Mainframe Applications Going Mobile
The Future of 3270 Terminal Emulation

Deb Hodson
dhodson@sdsusa.com
Software Diversified Services (SDS)
763-450-9124

Patrick Fournier
patrick.fournier@syspertec.us
SysperTec Communication
925-954-9649
Software Diversified Services
Proudly Serving Enterprise Customers for Over 34 Years

- Financially Rock Solid
- Several Hundred Satisfied Licensed Customers Worldwide
- Over 20 z/OS, z/VSE and z/VM Mainframe Systems and Distributed Products
- World Class Support

Full Time Development / Support Staff / USA

- Partner Solutions Virtel thin client
- Partner Solutions for capping workload and performance analytics
- VitalSigns for Network Management

HQ in Minneapolis
1322 81st Ave. NE
Spring Lake Park, MN
55432-2116 USA

(800) 443-6183, (763) 571-9000

www.sdsusa.com
The Future of 3270 Terminal Emulation
An alternative to traditional 3270 Terminal Emulation

Historical Background
New Challenges:
- Mobility, BYOD, and VDI
- Java Support Headaches
- Security Concerns

True* Thin-Client Web Access

* Two-Tier Browser-Based
3270 TE Technology Routed in Late 60s

- 3270 TE products
  - 20 years old design
  - Rely on TN3270 connections + client applets + Java

- TN3270 = Telnet (Teletype Network) 3270
  - Designed in 1969
  - Intended for private networks
  - TN3270 extends SNA connections over Internet
  - SNA techno = incompatible with Internet techno

- Client applets = client-specific
  - OK when all 3270 TE clients were traditional Windows workstations
  - Not OK when 3270 TE clients could be ... any web-enabled device

- Java
  - 2nd most insecure software after Flash
  - Needs frequent security patches
    - Challenging support + unstable 3270 TE solution + security exposure
  - Discontinued Java plugin support

- Traditional 3270 TE techno doesn’t support today’s client techno
BYOD and Mobility

- **BYOD = Bring You Own Device**
  - Formal or informal
  - Work anywhere anytime from any (web-enabled) device
  - Employees/BP (prefer to) use personal device to work
  - Not in business to manage client devices
    - Save $ + time + trouble
  - Support any web-enabled device
    - New versions of Windows
    - Apple products
    - Linux, AIX, UNIX
    - Mobile devices

- **Mobility**
  - Tablets and (large display) smartphones
  - Tablets outsell PC & notebooks
  - Android, iOS, W-10 Mobile, Firefox-OS ...

- **Most 3270 TE don’t fully support BYOD + mobility**
VDI

- VDI = Virtual Device Infrastructure
  - Take apps off client devices (except OS + browser)
  - Apps are in the Cloud
  - Not just Office Suite: all apps (including 3270 TE)
  - Security concern with client apps on web-connected devices
  - Strong trend in EU in past 2-3 years

- Most 3270 TE doesn’t support VDI
Java Support Headache

- Most 3270 TE rely on Java applets
  - Client or server based
- Java = 2\textsuperscript{nd} most insecure SW after Flash
  - Frequent Java updates to patch security issues
  - 3270 TE solution = highly sensitive to Java levels
  - Support can be headache ... and costly too
- Discontinued Java Plugin support
  - Oracle announcement early 2016
  - General trend with web browsers: Safari, Firefox ...
    - Discontinue support for plugins: Flash, Active-X ...
    - Part of HTML5 migration
  - Does your 3270 TE rely on Java plugin?
Security Concerns

- Frequent mainframe security breaches
  - weekly occurrence
- Eliminate security threats:
  - TN3270 = SNA extended over Internet
  - Java applets = potential Trojan horses
- Do not entrust host security to 3270 TE users
- Keep host access control on the host
From 3270 TE to “True” Thin-Client Web Access

An alternative to traditional 3270 Terminal Emulation

What is it and what does it do?
What does it look like?
How does it compare techno-wise?
How does it work?
How secure is it?
How do people use it?
Why switch?

patrick.fournier@syspertec.us

© SysperTec 2016

Presented by Software Diversified Services™
Thin-Client (Browser-Based) 3270 TE

- Serves 3270 screens (CICS, IMS, TSO, etc)

- As HTML/JavaScript Web pages with 3270 emulation ergonomics

- Replaces traditional 3270 emulators
  - Attachmate, PCOMM, RUMBA, BlueZone, etc

To thin clients straight off the mainframe (no middle-tier servers)
From 3270 TE to “True” Thin-Client Web Access
An alternative to traditional 3270 Terminal Emulation

What is it and what does it do?
What does it look like?
How does it compare techno-wise?
How does it work?
How secure is it?
How do people use it?
Why switch?

patrick.fournier@syspertec.us
3270 Terminal Emulation Web Page

Presented by Software Diversified Services™
From 3270 TE to “True” Thin-Client Web Access
An alternative to traditional 3270 Terminal Emulation

What is it and what does it do?
What does it look like?
How does it compare techno-wise?
How does it work?
How secure is it?
How do people use it?
Why switch?

© SysperTec 2016

Presented by Software Diversified Services™
Traditional 3270 TE = Client-Based

- Client-based 3270 terminal emulators
  - Two tiers = host + client
  - End-to-end TN3270 connection
  - Client-based applet typically coded in Java
Traditional 3270 TE = Server-Based

- Server-based 3270 TE emulator
  - Three tiers = host + middle-tier server + client
  - TN3270 connection between host and middle-tier server
  - Server-based “client” applet typically coded in Java
“True” Thin-Client

- Thin-client (browser-based) web access
  - No client applets + no middle-tier servers + no TN3270
  - Two tiers = host + client
  - End-to-end HTTP connection
  - HTML/JavaScript pages with 3270 TE ergonomics rendered by client web browser
From 3270 TE to “True” Thin-Client Web Access

An alternative to traditional 3270 Terminal Emulation

What is it and what does it do?
What does it look like?
How does it compare techno-wise?
How does it work?
How secure is it?
How do people use it?
Why switch?

patrick.fournier@syspertechnology.com

Presented by Software Diversified Services™
Thin-Client (Browser-Based) Architecture

- Client “app” is replaced by Web browser + Web page
  - 3270 application screens: CICS, IMS, TSO, Natural, etc
  - HTML/JavaScript web-pages with 3270 TE ergonomics
  - any web browser
  - any web-enabled device

- Works instantly with any Web client today ... or tomorrow
  - any version of Windows, Apple product, tablet or mobile device

- Simple deployment
  - nothing to install on clients or middle-tier servers
  - point Web browsers to predefined URL

- Simple support
  - no client app, no middle-tier server, no Java components
  - support is 100% host-based
No Middle-Tier Server + No Java

- None of issues assoc. with middle-tier server:
  - Cost → additional HW/SW and support
  - Latency → slow response times
  - Bottlenecks → load-balancing + scalability issues
  - Fragility → one more component to breakdown
  - Troubleshooting → one more item to troubleshoot
  - TN3270 → unencrypted data over IP
    - VPN required → additional $ + support

- None of issues assoc. with Java components:
  - Complexity and fragility → Java levels sensitivity
  - Discontinued Java plugin support
How Do Users Connect to 3270 Apps?

- 3270 applications have screen user interface
How Do Users Connect to 3270 Apps?

- Screens are served via VTAM/SNA connections
How Do Users Connect to 3270 Apps?

- Virtel behaves as a regular VTAM terminal
How Do Users Connect to 3270 Apps?

- Core of Virtel is a host/web protocol converter
How Do Users Connect to 3270 Apps?

- Integrated IP server handles web connections
How Do Users Connect to 3270 Apps?

- 3270 data + template → 3270 TE web page
How Do Users Connect to 3270 Apps?

- Can be rendered by any browser on any device
Performance and Efficiency

- **Light**
  - TN3270-like CPU consumption
  - webpage code (JavaScript/HTML) runs in client browser, not on mainframe
  - Host footprint limited to:
    - Merging 3270 data into Web page template
    - Sending Web page via HTTP server

- **Fast and scalable**
  - Short end-to-end instruction path
    - Assembler (no Java) on host
    - No middle-tier server(s)
  - Multiple VWA instances can coexist on same system
  - Works across LPARs or systems (SYSPLEX)
  - As fast and scalable as mainframe it runs on
From 3270 TE to “True” Thin-Client Web Access
An alternative to traditional 3270 Terminal Emulation

What is it and what does it do?
What does it look like?
How does it compare techno-wise?
How does it work?
How secure is it?
How do people use it?
Why switch?

patrick.fournier@syspertecc.us
Presented by Software Diversified Services™

TN3270 = Opened Tunnel Over Internet

- TN3270 Connections
  - Clients drive the exchanges: “pull” style communications
  - Synchronous connected connections
    - Permanently opened, even when inactive (99.99% of time)
  - Permanently opened “tunnel” from Web to host application
HTTP/S = Series of Discontinued Exchanges

- End-to-end HTTP/S connections
  - Host drives the exchanges: “push” style communications
  - Asynchronous disconnected connections
    - Closed when inactive (99.99% of time)
  - Session = series of discontinued host-driven exchanges
Break & Redirect Data Flow on Host

- Breaks and redirects data flow
  - SNA to HTTP/S and back
  - Inside host firewall
Token-Based Exchange Control

- Each host-initiated (push) exchange is controlled with:
  - Unique security token (man-in-the-middle attacks)
  - Expected message length (malware appending attacks)
  - Expected IP address (man-in-the-middle attacks)
TN3270 = Unencrypted Host Data Over Internet

- **TN3270 Connections**
  - TN3270 supports SSL but some 3270 TE applets don’t
  - Send unencrypted host data over the Internet
  - Run inside VPN to protect transmitted host data
  - VPN = additional SW licensing and support
**HTTPS = Encrypted Host Data Over Internet**

- **HTTPS Connections**
  - Send IBM SSL encrypted host data over Internet
  - Application Transparent Transport Layer Security (AT-TLS)
  - AT-TLS V1.2 V1.1 are FIPS 140-02 compliant
  - Don’t need VPN for data encryption
TN3270 = Ignores Hidden & Protected Attributes

TN3270 Connection
- Sends hidden data outside host
- Doesn’t verify if protected data comes back changed
- Relies on TN3270 client to implement host data access mode
- If TN3270 connection or client are compromised:
  - Hidden data may be exposed to unauthorized view
  - Protected data may be exposed to unauthorized update
- Host loses control of access mode once data sent via TN3270
Implements Requested Data Access on Host

- **Virtel Web Access**
  - Runs inside host firewall (protected from web attacks)
  - Implements requested host data access mode
    - Doesn’t send hidden data outside the host
    - Terminates session if protected data comes back changed
  - Host retains control of access mode
**TN3270 = Free To Roam After Crash**

- **TN3270 = one-time authentication**
  - Authenticated only once at logon
  - If/when 3270 application crashes:
    - 3270 TE session doesn’t typically crash
    - Session owner free to roam inside host: no re-authentication
Can’t Roam After Crash

- Virtel = memorized authentication
  - User authenticated at logon → application selection menu
    - Presented with authorized applications selection menu
  - If 3270 application crashes
    - Presented with same authorized applications selection menu
Application Selection Menu

Web browser tabs works as simple multi-session manager.

Available VTAM apps are listed in green.

Unavailable VTAM apps are listed in red.

Only authorized apps are listed. Unauthorized apps are not listed.

Existing session manager can be accessed directly or through Virtel application selection menu.
TN3270 = Well-Known Port

- TN3270 = defaults to “well-known” port 23
  - Port mapping program can display port details
    - Protocol + operating system + application
  - Gives potential attackers all information they need
User-Defined Port

- Virtel = relies on user-assigned registered port
  - Port number = unknown to outsiders
  - Port details (protocol, OS, application) = not displayed by port mapping programs
Client Applets = Potential Trojan Horses

Distributed 3270 TE applets
- Oftentimes coded in Java:
  - 2nd most notorious SW for security issues (after Flash)
  - Frequent security patches → solution instability
- “Sitting ducks” for attacks
- Can be used as Trojan Horses to access host assets
- Only as safe as their users are:
  - Antivirus, SW updates, safe Internet practices, etc.
- 100s or 1000s potential unauthorized host gateways
- Only takes 1 compromised applet → unauthorized access
- Host can’t insure/verify that applets are not compromised and used for unauthorized access
Thin-Client = No Client Applets

- Thin-client = no Java + no client applets
  - Serves new uncompromised webpages ...
  - ... rendered inside safer Web browser “sandbox”
  - Doesn’t rely on safe practices of distributed users
  - Host retains full control of access to host assets
User Macros = Potential Trojan Horse

- Distributed user-developed macros
  - Developed by users – escaped host security audit
    - Host logon (user name + password)
    - Activate 1000s of host transactions from spreadsheet
  - Stored on clients = “sitting ducks” for attacks by hackers
  - Can be used as Trojan Horses to access host assets
  - Only as safe as their users are
  - No inventory: 1000s potential unauthorized host gateways
  - Only takes 1 compromised macro → unauthorized access
  - Host can’t insure/verify that user macros are not compromised and used for unauthorized access
Keep Macros on Host

- User-developed macros can be stored on host
  - Developed and activated by users
  - Stored and executed on host inside host firewall
    - Undergo host security audit
    - Comprehensive centralized inventory
  - Host retains full control of access to host assets
Data-Less Client

- Thin-client = data-less client
  - Clear Web browser cache at end of session
  - No data, applet, macro, or webpage left on clients
  - No host exposure is client lost or stolen
Compatible With Any IP Security

- 3rd Party: PROXY & jump boxes, SSO, VPN ...
- Device (terminal, printer) control
- Multi-criteria authentication
- Biometrics authentication
From 3270 TE to “True” Thin-Client Web Access

An alternative to traditional 3270 Terminal Emulation

What is it and what does it do?
What does it look like?
How does it compare techno-wise?
How does it work?
How secure is it?
How do people use it?
Why switch?
Case Study – Car Manufacturer

- Replace costly SNA network with Internet connections
- Retain 3270 screen interface → no re-training
- 400K users 24x7 in 150 countries using local workstations
- Traditional client/server-hosted 3270 TE = NOT an option!
- Pure thin-client solution = no client app or middle-tier server
- Global BYOD (Bring Your Own Device) initiative
- Benchmarked with 16K concurrent users per instance
- 3K-average and 10K-peak concurrent sessions since 2003
- Localization services:
  - Language selection at logon
  - Automated DBCS/EBCDIC conversion for China, Japan, Russia, etc
Case Study – Car Manufacturer

- Replace costly SNA network with Internet connections
- Retain 3270 screen interface → no re-training
- 600K users 24x7 in 150 countries using local workstations

TAKE-AWAY:

- Simple deployment & support
- Supports very large deployments
- Perfect for BYOD

- Automated DBCS/EBCDIC conversion for China, Japan, Russia, etc
From 3270 TE to “True” Thin-Client Web Access

An alternative to traditional 3270 Terminal Emulation

What is it and what does it do?
What does it look like?
How does it compare techno-wise?
How does it work?
How secure is it?
How do people use it?
Why switch?
Why Consider Thin-Client

- **SUPPORT**
  - Reduce + simplify support requirements

- **ECONOMIC**
  - Reduce TCO (licensing + support)

- **EVOLUTION**
  - Support any web-enabled device instantly
  - Support mobility + BYOD + VDI initiatives

- **SECURITY**
  - Eliminate security threats: TN3270 + Java applets
  - Keep host access control on host
From 3270 TE to “True” Thin-Client Web Access
An alternative to traditional 3270 Terminal Emulation

Thank You

Deb Hodson
dhodson@sdsusa.com
Software Diversified Services (SDS)
763-450-9124

Patrick Fournier
patrick.fournier@syspertec.us
SysperTec Communication
925-954-9649