IP Connection

Fully Encrypted

Encrypted TN3270 (Failing Policy)



SNA LU-LU Session

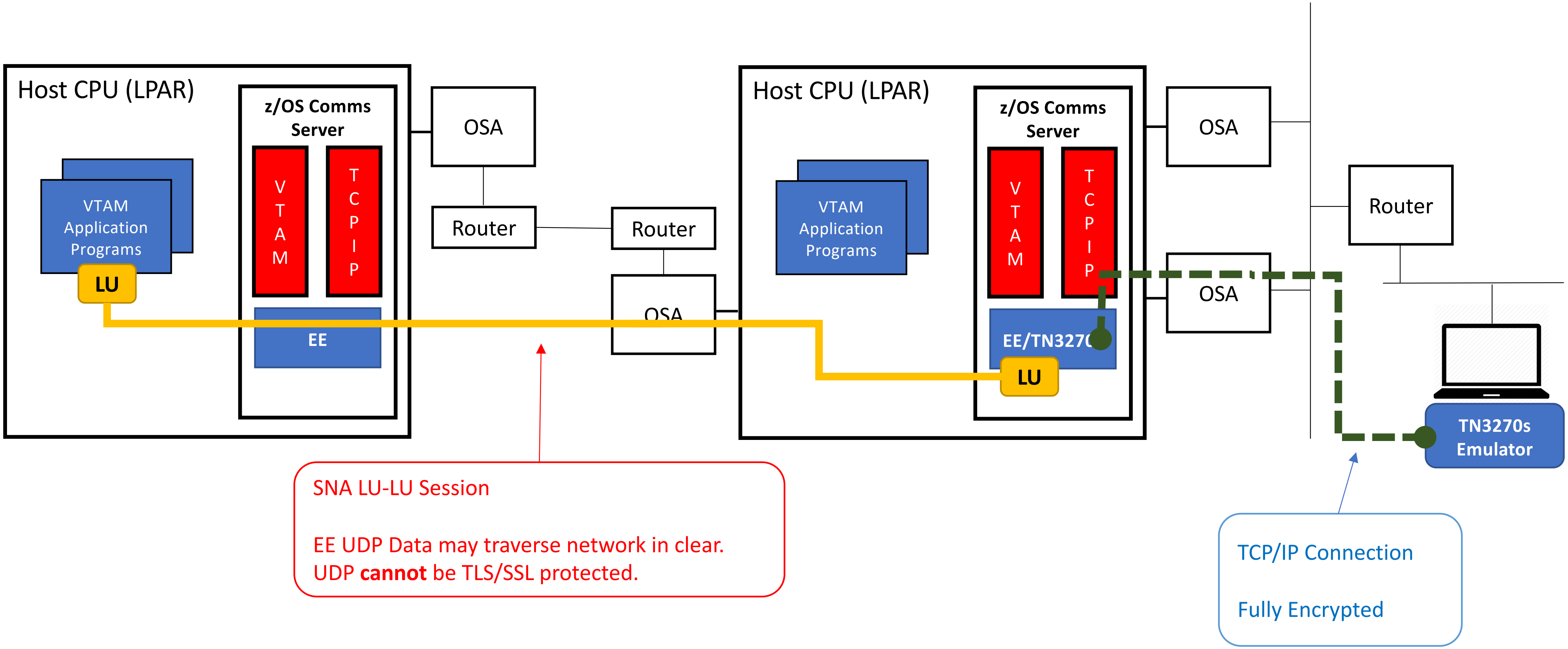
Flows over CTC or MPC link

TCP/IP Connection

Fully Encrypted

Unencrypted data leaves the LPAR … on a channel, so maybe not too much concern.

Encrypted TN3270 (Failing Policy)



SNA LU-LU Session

EE UDP Data may traverse network in clear.
UDP **cannot** be TLS/SSL protected.

TCP/IP Connection

Fully Encrypted

To comply with security policy, EE endpoints must be protected by IPSEC

VTAM Definition Redundancy/Protection

- Back in the day
  - VTAMLST defined many application ACBs
  - Some have become redundant SNA declined
    - Applications moved to native TCPIP
    - Less need for monitoring and management products such as NetView
  - Some have led to increased VTAM definitions
    - TCP/IP TN3270 terminal pools
    - Multi-session managers
- What does VTAMLST have in it today?
  - Are there any active ACBs not in use?
- Unless they are RACF protected (VTAMAPPL class)
  - Any job/user can open an ACB
  - Without any form of authorisation
  - APIs fully documented and freely published by IBM

SC27-3674-30 IBM z/OS Communications Server SNA Programming

SC27-3670-30 IBM z/OS Communications Server SNA Programmer’s LU6.2 Reference

Demo

- Simple batch job
  - Does NOT need to be APF authorised

Possible Exposures

- Any active ACB with AUTH=PPO,SPO or CNM is a potential exposure
- AUTH=PPO|PPO allows any application to issue VTAM commands
  - Demo used a redundant NetView ACB
- AUTH=CNM allows applications to drive CNM interface
  - Collect session awareness data
  - Potentially start, stop, view session tracing
  - Often left active after NLDM in NetView stopped
- Even without any redundant ACBs left open
  - < 100 lines of unauthorised code can disable your TN3270 server!

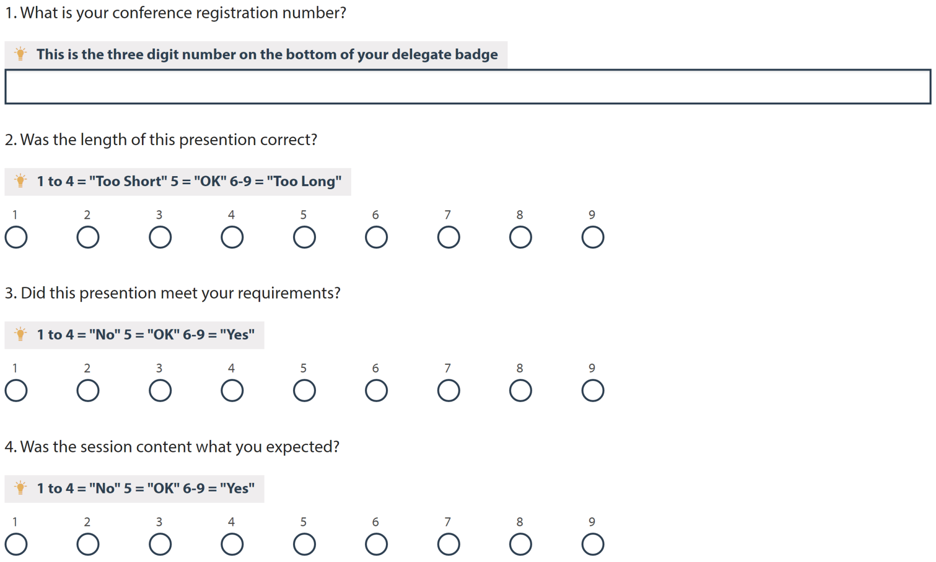
Always use RACF VTAMAPPL class to protect against this.

Summary

- VTAM is still a critical component of your system
  - Without it TCPIP and possibly other components will not work
- VTAM CSM important for performance
  - VTAM CSM buffer shortage can lead to TCPIP performance issues
- VTAM Security
  - Is still important
  - Do not leave redundant ACBs active
  - RACF VTAMAPPL protect all ACBs.

Please submit your session feedback!

- Do it online at http://conferences.gse.org.uk/2019/feedback/EA
- This session is EA



1. What is your conference registration number?

This is the three digit number on the bottom of your delegate badge

2. Was the length of this presention correct?

1 to 4 = "Too Short" 5 = "OK" 6-9 = "Too Long"

1	2	3	4	5	6	7	8	9
○	○	○	○	○	○	○	○	○

3. Did this presention meet your requirements?

1 to 4 = "No" 5 = "OK" 6-9 = "Yes"

1	2	3	4	5	6	7	8	9
○	○	○	○	○	○	○	○	○

4. Was the session content what you expected?

1 to 4 = "No" 5 = "OK" 6-9 = "Yes"

1	2	3	4	5	6	7	8	9
○	○	○	○	○	○	○	○	○