Accounting Requirements for Priority Services

IETF #55
18-21 November 2002
Mike Pierce, Artel

Please Note
I am not proposing packet level accounting, i.e., counting number of packets transferred at each "priority" level.

What is a "requirement"?

IEPREP Charter: RFC may identify "requirements for use in new protocol or protocol feature design".

Within the context of my presentation: For DoD: Something that the user requires the telecommunications system to support to meet its mission. (not an "objective" or "goal".)
(e.g., in draft-pierce-ieprep-assured-service-req-00)

In an IEPREP document: Something that IEPREP "requires" the next WG (SIPPING, etc.) to attempt to provide.

Later (not important for this presentation):
In a protocol doc: Something that a vendor or carrier "MUST" support in order to claim compliance with the RFC.

What is "accounting" and "auditing"?

RFC 2975, Introduction of Accounting Management, defines:

Accounting: The collection of resource consumption data for the purposes of capacity and trend analysis, cost allocation, auditing, and billing.

Auditing: The act of verifying the correctness of a procedure.

Section 1.4.3 says further:
"Auditing tasks include ... verifying conformance to usage policy."

What are Priority Services?

Any service that gives one user "priority", or better service, over another. ("Priority" here does not imply any particular mechanism, e.g., priority queuing.)

Examples (not all in the scope of IEPREP):
- Authorized Emergency (e.g., GETS in the US)
- Assured Service (equivalent to military MLPP service)
- Public Emergency calling (e.g., 911 in the US)
- Different service levels for different customers

Final two are presumed to be out-of-scope for this WG, but any mechanism defined for the first two may be useful for the final two.

Why is accounting (auditing) required?

RFC3334, Policy-based Accounting, states:
Even if we will have much more bandwidth in the future than now, the control of network resource utilization remains essential for the support of applications with special demands and for the prevention of (malicious or accidental) waste of bandwidth.

Required capabilities for Priority Services are to detect:
- Misuse by authorized persons (e.g., calls from areas without emergencies, excessively long calls, precedence "creep")
- Use by unauthorized persons (stolen or guessed password or PIN)
- Attempts to use service (even if they fail)

What may be useful?

For each call setup or attempt, the following are most common:
- Calling and called party identification
- Time and duration of call attempt
- Priority level or special treatment requested and received
- Password or access code used *
- Disposition of call attempt

* It is recognized that security policies would normally require that the actual password or access code should not be stored in the accounting record, but there must be some way to determine, when examining the records, which code was (mis)used. For example, when a simple 4-digit pin is entered, which is sent through the audio path "in the clear" anyway, then storing the actual code received is not a further security problem.