The Application-Driven Enterprise Network

Diane Schmidt
Director, Ethernet Switching & WLAN
May 12, 2004
Agenda

• The Changing Enterprise Applications Environment
• Resulting “convergence” of technologies
• Impact on Infrastructure Design
  – Availability
  – Security
  – Management
  – Flexible Application Delivery
• Summary
Trends Driving Changes in Enterprise Networks

• Online collaboration
• Increasing number and variety of devices requiring higher bandwidth
• Increased security requirements
• New applications introducing new traffic patterns
The Emerging Enterprise Applications Model

Converged communications improve productivity while lowering cost
Technology enablers

**Internet Protocol (IP)**
The foundation for networking

**Extensible Markup Language (XML/VXML)**
Universal format for data and voice exchange
- Speech recognition and conversion become easy extensions to Web applications

**Session Initiation Protocol (SIP)**
Enables the application to dynamically adapt to the device you’re currently using

**Web Application Middleware**
(J2EE & .Net) provide standard interfaces to Enterprise business systems
Conceptual Network Model for Converged Applications
Convergence(s)

Convergence is not a singular event, it operates on multiple simultaneous planes, each with its own drivers, impacts, risks and rewards………..

- Protocol Convergence
- Infrastructure Convergence
- Application Convergence
Optical/Ethernet/IP
Convergence = Simplification

Layer 4-7 Added Value
Security
IPv4 and IPv6
Ethernet
Copper | Fiber | Wireless

- Enterprise Edge
- Campus Core
- Wiring Closet
- Data Center
- Wireless
- Security AAA
- DMZ Services
- VPN
- Multi-service Edge
- MPLS/GMPLS
- Subscriber Management
- etc.
Converging the Infrastructure

Today

- Multiple separate networks
- Disparate services
- Different Characteristics

Converged

- Single Infrastructure
- Highest Common Characteristics
- Common Services

<table>
<thead>
<tr>
<th>Characteristics</th>
<th>Reliability</th>
<th>Pkt Loss</th>
<th>Latency</th>
<th>Bandwidth</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>M-H</td>
<td>M</td>
<td>M</td>
<td>H</td>
</tr>
<tr>
<td></td>
<td>H</td>
<td>L</td>
<td>L</td>
<td>L</td>
</tr>
<tr>
<td></td>
<td>L-M</td>
<td>L-M</td>
<td>M-H</td>
<td>H</td>
</tr>
<tr>
<td></td>
<td>H</td>
<td>L</td>
<td>L</td>
<td>H</td>
</tr>
</tbody>
</table>

Today Converged Characteristics

Reliability: M-H, M, M, H
Packet Loss: M, L, L, L
Latency: M, L, L, H
Bandwidth: H, L, L, H
Application-Optimized Converged Networks

• Attributes
  – Resilient infrastructure
  – Secure communications
  – Policy-based traffic management
  – Flexible delivery of application services

• Value Proposition
  – Provides the foundation for supporting multimedia applications that improve productivity and increase revenues through innovative communication services
  – Unprecedented flexibility
  – Uncompromised resiliency, security and performance
Availability Requirements

Typical Infrastructure
99.95 – 99.85
4-8 Hours Per Year
Availability Requirements

Resilient Application-Optimized Infrastructure
99.995 – 99.993
25-40 min per year
Security Implications of Converged Applications

- Combat threats in the IP world
  - Theft of service
  - Disruption of service
  - Eavesdropping
- Support and inspect new protocols
  - H.323
  - Session Initiation Protocol (SIP)
  - XML
- Ensure application quality by removing traffic delays
  - Quality of Service
  - Low latency inspection and forwarding
  - Find the shortest path
  - Fast fail-over

Security is an often overlooked, but essential, item in a Application-oriented infrastructure plan.
Managing Application Performance and Security

Proactive Voice Quality Management

Manage scalable IP Telephony deployments with tools that ensure quality, performance, and reliability.

Manage infrastructure security with tools that support policy-based provisioning, password control, disaster recovery, virus protection, and audit compliance.
## Flexible Delivery of Application Services using Layer 4-7 Services

<table>
<thead>
<tr>
<th>Content Intelligence</th>
<th>Server Load Balancing</th>
<th>Application Redirection</th>
<th>Advanced Filtering</th>
</tr>
</thead>
<tbody>
<tr>
<td>Layer 7 Inspect</td>
<td>Application LB</td>
<td>Web Site</td>
<td>Layer 2-7 Attributes</td>
</tr>
<tr>
<td>Cookie, URL, HTTP Header</td>
<td>Global Server LB</td>
<td>Cache</td>
<td>VLAN Filtering</td>
</tr>
<tr>
<td>User Agent (PDA, Browser)</td>
<td>Application Health Checks</td>
<td>Web Services</td>
<td>Accept, Deny, NAT, Redirect</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>DoS Attack Prevention</td>
<td>Bandwidth Mgt.</td>
<td>Source IP</td>
<td>Firewall / VPN / IDS</td>
</tr>
<tr>
<td>Application Abuse Protection</td>
<td>Peer-to-peer applications mgmt</td>
<td>Cookies</td>
<td>WAN Links</td>
</tr>
<tr>
<td>SSL Acceleration &amp; VPN</td>
<td>ToS Marking</td>
<td>SSL Identifier</td>
<td>WAP Gateways</td>
</tr>
</tbody>
</table>

- **Flexible Delivery of Application Services**
- **Using Layer 4-7 Services**
- **Content Intelligence**
  - Layer 7 Inspect
  - Cookie, URL, HTTP Header
  - User Agent (PDA, Browser)
- **Server Load Balancing**
  - Application LB
  - Global Server LB
  - Application Health Checks
- **Application Redirection**
  - Web Site
  - Cache
  - Web Services
  - Streaming Media
- **Advanced Filtering**
  - Layer 2-7 Attributes
  - VLAN Filtering
  - Accept, Deny, NAT, Redirect
- **Embedded Security Svcs**
  - DoS Attack Prevention
  - Application Abuse Protection
  - SSL Acceleration & VPN
- **Intelligent Traffic Management**
  - Bandwidth Mgt.
  - Peer-to-peer applications mgmt
  - ToS Marking
- **Persistence Support**
  - Source IP
  - Cookies
  - SSL Identifier
- **Network Device Load Balancing**
  - Firewall / VPN / IDS
  - WAN Links
  - WAP Gateways

- **Flexible Delivery of Application Services using Layer 4-7 Services**
- **Content Intelligence**
  - Layer 7 Inspect
  - Cookie, URL, HTTP Header
  - User Agent (PDA, Browser)
- **Server Load Balancing**
  - Application LB
  - Global Server LB
  - Application Health Checks
- **Application Redirection**
  - Web Site
  - Cache
  - Web Services
  - Streaming Media
- **Advanced Filtering**
  - Layer 2-7 Attributes
  - VLAN Filtering
  - Accept, Deny, NAT, Redirect
- **Embedded Security Svcs**
  - DoS Attack Prevention
  - Application Abuse Protection
  - SSL Acceleration & VPN
- **Intelligent Traffic Management**
  - Bandwidth Mgt.
  - Peer-to-peer applications mgmt
  - ToS Marking
- **Persistence Support**
  - Source IP
  - Cookies
  - SSL Identifier
- **Network Device Load Balancing**
  - Firewall / VPN / IDS
  - WAN Links
  - WAP Gateways

---

**Page 15**
Layer 4-7 Services in Action: Intelligent Peer-to-Peer Management

Customer Challenges
- > 60% of the Internet traffic is Peer to Peer (P2P) traffic (Kazza, Kazza v2, eDonkey, Morpheous, iMesh, etc.) [NetworkWorld 7/03]
- New P2P protocols use dynamic port hopping, evading standard ACL rate limiting & first generation Bandwidth Management
- University, cable MSO, and ISPs see serious QoS and financial impacts.

The infrastructure controls the application by:
- Switch inspects and identifies P2P protocols irrespective of ports used
- Once identified P2P traffic can be blocked, rate limited or shaped
- Multi-tiered rate limiting/shaping allows one aggregate community limit and multiple sub-tier limits for individual users
- Time of Day Bandwidth Management
Customer Challenges

• Proliferation of Web Services brings big benefits for application integration with 3rd parties, but security concerns are increase
• SOAP packets flow on port 80 (security, identification challenges)
• How do I scale Web Services?
• A single Web Services request can spawn as many as 10 other requests

The infrastructure improves and secures application delivery by:

• Inspects and identifies Web Services protocols (SOAP, XML, etc.)
• Once identified application traffic can be accelerated, redirected or load balanced
• Web Services traffic can be secured by encrypting with SSL
Layer 4-7 Services in Action: Resilient IP Telephony

Customer Challenges
- VoIP networks require 5 x 9's uptime
- SIP Proxy server is the ‘brain’ of the VoIP networks
- Must ensure redundancy, reliability, utilization and effective use of processing power

The infrastructure improves application resiliency and delivery by:
- Front end SIP Proxy Load Balancing
- Ensures persistence based on the call ID in the SIP protocols
- Secures Proxy with wire speed NAT and filtering to ensure absolute minimum latency in VoIP networks
- SIP Proxy application level Health checking
- Offloads SIP proxy need to respond to SIP client health/info pings
- SSL acceleration secures VoIP
The Future of Enterprise Communications

Applications and services
- People are names; calls are URLs
- Services available anytime, anywhere
- Much simplified user interfaces
- Convergence of voice, data, and video

Application-optimized infrastructure for IP data, telephony and multimedia

Infrastructure – Optimized for Applications
- Resilient
- Secure
- Policy-based traffic management
- Flexible delivery of application services