Hardware Specifications
for the
Network Backbone Architecture

NCC98 LAN Upgrade

2-12-97

Outline:
1) General Hardware Requirements
   A) Standards, Protocols and Physical Layer
   B) Architectural Features
   C) Features, Functions, Configuration
2) Security
3) Redundancy
4) Network Management
5) Scalability
6) Stability/Customer Support

1) General Hardware Requirements:

A) All network hardware components must support IEEE 802.3 and all it's inherent subclasses (e.g., 802.3u, Fast Ethernet). All component interfaces must support 10BaseT/F and 100BaseTX/FX (full-duplex desirable) for use with shielded twisted pair (STP) cabling or standard multi-mode fiber as required. Additionally, support for FDDI and/or ATM expandability is a plus.

B) The network hardware components shall employ or support compatibility with (as in hubs) switching architecture consisting of the following features: packet (or cell) forwarding employing "store and forward" methodology, full-duplex port capability, and a minimum of 1024 MAC addresses per port. The following architectural features are left to the discretion of the OEM (although written specs must be obtainable): switching fabric (cross-point, shared media or memory) and its inherent bandwidth, buffering per port, and congestion control functions.

C) Required features, functions, and configuration capabilities are as follows:

a) Configuration - expandable, cascadable, and/or modular with all components having hot-swappable, fault tolerant capabilities including power supplies

Hardware Specifications
for the
Network Backbone Architecture

NCC98 LAN Upgrade

2-12-97

Outline:
1) General Hardware Requirements
   A) Standards, Protocols and Physical Layer
   B) Architectural Features
   C) Features, Functions, Configuration
2) Security
3) Redundancy
4) Network Management
5) Scalability
6) Stability/Customer Support

1) General Hardware Requirements:

A) All network hardware components must support IEEE 802.3 and all it's inherent subclasses (e.g., 802.3u, Fast Ethernet). All component interfaces must support 10BaseT/F and 100BaseTX/FX (full-duplex desirable) for use with shielded twisted pair (STP) cabling or standard multi-mode fiber as required. Additionally, support for FDDI and/or ATM expandability is a plus.

B) The network hardware components shall employ or support compatibility with (as in hubs) switching architecture consisting of the following features: packet (or cell) forwarding employing "store and forward" methodology, full-duplex port capability, and a minimum of 1024 MAC addresses per port. The following architectural features are left to the discretion of the OEM (although written specs must be obtainable): switching fabric (cross-point, shared media or memory) and its inherent bandwidth, buffering per port, and congestion control functions.

C) Required features, functions, and configuration capabilities are as follows:

a) Configuration - expandable, cascadable, and/or modular with all components having hot-swappable, fault tolerant capabilities including power supplies

b) All chassis based components shall be rack or shelf mountable within standard 19" equipment racks
c) Fault tolerance at every level is mandatory due to the critical use of the network. Each module shall be stand-alone. Support of IEEE 802.1d (Spanning Tree protocol) or a similar vendor unique methodology is indicated specifically (refer to Section 3 for more details concerning redundancy).
d) Support for Virtual LAN (VLAN) segmenting
e) Support for standards-based SNMP management
f) In-band/out-of-band management (CLI/SNMP/SLIP) ports

Requested (not required, but desirable) features, functions, and configuration capabilities are as follows:

a) Packet filtering based on source/destination MAC and/or IP address, protocol type, broadcast/multicast exceeding a preset threshold
b) Port mirroring/traffic replication or a similar vendor specific methodology for use in protocol analysis/sniffing
c) Network management software which integrates a graphical user interface, logical menu structure, and requires minimal training.see Section 4 for more details
d) Multiple VLAN memberships with varying criteria based on port, MAC address, IP address, protocol type or any other possibilities
e) Support for RMON agents per RFC 1271

2) <u>Security:</u>

The network hardware components will be used in a "sensitive data" type environment with at least two distinct levels of data sensitivity. The users with access to the less sensitive level must not be allowed access to the more sensitive data in the other level, although the two levels of data can co-exist in the same network environment (i.e., reside on the same backplane, wire etc.). Therefore, sufficient security measures must be undertaken to effect this policy and the network hardware components must at least allow for this policy to be enforced if not support it through built-in security provisions (such as packet filtering, etc.). NCC Security requirements/guidelines defines *communications security as "protection of electronically transmitted information from unauthorized access, disclosure, acquisition, manipulation, modification, and loss during the communications process."*

The following issues/questions must be addressed by the vendor:

A) How is the component's configuration (i.e., what node is switched where, or individual node segmentation, or IP address of the component, etc.) affected by device, module, or component failure?

B) What could prevent an unauthorized switch configuration due to either i) human error, or ii) a module or component failure?
An unauthorized switch configuration would be defined as allowing a node without access to sensitive data to have access to the sensitive data through switching or segmentation.

C) What feedback is given to the network manager upon making configuration changes to allow for verification?

D) If a network hardware component can be managed remotely (SNMP/SLIP/Telnet), what precautions are taken to ensure that only authorized manager(s) are given access (e.g., passwords or other forms of authentication, password encryption)?

E) What forms of warning are available to the network manager to indicate the presence of an unauthorized intruder, connection violation, or breach of security?

F) Are there any methods to assign security to a particular VLAN such that traffic from this VLAN would be prohibited/allowed access to a different VLAN based on its security level assignment. What procedures (alarms, etc.) would alert the network manager that traffic from a non-secure VLAN had attempted to violate a secure VLAN segment?

3) <u>Redundancy:</u>

Due to the critical nature (24 x 7) of the data that the NCC LAN supports, full network redundancy and fault tolerance is mandatory. All modules and network hardware components must be hot swappable so as to ensure full traffic functionality in a short enough time span based on the following calculations:

$$\text{Network Availability:} \quad \frac{\text{MTBF}}{\text{MTBF} + \text{MDT}} >= 0.9990$$

MDT: Mean Down Time = Realization Time + Access Time + Diagnosis Time + Replacement Time

As a general rule of thumb, no single “critical” component may be down for longer than 15 minutes. All LAN backbone hardware such as switches, hubs, and cabling are designated as critical. Components (switches, hubs) whose modules can function as stand-alone units with respect to traffic forwarding and not have to rely on another module (such as a management module) for throughput are highly desirable.

At the least, redundancy should be supported by use of IEEE 802.1d (Spanning Tree protocol) in order to provide for the control of active loops such that switches could be employed in parallel with redundant trunks and feeder links to switching supportive hubs (or similar components). Other vendor unique

solutions (such as link state protocols) will be reviewed and any supporting documentation such as “white papers” are welcome.

4) Network Management:

The network management software for the network hardware components should be able to reside on a UNIX platform (HP-UX, currently running 10.20)) with a GUI interface. It should be compatible with Hewlett Packard Open View Network Node Manager for HP-UX (Version 4.1). It should support a client/server architecture. It should allow for remote management and provide sufficient security features for this support such as password protection or authorization. Additionally, it should provide for full functionality and manageability of the hardware’s supported VLAN features. (Support for RMON agents as defined by RFC 1271 and MIB (II) functionality is desired but not required.)

5) Scalability:

Current network architecture supports two separate subnets (sensitivity level A and sensitivity level B) consisting of approximately 60 nodes each with all nodes connected via shared segment ethernet hubs with each hub’s uplink connected to a NASA designed cross-point matrix switch. The network hardware components should support scalability on a node level basis (<200 nodes presently) for both ethernet and fast ethernet as a requirement. Support for FDDI and ATM is desired for potential future applications and bandwidth demands.

6) Stability/Customer Support:

Due to the generally volatile financial state and aggressive growth philosophy of the original equipment manufacturers (OEMs) within the networking products industry, company stability must be considered as buyouts and mergers have been flagrant recently. This can lead to product obsolescence, lack of future support, and unavailability of replacement/spare parts. Thus, in order to increase the potential longevity of the backbone architecture and diminish the possibility of a chosen component becoming obsolete, only core component (switches, hubs) OEMs with annual revenues greater than one billion US dollars will be considered for evaluation.*

Customer support should be able to support network administrators and maintenance personnel on a 24x7 basis. Adequate sparing levels will be maintained for all network hardware components, although a rapid replacement program (next day replacement upon obtaining RMA #) is desired for component failures within at least the first year of operation. After one year, sufficient maintenance contracts may be required. Documented details of same are requested from the vendor. The useful technological life for this implementation is projected to be 3 to 5 years. This is based on the advancement in LAN

component technology within the past 3 to 5 years and technology forecasts for the next 3 years.

*****This information is based on data available at the web site for Strategic Networks Consulting (an independent, 3rd party testing/consulting firm for the networking industry) and is current as of August 1996. Five vendors meet this criteria, they are listed by market share: Cisco, 3Com, Bay Networks, IBM, and Cabletron.