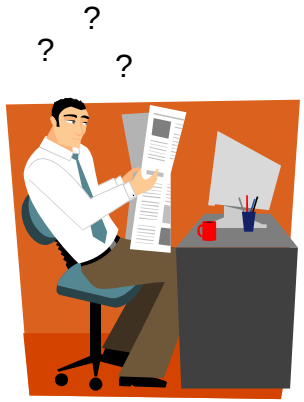
INTERNET2®

Diagnostic Perspectives

From the end-user's view



Workstation Centric:

- The performance of my workstation seems slow!
- The network is down!
- The network is slow?

Application centric:

- I can't open or launch the application!
- I can't authenticate with the application!
- The application says I'm not authorized to use it!
- The application is behaving inconsistently!
- The application is giving errors!
- I can't use all the features of the application!
- The application's performance is poor!

From the help desk's view

Workstation Centric:

- Does the user have the correct version and configuration?
- Can the user connect to the network and if so, what is their performance?
- Security problem? E.g. Botnet, virus, worm, other compromise?
- Is the user having a hardware problem?

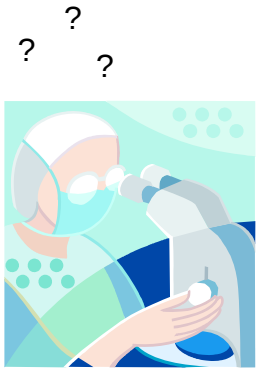
Infrastructure centric enterprise based:

- Can the user get to key local services? E.g. DHCP, DNS, SMTP, POP/IMAP, NTP, Authn, etc
- Can the user get to key external services?.
- Are these services operating properly?

Application centric:

- Vital Signs – "Is the applications basic functionality working?"
    - Authn: "can the user log in?"
    - Authz: "what are the user's privileges?"
- Highly focused – "Is a specific feature of the app working?"

From the diagnostician's view



Network Centric:

- Is there an connectivity problem between the user and the application?
- Could there be a routing or firewall problem?
- Is the performance or loss of the network at an acceptable level?

Service Centric:

- Are the lower, upper, and middleware services that the end user is dependent upon functioning within an acceptable level and can they get to them?
- E.g. DHCP, Authn, Authz, DNS, NTP, Email, VPN, Web, etc.

Application Centric:

- Does the application have enough critical resources?
- Is the application reporting any internal or external errors?
- Are the lower, upper middleware and services that the application is dependent on functioning an expectable level?
- What about any external services that the application needs?

From the CIO's view

Business centric:

- Are my customers being serviced properly?
- How is the infrastructure operating?

Finance centric:

- What do and will I need to spend resources on?
- Is my staff's time being used effectively?
- What is the growth in specific areas?

Compliance centric:

- Are our diagnostic procedures consistent with our security and privacy policies?
- Are we in compliance boundaries for
  - Processes and procedures
  - Legal issues

The end-user's needs

Workstation centric tool that:

- Verifies basic hardware operation
- Reports on software versions and any internal errors
- Reports on network connectivity and performance
- Verifies that key network services are available
- Scans system for security external and internal security vulnerabilities
- Publishes results to diagnostic backplane

Application centric tools that:

- Verifies that the user has the correct resources
- Conforms a baseline of functions to the user. E.g. what can the user do and a test to prove to them that they can
- Provides ways for users to tag errors at any phase of the applications operation and publish them to the diagnostic backplane

The help desk's needs

Workstation centric tool that verifies the users:

- Baseline software and hardware configuration
- Network connectivity and performance
- Key network services are available (DHCP, DNS, NTP, Authn/Authz etc.)

Service centric enterprise based tools:

- Testing enterprise base services (DNS, SMTP, POP/IMAP, NTP, Authn, Authz, etc.) from the perspective of the user
- Querying the infrastructure about internal and external problems
- The ability to share diagnostic information with internal groups

Application centric tools:

- Real-time views into the application as the user is operating
- Medium depth tools verifies the operation of the application and its supporting services
- The ability to share diagnostic information with external groups

The diagnostician's needs

Network Centric Tools:

• Forensic tools that query the infrastructure about internal and external connectivity problems

• Active testing tools that perform network tracers at specific intervals and report anomalies into a reporting infrastructure

Service Centric Tools:

• Highly focused passive and active lower, upper, and middleware diagnostic tools that report anomalies

• Forensic tools that query detailed events of key services using their logs and other means

Application Centric Tools:

• Verification that the application has the correct resources

• Highly focused tests into specific features and modules

• The ability to share detailed diagnostic information to the developer in near real-time

The CIO's needs

Business centric:

- Reporting on help desk problems and resolution
- Reporting on infrastructure health

Finance centric:

- Anomaly and problem event reporting
- Reporting infrastructure growth

Compliance centric:

- Security event reporting
- Reporting that specific processes are being done

Enabling other Efforts and Tools

Diagnostic assistance is provided through the system in several ways:

- Existing diagnostic tools have been or can be fitted with EDDY normalizers and translators to join into the backplane and make their data available to other applications or to specific help desk/service personnel.
- Applications can be fitted with similar EDDY normalizers to inject their error logs and diagnostic information into the Backplane.
- Existing diagnostic tools can be enriched though access to additional diagnostic data through tapping into other sources of information within the backplane.
- New diagnostic consoles can be developed and assembled from components that access and analyze the rich resources on the backplane.
- Applications can utilize diagnostic data at lower levels of the protocol stack and present better information to users about problems in access or performance.
- The diagnostic capabilities can be positioned to provide audit mechanisms as well.

This material is based upon work supported by the National Science Foundation under Grant No. 0330626, Carnegie Mellon University, and Internet2. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.