BRANCH QoS DESIGN
AT–A–GLANCE

Branch routers are connected to central sites via private-WAN or VPN links which often prove to be the bottlenecks for traffic flows. QoS policies at these bottlenecks align expensive WAN/VPN bandwidth utilization with business objectives.

QoS designs for Branch routers are—for the most part—identical to WAN Aggregator QoS designs. However, Branch routers require three unique QoS considerations:

1) Unidirectional applications

2) Ingress classification requirements

3) Network Based Application Recognition (NBAR) policies for worm policing

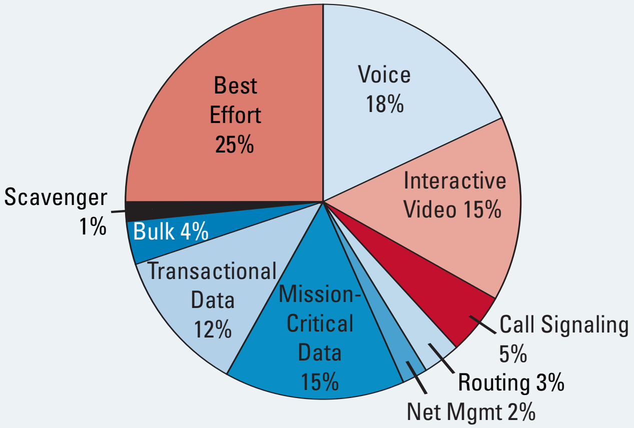
Each of these Branch router QoS design considerations will be overviewed.

1) UNIDIRECTIONAL APPLICATIONS

Some applications (like Streaming Video) usually only traverse the WAN/VPN in the Campus-to-Branch direction; and therefore, do not require provisioning in the Branch-to-Campus direction on the Branch router's WAN edge.

Bandwidth for such unidirectional application classes can be reassigned to other critical classes, as shown in the following diagram. Notice that no Streaming Video class is provisioned and the bandwidth allocated to it (on the Campus side of the WAN link) is reallocated to the Mission-Critical and Transactional Data classes.

An Example 10-Class QoS Baseline Branch Router WAN Edge Queuing Model



2) INGRESS CLASSIFICATION

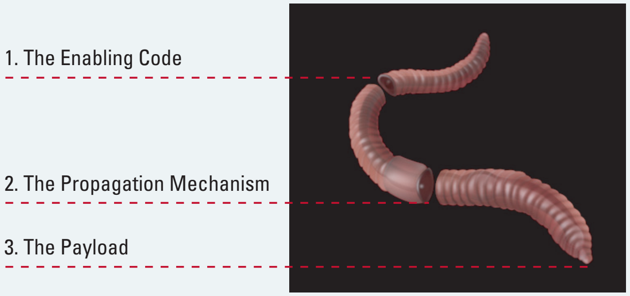
Branch-to-Campus traffic may not be correctly marked on the Branch Access Layer switch.

These switches—which are usually lower-end switches—may or may not have the capabilities to classify and mark application traffic. Therefore, classification and marking may need to be performed on the Branch router's LAN edge (in the ingress direction).

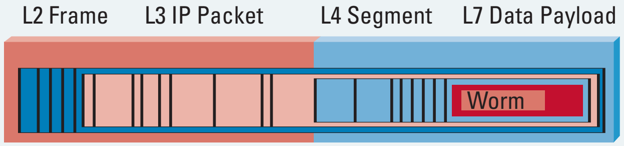
Furthermore, Branch routers offer the ability to use NBAR to classify and mark traffic flows that require stateful packet inspection.

3) NBAR FOR KNOWN WORM POLICING

Worms are nothing new, but they have increased exponentially in frequency, complexity, and scope of damage in recent years.

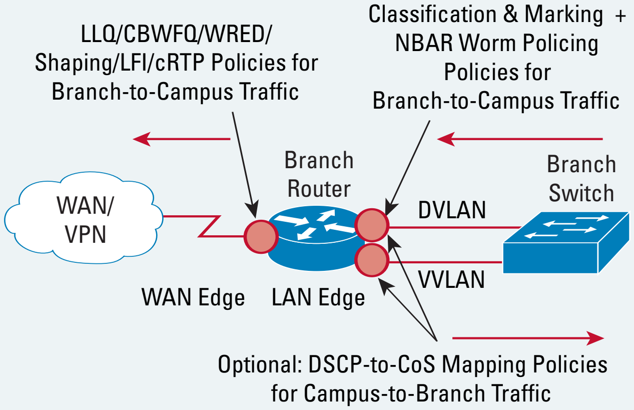


The Branch router's ingress LAN edge is a strategic place to use NBAR to identify and drop worms, such as CodeRed, NIMDA, SQL Slammer, MS-Blaster, and Sasser.



NBAR extensions allow for custom Packet Data Language Modules (PDLMs) to be defined for future worms.

Where is QoS Required on Branch Routers?


LLQ/CBWFQ/WRED/ Shaping/LFI/cRTP Policies for Branch-to-Campus Traffic
Classification & Marking + NBAR Worm Policing Policies for Branch-to-Campus Traffic
WAN/ VPN
Branch Router
Branch Switch
DVLAN
VVLAN
WAN Edge
LAN Edge
Optional: DSCP-to-CoS Mapping Policies for Campus-to-Branch Traffic