AlliedWare™ OS

How To | Achieve Quality of Service over a Low-Speed WAN that has a Non-QoS-Capable Gateway Device

Introduction

Firstly, to set the scene, let's review a few well-known facts of networking life.

- Wide Area Network (WAN) links are almost invariably of lower bandwidth than Local Area Networks (LANs).
- The desire for LAN users to access services via their WAN almost always exceeds the bandwidth available on the WAN, so packets are frequently being dropped at the WAN gateway point.
- Real-time applications like voice and video are very sensitive to packet loss or delay.

As a result, in an uncontrolled situation, real-time applications typically do not work well across WAN links.

To deal with this problem it is necessary to exert control over which applications get preferential access to WAN bandwidth. Network administrators achieve this by introducing Quality of Service policies on their WAN access devices.

But, they have a problem if either:

- the WAN access device is provided by the WAN service provider, so the network administrator is not allowed to alter its configuration, or
- the WAN access device is a low-featured device that simply does not support Quality of Service features.

The purpose of this document is to look at a solution to this problem that can be achieved using an Allied Telesis router.

Which products does this information apply to?

This document applies to the following Allied Telesis routers and managed layer 3 switches:

- AR400 series routers
- AR700 series routers

running software version 2.7.1 or later.

Related How To Notes

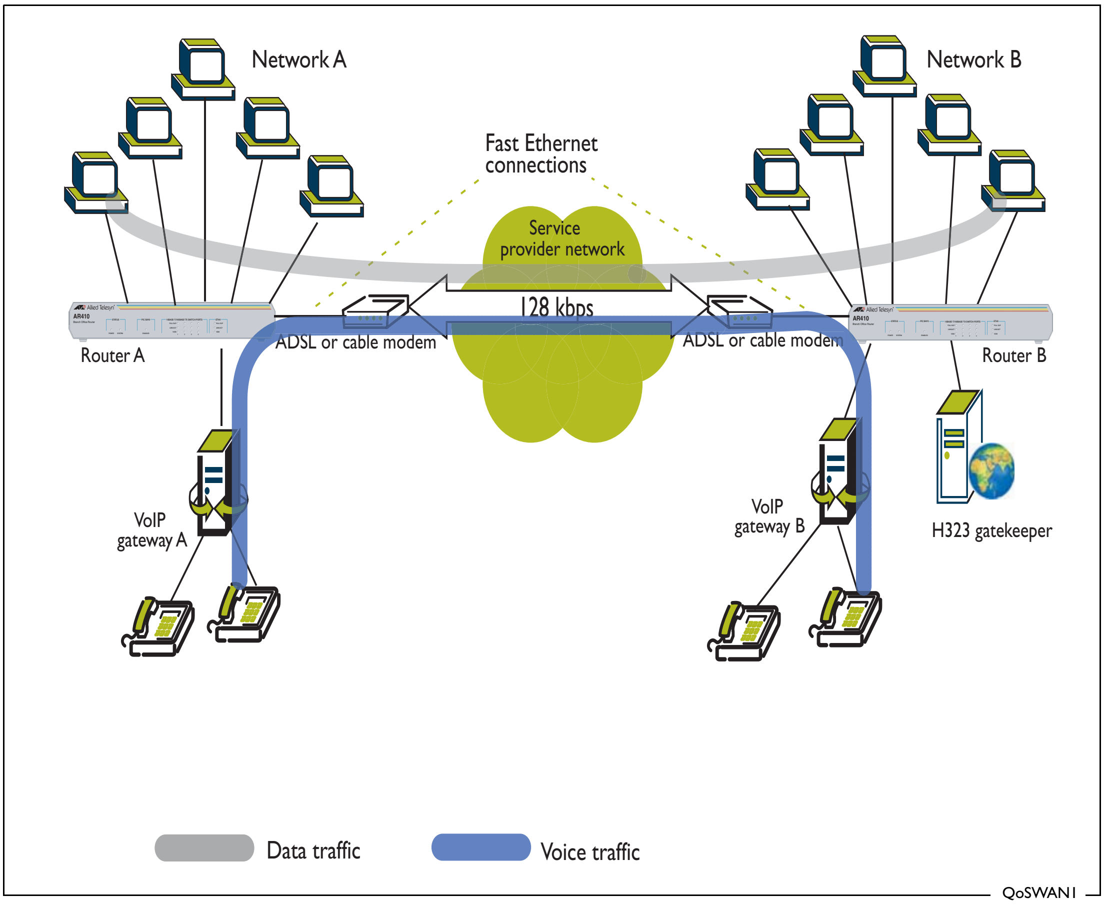
You also may find the following How To Note useful:

- *How to configure software QoS for some specific customer scenarios*

How To Notes are available from www.alliedtelesis.com/resources/literature/howto.aspx.

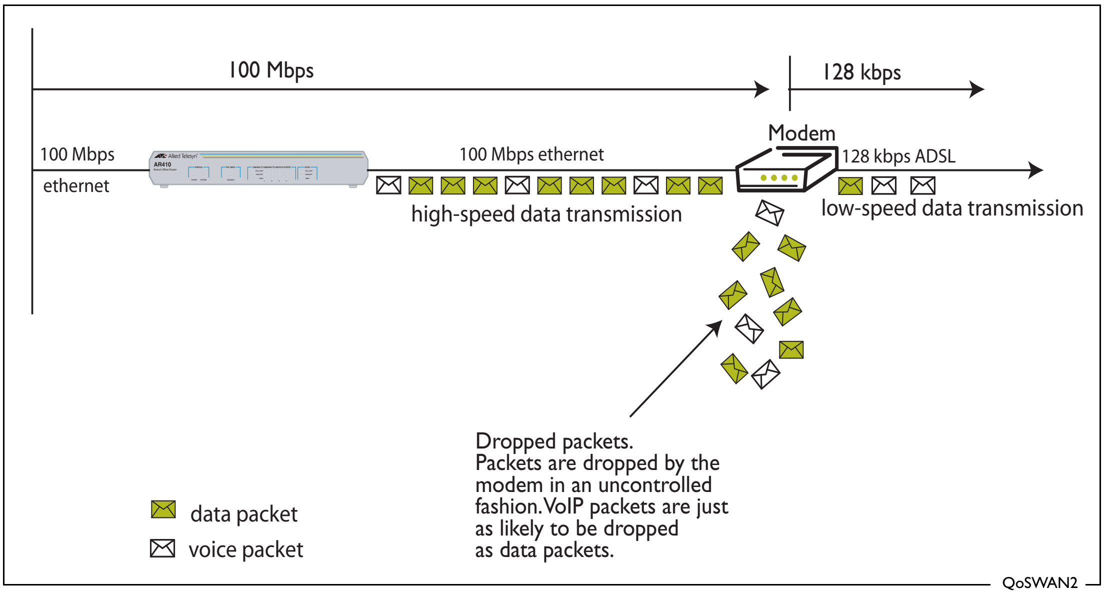
The network scenario

A common scenario in which this problem will be experienced is illustrated in the following figure, in which large volumes of data and voice are being transferred over a WAN link.



Potentially large volumes of data are being exchanged between computer networks A and B, whilst Voice over IP (VoIP) calls are also being transported across the WAN link.

Given the relatively low bandwidth of the WAN link (128 kbps), it will be frequently oversubscribed, and packets will be dropped at the ASDL or cable modem. But if the modem has no QoS capability, packets will be dropped in an uncontrolled manner, as shown in the following figure.


100 Mbps
128 kbps
100 Mbps
ethernet
100 Mbps ethernet
Modem
128 kbps ADSL
high-speed data transmission
low-speed data transmission
Dropped packets.
Packets are dropped by the modem in an uncontrolled fashion.VoIP packets are just as likely to be dropped as data packets.
data packet
voice packet
QoSWAN2

This has a major impact on the quality of the VoIP calls that are being transported over the link.

The solution

The solution to the problem is to recognise the fact that the 100 Mbps link between the router and the modem is effectively a point-to-point link. So, the router has complete control over the data that is being put onto that link. Hence, if the router is a QoS-capable device, and a QoS policy is configured on the router, that effectively controls what data is sent over the WAN link.

However, it is not simply at a matter of configuring a packet prioritisation policy on the router. The fact is that packet prioritisation only has effect if the router has data queued on its egress interface, i.e. if the egress interface is oversubscribed.

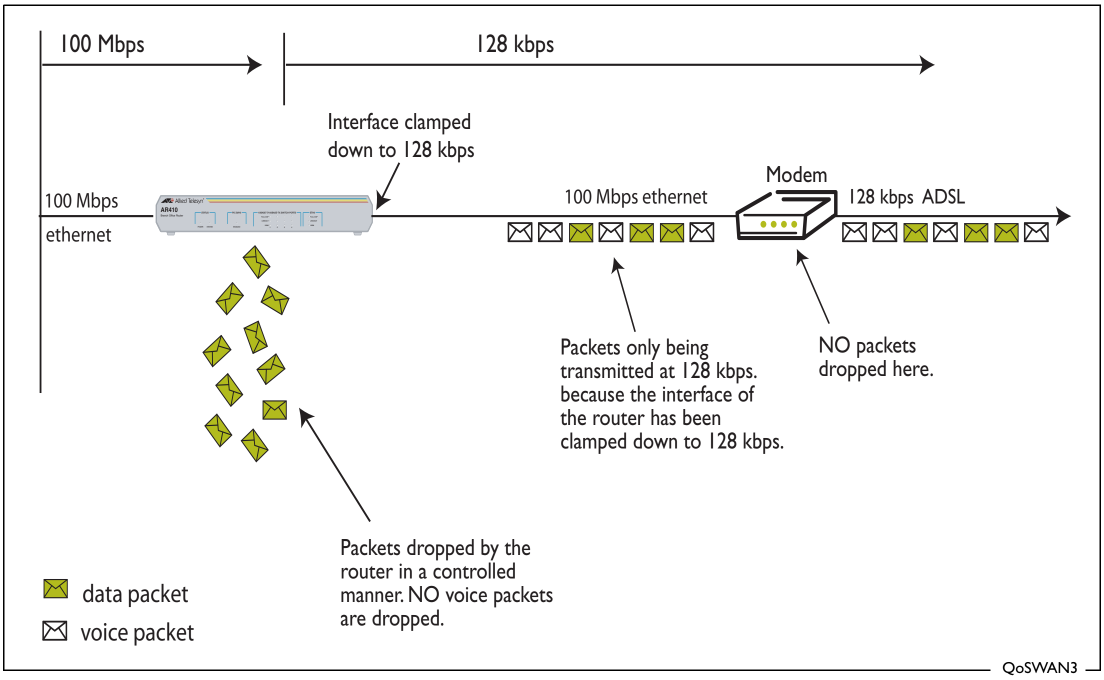
But, the egress interface of the router is a 100 Mbps interface, and will not become oversubscribed until **well** after the modem's WAN interface has become oversubscribed. Therefore, you need to artificially clamp the egress bandwidth on the router's interface down to 128 kbps. That way, the router's egress interface becomes oversubscribed (and so the QoS policy starts to have effect) as soon as the LAN is directing more than 128 kbps of traffic towards the WAN.

Additionally, it is very useful to force the egress interface on the router to fragment packets. This will limit the maximum delay time that any given voice packet will experience if it is queued behind a data packet. It can take some milliseconds for a 1500-byte packet to be placed onto a 128 k link, so if a voice packet is stuck behind a 1500-byte data packet, then the voice packet will be naturally delayed as it waits for the data packet to be sent out onto the line. If the maximum packet size sent out the egress interface of the router is limited to 512 bytes, then the longest queueing delay a voice packet will experience is the time required to put a 512-byte packet onto the 128 k line.

In summary, the solution to the problem involves the following steps:

1. clamp the egress bandwidth on the router down to 128kbps.
2. institute a QoS policy on the router so that it ensures that VoIP packets are transmitted in preference to data packets.
3. set a maximum size for packets transmitted from the router to the modem.

Then you have a situation as illustrated in the following figure, in which the router egress interface is clamped to 128 kbps.


100 Mbps
128 kbps
Interface clamped down to 128 kbps
Modem
100 Mbps ethernet
100 Mbps ethernet
128 kbps ADSL
Packets only being transmitted at 128 kbps. because the interface of the router has been clamped down to 128 kbps.
NO packets dropped here.
Packets dropped by the router in a controlled manner. NO voice packets are dropped.
data packet
voice packet
QoSWAN3

The configuration commands

The *eth0* interface of the router supports the bandwidth limiting feature – the egress bandwidth can be clamped to multiples of 128kbps. The *eth0* interface of the router must be connected to the Ethernet interface of the ADSL or cable modem.

Specific commands to enter on the router

1. Limit the egress bandwidth, enter the command:

```
set eth=eth0 maxbandwidth=128
```

2. Set the maximum size for the packets transmitted:

```
set int=eth0 mtu=512
```

3. Put the VoIP packets into the high priority egress queue on the eth0 port.

   This involves identifying the VoIP packets and putting them into the priority queue. The most effective way to identify the VoIP packets is to use Dynamic Application Recognition (DAR) to automatically detect VoIP sessions, and allocate them to a traffic class.

   In this case, we will assume that the VoIP sessions are signalled using the SIP protocol.

   The commands to create and apply a software QoS policy that uses DAR to identify VoIP traffic, and then give it a high priority are:

```
enable sqos

# Make a DAR entity to match all sessions initiated by SIP signalling.
create sqos dar=0 protocol=sip

# The DAR does not actually match the signalling traffic itself, so make
# a separate classifier to match on the signalling traffic.
create classifier=1 udpdport=5060

# Put the DAR onto the incoming switch instance so it will check for VoIP
# packets arriving via the switch ports.
add sqos int=swi0 dar=0

# Prioritise the SIP signalling traffic above the VoIP data packets.
create sqos trafficclass=1  priority=14
create sqos trafficclass=2  priority=15

# Create a software QoS policy.
create sqos policy=1

# Attach SIP-signalling and VoIP data traffic classes to the policy.
add sqos policy=1 trafficclass=1,2

# Add DAR 0 to traffic class 1, so that the packets that DAR 0 recognises
# as voice packets will be associated with traffic class 1.
add sqos trafficclass=1 dar=0

# Add classifier 1 to traffic class 2, so that the SIP signalling packets
# will be associated with traffic class 2.
add sqos trafficclass=2 classifier=1

# Set policy 1 to be the egress QoS policy on interface eth0.
set sqos int=eth0 outpolicy=1
```

   The result of this configuration is that the VoIP packets are given a high priority, and all other data will be given a default (low) priority.

USA Headquarters | 19800 North Creek Parkway | Suite 200 | Bothell | WA 98011 | USA | T: +1 800 424 4284 | F: +1 425 481 3895
European Headquarters | Via Motta 24 | 6830 Chiasso | Switzerland | T: +41 91 69769.00 | F: +41 91 69769.11
Asia-Pacific Headquarters | 11 Tai Seng Link | Singapore | 534182 | T: +65 6383 3832 | F: +65 6383 3830
www.alliedtelesis.com