White Paper

Telecom 5G/Wi-Fi Access
NEP, CSP, Enterprise

Wipro and Intel Show QoS of Unsecured Wi-Fi Packets on 5G Core

Wipro worked with Intel to showcase Wi-Fi QoS functionality on servers powered by 4th Gen Intel® Xeon® Scalable processors

Table of Contents

Wi-Fi networks are the dominant wireless LAN and cellular technology the dominant wireless WAN. Now, these use cases are converging with Wi-Fi growing as the wireless access technology in public spaces and private 4G/5G networks emerging to support certain enterprise applications.

Given these trends there is an opportunity for MNOs to use Wi-Fi networks as a cost effective wireless access technology by supporting untrusted Wi-Fi wireless LAN traffic on a secure 5G core network.

In this way, MNOs can support more users cost-effectively by relying on Wi-Fi networks to serve customers in areas with networks already in place. In areas with both 5G and Wi-Fi coverage, MNOs can consolidate data traffic from both networks on their 5G core backbone reducing backhaul network costs and providing better coverage in high density locations. The interworking between untrusted Wi-Fi and 5G also opens up the opportunity for delivering enhanced consumer services to untrusted Wi-Fi users.

To accommodate the support of untrusted Wi-Fi on a 5G core, the 3GPP has developed the Non-3GPP Interworking Function (N3IWF). Using the N3IWF gateways, MNOs can support multi-access protocol data unit (PDU) sessions and provide Wi-Fi access for edge computing.

Wipro, an Intel® Network Builders ecosystem member has collaborated with Intel to demonstrate the performance of its N3IWF gateway.[1] The companies have also worked together to explore quality of service (QoS) functionality built into Wipro's N3IWF gateway. This QoS functionality allows the Wi-Fi and other untrusted data packets to leverage 5G QoS mechanisms in order for the MNO to deliver service differentiation to both Wi-Fi and 5G data flows.

Wipro N3IWF gateway allows unsecure Wi-Fi on 5G core

Wipro's N3IWF virtual gateway reference solution allows mobile user equipment (UE) to access a 5GCN from an untrusted WLAN through secure registration and authentication using IPsec tunneling.

In Figure 1, all of the 5G core services are across the top of the diagram with two access paths, one path running through the 5G NR RAN and the other through Wi-Fi (WLAN). That traffic passes through to the N3IWF gateway to apply services and policies before heading to the user plane function (UPF). The gateway's control plane protocol stacks provide protocols used in UE, WLAN, N3IWF and AMF to establish initial registration and authentication, NAS mobility and session management, and establish a user plane (UP) between the N3IWF and the UE.

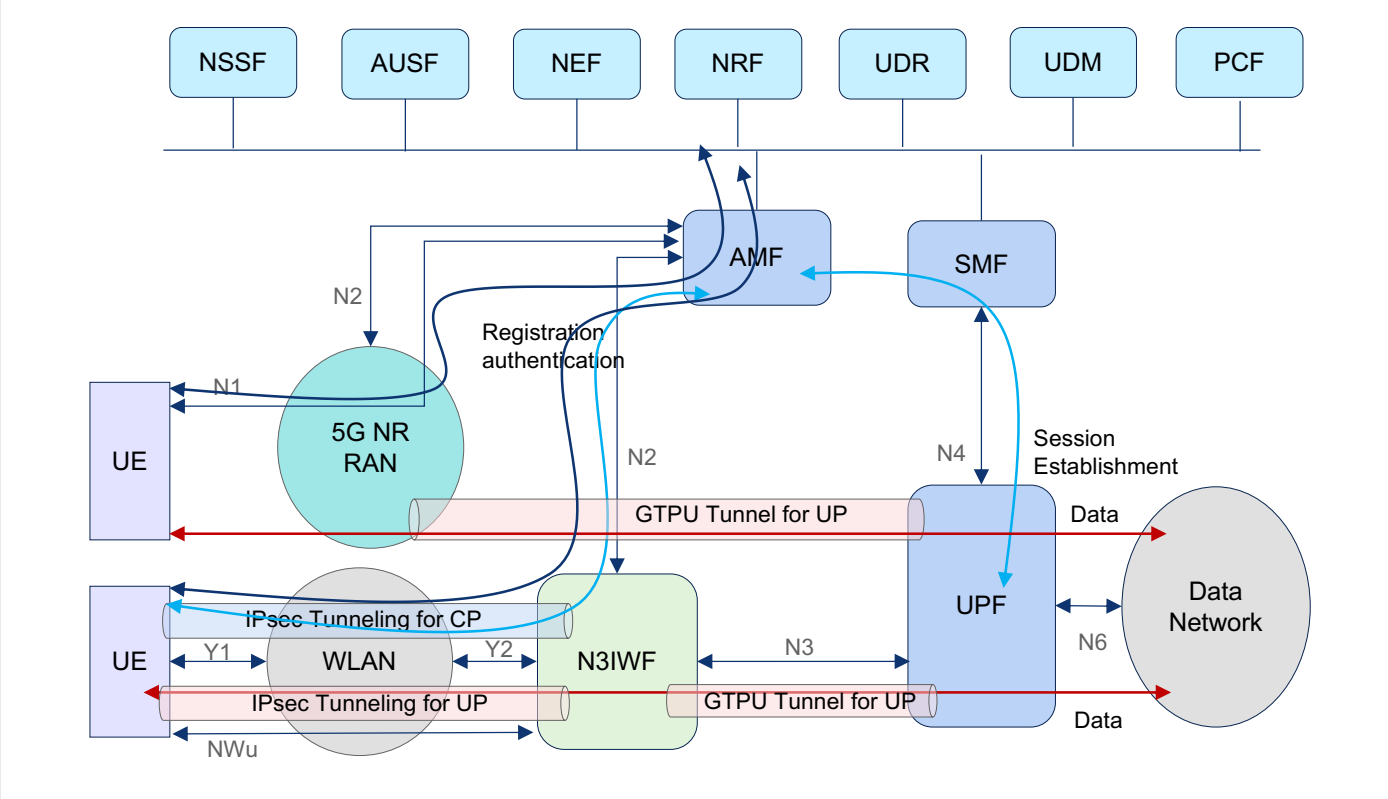

Figure 1. Architecture for untrusted WLAN internetworking with a 5G core network; diagram shows the data path for both a trusted 5G UE and an untrusted Wi-Fi UE to access the 5GCN.

Wipro's N3IWF virtual gateway maintains secure access to the 5GCN from untrusted WLAN with high throughput, up to 100Gbps[1]. The gateway can utilize open source functionality to improve performance, such as the Intel-developed open source Data Plane Development Kit (DPDK), a family of software libraries designed to improve virtual networking throughput. The gateway also supports the Vector Packet Processing (VPP) platform an open source layer-three switch.

Mapping Wi-Fi QoS

For a UE accessing the 5GCN through an untrusted WLAN, the N3IWF supports QoS differentiation and mapping of QoS flows to non-3GPP access resources (Figure 2). This provides revenue opportunities for MNOs who can add QoS to Wi-Fi packets or enables the application of existing Wi-Fi QoS.

To deliver the QoS, Wipro has built into its gateway and user plane function (UPF) the ability to tag packets using 5G QoS identifier (5QI) on both the upload (UL) and download (DL) traffic. The functionality is split between the gateway and the UPF:

1. N3IWF gateway functions

1. Maps PDUs from QoS flows to IPsec security associations (SAs) based on QoS flow identifier (QFI).
2. Enforces the aggregate maximum bit rate (AMBR) in both UL/DL data flows for all UEs.
3. Performs transport level packet marking in UL/DL data flows.
4. Enforces UL/DL maximum flow bit rate (MFBR).

2.UPF functions

1. Maps DL traffic to QoS flows using packet detection rules (PDRs).
2. Enforces session-AMBR in UL/DL.
3. Performs transport level packet marking in the DL.
4. Enforces MFBR in DL.

More details on the data flows from the UE through the gateway to the UFPF are seen in Figure 2.

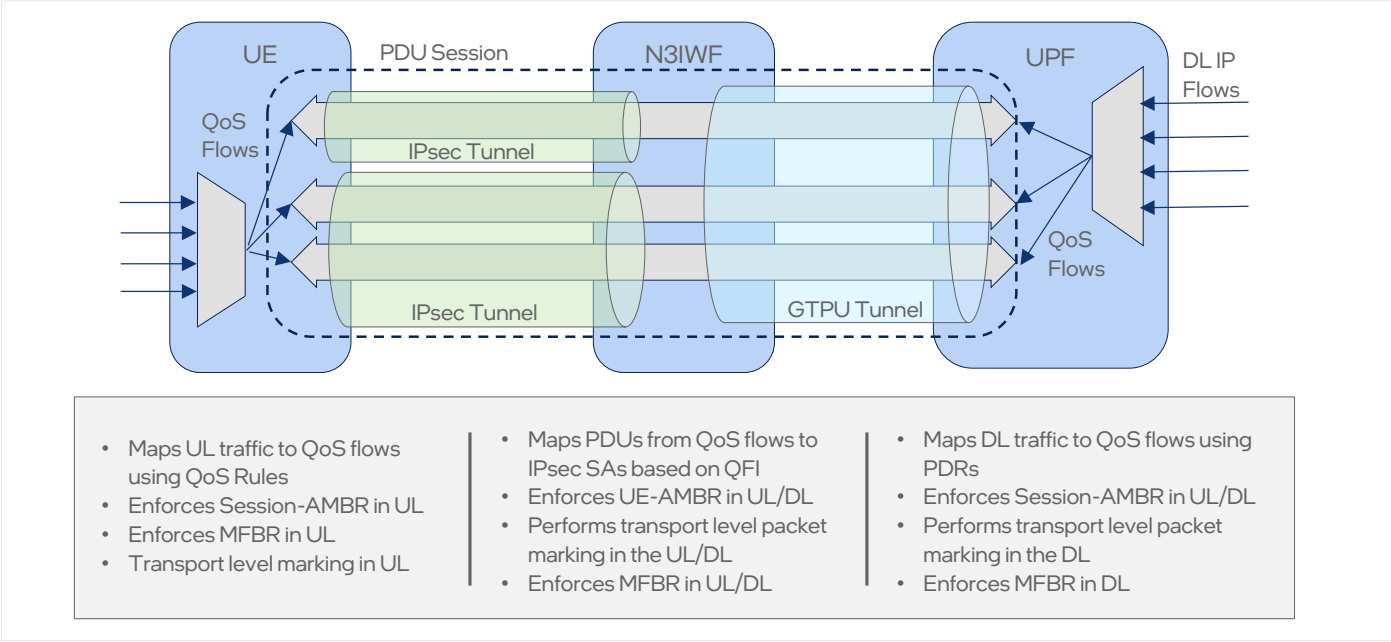

Figure 2. QoS for untrusted WLAN access to a 5GCN.

5QI to DSCP Mapping in N3IWF

Table 1 shows the transport level packet marking, i.e. DSCP value mapping, for various 5QI values corresponding to both GBR and non-GBR flows in the UL and DL.

5QI Value	Default Priority Level	Packet Delay Budget	Packet Error Rate	Mapping DSCP Value	DSCP Meaning
GBR 5QIs					
1	20	100 ms	10 E-2	44	EF
2	40	150 ms	10 E-3	34	AF41
3	30	50 ms	10 E-3	32	CS4
4	50	300 ms	10 E-6	28	AF32
65	7	75 ms	10 E-2	44	EF
66	20	100 ms	10 E-2	44	EF
67	15	100 ms	10 E-3	38	AF43
Non GBR 5QIs					
5	10	100 ms	10 E-2	30	CS5
6	60	150 ms	10 E-3	26	AF31
7	70	50 ms	10 E-3	22	AF23
8	80	300 ms	10 E-6	28	AF32
9	90	75 ms	10 E-2	0	CS0
69	5	60 ms	10 E-6	44	EF
70	55	200 ms	10 E-6	30	AF33
79	65	50 ms	10 E-2	32	CS4
80	68	10 ms	10 E-6	24	CS3

Table 1. 5QI to DSCP mapping.

AMBR and MFBR Enforcement

The N3IWF supports UE-AMBR enforcement in the UL and DL for all non GBR flows and MFBR enforcement in the UL and DL for all GBR flows (see Figure 3). During the control plane procedures, the N3IWF configures the UE-AMBR and MFBR values in the DPDK QoS through the custom QoS VPP plugin. The DPDK QoS applies the UE AMBR rate in the UL and DL for all non-GBR flows corresponding to all UE sessions. DPDK QoS applies the MFBR rate in the UL and DL corresponding to each of the GBR flows for each session for all the UE

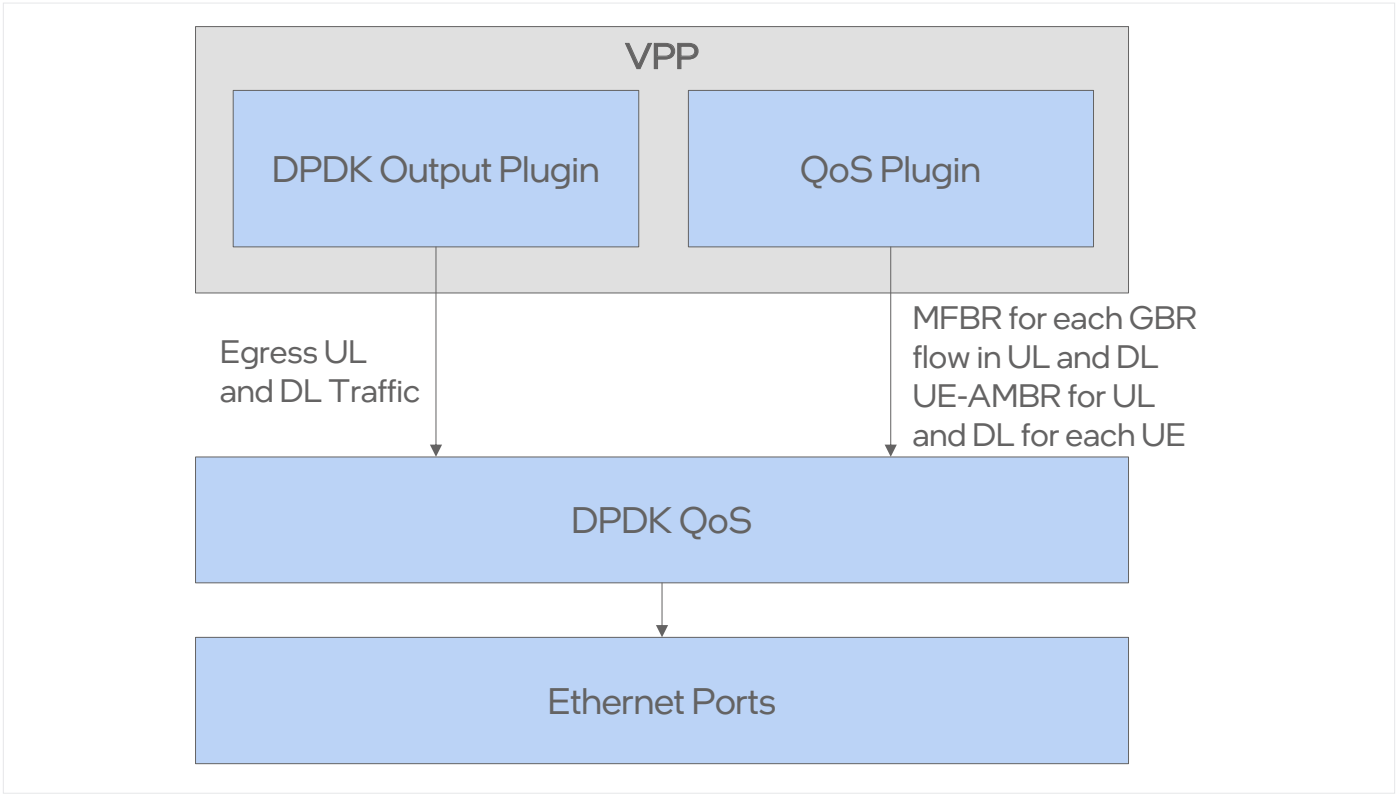

Figure 3. UE-AMBR and MFBR rate configuration and enforcement in DPDK QoS.

4th Gen Intel® Xeon® Scalable Processors Brings Accelerated Performance

The N3IWF virtual gateway leverages the performance of servers that use 4th Gen Intel Xeon Scalable processors and Intel® Ethernet 800 Series Network Adapters for N3IWF deployments.

4th Gen Intel Xeon Scalable processors offer a new microarchitecture designed to address dynamic and demanding workloads. These processors provide more performance per watt, reducing the number of watts required for the same workloads to improve sustainability. They have up to 52 cores in addition to six built-in accelerators to help maximize performance efficiency (see Figure 4).

Some of these accelerators are uniquely beneficial to help N3IWF systems deliver performance. Securing Wi-Fi traffic requires encryption and the built-in Intel® QuickAssist Technology (Intel® QAT) accelerates data encryption and compression; accelerating the IPsec tunneling needed for the gateway.

Figure 4. 4th Gen Intel® Xeon® Scalable processor features six accelerators and up to 52 cores for performance.

Intel® Ethernet 800 Series Network Adapters

4th Gen Intel Xeon Scalable processor-based servers also support the 100GbE Intel Ethernet Network Adapter E810. Its innovative and versatile capabilities optimize high-performance server workloads such as virtualization, storage, high performance computing AI, and hybrid cloud. Its high throughput can carry intensive network traffic without impeding data speed.

100GbE Intel Ethernet 800 Series Network Adapters offer exceptional compatibility, interoperability, and performance to meet the requirements of an interworking workloads. The Intel Ethernet Network Adapter E810-CQDA2 improves N3IWF application efficiency and network performance with its dual port configuration and 100/50/25/10GbE per port data rates, packet-classification, and sorting optimizations, hardware-enhanced timing capabilities, and a fully programmable pipeline.

QoS Handling Test Set Up

The goal of this test is to show the QoS handling within N3IWF for traffic with different QoS requirements as specified by 5G QFI.

The system under test (SUT) server was based on an Intel® Xeon® Platinum 8470N processor with integrated Intel® QAT. The testing also used the Intel Ethernet Network Adapter E810-CQDA2 using both 100 Gbps ports (see Figure 5).

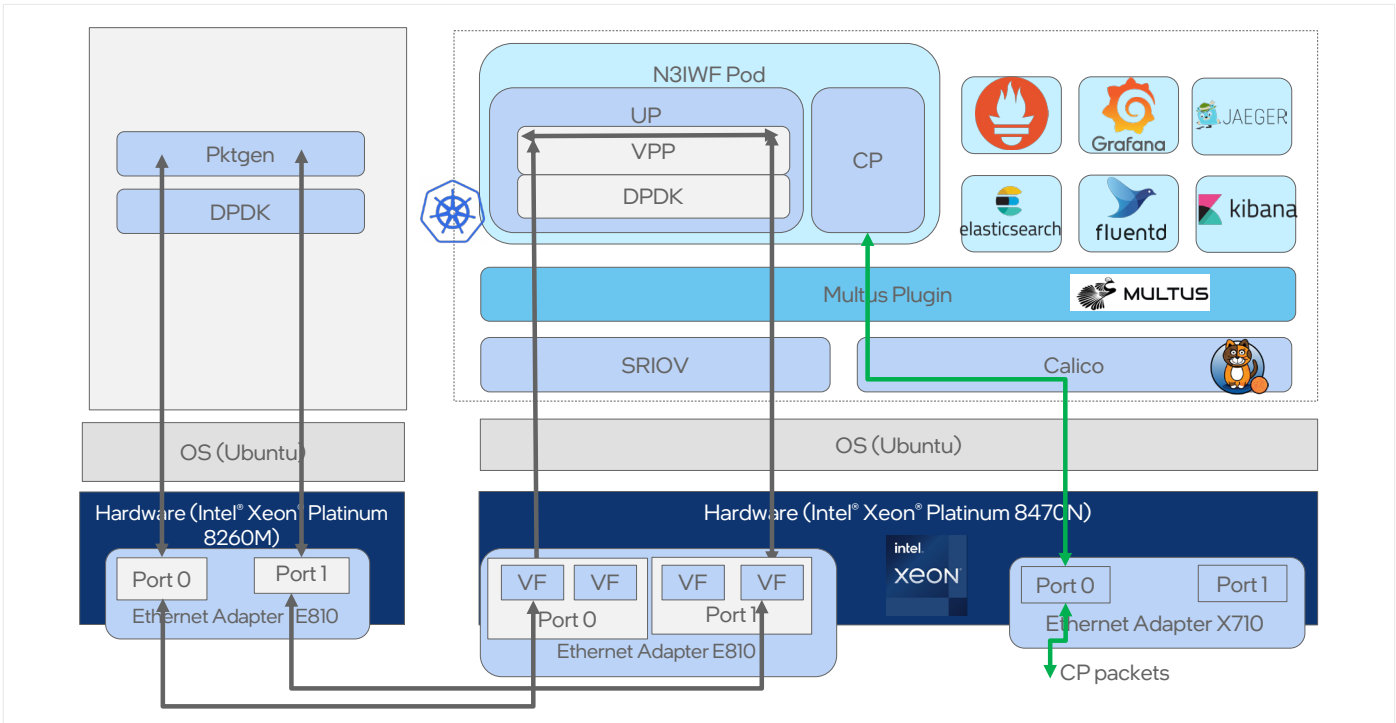

Figure 5. N3IWF is run in a container with PktGen on another server. N3IWF runs with one core for the main thread and two worker threads each with one core, one Rx, and one Tx queues. The DPDK PktGen packet generator ran using five cores – one core for main, two cores each for two ports.

Software Configuration

The SUT utilized the Wipro N3IWF software configuration including Ubuntu operating system (OS) and the 5.15.0-87-generic kernel. The N3IWF is based on VPP and DPDK stack for fast path processing utilizing single root I/O virtualization (SR-IOV) virtual functions (VFs) for input and output. The N3IWF was deployed as a pod in a Kubernetes cluster along with required plugins as a cloud native function in cloud native environment with EFK stack for logging and Prometheus and Grafana for monitoring. The N3IWF was deployed utilizing one core for the main thread and two worker threads each with one core, one Rx and one Tx queues along with 2 Intel® QAT VFs.

DPDK PktGen packet generator deployed in another server was used to send the uplink/downlink packets through the N3IWF corresponding to various QoS flows and utilized one core for main thread and two cores each for two ports.

Test Results

The test results show that the reference N3IWF based on 4th Gen Intel Xeon Platinum processor with integrated Intel® QAT enables customers to support Wi-Fi clients with different QoS requirements by supporting the following QoS functionalities.

1. Performs transport level packet marking in UL/DL data flows.

   a. Packets corresponding to various QoS flows with QFI having the same value as 5QI are observed to be marked with corresponding DSCP at the transport level as show in Table 1 in both the UL and DL.

2. Enforces UL/DL UE aggregate maximum bit rate (UE-AMBR) for all non GBR data flows for a UE.

   a. Multiple sessions created with multiple non GBR flows for a UE are observed to be rate limited with the corresponding configured UE-AMBR.

3. Enforces UL/DL maximum flow bit rate (MFBR) for GBR flows.

   a. Multiple sessions created with multiple GBR flows for a UE are observed to be rate limited corresponding to the configured MFBR for each of the flow in each session.

Conclusion

By implementing the Wipro N3IWF on 4th Gen Intel® Xeon® Platinum CPUs, along with the Intel® Ethernet Network Adapter E810 and Intel® QAT acceleration, untrusted non-3GPP networks and UE can securely access the 5GCN with different QoS requirements. This paves the way for MNOs and enterprises to unify heterogenous access networks to gain all the QoS benefits delivered by 5G.

Learn More

Wipro N3IWF

Wipro homepage

4th Gen Intel® Xeon® Scalable Processors

Intel® Network Builders

Notices & Disclaimers

[1] https://networkbuilders.intel.com/solutionslibrary/wipro-n3iwf-reference-delivers-100gbps1-throughput-to-5g-core

Performance varies by use, configuration and other factors. Learn more on the Performance Index site.

Performance results are based on testing as of dates shown in configurations and may not reflect all publicly available updates. See backup for configuration details. No product or component can be absolutely secure.

Your costs and results may vary.

Intel technologies may require enabled hardware, software or service activation.

Intel does not control or audit third-party data. You should consult other sources to evaluate accuracy.

THIS IS THE SET CONFIGURATION:

Test Server: 1-node, 2x 1.7GHz Intel® Xeon® Platinum 8470 with 256 GB (16 slots/16GB) total DDR5 memory, microcode 0x2b0004d0, HT on, Turbo on, dual port 100GbE Intel® Ethernet E810-CQDA2. Operating system was Ubuntu 5.15.0-87-generic, 1x Intel_SSDSC2KG96 960 GB, Wipro UPF and N3IWF compiler is gcc, other software is DPDK and VPP, test conducted by Wipro in Nov. 2023.

0124/LV/H09/PDF ♻Please Recycle 358331-001US