April 9, 2003

San Gabriel Valley
Pilot Project

Information Exchange Network (IEN)
System Administrator Training
Day 2

Final

Prepared by:

TRANSCORE
35 South Raymond Avenue, Suite 200
Pasadena, California 91105

IEN System Administrator's Training
Part 2

San Gabriel Valley Pilot Project

Countywide Information Exchange Network

TRANSCORE

April 9, 2003

Countywide Information Exchange Network

Training Agenda - Part 2

- IEN Network Components
- IEN System Components
- Maintenance Activities
  - Domain User Account Configuration
  - E-mail Configuration
  - System and Database Backups
- Troubleshooting IEN Connections
- Day 2 Wrap Up

Administration Overview

Administrative roles within the IEN:

Role	Description
IEN Administrators	Perform tasks specific to the IEN software, including tasks that may require knowledge of traffic engineering principles and devices.
System/Network Administrators	Perform standard system and networking administration tasks. These tasks could be delegated to local agency IT departments.

IEN Administrators

- IEN administrators are responsible for supporting and maintaining the IEN software.
- Their duties include:
  - Adding and removing users and resources
  - Configuring security settings governing access to resources
  - Setting application configuration parameters
- IEN administrative tasks are covered in Part 1 of the IEN System Administrator's Training.

System/Network Administrators

- System/Network administrators are responsible for maintaining the systems and network components that support the IEN software.
- Their duties involve:
  - Monitoring system and network status
  - Managing the IEN E-mail system
  - Performing system backups
- System/Network administrative tasks are covered in Part 2 of the IEN System Administrator's Training.

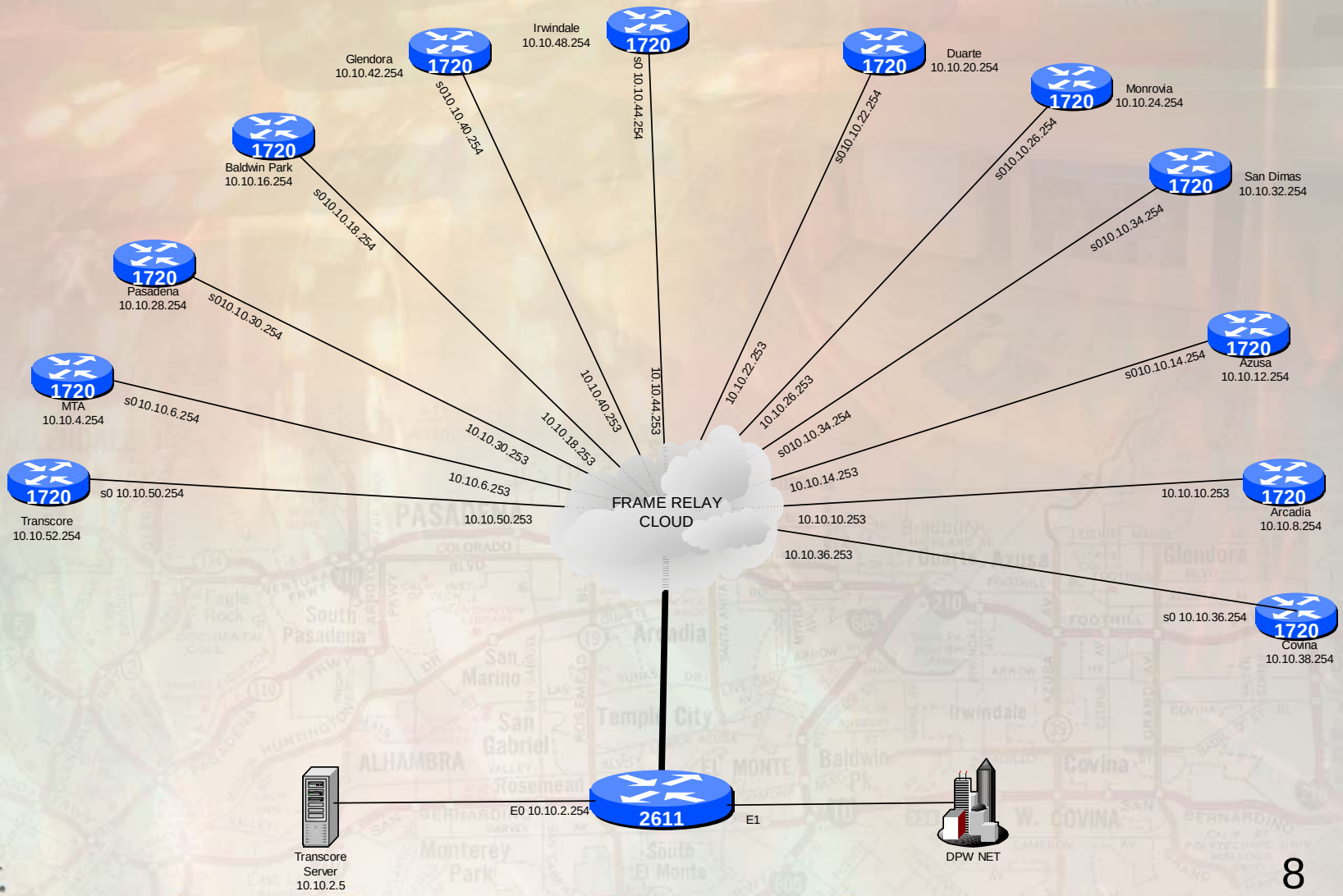
Administrative Resources

- IEN System Database Reference Manual
- IEN Detailed Design Document (DDD) Volume Set
- IEN System Overview Manual
- IEN System Operators Manual
- IEN System Technical Reference Manual
- Online Help Screens

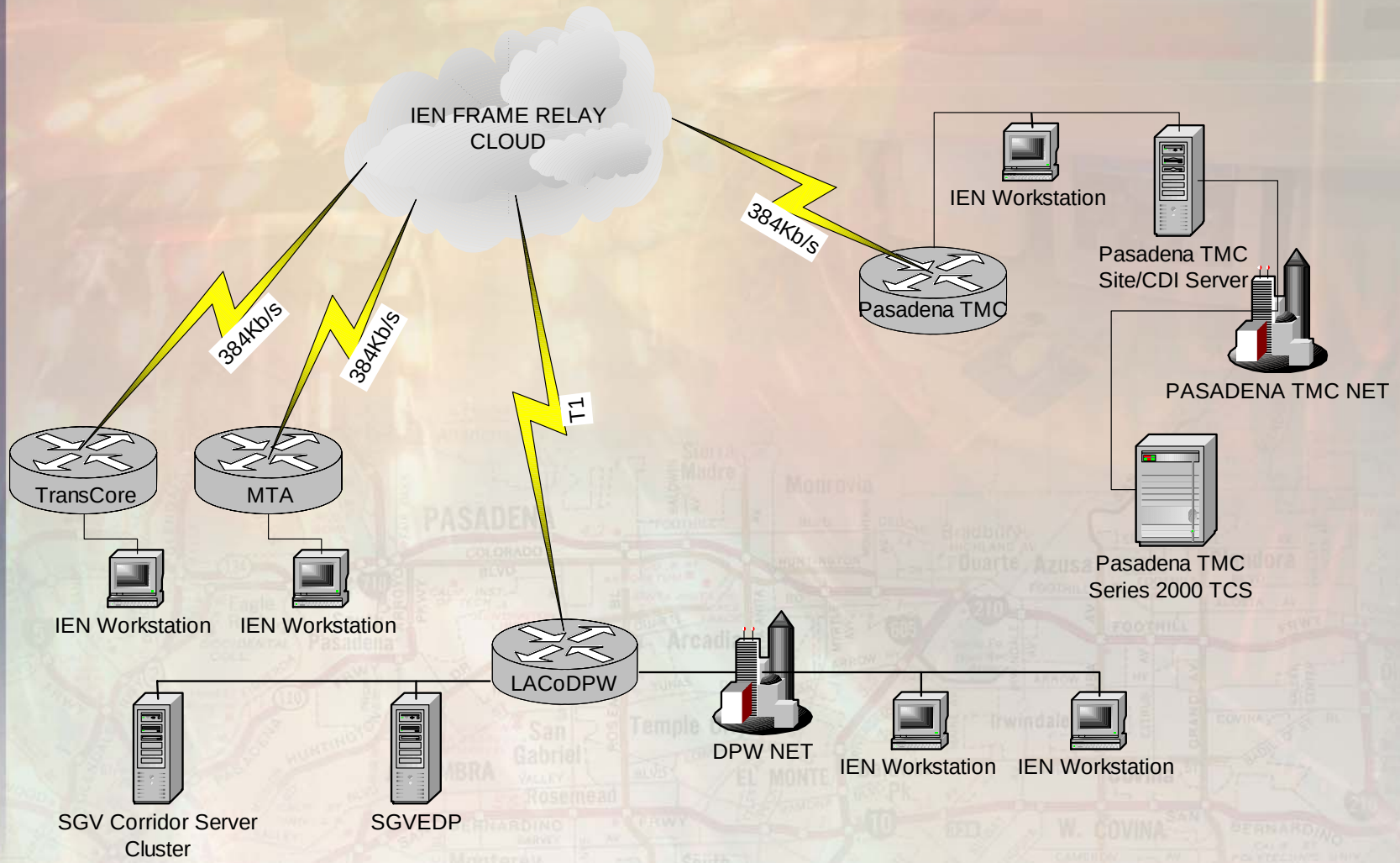
Administrative Applications and Tools

- IEN System Configuration Manager
- ATMS Database Administration
- IEN Component Viewer
- COTS software:
  - WhatsUp Gold
  - Windows 2000 Active Directory Users and Computers console
  - Microsoft Exchange Administrator
  - Microsoft Cluster Administrator and Oracle Failsafe Manager

IEN/EDP WAN Circuits



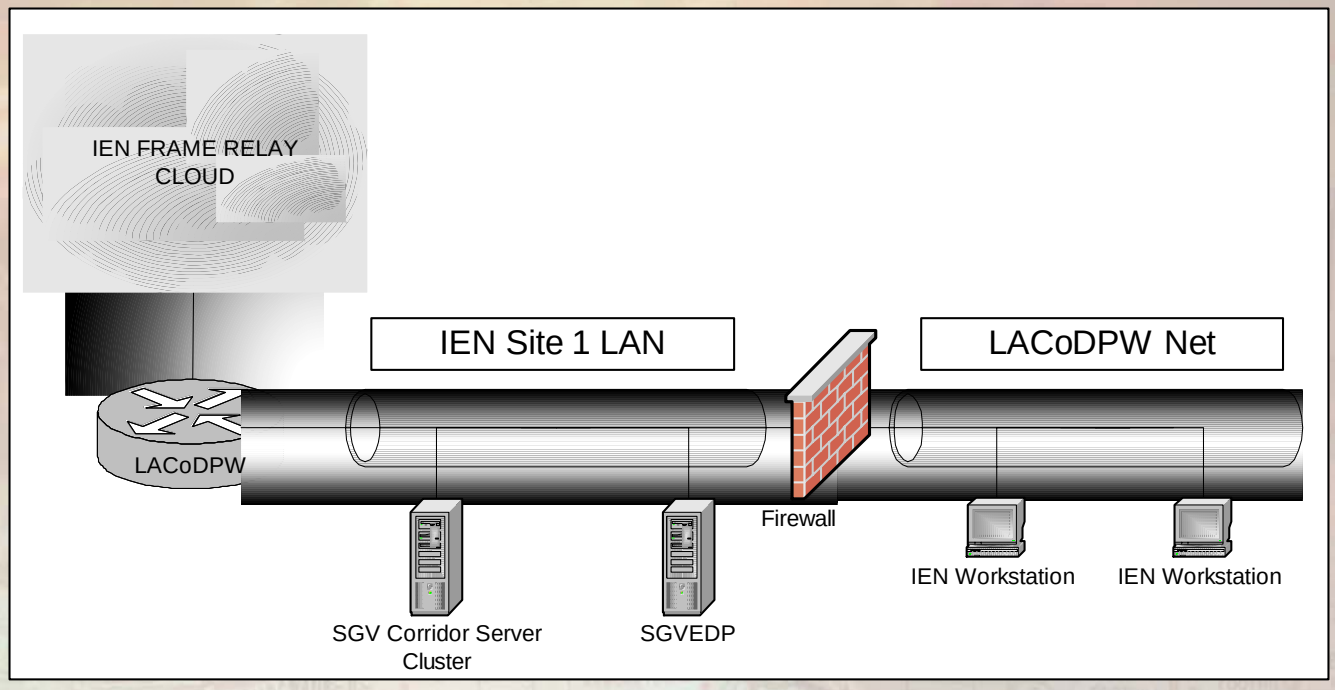
IEN Network Overview



IEN Locations

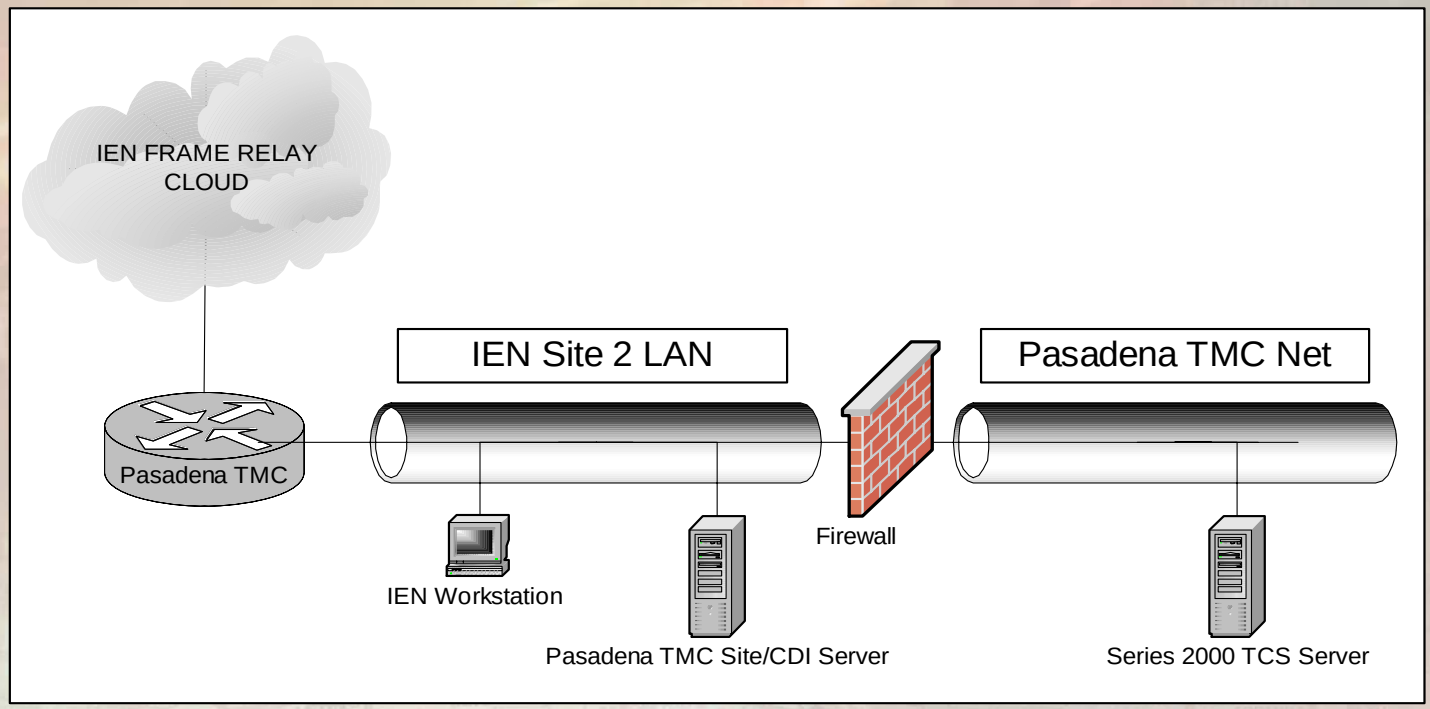
- Under the San Gabriel Valley Pilot Project (SGVPP), IEN systems have been deployed at the following locations:
  - LACoDPW
  - LACoMTA
  - Pasadena TMC
  - TransCore ITS - Pasadena

LACoDPW IEN Network



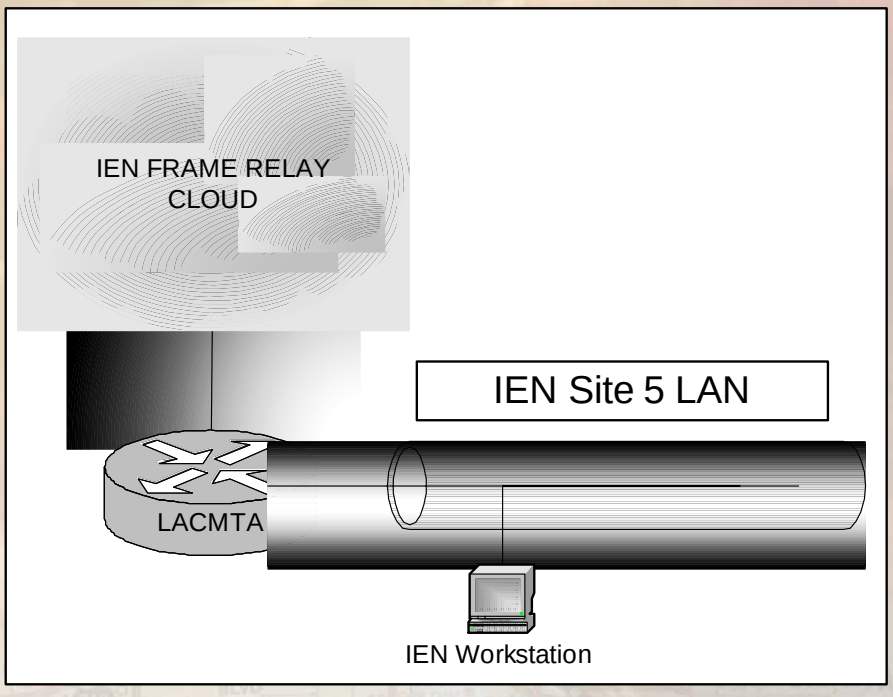
- LACoDPW hosts the SGV Corridor Server and IEN Active Directory Server.
- Two IEN Workstations have been installed in the Traffic and Lighting Division offices.

Pasadena TMC IEN Network



- Pasadena TMC connects their Series 2000 TCS to the IEN.
- An IEN Workstation and the Pasadena TMC Site/CDI Server have been installed in the TMC offices.

MTA & TransCore IEN Networks



- IEN Workstations have been installed in the LACMTA and TransCore ITS – Pasadena offices.

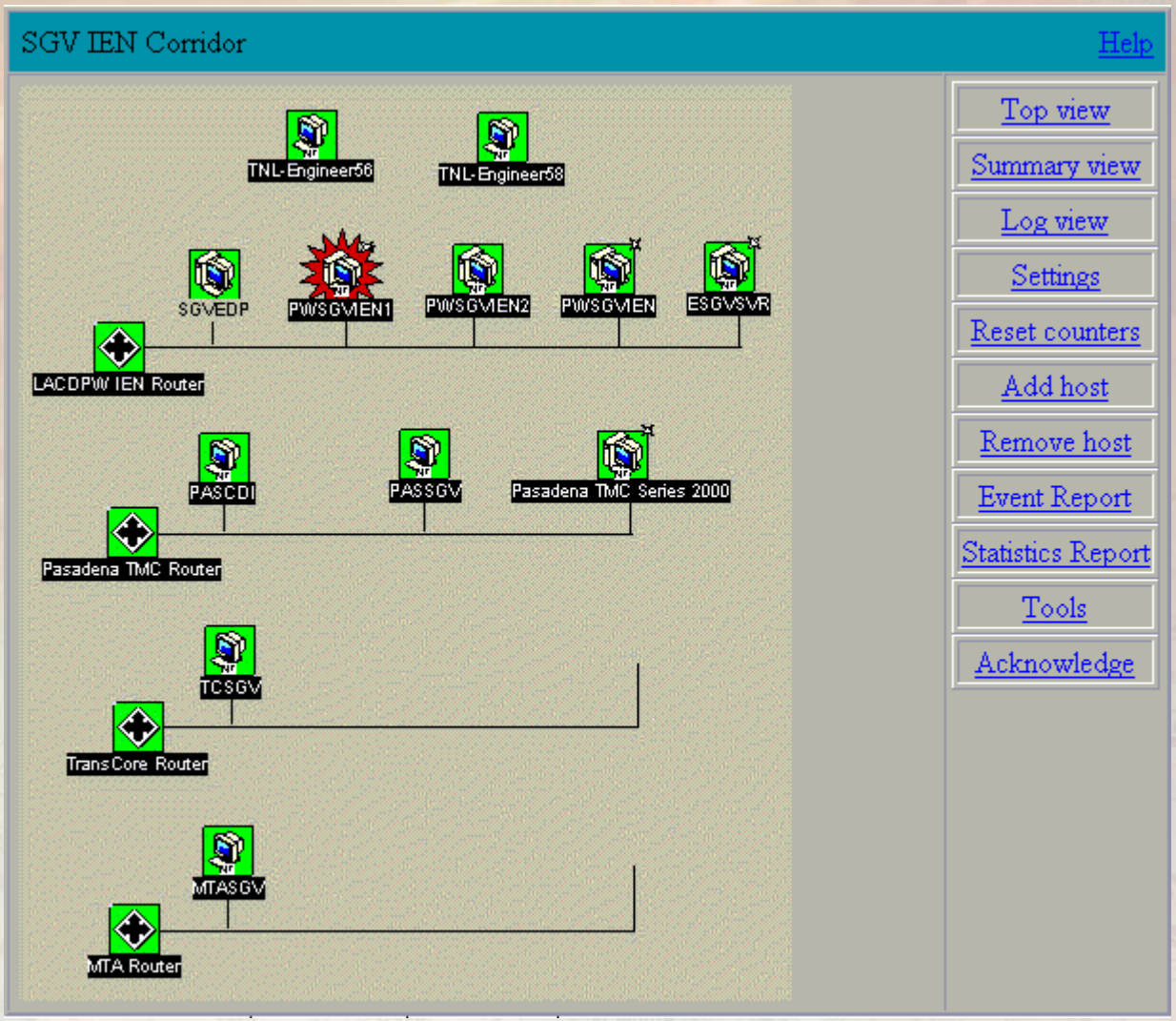
WAN/LAN Administration Tools

- The following tools are available to help pinpoint and diagnose IEN network issues:
  - WhatsUp Gold
  - IEN Component Viewer
- IEN network and system configuration information may be found in the IEN System Technical Reference Manual.

WhatsUp Gold

- *WhatsUp Gold* is a network monitoring and notification tool.
- The application monitors connectivity conditions across the IEN and can generate notifications when a device or a service goes down.
- The application provides several diagnostic utilities and views of collected network polling information.

WhatsUp Gold (cont.)



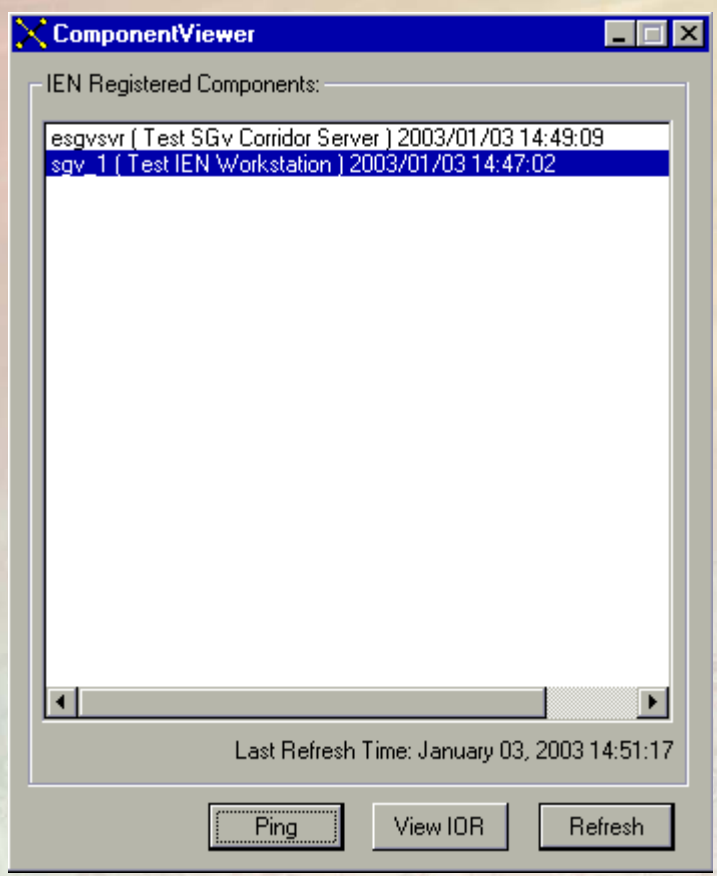
WhatsUp Gold (cont.)

- The WhatsUp Gold software is hosted on the SGVEDP system and can be accessed remotely through its web interface @ http://10.10.2.10:8000/.
- The following user accounts have been configured for the web interface:
  - Admin (pw: admin): The admin account has full access to the web interface, including the ability to modify the map components and notification configuration settings.
  - Guest (pw: guest): The guest account is able to monitor network conditions and use diagnostic tools.

IEN Component Viewer

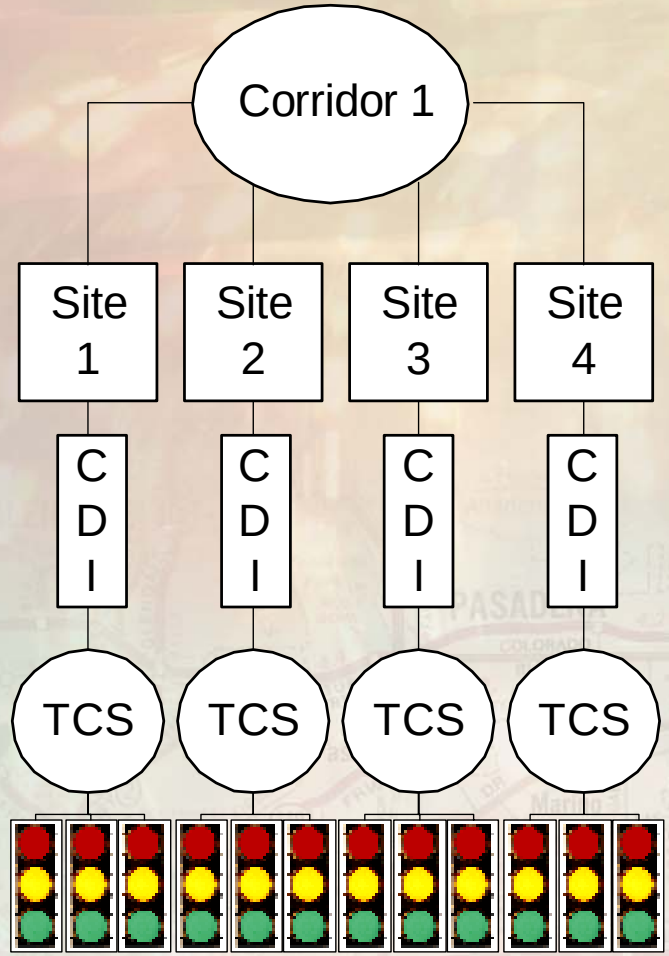
- The IEN Component Viewer indicates the status of CORBA components within the IEN.
- The Viewer lists the components that are currently registered with the Corridor Data Service and the time/date of the last status notification from each component.

IEN Component Viewer (cont.)



- Users can ping components to test connectivity and measure Return Trip Time (RTT).

IEN TCS Data Distribution



- The IEN uses CORBA to distribute TCS data around the network.
- Data is collected from local agency TCSs and propagated to Site and Corridor level processes.
- Site and Corridor processes provide data to Workstations to drive the IEN User Interfaces.

TCS Data Distribution Components

Type	Description
Command Data Interface (CDI)	Connects the IEN to a TCS or other system that provides data to or accepts commands from the IEN.
Site Server	Collects TCS data from a CDI and distributes that data to the Corridor Server and Workstations connected to the Site Server. Distributes TCS data from other agencies (received through the Corridor Server) to Workstations connected to the Site Server. Sends IEN commands for local TCS devices to the CDI.
Corridor Server	Collects TCS data from Site Servers and distributes that data to other sites within the corridor. Corridor Server components are also responsible for distributing security, scenario, and alarm data to Workstations.

TCS Data Distribution Components (cont.)

Type	Description
Workstation	Workstation components provide data to IEN User Interfaces.
Naming Service	Naming Service components maintain references to CORBA objects within the IEN to support client/server connections.

IEN User Interfaces

User Interface	Description
Alarm Viewer	Displays alarm conditions for TCS devices.
ATMS Database Administration	Provides access to the ATMS database table values.
ATMS Explorer	Allows users to construct schematic diagrams of intersections and roadway segments. Explorer diagrams can be populated with dynamic icons representing TCS field devices connected to the IEN.
ATMS Map	Provides a geographically-accurate map display with dynamic icons for intersections, links, incidents, and other types of information.
ATMS System Log Viewer	Displays event messages generated by IEN components.

IEN User Interfaces (cont.)

User Interface	Description
IEN Component Viewer	Displays the status of CORBA components within the IEN and tests connectivity between IEN systems.
IEN Scenario Manager	Allows authorized users to activate and deactivate pre-configured sets of TCS device actions.
IEN System Configuration Manager	Administration of configuration parameters, including security, database, network configuration, and TCS device configuration, and generation of printed database reports
MICE	Displays incident status information.

IEN Systems

System	Type	Location
MTASGV	Workstation	LACoMTA
PASSGV	Workstation	Pasadena TMC
PASCDI	Site/CDI Server (Site 2)	Pasadena TMC
PWSGVIEN1	Corridor/Site Server (Site 1)	LACoDPW
PWSGVIEN2	Corridor/Site Server (Site 1)	LACoDPW
SGVEDP	Domain Controller	LACoDPW
TCSGV	Workstation	TransCore – Pasadena
TNL_Engineer56	Workstation	LACoDPW
TNL_Engineer58	Workstation	LACoDPW

SGVEDP

- SGVEDP hosts the following services:
  - IEN Active Directory Services
  - IEN E-mail server
  - WhatsUp Gold host
- No IEN software components are installed on SGVEDP.

Pasadena TMC Series 2000 CDI

- Pasadena TMC Series 2000 CDI components are located on the Pasadena Site/CDI Server and Series 2000 Server.
- The CDI is responsible for collecting Series 2000 data, repackaging the data into the IEN format and passing the data to the Pasadena TMC Site Server.
- The CDI is also responsible for receiving IEN commands for Pasadena TMC devices, translating the commands into a Series 2000 format, and then issuing the commands to the Series 2000 Server.

Pasadena TMC Series 2000 CDI (cont.)

- The CDI process reads a static configuration file at startup. This configuration file specifies the devices from which the CDI will collect data.
- The CDI configuration file will need to be updated as devices are added and removed from the TCS.
- Series 2000 screens have been updated to allow Pasadena TMC staff to enable/disable IEN commands at the global and device levels.
- Pasadena TMC Series 2000 CDI operation and configuration information is provided in the IEN System Technical Reference Manual.

Pasadena TMC Site/CDI Server

- The Pasadena TMC Site Server is responsible for collecting data from the Series 2000 CDI and making that data available to local Workstations and the SGV Corridor Server.
- The Site Server process reads a static configuration file at startup. This configuration file specifies the device data sets to be distributed to other sites within the corridor.

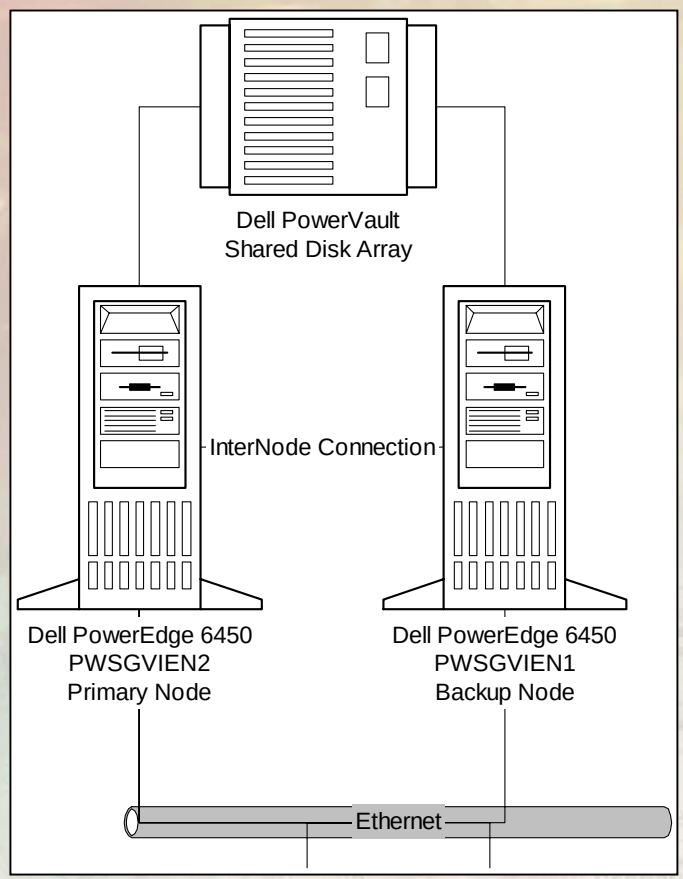
Pasadena TMC Site/CDI Server (cont.)

- The Site Server configuration file will need to be updated as devices are added and removed from the Series 2000 TCS.
- Site Server configuration information is provided in the IEN System Technical Reference Manual.

SGV Corridor Server

- The SGV Corridor Server is responsible collecting TCS data from Site Servers and distributing the data to other sites within the corridor.
- SGV Corridor Server hosts the SGV Corridor Database and other corridor-level services responsible for distributing IEN security, scenario, and alarm data to Workstations.

SGV Corridor Server Cluster



- The SGV Corridor Server cluster consists of a set of redundant server nodes that share an external disk array.
- IEN Corridor Server components can be run from either node.
- SGV Corridor Database files are located on the external disk array.

SGV Corridor Server Cluster (cont.)

- In the event of the failure of the active node, the standby node will automatically assume the responsibilities of the corridor server.
- Client systems use a single network name and IP address to access the cluster regardless of which node is currently active.
- Client connections will be disrupted for a few minutes while the standby node takes over.
- IEN client components will attempt to reconnect once the Corridor Server components become available on the secondary node.

SGV Corridor Server Cluster (cont.)

- IEN applications will post disconnection messages to the screen after a failover event has occurred.
- Users should be able to continue working after the secondary node comes online.
- In some cases the user may need to close and reopen an IEN application that was open during a failover event.

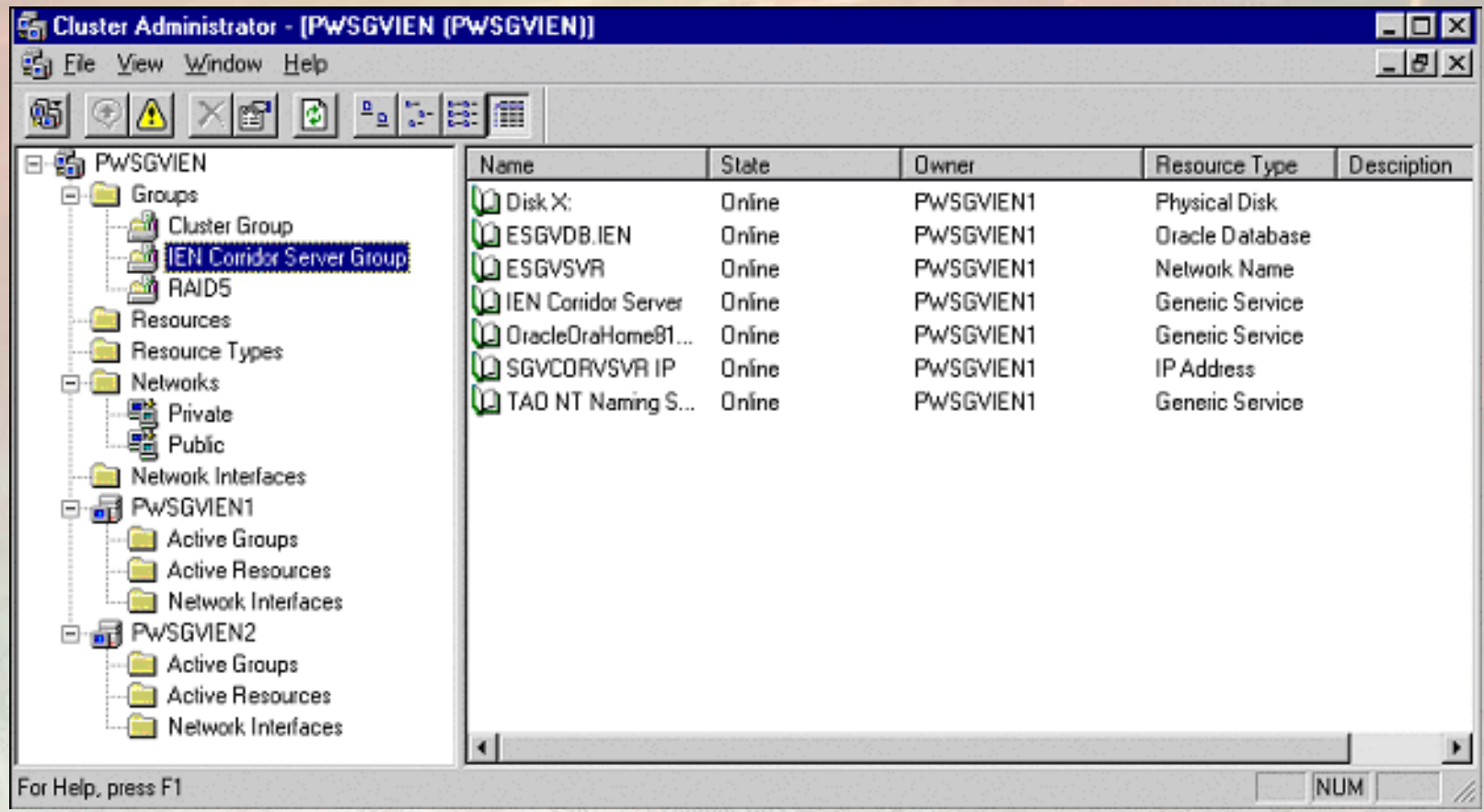
Monitoring the Status of the Cluster

1. Log onto one of the corridor server cluster nodes with a "cluster administrator" account.
2. Launch the Cluster Administrator from the Windows NT Start Menu (Start → Programs → Administrative Tools → Cluster Administrator).
3. The "Open Connection to Cluster" dialog will be displayed. Enter “PWSGVIEN” for the name of the cluster and click the **Open** button.

Monitoring the Status of the Cluster (cont.)

- In the Cluster Administrator, the left-hand browser box contains a tree-view of the components that make up the cluster.
- The right-hand browser box shows the details and status of the component(s) selected in the left-hand cluster tree.
- If a cluster node or resource is unavailable, it will be shown on the left-hand cluster tree with a red circle and slash.

MSCS Cluster Administrator



Manual Failover/Failback

- Administrators will periodically need to move cluster resources from one node to another in order to perform regular system maintenance and software upgrades.
- This process can also be used to "fail back" the cluster resources to the primary node after a failover has occurred.
- Be sure to reboot the primary node prior to a "fail back" procedure in order to reset the system within the cluster.

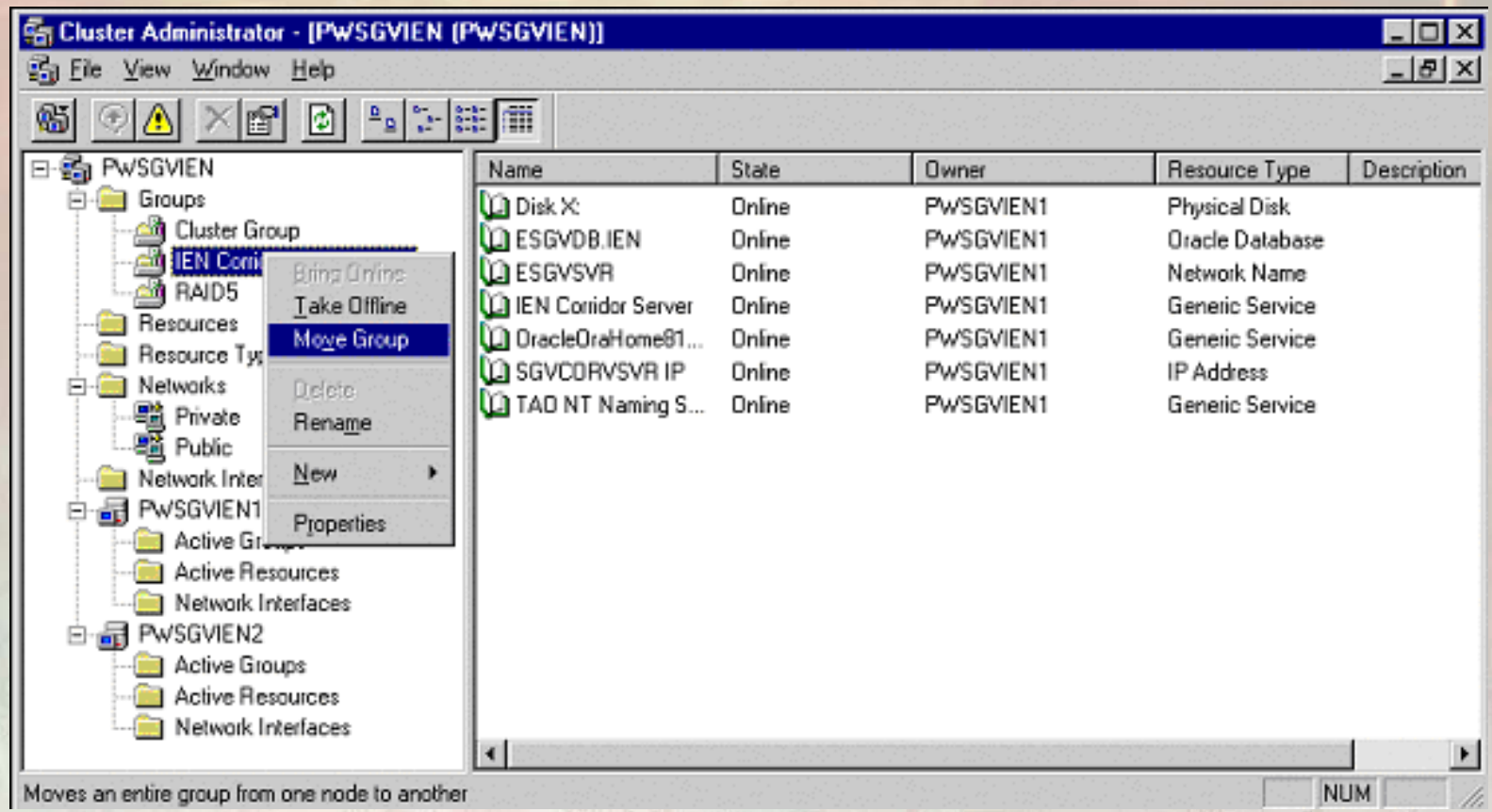
Manual Failover/Failback Procedures

1. Log onto either cluster node with a "cluster administrator" account.
2. Launch the Cluster Administrator from the Windows NT Start Menu (Start → Programs → Administrative Tools → Cluster Administrator).
3. The "Open Connection to Cluster" dialog will be displayed. Enter “PWSGVIEN” for the name of the cluster and click the **Open** button.

Manual Failover/Failback Procedures (cont.)

4. Verify the status of the receiving node prior to moving the cluster resources.
5. Move the cluster groups by right-clicking each group on the left- hand cluster tree and selecting **Move Group** from the pop-up menu.

Manual Failover/Failback Procedures (cont.)



Manual Failover/Failback Procedures (cont.)

- The right-hand browser box will show the status of the resources as they are taken offline on the first node and then restarted on the second node.
- Once the cluster resources have been moved, the empty node can be serviced without affecting the IEN software.

IEN Workstations

- IEN Workstations host the User Interfaces that are used to monitor and control TCS devices connected to the IEN.
- IEN Workstations provide access to the following:
  - TCS device status data displays
  - TCS device command interfaces
  - IEN E-mail
  - Incident tracking and management
  - Scenario management
  - IEN administrative applications

IEN Security Overview

- Security within the IEN is based on two concepts
  - Authentication
  - Access control
- Each IEN user will have a unique, password-protected user account. A valid user name and password are required in order to log onto any of the IEN systems.
- A user's access to resources and functions within the system will depend upon privileges assigned to their user account. Users will only be allowed to view the data and execute the operations for which they have the necessary set of privileges.

User Login

- The IEN takes advantage of the Windows login system to validate user account information.
- After a user logs onto a workstation, the workstation passes the security information along to the IEN.
- Users will not need to separately log onto the IEN applications.

IEN Access Privileges

- The access privileges granted to a user account determine the set of applications and functions that are available during the current login session.
- Types of privileges within the IEN:
  - ATMS domain group privileges
  - IEN resource privileges

ATMS Domain Group Privileges

- ATMS domain group privileges determine the broad level functionality available to an IEN user.
- The privileges are assigned through membership in one of four ATMS domain groups.
  - ATMS Supervisors
  - ATMS Operators
  - ATMS Editors
  - ATMS Guests

IEN Resource Privileges

- Resource privileges determine user access to resources within the IEN and the actions that the user may take on those resources.
- Resource privileges are configured within the IEN System Configuration Manager.

IEN User Administration

- IEN User administration includes the following tasks:
  - Adding/removing IEN domain user accounts
  - Assigning ATMS domain group memberships
  - Managing IEN E-mail accounts
  - Configuring IEN resource privileges

- Note: IEN administrator's will be responsible for configuring IEN resource privileges (covered in Part 1 of the IEN System Administrator's Training).

IEN Domain User Accounts

- Users must enter the name and password of their domain user account in order to log onto an IEN system.
- IEN domain user accounts are created through the Windows 2000 *Active Directory Users and Computers* console.

Adding Domain User Accounts

1. Log onto the SGVEDP system with a "domain administrator" account.
2. Launch the *Active Directory Users and Computers* consol from the Windows 2000 Start Menu (Start → Programs → Administrative Tools → Active Directory Users and Computers).
3. Right-click the "Users" directory under the IEN domain tree in the left hand browser list and select New → User from the pop-up menu.

Adding Domain User Accounts (cont.)

4. Complete the user information fields and click **Next**.
5. Enter the password for the user account and specify the password policy. Click **Next**
6. Review the new user information and click **Finish**.

Removing Domain User Accounts

1. Log onto the SGVEDP system with a “domain administrator” account.
2. Launch the Active Directory Users and Computers consol from the Windows 2000 Start Menu.
3. Select the “Users” directory under the IEN domain tree in the left-hand browser list.
4. Right-click the appropriate user account in the right-hand browser list and select **Delete** from the pop-up menu.
5. Complete the deletion by selecting **OK** on the confirmation dialog.

Configuring Domain Group Memberships

1. Log onto the SGVEDP system with a domain administrator account.
2. Launch the Active Directory Users and Computers consol from the Start Menu.
3. Select the “Users” directory under the IEN domain tree in the left-hand browser list.
4. Double-click the appropriate user account in the right-hand browser list and turn to the "Member Of" tab.

Configuring Domain Group Memberships

5. The groups that the user is currently a member of are displayed.
   - To grant membership to a group: Click the **Add** button, select the desired group in the popup window and click the **OK** button. The user will be granted the group membership.
   - To remove membership to a group: Select the appropriate group in the browser list and click the **Remove** button. Complete the confirmation dialog and the membership will be removed.

- When the user account has been configured, click the **OK** button to apply the settings and close the properties window.

IEN E-mail Accounts

- The IEN provides an internal E-mail system to facilitate communication between users at the various locations connected to the IEN.
- The E-mail system does not provide access to mailboxes located on external networks (such as the Internet).
- The *Microsoft Exchange Server* software is located on the SGVEDP system.
- Each IEN user account will be issued an E-mail account.

Creating IEN Mailboxes

1. Log onto the SGVEDP system with a “domain administrator” account.
2. Launch the *Microsoft Exchange Administrator* console from the Windows 2000 Start Menu (Start → Programs → Microsoft Exchange → Microsoft Exchange Administrator).
3. Enter **SGVEDP** for the server name and click **OK**.
4. Select the appropriate recipient container in the left-hand list tree and click the **New Mailbox** button on the toolbar.

Creating IEN Mailboxes (cont.)

4. Complete the fields found on the General tab of the Properties Window.

5. Click the Primary Windows NT Account button. Select the appropriate option ...

   - **Select an existing Windows NT account** opens the "Add User or Group" dialog window. Select a user account or group in the browser window and click the **Add** button. The name will be displayed in the "Add Name" field. Click **OK** to return to the "Mailbox Properties" window.
   - **Create a new Windows NT account** opens the "Create Windows NT Account" dialog window. The "NT domain" and "Account name" fields are filled in automatically. Click **OK** to create the new account and then **OK** again to clear the password reminder message and return to the “Mailbox Properties” window.

IEN Backups

- Backups are primarily taken to safeguard against unexpected failures resulting in loss of data. If such a failure occurs, data can be re-constructed using a backup.
- IEN configuration and application related data is almost solely maintained on the SGV Corridor Server Cluster. IEN Workstations are able to reconstruct local copies of configuration data by synchronizing with the Corridor Server over the network.
- Example backup and restore procedures are provided in the IEN System Administrator's Guide.

Key Files to Back Up

System	Key files
IEN Workstations	- Locally maintained user-generated files (as needed). - Files contained in the C:\Program Files\TransCore directory.
Pasadena TMC Site/CDI Server	- Files contained in the C:\Program Files\TransCore directory.
SGV Corridor Server Cluster	- SGV Corridor Database files located in the X:\IEN directory. - Files contained in the C:\Program Files\TransCore directory. - PWSGVIEN cluster quorum located on drive Z. - ATMS Streets Database located in the D:\ATMSStreetsDatabase directory on PWSGVIEN2. - ATMS Explorer Diagrams located in the Y:\ATMSStreetsDatabaseRepository directory.
SGVEDP	- Active Directory directory service data and files located on drive C. - IEN Exchange Server files located on drive C.

Corridor Server Backups

- The SGV Corridor Server Cluster hosts several critical components that will need to be backed up on a regular basis. The use of clustered servers and fault tolerant disk arrays is intended to further reduce the likelihood of data loss.
- The SGV Corridor Database is implemented as an Oracle 8i Relational Database. The SGV Corridor Database files are located in the X:\IEN directory.

Corridor Server Backups (cont.)

- Corridor level components of the IEN architecture are hosted on the SGV Corridor Server. A number of processes read configuration files during initialization. By default these files are stored in the C:\Program Files\TransCore directory.
- The SGV Corridor Server makes the following directories available to client systems on the IEN network to support the IEN User Interfaces:
  - The ATMS streets database located in the Y:\ATMSStreetsDatabase directory.
  - The central ATMS Explorer Diagram Repository is located in the Y:\ATMSStreetsDatabaseRepository directory (IEN Workstations maintain local copies of the diagrams stored in the repository).

Corridor Server Backups (cont.)

- The SGV Corridor Server Cluster does not include a backup device. Backups will be performed to a device located on the LACoDPW network.
- It is expected that a COTS backup system to automate the process.

Workstation Backups

- Since no critical IEN data is maintained on workstations, the main purpose of workstation backups would be to limit down time in the event of a system failure and to preserve locally generated map views and diagrams.
- By default these files are stored in the C:\Program Files\TransCore directory.
- Each IEN Workstation includes a CD-writer drive. Selective backups can be performed using the CD Writing software provided with the system.
- System backups can be performed using a COTS (Commercial Off The Shelf) imaging application such as Power Quest Drive Image.

Pasadena TMC SITE/CDI Server Backups

- Similar to an IEN Workstation, data is not maintained on the Pasadena TMC Site/CDI Server.
- The main purpose of a backup would be to preserve modifications made to the Site Server's configuration file.
  - C:\Program Files\TransCore \Site2Svr.cfg.
- The Pasadena TMC Site/CDI Server includes a CD-writer drive. Selective backups can be performed using the CD Writing software provided with the system.
- System backups can be performed using a COTS (Commercial Off The Shelf) imaging application such as Power Quest Drive Image.

SGVEDP Backups

- The SGVEDP system functions as the Active Directory and E-mail server for the IEN. Backups of Active Directory directory service data and Exchange Server files will need to be performed.
- The SGVEDP Server does not include a backup device. Backups will need to be performed to a device located on the LACoDPW network.
- While the Windows 2000 Operating System does include a native backup utility, it is expected that a more robust COTS backup system will be used to automate the process.

Troubleshooting Connections

- Due to the distributed nature of the IEN and the use of relatively slow network links, it is anticipated that IEN client/server connections will periodically be broken.
- IEN client and server components will attempt to reconnect in the event of a disconnection.
- Disconnections may result in a disruption of IEN software components such as User Interfaces and the TCS data distribution subsystem.

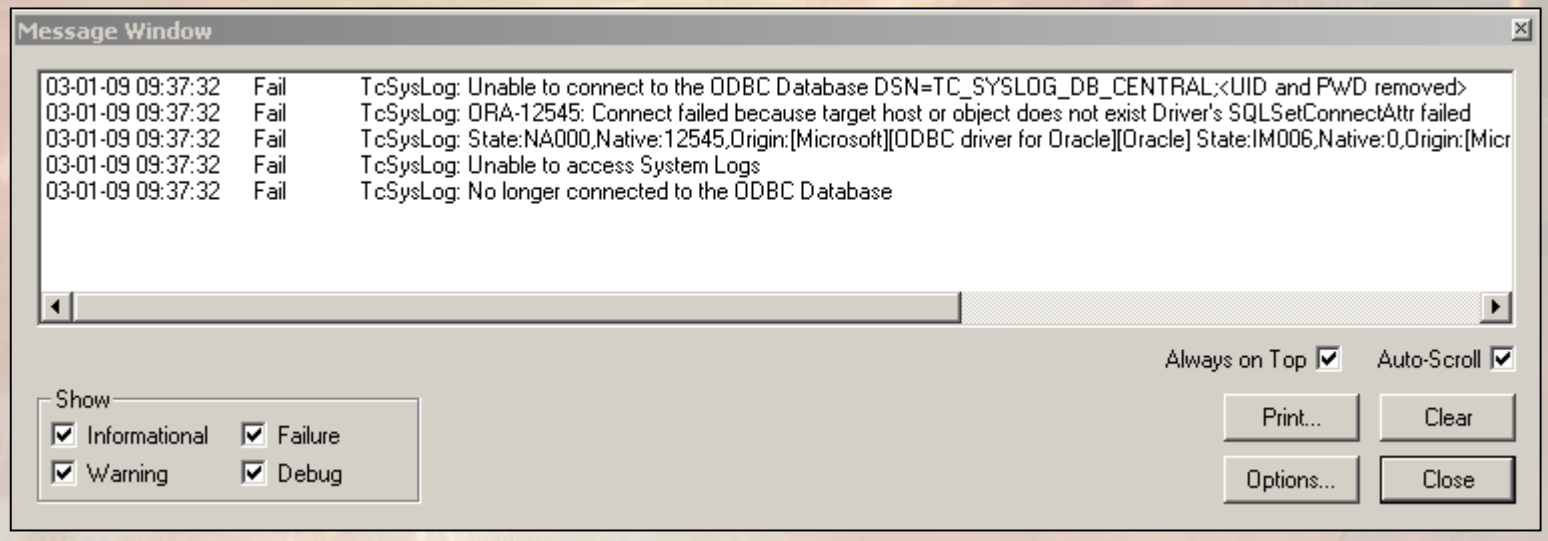
Troubleshooting Connections (cont.)

- IEN software components should automatically recover in the event of short-term disconnections.
- Users may need to clear error messages and in some cases close and restart User Interfaces.
- Longer-term disconnections may require user intervention to reset client or server side components.

Checking IEN Error Messages

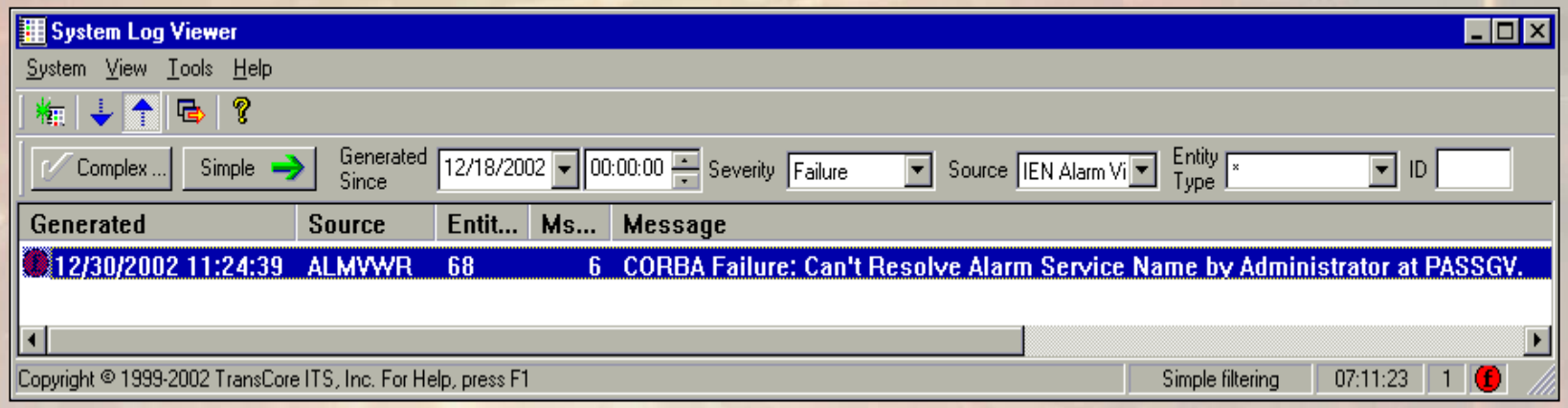
- IEN applications and subsystem components log detailed error information, including the source and action that generate the error.
- Error messages are output to the following locations:
  - TcMessageWindow
  - System Log
  - Component-specific log files

TcMessage Window



- The TcMessage Window is used by IEN applications and underlying components to display debug, informational, failure, and warning messages to users.

System Log



- Errors and other types of messages are written to the System Log.

Component Log Files

- INFO: 2002-12-23 10:35:41 (2200) (AlarmSvr::initConfig) Read from Configuration File c:\Program Files\TransCore\CorridorSvr.cfg
- INFO: 2002-12-23 10:35:41 (2200) (AlarmSvr::initConfig) CorridorID Set to 1
- INFO: 2002-12-23 10:35:42 (2200) (AlarmSvr::initCorba) CORBA ORB Initialized
- INFO: 2002-12-23 10:35:42 (2200) (AlarmSvr::initCorba) Resolved Root POA
- INFO: 2002-12-23 10:35:42 (2200) (AlarmSvr::initCorba) Resolved CORBA Naming Service
- INFO: 2002-12-23 10:35:42 (2200) (CorridorAlarm::init) CorridorAlarm Interface Registered with Root POA
- INFO: 2002-12-23 10:35:42 (2200) (CorridorAlarm::publishCorridorAI) CorridorAlarm Interface Published
- ERROR: 2002-12-23 10:35:49 (2200) (CorridorAlarm::initEntityMap) Could not read entities of type INTERSECTION from database. Error -2147220988

- IEN client/server components output detailed status messages to log files located in the C:\Program Files\TransCore directory.

Workstation Data Service Status Indication

- The workstation data service status icon, located in the system tray of IEN Workstations, indicates whether or not the local Workstation Data Service is receiving data from its Site Server.
  - A green indication means that the Workstation Data Service is receiving TCS data correctly.
  - A red indication means that the Workstation Data Service cannot connect to it's Site Server.
  - A black indication means that the Workstation Data Service is running and connected but not receiving updated data.

Reinitializing the IEN Naming Service

- Each machine within the IEN runs a local instance of the IEN's CORBA Naming Service. The Naming Service contains references to CORBA objects within the network.
- Client processes will not be able to locate server processes on the network if references within the local naming service are lost, outdated, or corrupted.
- The local naming service can be reinitialized from the Start Menu (Start → Program Files → Information Exchange Network → Administrative Tools → Initialize IEN Naming Service).

What's Next for the IEN?

- Connecting other local agencies.
- Adding support for other types of devices such as CCTV, VMS, and HAR.
- Implementation of the regional components of the IEN architecture.
- Sharing data with other regional systems such as Showcase.

IEN Administrator's Training Wrap Up

Questions &
Answers