NRIC VI FG4
Broadband

Report for December 5th 2003

Network Reliability and Interoperability Council
Network Reliability and Interoperability Council

FG4 Participation

Logos of various companies and organizations.
"The Committee will make recommendations to ensure the compatibility and deployment of Broadband technologies and services, and will evaluate the need for improvements in the reliability of Broadband technologies and services."
Accomplishments

Four White Papers
- Concepts of Broadband
- Access / Onramp
- Service Transparency
- Traffic Policy / Traffic Management

13 Recommendations
Concepts of Broadband

NRIC VI, Focus Group 4
Focuses on the ever-evolving definitions of Broadband

What exactly is Broadband?
Always on?

Speeds?
Throughput?
Goodput?
It seems that some days everyone has an opinion.
Concepts of Broadband

Throughput

FCC 200/200

Latency

Narrowband

Broadband
Access/Onramp

NRIC VI, Focus Group 4
The Access/Onramp group provided insight and information on the existing and emerging technologies for Broadband access.

Current access speeds and onramp technologies are described in our white-paper.
Network Reliability and Interoperability Council

We’ve come a long way...

but we have a long way to go.
Getting Broadband is still not as simple as we would like it to be.
The National Academy of Sciences proposed a broadband access segregation model with “typing of areas” in their publication *Bringing Home the Bits*.

FG4 has updated this to match today's marketplace from a providers perspective.
Type 0 - no terrestrial providers of broadband: This situation is becoming increasingly uncommon, and is isolated to the most remote and hard to reach areas.

Methods exist, but they are cost prohibitive to the average consumer ..
Type 1 - one terrestrial facilities-based provider in the area: This circumstance has diminished significantly as telephone companies and cable operators have expanded their broadband coverage. The notion no longer exists that there are markets unable to support more than one provider.
Type 2 - two terrestrial facilities-based providers: This is the most common situation today. The entrance of one provider in the market typically has encouraged other facilities providers to upgrade their networks and provide competitive services. However, due to certain limitations of the technologies, broadband may not be available to every household in a particular market.
Type 3 – three or more providers via terrestrial or wireless: This is an increasingly common situation since generally there are two terrestrial providers available in most markets, satellite is available virtually everywhere, and a number of Wi-Fi based providers are launching services in otherwise underserved areas. New technologies such as Powerline show promise as well.
Focus Group 4 has made several recommendations in the area of increased access and deployment of Broadband:

“Service providers, network operators, and equipment providers should work to establish operational standards and practices which support Broadband capabilities and interoperability. (eg. (point-to-point videoconferencing, telephony, etc).”
Focus Group 4 has made several recommendations in the area of increased access and deployment of Broadband:

“Service Providers should make available meaningful information about expected performance with respect to upstream and downstream throughput and any limitations of the service; best effort services “up to” or unspecified bit rate services should be specified as such in a clearly identifiable manner.”
<table>
<thead>
<tr>
<th>Wizzo Internet Access</th>
<th>200 Times faster than dialup</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yoyodyne Networking</td>
<td>Broadband Internet in your hand</td>
</tr>
<tr>
<td>Access &amp; Onramp</td>
<td>Wizzo Internet Access</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------</td>
</tr>
<tr>
<td>1m/256k Best Effort</td>
<td>2.5G 256k/128k Best Effort</td>
</tr>
</tbody>
</table>
Access & Onramp

The significance of this is that consumers should have clear expectations on what the service will deliver.

- Best effort vs burst vs committed rate.
- Congestion policies (if any).
Service Transparency

NRIC VI, Focus Group 4
There has been an underlying assumption that once you have an IP address on the public Internet, network based applications should work.

However, as network based applications for Broadband evolve, transport layer transparency will play a more important role.
This sub-group found that service transparency issues revolved around three distinct categories:

*Static Policies* .. Those policies which are inherent in a service provider’s operational design.

*Dynamic Policies* .. Those policies which change due to unforeseen or reactive needs.

*Firewall Policies* .. Policies which dictate or determine what is allowed into and out of a network.
Use of “port blocking” in the core by providers contributes to transparency issues and application functionality issues by end users.

Incorrectly administered firewalls (or the implementation of bad policies) break application service transparency.
Non-disclosure of network policies creates a condition where considerable expense and time is spent in diagnosis of a “non problem.”

Furthermore, customers cannot do “like for like” network comparisons.
A End User has a file-sharing application which exists on ports 135, 137 & 139. These are common ports for SMB (Microsoft) File sharing applications. However, due to a recent outbreak of attacks, some providers have chosen to block traffic using these ports.
The good packets get through, the bad packets are blocked.
The simpler firewall systems are port (not algorithm) based.

Increased deployments of bad network policies have given rise to application port masquerading.

The use of NAT (PAT) for handling IP allocation issues solves some problems, but application support for port mapping is limited.
Sometimes, data is allowed through for business reasons.
Port masquerading allows bad packets in again.
Firewalls are a little-known and not well-understood, contributor to service transparency issues.

Considerable effort is being spent on developing “security” policies.

There is need for consideration of service transparency when developing these policies.
Service Transparency

Firewall
Port Address Translation Example
Each connection goes to the same destination IP address, but to a specific port.
Incoming packets are sent to the destination machines based on their port to (internal) IP address mapping.
PAT allows access to applications when implemented correctly.
Focus Group 4 has made several recommendations in the area of service transparency:

“Service Providers should internally establish and develop controls to administer the network policies associated with protocol or port filtering. To whit: a process that defines generic circumstances when dynamic filtering may occur, (i.e. DDOS, Virus) and made available to customers.”
Focus Group 4 has made several recommendations in the area of service transparency:

“Service providers should make policy information available to customers which include content filtering Static Policies -- those policies which by design are not likely to change.”
Service Transparency

Focus Group 4 has made several recommendations in the area of service transparency:

“Service providers and/or network operators should work to establish operational standards which provide transparency for current products and applications as well as insure continued multi-provider solutions with minimal operational interference as products and systems evolve.”
Service Transparency

Focus Group 4 has made several recommendations in the area of service transparency:

“Service Providers should establish and develop internal controls to administer the network policies associated with protocol or port filtering whereby network security takes precedence in maintaining overall reliability, integrity, and availability of the carrier’s network and interconnection “peering” or “transit” points.”
Traffic Policy & Management

NRIC VI, Focus Group 4
While a number of methodologies exist for implementation of traffic policies, there is little if any operational standardization in the methods, practices and disclosure of such policies.
Focus Group 4 has made several recommendations in the areas of Traffic Policy and Traffic Management:

“Service providers should consider utilizing traffic management mechanisms and technologies to ensure facilities are utilized most efficiently.”
Focus Group 4 has made several recommendations in the areas of Traffic Policy and Traffic Management:

“Equipment suppliers should incorporate traffic management technology into their equipment, as necessary, with the tools necessary to maintain performance of facilities and to manage traffic flows from customers per contracts/SLA's and to prevent degradation of quality of service experienced by network users.”
Focus Group 4 has made several recommendations in the areas of Traffic Policy and Traffic Management:

“Service providers, network operators, and equipment providers should work to establish operational standards and practices which support Broadband capabilities and interoperability. (point-to-point videoconferencing, telephony, etc.)”
Focus Group 4 has made several recommendations in the areas of Traffic Policy and Traffic Management:

“Service providers should consider appropriate means for providing their customers with information about their traffic policies so that users may be informed when planning and utilizing their applications.”
NRIC VI FG4
Broadband