Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD
Informatiksteuerungsorgan des Bundes ISB

AR003 – Architektur QoS. Beilage 1

Beilage zu IKT-Vorgabe

Sachtitel (der Beilage):	**Umsetzungsempfehlung**
Ausgabedatum dieser Beilage:[1]	21. August 2018
Gehört zu:	AR003, Version 1.0.1
Status der IKT-Vorgabe:	Genehmigt

[1] Das *Ausgabedatum* stimmt bei der Erstpublikation der Beilage mit dem *Beschlussdatum* der genehmigten Version einer IKT-Vorgabe überein, zu der die Beilage gehört. Geringfügige Änderungen/Ergänzungen in einer Beilage zu einer IKT-Vorgabe (z.B. bei einem neu aufzunehmenden Listeneintrag) können unter bestimmten Bedingungen ohne Versionierung der IKT-Vorgabe erfolgen: Voraussetzung ist, dass diese Änderung über eine IKT-Anforderung beantragt wurde und im Beschluss die Änderung der IKT-Beilage ohne Versionierung der IKT-Vorgabe explizit festgehalten ist. In diesem Fall ist lediglich das *Ausgabedatum* der Beilage anzupassen sowie die Änderung in *Anhang A* zu beschreiben.

Inhaltsverzeichnis

1 Einleitung 4

2 Begrifflichkeiten 5

2.1 Verkehrsklassen 5
2.2 Dienstgüte 6
2.3 Serviceklassen 7
2.4 Differentiated Service Code Point - DSCP 8
2.5 Klassifizierung und Markierung 9
2.6 Scheduling 10

2.6.1 Queueing 10

2.6.2 Policing 11

2.6.3 Re-marking 11

2.7 Admission Control 12
2.8 DSCP Transparenz 12

3 QoS Umsetzung - AR003 13

3.1 QoS Umsetzungsprozess 13
3.2 Erhebung 14
3.3 Entwicklung 15
3.4 Umsetzung 16
3.5 Monitoring 16

4 Umsetzungsempfehlungen 17

4.1 Verkehrsklassen 17

4.1.1 Verkehrsklassenmodelle 17

4.1.2 Mappings 18

4.1.2.1 Serviceklasse zu Verkehrsklasse 18

4.1.2.2 Layer 2 QoS 19

4.1.2.3 IP Tunneling 19

4.1.2.4 Wireless LAN 20

4.1.2.4.1 User Priority 20

4.1.2.4.2 CAPWAP 20

4.1.3 Scheduling 22

4.1.3.1 Queueing 22

4.1.3.2 Policing 23

4.1.3.3 Re-marking 24

4.1.3.4 Queue Management 24

4.1.3.5 Scheduling Profile 25

4.2 Klassifizierung und Markierung 26

4.2.1 DSCP-Markierung 26

4.2.2 Klassifizierung und Markierung auf dem Endsystem 29

4.2.3 Klassifizierung und Markierung im Netzwerk 30
4.2.4 Netzübergänge 32
4.2.4.1 Bundesinterne Netzübergänge 32
4.2.4.2 Externe Netzübergänge 32
4.3 Admission Control 35
5 Fallbeispiele 36
5.1 Verkehrsklassen 36
5.2 Klassifizierung und Markierung 37
5.2.1 Klassifizierung und Markierung im Netzwerk 37
5.2.2 Klassifizierung und Markierung auf dem Endsystem 38
5.2.2.1 BA / Windows Server 38
5.2.2.2 UCC Server 39
5.2.2.3 BA / APS 40
5.2.2.4 Unix Server 41
5.2.2.5 Virtualisierung 42
5.3 UCC 43
5.4 Softwareverteilung 44
5.5 Printing 45
5.6 Internet 46
5.7 VDI 47
Anhänge 48
A. Änderungen gegenüber Vorversion 48
B. Referenzen 48
C. Abkürzungen 48

1 Einleitung

Mittels *Quality of Service (QoS)* können die Übertragungseigenschaften der Netzwerke bezüglich Latenzzeit, Laufzeitvariation und Paketverlust für kritische Anwendungen optimiert werden. Die IKT-Architekturvorgabe [AR003] macht auf Stufe Bund Vorgaben für die Umsetzung von QoS und soll die Kompatibilität und Interoperabilität in der Bundesverwaltung sicherstellen. Sie soll ein stabiles und belastbares Regelwerk schaffen.

[AR003] basiert auf [DiffServ] (Differentiated Services Architektur[2]), welche ein Schema für die Klassifizierung und Markierung von IP-Paketen verwendet und einen Geltungsbereich auf OSI Layer 3 (IP) besitzt. IP-Pakete werden anhand der Anwendung klassifiziert und mit einem sog. DSCP-Wert gekennzeichnet, so dass Netzelemente im Übertragungspfad anhand dieses DSCP-Wertes das Behandlungsverfahren (Per Hop Behavior – PHB) des Paketes bestimmen. Auf diese Weise können IP-Pakete von unterschiedlichen Anwendungen mit unterschiedlichen DSCP-Werten gekennzeichnet und im Netzwerk differenziert behandelt werden. Ziel ist es, dass jede Anwendung eine den Anforderungen entsprechende Übertragungsqualität im Netzwerk erhält.

Die IKT-Architekturvorgabe [AR003] regelt insbesondere:

- Verkehrsklassen und Dienstgüte (Latenzzeit, Laufzeitvariation, Paketverlust) für die End-to-End Datenübertragung in den Bundesnetzen
- Serviceklassen und DSCP-Werte
- Mapping von DSCP zu Verkehrsklassen
- Zuweisung der Anwendungen zu den Serviceklassen
- Klassifizierung und Markierung der IP-Pakete
- Schutz der Netzwerkgrenze mit Admission Control

Das vorliegende Dokument ist eine Beilage zu [AR003] und enthält Empfehlungen für die Planung und Umsetzung im Netzwerk und auf den IKT-Endsystemen.

In Kapitel 2 werden die technischen Begriffe erläutert, die für das allgemeine Verständnis von QoS im Zusammenhang mit der Architekturvorgabe [AR003] erforderlich sind.

Kapitel 3 enthält Empfehlungen für die Planung und Organisation der Umsetzung von QoS.

Kapitel 4 enthält Empfehlungen für die Leistungserbringer, wie die Vorgabe technisch auf betroffenen Systemen umgesetzt werden kann.

Kapitel 5 enthält Fallbeispiele, die darstellen, wie eine mögliche Umsetzung in verschiedenen Szenarien erfolgen könnte.

[2] RFC 2475 - An Architecture for Differentiated Services

2 Begrifflichkeiten

2.1 Verkehrsklassen

In eine Verkehrsklasse, im Sinne von DiffServ, wird Verkehr von verschiedenen Anwendungen resp. Serviceklassen (siehe Kapitel 2.3) mit ähnlicher Verkehrscharakteristik und vergleichbaren Anforderungen an die Übertragungsqualität zusammengefasst (aggregiert[3]). Die Übertragungsqualität wird sichergestellt, indem ein geeignetes Weiterleitungsverfahren (Per Hop Behavior – PHB[4]) für jede Verkehrsklasse verwendet wird.

Die Differentiated Services Architektur unterscheidet nachfolgende Weiterleitungsverfahren:

- *Default Forwarding DF (RFC 2474[5])* für Best Effort Anwendungen. Dieses Weiterleitungsverfahren übermittelt Verkehr solange im Netzwerk freie Ressourcen vorhanden sind. Eine fehlerfreie und vollständige Übermittlung der Daten ist nicht garantiert und die Übermittlung kann von Paketverlust und variablen Laufzeiten betroffen sein. Anwendungen adaptieren bei Bedarf ihre Übertragungsrate und senden im Netzwerk verworfene Pakete gegebenenfalls erneut (Re-transmission).
- *Assured Forwarding AF (RFC 2597[6])* für Geschäftsanwendungen, die eine garantierte Übertragungsqualität benötigen. Dieses Weiterleitungsverfahren kann bei Bedarf einen definierten Anteil Netzkapazität nutzen, so dass Verkehr innerhalb der vorgesehenen Kapazität verlustfrei und mit einer festgelegten Dienstgüte (Siehe Kapitel 0) übermittelt wird. Verkehr über der vorgesehenen Kapazität kann von Paketverlust und variablen Laufzeiten betroffen sein.
- *Expedite Forwarding EF (RFC 3246[7])* für Anwendungen, die eine minimale Latenzzeit, Laufzeitvariation und Paketverluste erfordern. Dieses Weiterleitungsverfahren übermittelt den Verkehr immer zuerst und ist insbesondere geeignet für Echtzeitanwendungen wie VoIP.

[3] RFC 5127 - Aggregation of DiffServ Service Classes

[4] RFC 2475 - An Architecture for Differentiated Services

[5] RFC 2474 - Default Forwarding Per-Hop Behavior

[6] RFC 2597 - Assured Forwarding Per-Hop Behavior

[7] RFC 3246 - Expedited Forwarding Per-Hop Behavior

2.2 Dienstgüte

Die Übertragungsqualität oder Dienstgüte der Datenübermittlung wird, im Zusammenhang mit [AR003], durch die Bandbreite, Latenzzeit, Laufzeitvariation und Paketverlust der End-to-End Kommunikation definiert.

Merkmal	Beschreibung
Bandbreite (Bandwidth)	Garantierte Bandbreite der Datenübermittlung (Committed Information Rate – CIR)
Latenzzeit (Latency/Delay)	End-to-End Einweg-Laufzeit über alle Kommunikationsverbindungen. Latenz entsteht auf jedem Netzelement im Übertragungspfad und ist die Summe aus *Serialization Delay*, *Propagation Delay* und *Switching Delay* aller Netzelemente im Übertragungspfad. • *Serialization Delay* ist die benötigte Zeit für die Ausgabe eines Datenpaketes über eine Schnittstelle und ist abhängig von der Bandbreite der Schnittstelle und der Paketgrösse. • *Propagation Delay* ist die benötigte Zeit für die Übertragung über eine physische Verbindung und ist abhängig von der Distanz zwischen Sender und Empfänger. • *Switching Delay* ist die Zeit, die ein Netzelement benötigt, um ein Paket von einer Schnittstelle zu einer anderen zu übermitteln. Der Switching Delay ist abhängig von der Kapazität eines Netzelements, dessen Auslastung und der Netzwerklast.
Laufzeitvariation (Jitter)	Varianz der End-to-End Laufzeit. Netzelemente speichern Pakete vor der Übertragung in Queues ab. Abhängig von der Netzwerklast, bleiben die Pakete für kürzere oder für längere Zeit in der Queue gespeichert, bevor sie über die Verbindung weitergeleitet werden. Dadurch können unterschiedliche Laufzeiten für verschiedene Pakete über denselben Netzwerkpfad entstehen, was als Laufzeitvariation bezeichnet wird.
Paketverlust (Packet loss)	Pakete, die irgendwo im Übertragungspfad durch ein Netzelement verworfen werden. Paketverluste treten typischerweise bei überlasteten Netzwerkverbindungen auf.

Tabelle 1: Merkmale Dienstgüte

Um eine angemessene Dienstgüte für alle Anwendungen zu garantieren, muss neben genügend Bandbreite auch immer QoS implementiert werden.

- Eine priorisierte Übermittlung des Verkehrs von Echtzeitanwendungen kann nur mit QoS sichergestellt werden.
- Kurze Überlastungen von Netzwerkschnittstellen verursachen Laufzeitvariation und erhöhen die Latenzzeiten. Kurzzeitig und stochastisch überlastete Netzwerkverbindungen bewirken bereits nach wenigen Millisekunden Paketverluste. Eine Überlastung kann an jeder Stelle im Netzwerk entstehen wo eine Aggregation von Verkehr stattfindet.
- Bandbreite ist kostenrelevant. Insbesondere wenn Netzwerkverbindungen eingekauft werden müssen (wie z.B. den Einkauf von Carrier-Ethernet-Diensten/Layer-2-Diensten).

2.3 Serviceklassen

Anwendungen werden entsprechend ihrer Verkehrscharakteristik und Anforderungen an die Dienstgüte in Serviceklassen zusammengefasst. Nachfolgende 12 Serviceklassen werden gem. RFC 4594[8] unterschieden:

Serviceklasse	Verkehrscharakteristik	Toleranz zu		
		Paket-verlust	Latenz-zeit	Laufzeit-variation
Network Control	Variable Paketgrössen, kurze unelastische Verbindungen (BGP)	Low	Low	Yes
Telephony	Fixe Paketgrösse, kleine Pakete, konstante Übertragungsrate, geringe Bandbreite	Very Low	Very Low	Very Low
Signalling	Variable Paketgrösse, kurze Bursts, kurzlebige Verbindungen	Low	Low	Yes
Multimedia Conferencing	Variable Paketgrössen, konstante Übertragungsrate, adaptive Bandbreite	Low – Medium	Very Low	Low
Real time Interactive	Variable Übertragungsrate, unelastische Streams	Low	Very Low	Low
Multimedia Streaming	Variable Paketgrösse, variable Übertragungsrate	Low – Medium	Medium	Yes
Broadcast Video	Konstante und variable Übertragungsraten, unelastische Verbindungen, keine Bursts.	Very Low	Medium	Low
Low Latency Data	Variable Übertragungsraten, kurze Bursts, kurzlebige elastische Verbindungen	Low	Low - Medium	Yes
OAM	Variable Paketgrössen, elastische und unelastische Verbindungen	Low	Medium	Yes
High Throughput Data	Variable Übertragungsrate, lange Bursts, langlebige Verbindungen	Low	Medium-High	Yes
Standard	Undifferenzierte Anwendungen	Nicht definiert		
Low-Priority Data	Nichtechtzeit, elastisch	High	High	Yes

Tabelle 2: DiffServ Serviceklassen

[8] RFC 4594 - Configuration Guidelines for Differentiated Service Classes

2.4 Differentiated Service Code Point - DSCP

Im Falle von DiffServ erfolgt die Kennzeichnung der Serviceklassen anhand eines Code-points, des sog. DSCP-Wertes im DS-Field[9] des IP-Headers. Jedes IP-Paket besitzt einen solchen DSCP-Wert und Netzelemente können diesen nutzen, um die Priorisierung bei der Übermittlung eines IP-Pakets zu bestimmen.

ToS Feld im IPv4 Header:

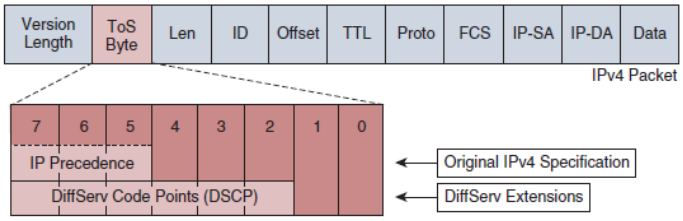


Abbildung 1: DS-Field (Type of Service) in IPv4 header

Im Fall von IPv6 wird der DSCP-Wert im Traffic Class Feld transportiert.

Traffic Class Feld im IPv6 Header:

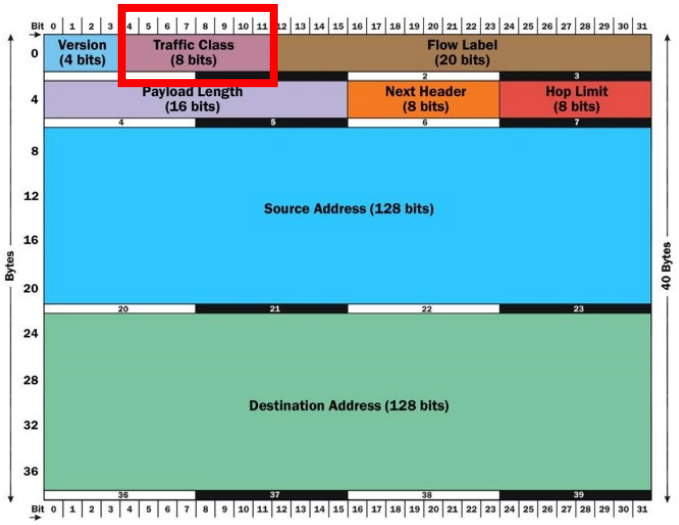


Abbildung 2: Traffic Class in IPv6 Header

[9] RFC 2474 - Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers (RFC2474 aktualisiert durch RFC3168 und RFC3260)

2.5 Klassifizierung und Markierung

Die Klassifizierung ist die Zuweisung der IP-Pakete zu den entsprechenden Serviceklassen.

Die Markierung beinhaltet das Setzen der DSCP-Werte im DS-Field der IP-Pakete entsprechend der klassifizierten Serviceklasse. Idealerweise erfolgt die Markierung der IP-Pakete mit entsprechenden DSCP-Werten einmalig und möglichst nahe beim Absender.

Ein Netzwerk oder eine Netzwerkzone, in der bestimmte DSCP-Werte Gültigkeit besitzen, wird als *DiffServ Domäne* bezeichnet. Die Grenze an der die DSCP-Werte gesetzt werden, ist die *Trust Boundary*. Systeme, die Teil der *Trust Boundary* sind, müssen die Vorgaben bez. DSCP-Markierung und -Nutzung einhalten, so dass innerhalb der *Trust Boundary* jedes IP-Paket einen gültigen DSCP-Wert besitzt und die Netzelemente im Übertragungspfad dem vorhandenen DSCP-Wert im IP-Paket vertrauen, und damit die zugehörige Verkehrsklasse bestimmen, ohne dass jedes Paket weiter klassifiziert und markiert werden muss.

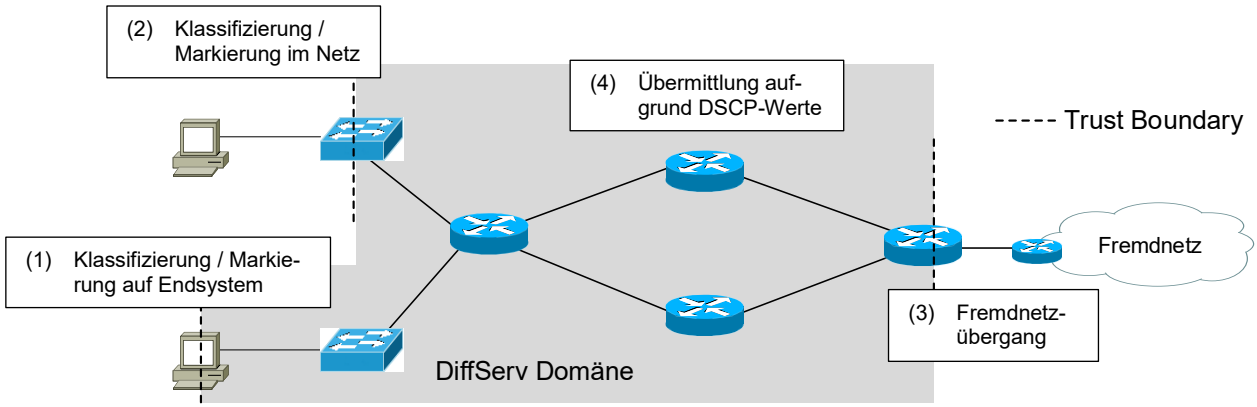


Abbildung 3: Klassifizierung und Markierung

(1) Die Klassifizierung und Markierung des Verkehrs findet auf dem sendenden Endsystem statt. Solche Endsysteme (Absender) sind Teil der *Trust Boundary* und müssen die Vorgaben bez. DSCP-Markierung und -Nutzung einhalten. Nachfolgende Netzelemente im Übertragungspfad vertrauen den vom Endsystem gesetzten DSCP-Werten und bestimmen damit das Weiterleitungsverfahren und die Verkehrsklasse für die Übermittlung der Pakete.

(2) Die Klassifizierung und Markierung des Verkehrs findet im Netzwerk statt. In diesem Falle sollte die Klassifizierung und Markierung von einem Netzelement (Switch/Router), möglichst nahe beim Absender, durchgeführt werden. Allfälligen durch das Endsystem gesetzten DSCP-Werten werden nicht vertraut und mit neuen Werten überschrieben.

(3) An Netzübergängen zu Fremdnetzen für welche keine oder andere QoS Vorgaben gelten, wird der Verkehr im Netzwerk von einem Netzelement möglichst nahe beim Netzübergang klassifiziert und markiert. DSCP-Werten aus dem Fremdnetz werden nicht vertraut und mit neuen Werten überschrieben.

(4) IP-Pakete innerhalb der *Trust Boundary* werden aufgrund des bestehenden DSCP-Wertes behandelt und erfordern keine weitere Klassifizierung oder Markierung durch die Netzelemente im Übertragungspfad.

2.6 Scheduling

2.6.1 Queueing

Netzelemente speichern Datenpakete vor der Übertragung über eine Leitung in *Queues* ab. Abhängig von der Netzwerklast bleiben Pakete für kürzere oder für längere Zeit in der *Queue* gespeichert, bevor sie über die Leitung gesendet oder gegebenenfalls verworfen werden. Anhand der DSCP-Markierung können Datenpakete durch unterschiedliche *Queues* übermittelt werden. Der Scheduler bedient die *Queues* einer Schnittstelle und entscheidet wann welche *Queue* bedient wird. Die unterschiedlichen *Queues* müssen bezüglich der Dienstgüte abgestimmt sein, wobei zu beachten gilt, dass generell eine kleine *Queue* die Latenzzeit und Laufzeitvariation verringert und gleichzeitig den Paketverlust erhöht, während eine grosse *Queue* den Paketverlust verringert und gleichzeitig die Latenzzeit und Laufzeitvariation erhöht.

Folgende grundlegende *Queueing*-Verfahren werden unterschieden:

- **Priority Queueing**
  Pakete in einer *Priority Queue* werden immer zuerst übermittelt. Andere *Queues* werden nur bedient, wenn alle *Priority Queues* leer sind. *Priority Queueing* eignet sich insbesondere für Verkehr von Echtzeitanwendungen wie VoIP.
- **Weighted Queueing**
  Weighted Queues können mit unterschiedlicher Gewichtung bedient werden. Somit erhält eine *Queue* entsprechend ihrer Gewichtung einen definierten Anteil der verfügbaren Ressourcen zugeteilt. Mittels geeignetem Design kann so jeder *Queue* eine bestimmte Bandbreite zugeteilt werden. Eine *Weighted Queue* wird nur bedient, wenn alle *Priority Queues* leer sind.

Beispiel Queue-Stuktur:

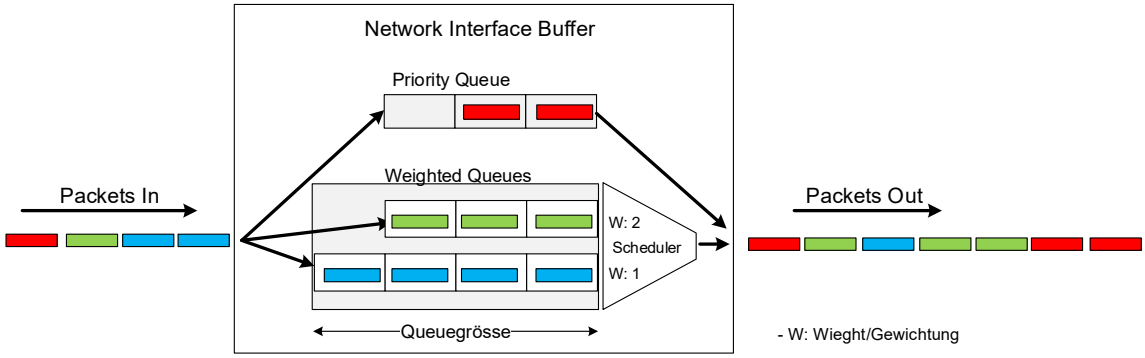


Abbildung 4: Queue-Struktur

2.6.2 Policing

Mittels *Policing* begrenzen Netzelemente die nutzbare Bandbreite für Verkehr auf eine zulässige Rate (*CIR - Commited Information Rate*). Verkehr über dieser Rate wird typischerweise verworfen. Mittels *Policing* kann die Rate des Gesamtverkehrs auf einer physischen Schnittstelle, oder auch die Rate von nur ganz spezifischem Verkehr begrenzt werden. *Policing* ist wichtig im Zusammenhang mit *Priority Queueing* um *Starvation*[10] zu verhindern.

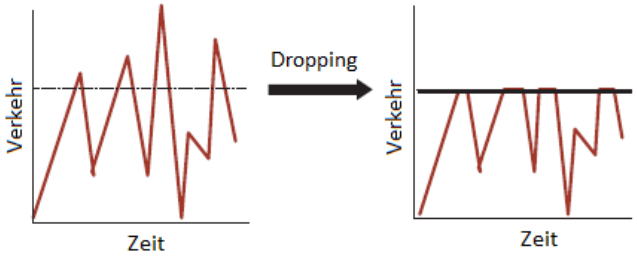


Abbildung 5: Policing

2.6.3 Re-marking

Mittels *Re-marking* wird Verkehr über der zulässigen Rate (CIR) nicht verworfen und stattdessen mit einem neuen DSCP-Wert markiert und übertragen, falls im Netzwerk genügend freie Ressourcen vorhanden sind.

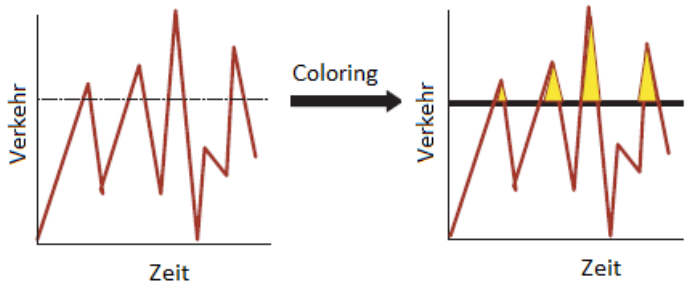


Abbildung 6: Re-marking

Aufgrund der neuen DSCP-Markierung können diese Pakete auch von nachfolgenden Netzelementen im Übertragungspfad als «Out-of-Profile» erkannt und im Falle einer Überlast zuerst verworfen werden. *Re-marking* wird verwendet, um eine minimale Bandbreite zu garantieren. Eine definierte Dienstgüte gilt dann nur für Verkehr, welcher innerhalb der zulässigen Rate (CIR) übertragen wird.

[10] Aushungern einer tiefer priorisierten Queue aufgrund dauerhaft anhaltendem Verkehr in einer *Priority Queue*.

2.7 Admission Control

Mittels *Admission Control* wird das Netzwerk vor unzulässigem Verkehr von Endsystemen und an Netzübergängen geschützt. Dabei wird insbesondere sichergestellt,

- dass nur zulässige DSCP-Werte in die *Trust Boundary* weitergeleitet werden.
- dass die Nutzung bestimmter (kritischer) DSCP-Werte nur unter geregelten Bedingungen möglich ist.

Admission Control sollte immer auf einem Netzelement möglichst nahe beim Absender eingesetzt werden.

2.8 DSCP Transparenz

Unter *DSCP Transparenz* wird in Zusammenhang mit [AR003] verstanden, dass der an der *Trust Boundary* gesetzte DSCP-Werte bei der Übermittlung nicht verändert werden. Davon sind insbesondere Netzelemente im Übertragungspfad betroffen (z.B. Router, Switches, Firewalls, Gateways, Loadbalancer etc.).

3 QoS Umsetzung - AR003

3.1 QoS Umsetzungsprozess

Die Umsetzung der QoS Architekturvorgabe [AR003] wirkt sich grundsätzlich auf alle IKT-Systeme in der zivilen Bundesverwaltung aus und stellt Anforderungen sowohl an die Betreiber von Netzelementen wie auch an die Betreiber von Endsystemen. Die Umsetzung und der Betrieb von QoS erfordert daher von den Leistungserbringern eine entsprechende Planung und Organisation. Insbesondere müssen alle Betreiber von Informatiksystemen im Geltungsbereich der Weisung

- prüfen welche QoS-Anforderungen gemäss [AR003] an sie gestellt werden und abklären welche Systeme betroffen sind.
- die technischen Massnahmen für die betroffenen Systeme definieren und umsetzen, damit die QoS-Anforderungen gemäss [AR003] möglichst gut erfüllt werden.
- verifizieren ob die Massnahmen korrekt umgesetzt wurden und das gewünschte Verhalten bewirken.

Der nachfolgend beschriebene Umsetzungsprozess bietet zusammen mit den Umsetzungsempfehlungen und Fallbeispielen eine hilfreiche Ergänzung zu der QoS-Architektur [AR003].

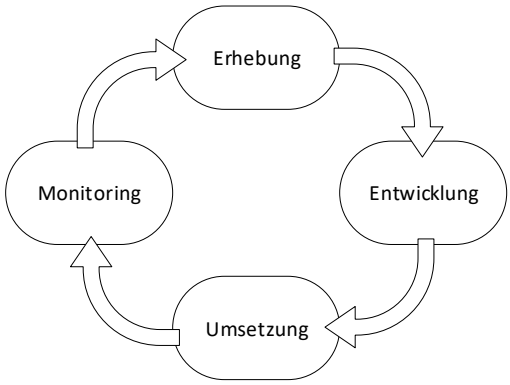


Abbildung 7: QoS Umsetzungsprozess

Um die Einführung der QoS-Architektur in der Bundesverwaltung zu unterstützen und insbesondere um den Austausch von Informationen zwischen den Leistungserbringer zu fördern, wurde eine Sharepoint-Seite für die Umsetzung der QoS-Vorgabe [AR003] aufgeschaltet:

https://sharepoint.admin.ch/sites/609-QoS_AR003/_layouts/15/start.aspx#/SitePages/Homepage.aspx

Die Sharepoint-Seite bietet den Leistungserbringern eine Struktur, um ihre Ergebnisse der Phasen «Erhebung», «Entwicklung» und «Umsetzung» zu dokumentieren sowie eine Datenablage, um technische Konzepte unter den Leistungserbringern zu teilen.

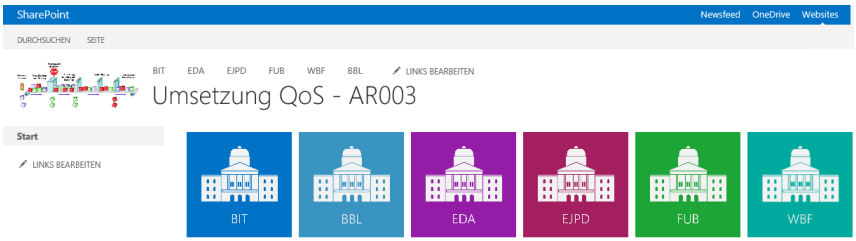


Abbildung 8: Sharepoint Seite Umsetzung QoS - AR003

3.2 Erhebung

Der QoS-Umsetzungsprozess ist wiederkehrend und kann jeweils mit einer (neuen) Erhebung aufgrund verschiedener Umstände angestossen werden.

- Initiale Einführung von QoS.
- Änderungen in der QoS Vorgabe [AR003].
- Beschaffung und Einführung neuer IT-Systeme.
- Life Cycle bestehender IT-Systeme.
- Performance- oder betriebliche Probleme oder Anforderungen.

Bei der «Erhebung» müssen die betroffenen Bereiche und Systeme beim Leistungserbringer identifiziert werden, wobei für jedes System zu beurteilen ist, welche Anforderungen aus der QoS Vorgabe dafür hervorgehen.

Die Leistungserbringer können die Ergebnisse ihrer Erhebung auf der Sharepoint-Seite in der entsprechenden Rubrik dokumentieren.

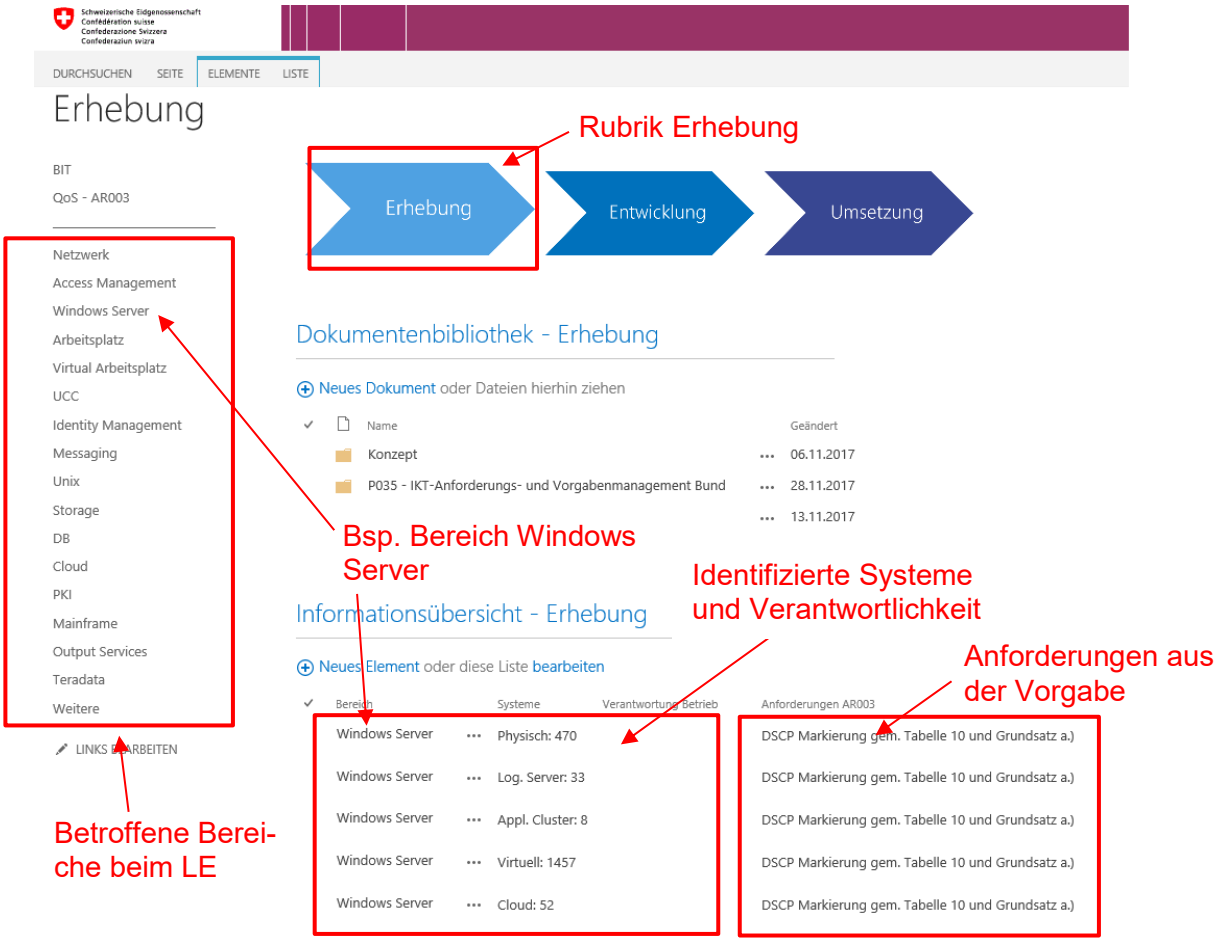


Abbildung 9: Sharepoint Seite AR003 – Erhebung

Von den Anforderungen bezüglich der Verkehrsklassen sind die Netzelemente betroffen. In diesem Zusammenhang ist ein Netzelement eine aktive Komponente im Übertragungspfad zwischen zwei Endsystemen. Die Anforderungen bezüglich Klassifizierung und Markierung betreffen primär die Endsysteme und Netzübergänge. Ein Endsystem ist in diesem Zusammenhang jedes System, welches an einem Netzwerk des Bundes angeschlossen ist.

Anforderungen bezüglich Verkehrsklassen und/oder die Zuweisung von DSCP-Werten zu den Anwendungen, die in der QoS-Vorgabe [AR003] nicht genügend berücksichtigt wurden, können als IKT-Anforderung auf Stufe Bund gemäss [P035] eingegeben werden.

3.3 Entwicklung

In der Phase «Entwicklung» werden die technischen Lösungen und Konzepte für die betroffenen Systeme erarbeitet. Die Anforderungen an die jeweiligen Bereiche und Systeme gehen aus der «Erhebung» hervor. Die QoS-Systemeinstellungen sollten nach Möglichkeit in einer Test- und Integrationsumgebung entwickelt und mit der entsprechenden Betriebsdokumentation für die Produktionsumgebung freigegeben werden.

Die Leistungserbringer können die Ergebnisse ihrer Entwicklung auf der Sharepoint-Seite in der entsprechenden Rubrik dokumentieren und allfällige Konzepte für andere Bereiche verfügbar machen.

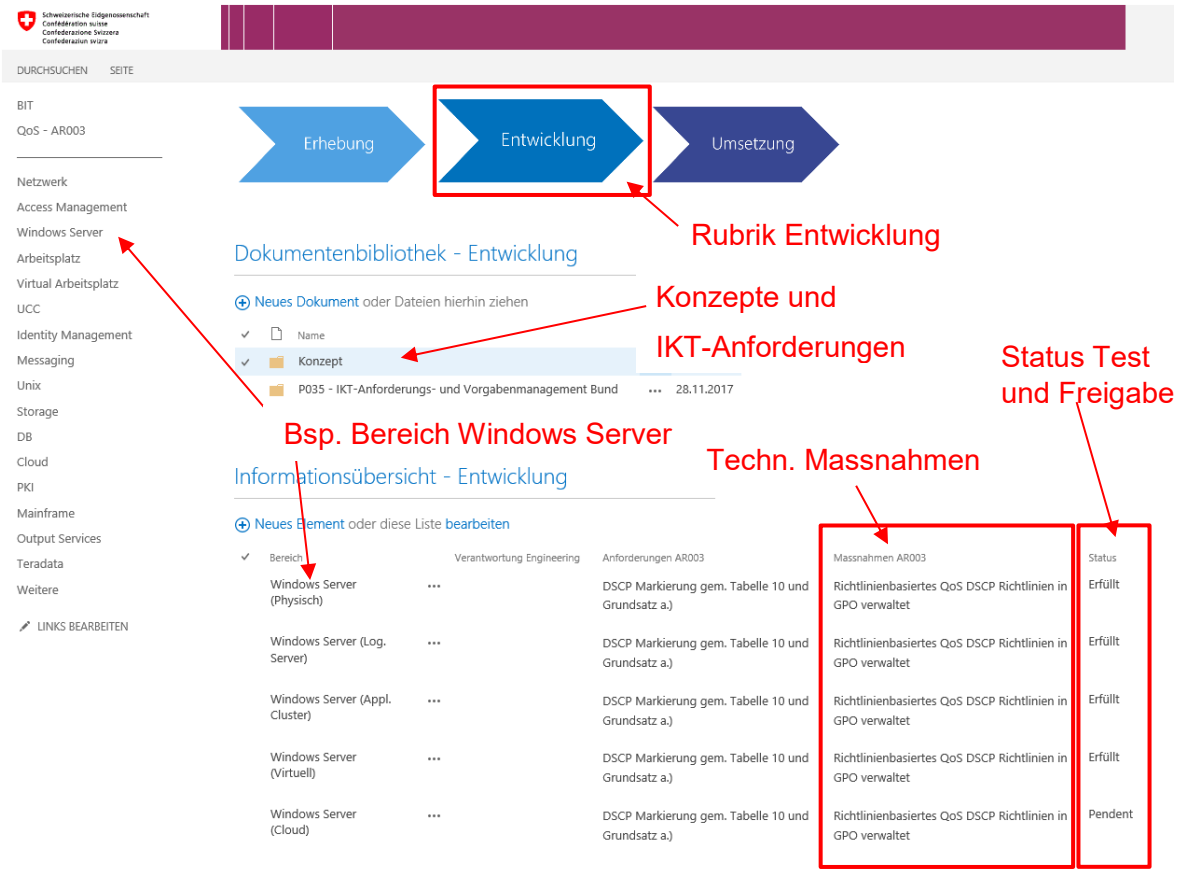


Abbildung 10: Sharepoint Seite AR003 - Entwicklung

Abweichungen von der QoS Vorgabe [AR003] müssen als IKT-Anforderung auf Stufe Bund gemäss [P035] eingegeben werden.

Endsysteme im Geltungsbereich [AR003], für welche die Klassifizierung und Markierung des Verkehrs im Netzwerk erfolgen soll, erfordern eine IKT-Anforderung auf Stufe Bund [P035]. Dabei sind folgende Information zwingend anzugeben:

- Betroffene Systeme (inkl. allfällig genutzte Übergänge zu externen Fremdnetzen)
- Netzwerkanschlüsse der betroffenen Systeme
- Art des Verkehrs und benötigte Dienstgüte und Bandbreite
- Kommunikationsmatrix

3.4 Umsetzung

In der Phase «Umsetzung» wird die Aktivierung der neuen QoS-Systemeinstellungen in der Produktionsumgebung geplant und durchgeführt. Dabei sind technische und organisatorische Abhängigkeiten vorgängig zu klären und ggf. die Systemänderungen über einen ordentlichen Change-Prozess oder eine Releaseplanung anzumelden.

Die Leistungserbringer können den Stand der Umsetzung auf der Sharepoint-Seite in der entsprechenden Rubrik dokumentieren.

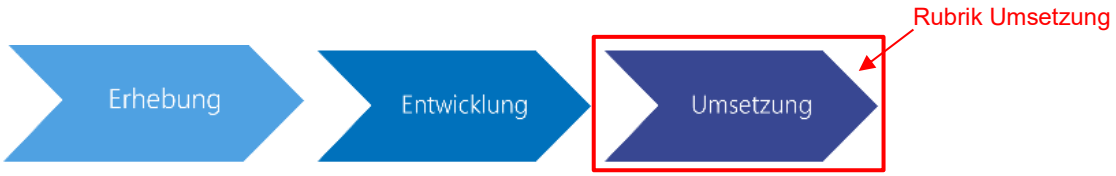


Abbildung 11: Sharepoint Seite AR003 - Umsetzung

3.5 Monitoring

In der QoS-Vorgabe [AR003] werden keine spezifischen Anforderungen an das Monitoring definiert. Es ist aber dennoch sinnvoll und wird empfohlen, dass die Leistungserbringer die Auswirkungen und die Konformität der QoS-Einstellungen auf den Systemen überwachen um bei unerwünschten Effekten entsprechende Massnahmen einleiten.

Neben der End-to-End Dienstgüte (Latenz, Laufzeitvariation, Paketverlust) gem. *Tabelle 3*, sind auch nachfolgende Informationen von besonderem Interesse und geben wertvolle Auskunft über die Qualität der Datenübermittlung und über potentielle Fehlkonfigurationen und Engpässe.

- DSCP-Statistik (Statistik über die Nutzung der DSCP-Werte pro Endsystem)
- Queuestatistik der Interfaces von Netzelementen (Statistik über die Anzahl übertragen/verworfene Pakete pro Verkehrsklasse)

4 Umsetzungsempfehlungen

4.1 Verkehrsklassen

4.1.1 Verkehrsklassenmodelle

Die QoS-Vorgabe [AR003] definiert folgende obligatorische und optionale Verkehrsklassen und Dienstgüteparameter, welche für die End-to-End Einwegkommunikation gelten:

Verkehrs-klasse	Network Con-trol [NC]	Real Time [RT]	Multimedia [MM]	Business [BU]	Best Effort [BE]
Latenzzeit	Nicht definiert	< 100ms	<150ms	<150ms	Best Effort
Laufzeitvariation	Nicht definiert	< 20ms	< 30ms	< 100ms	Best Effort
Paketverlust	Nicht definiert	< 0,5%	< 1%	< 0,5%	Best Effort
Verbindlichkeit	Optional	Obligatorisch	Optional	Obligatorisch	Obligatorisch

Tabelle 3: Verkehrsklassen

Verkehrsklassen müssen auf allen Netzelementen im Geltungsbereich von [AR003] implementiert werden, insbesondere wenn

- sich das Netzelement im Übertragungspfad von End-to-End Datenkommunikation befindet und
- eine Aggregation von Datenverkehr im Netzelement stattfindet und
- Verkehr von mehreren Verkehrsklassen vom Netzelement übertragen wird.

Dies gilt insbesondere für Router, Switches, Firewalls, Proxies, Gateways, Loadbalancer …

Gemäss der QoS-Vorgabe [AR003] obliegt es den Leistungserbringern, ein für das jeweilige Netzwerksegment optimales Verkehrsklassenmodell zu implementieren, so dass die Dienstgüteparameter End-to-End eingehalten werden. Es ergeben sich nachfolgende Modelle, die interoperabel sind und in unterschiedlichen Netzwerkzonen zum Einsatz kommen können.

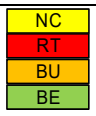
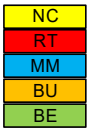
Modell	VK	Beschreibung
3VK		*Drei Verkehrsklassen.* Diese obligatorischen Verkehrsklassen entsprechen der Mindestanforderung gem. [AR003], die für alle betroffenen Netzelemente im Geltungsbereich gilt. Geeignet in LANs (z.B. Campus LAN oder Datacenter LAN), wo üblicherweise genügend Bandbreite vorhanden ist und/oder eine geringere Aggregation von Netzverkehr verschiedener Kunden stattfindet.
3VK+NC		*Drei Verkehrsklassen + Network Control.* Zusätzlich zu den obligatorischen Verkehrsklassen wird die Verkehrsklasse *Network Control* verwendet. Geeignet für Verbindungen mit kritischen Routingupdates zwischen Netzelementen.
4VK+NC		*Vier Verkehrsklassen + Network Control.* Punktuell oder flächendeckend kann die optionale Verkehrsklasse «Multimedia» verwendet werden. Geeignet für Netzwerkzonen mit einer hohen Aggregation von Verkehr verschiedener Kunden und/oder verschiedener Verkehrsklassen und grossem Verkehrsvolumen.

Tabelle 4: Verkehrsklassenmodelle

4.1.2 Mappings

4.1.2.1 Serviceklasse zu Verkehrsklasse

Die QoS-Vorgabe [AR003] gibt nachfolgende Serviceklassen und DSCP-Werte vor, die im gesamten Geltungsbereich der Weisung zweckgebunden sind:

Serviceklasse	DSCP-Name	DSCP (Dez.)
Network Control (Backbone)	CS7	57
Network Control (Access)	CS6	48
Telephony	EF	46
Signalling	CS5	40
Multimedia Conferencing	AF41-43	34-38
Real time Interactive	CS4	32
Multimedia Streaming	AF31-33	26-30
Broadcast Video	CS3	24
Low Latency Data	AF21-23	18-22
OAM	CS2	16
High Throughput Data	AF11-13	10-14
Standard	DF	0
Low-Priority Data	CS1	8

Tabelle 5: Serviceklassen und DSCP-Werte

In der QoS-Vorgabe [AR003] ist das Mapping zwischen den Serviceklassen und den Verkehrsklassen geregelt und damit auch die Interoperabilität zwischen den verschiedenen Verkehrsklassenmodellen. Abhängig vom gewählten Verkehrsklassenmodell ist gemäss [AR003] das Mapping wie folgt vorgegeben:

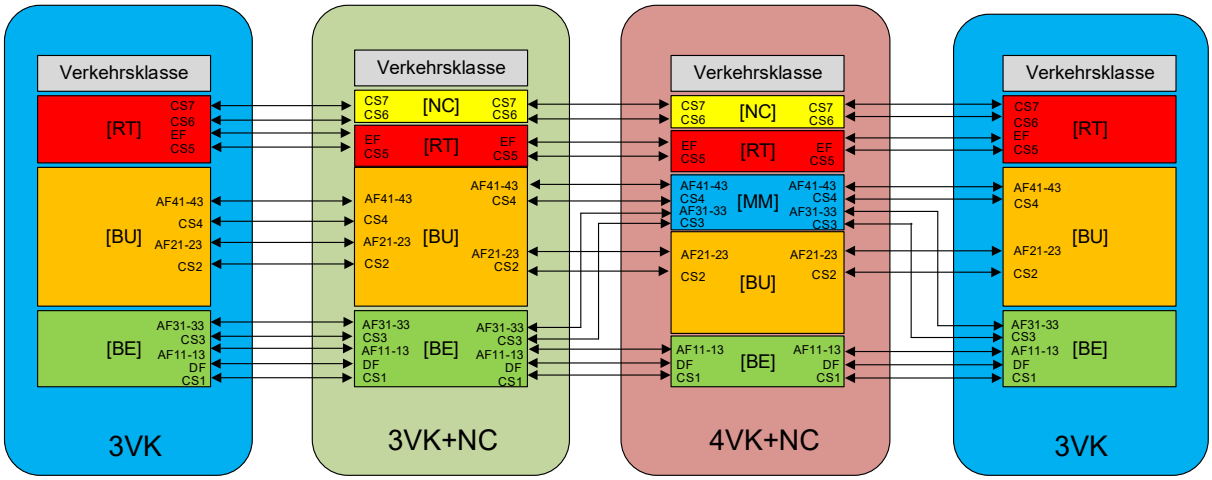


Abbildung 12: End-to-End Mapping der Serviceklassen zu Verkehrsklassen

Hinweis:

Leistungserbringer dürfen innerhalb ihrer Netze auch zusätzliche Serviceklassen und DSCP-Werte betreiben. Alle DSCP-Werte, die in der QoS-Vorgabe [AR003] nicht expliziert reserviert sind, stehen den Leistungserbringern zur Nutzung frei. Es gilt zu beachten, dass zusätzliche Serviceklassen nicht im gesamten Geltungsbereich [AR003] Gültigkeit besitzen und bei der Übertragung durch Netze anderer Leistungserbringer typischerweise in der [BE] Verkehrsklasse übermittelt werden.

4.1.2.2 Layer 2 QoS

Die Leistungserbringer müssen sicherstellen, dass QoS durchgängig über alle Übertragungsschichten implementiert ist. Ein einfaches Standardmapping der DSCP-Werte auf die *Layer 2 Codepoints* (IEEE 802.1p/MPLS Exp) für die *VLAN/Trunk* und MPLS-Übermittlungen, wird gemäss nachfolgender Abbildung empfohlen:

Serviceklasse	DSCP	802.1p/ MPLS Exp.	VK
Network Control	CS7	7	[NC]
Network Control	CS6	6	
Telephony	EF	5	[RT]
Signalling	CS5		
Multimedia Conferencing	AF4	4	[MM]
Real Time Interactive	CS4		
Multimedia Streaming	AF3	3	
Broadcast Video	CS3		
Low Latency Data	AF2	2	[BU]
OAM	CS2		
High Throughput Data	AF1	1	[BE]
Low Priority Data	CS1		
Standard	DF	0	

Abbildung 13: Mapping DSCP zu Layer-2 Codepoints

Die *Layer 2 Codepoints* sind nur innerhalb der jeweiligen *Layer 2 Domäne* von Bedeutung, weshalb keine bundesweite Standardisierung erforderlich ist und in [AR003] keine weiteren Vorgaben dazu spezifiziert sind. Es obliegt den Leistungserbringern, die gemäss ihren Anforderungen optimale Zuweisung der *Layer 2 Codepoints* festzulegen.

Insbesondere für folgende *Layer 2 Netze* sind entsprechende Mappings durch die Leistungserbringer festzulegen:

- Campus LAN – IEEE 802.1Q/p
- Carrier Ethernet und Layer 2 Datentransport – IEEE 802.1Q/p
- MPLS Backbone – MPLS EXP
- Datacenter (SDN, DCB)

4.1.2.3 IP Tunneling

Bei der Verwendung von Tunnel-Protokollen wird ein neuer IP-Header erzeugt und dem originalen Paket vorangestellt. Soll der ursprüngliche DSCP-Wert des originalen IP-Paketes erhalten bleiben, so muss dieser jeweils in den neuen Tunnel-Header kopiert werden (Beispiel: GRE Tunnel mit IPSEC Verschlüsselung).

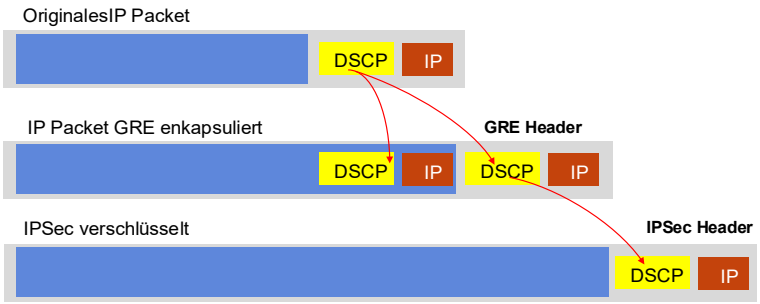


Abbildung 14: Tunnel Protokolle

Bei der Übertragung von verschlüsselten Verbindungen durch das öffentliche Internet kann es ggf. besser sein, den DSCP-Wert nicht zu kopieren und stattdessen den Standard DSCP-Wert DF im äusseren Header zu verwenden.

4.1.2.4 Wireless LAN

4.1.2.4.1 User Priority

Wireless LAN verwendet für die Priorisierung auf der Funkstrecke IEEE 802.11e *User Priority (UP)*. Es stehen vier Klassen mit acht fix zugewiesenen Priorisierungsleveln (User Priority UP1 – UP7) zur Verfügung.

Ein einfaches Standard-Mapping zwischen DSCP und 802.11e UP wird wie folgt empfohlen:

Serviceklasse	DSCP	802.11 UP
Telephony	EF	UP 7, UP 6 – Voice Access Category
Signalling	CS5	
Multimedia Conferencing	AF41	UP 5, UP 4 – Video Access Category
Real Time Interactive	CS4	
Multimedia Streaming	AF31	
Broadcast Video	CS3	
Low Latency Data	AF21	UP 3, UP 0 – Best Effort Access Category
OAM	CS2	
High Throughput Data	AF11	UP 2, UP 1 – Background Access Category
Standard	DF	
Low Priority Data	CS1	

Abbildung 15: Mapping DSCP zu 802.11e UP

Die *User Priority* ist nur innerhalb der jeweiligen Funkdomäne von Bedeutung und erfordert keine bundesweite Standardisierung und wird in [AR003] nicht weiter spezifiziert. Es obliegt den Leistungserbringern, die gemäss ihren Anforderungen optimale Zuweisung der *User Priority* festzulegen.

4.1.2.4.2 CAPWAP

Verkehr zwischen *Access Points* und *Wireless LAN Controller*, der in einem CAPWAP[11]-Tunnel 'enkapsuliert' wird, besitzt einen zusätzlichen IP-Header mit eigenem DSCP-Wert (ähnlich wie bei IP-Tunneling, Kapitel 4.1.2.3).

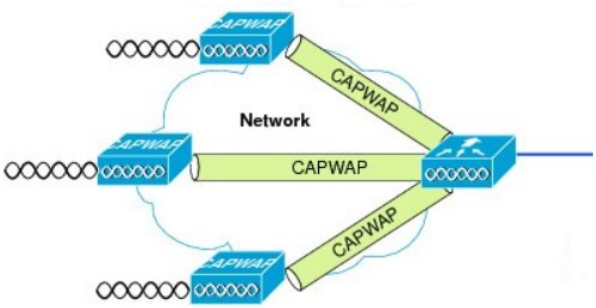


Abbildung 16: CAPWAP Tunnel zwischen Access Point und Controller

Um die Priorisierung durchgängig sicherzustellen, muss der *Wireless LAN Controller* beim «Downstream» (d.h. Verkehr vom Controller zum *Access Point* und dann über die Funkstrecke zum mobilen Endsystem) den DSCP-Wert für den CAPWAP-Header aus dem originalen IP-Paket kopieren. Vor der Übermittlung über die Funkstrecke nimmt der *Access Point* das Mapping von DSCP auf 802.11e UP vor.

[11] CAPWAP – Control And Provisioning of Wireless Access Point

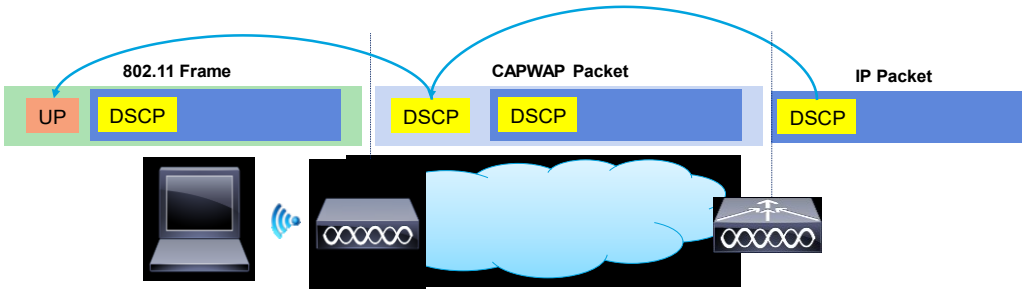


Abbildung 17: DSCP zu 802.11e UP Mapping Downstream

Im Upstream, d.h. im Verkehr vom mobilen Endsystem über die Funkstrecke zum *Access Point* und weiter zum *Wireless LAN Controller*, muss sowohl der DSCP-Wert wie auch die 802.11e UP auf dem Endsystem eingestellt werden, wobei letzteres ein WMM[12]-fähiges Endsystem voraussetzt. Der *Access Point* kopiert den DSCP-Wert für den CAPWAP-Header aus dem originalen IP-Paket.

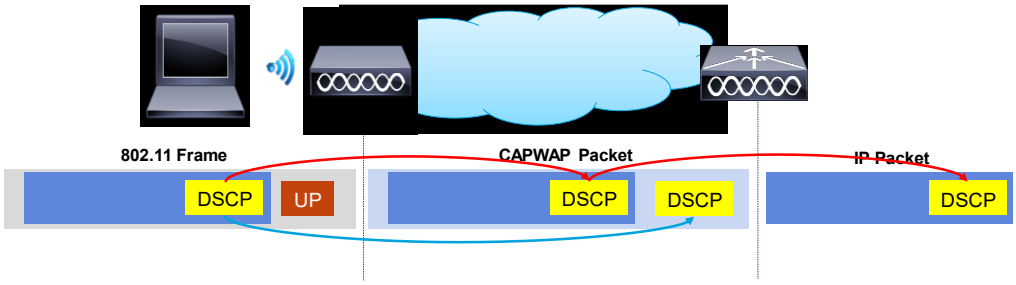


Abbildung 18: DSCP zu 802.11e UP Mapping Upstream

Beim öffentlichen WLAN-Zugang des Bundes soll der DSCP-Wert des CAPWAP-Headers nicht vom originalen IP-Paket kopiert und stattdessen der Standard DSCP-Wert DF verwendet werden.

[12] WMM – WiFi Multimedia (teilweise bekannt als Wireless Multimedia Extensions)

4.1.3 Scheduling

4.1.3.1 Queueing

Es wird empfohlen den Verkehr durch die Netzelemente anhand der DSCP-Werte den Queues zuzuweisen (*DSCP-to-Queue Mapping*). Für jede Verkehrsklasse sollte eine separate Queue verwendet werden.

- Verkehr aus der [RT] Verkehrsklasse sollte in *Priority Queues (PQ)* übermittelt werden.
- Verkehr aus anderen Verkehrsklassen kann in *Weighted Queues (WQ)* übermittelt werden.

Die *Queues* sind so abzustimmen, dass die Dienstgüteparameter eingehalten werden und für jede Verkehrsklasse ein definierter Anteil der Bandbreite garantiert wird (*CIR - Committed Information Rate*). Abhängig vom eingesetzten Verkehrsklassemodell kann ein einfaches Standardmapping *DSCP-to-Queue* wie folgt umgesetzt werden:

Verkehrsklassemodell: 3VK

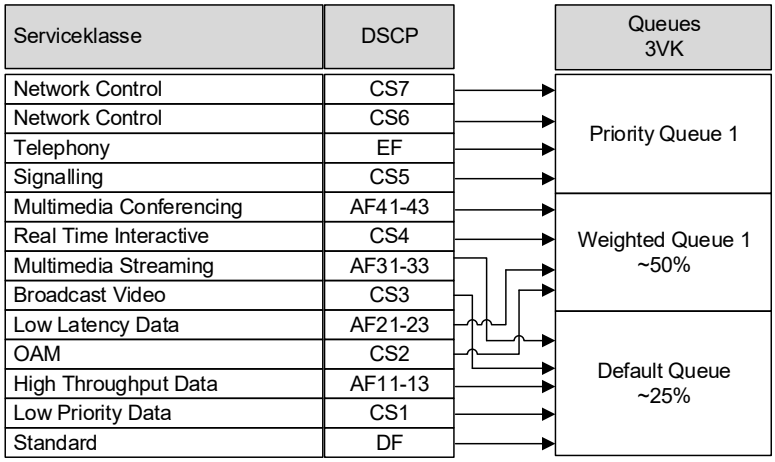


Abbildung 19: DSCP-to-Queue Mapping 3VK

Verkehrsklassemodell: 3VK+NC

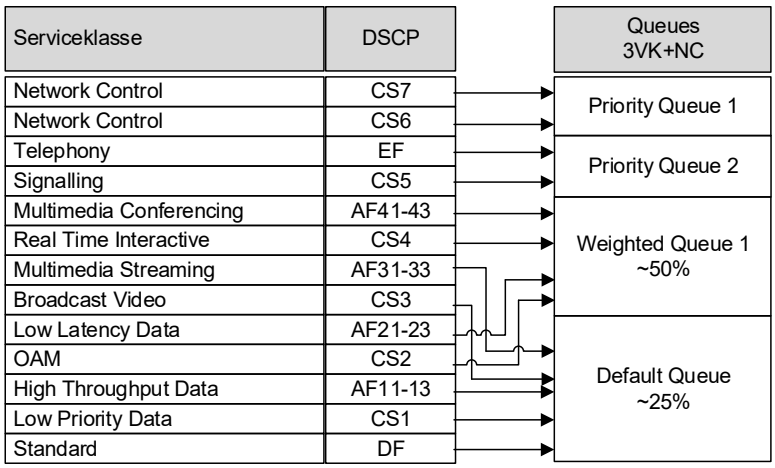


Abbildung 20: DSCP-to-Queue Mapping 3VK+NC

Verkehrsklassemodell: 4VK+NC

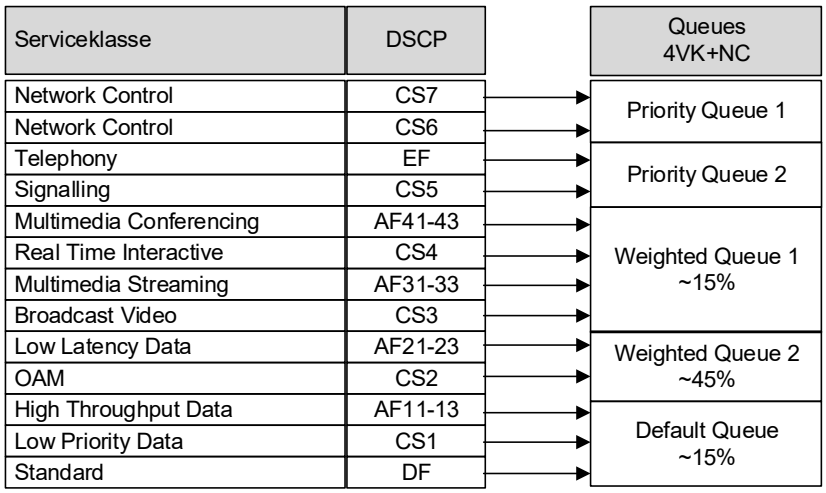


Abbildung 21: DSCP-to-Queue Mapping 4VK+NC

Die angegebenen Prozentwerte sind als Beispiel zu verstehen. Die *Queue*-Strukturen in Netzelementen können, abhängig vom Hersteller und Hardware, sehr unterschiedlich gestaltet sein. Es obliegt den Leistungserbringern die optimale Abstimmung der *Queues* für ihre Infrastrukturen festzulegen.

4.1.3.2 Policing

Policing soll eingesetzt werden, um den Verkehr von bestimmten Verkehrsklassen und/oder Netzverbindungen zu begrenzen. *Policing* sollte insbesondere eingesetzt werden, um

- die Bandbreite der Verkehrsklasse [RT] zu limitieren. Es sollte generell nie mehr als 33% der Referenzbandbreite[13] für Verkehr aus der Klasse [RT] zugelassen werden.
- die Bandbreite der optionalen Verkehrsklasse [MM] zu limitieren.
- den Gesamtverkehr über eine physische Schnittstelle auf die Referenzbandbreite zu limitieren, bevor dieser über eine Verbindung mit geringerer Bandbreite gesendet wird (Swisscom WARP).

Verkehr unterhalb der Begrenzung des *Policers* soll vom Netzelement, ohne Veränderung der DSCP-Werte, übermittelt werden (DSCP-Transparenz). Alle Pakete über der im *Policer* definierten Rate sollen verworfen werden (Drop).

[13] Als Referenzbandbreite kann die Bandbreite der physischen Schnittstelle oder die SLA Bandbreite gewählt werden.

4.1.3.3 Re-marking

Für jede Verkehrsklasse soll eine «Ziel-Bandbreite» (*CIR - Commited Information Rate*) festgelegt werden. Verkehr innerhalb der CIR soll übermittelt werden, ohne dass die DSCP-Werte verändert werden (DSCP-Transparenz). Sofern das Netzwerk freie Ressourcen besitzt, darf Verkehr über der CIR grundsätzlich auch übermittelt werden, so dass freie Bandbreite bis hin zur maximalen Auslastung (*PIR – Peak Information Rate*) genutzt werden darf.

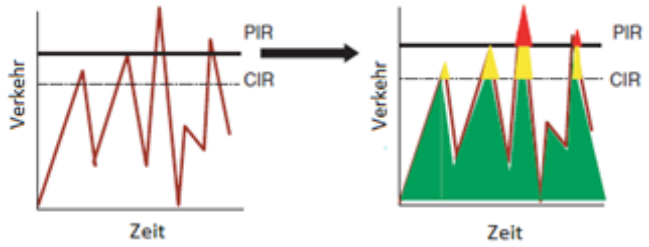


Abbildung 22: Re-Marking

Bei Verkehr über der CIR dürfen die DSCP-Werte des betroffenen Verkehrs mit dafür vorgesehenen Werten ersetzt werden (*Re-marking*). In [AR003] sind nachfolgende Serviceklassen für diesen Zweck vorbehalten:

Serviceklasse	Conforming	Exceeding	Violating
Multimedia Conferencing	AF41	AF42	AF43
Multimedia Streaming	AF31	AF32	AF33
Low Latency Data	AF21	AF22	AF23
High Throughput Data	AF11	AF12	AF13

Tabelle 6: Reservierte Serviceklassen für netzinternen Gebrauch AR003

Es obliegt den Leistungserbringern, die optimale Nutzung dieser Serviceklassen zu bestimmen.

4.1.3.4 Queue Management

Mittels Mechanismen wie *Random Early Detection (RED)* lässt sich Durchsatz der Verkehrsklassen weiter optimieren. Es wird empfohlen, dass die Netzelemente den Re-markierten Verkehr (gem. Kapitel 4.1.3.3) mittels RED bei einer Überlast zuerst zu verwerfen.

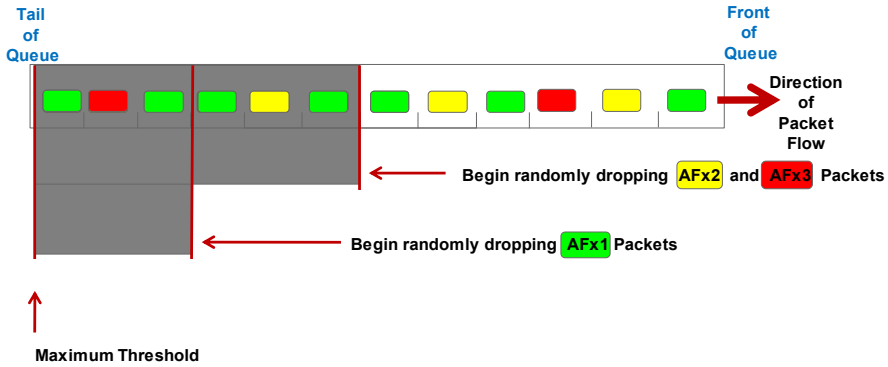


Abbildung 23: Random early detection (RED)

RED eignet sich insbesondere für die Verkehrsklassen [BE] und [BU] um den Durchsatz zu maximieren. RED ist ausdrücklich NICHT GEEIGNET für die Verkehrsklasse [RT].

4.1.3.5 Scheduling Profile

In verschiedenen Netzwerkzonen und für verschiedene Interface-Geschwindigkeiten von Netzelementen müssen die Ressourcen entsprechend dem Verkehrsaufkommen und der Art des Verkehrs optimiert werden. Insbesondere müssen die Leistungserbringer, gemäss ihren Anforderungen und SLA's, die Zuteilung der Netzressourcen zu den Verkehrsklassen festlegen. Für jede Verkehrsklasse soll eine garantierte Bandbreite (*CIR – Commited Information Rate*) und eine maximale Bandbreite (*PIR – Peak Information Rate*) festgelegt werden. Als Referenzbandbreite für die Zuteilung der Netzressourcen kann, abhängig von der Netzwerkzone, die physische Interfacegeschwindigkeit oder die SLA-Bandbreite sinnvoll sein (bei Verwendung der SLA-Bandbreite als Referenz kann hierarchisches QoS erforderlich sein.) Eine mögliche Zuweisung der Netzressourcen ist in nachfolgender Abbildung dargestellt:

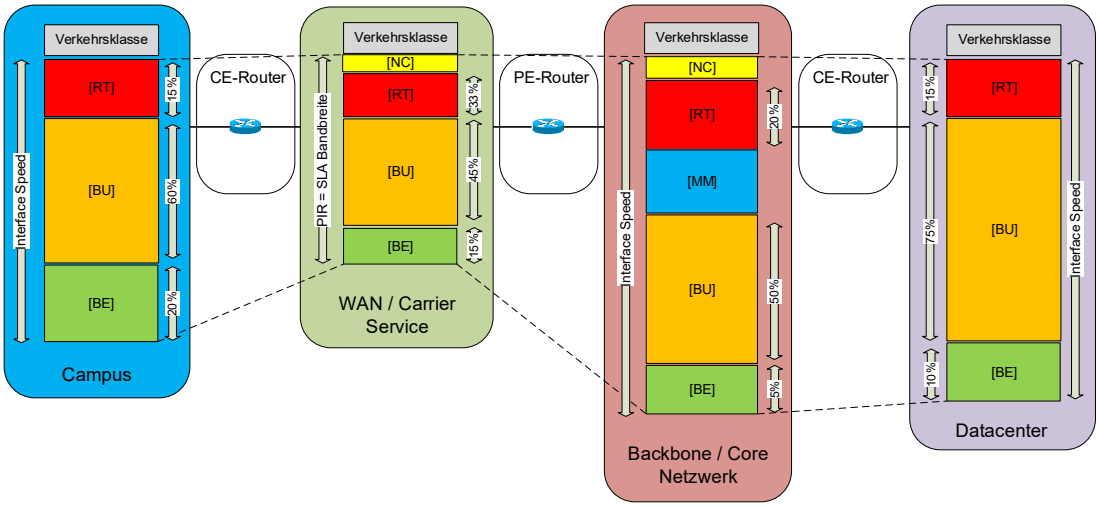


Abbildung 24: Netzressourcen pro Netzwerkzone End-to-End

Die angegebenen Prozentwerte sind als Beispiel zu verstehen. Es obliegt den Leistungserbringern, die optimale Abstimmung festzulegen.

In nachfolgender Tabelle sind die empfohlenen Mechanismen für ein einfaches Standardscheduling, pro Verkehrsklasse und Netzwerkzone, aufgeführt:

	Campus			WAN/Carrier Service				Backbone/Core Netzwerk					Datacenter		
Referenz-Bw.	Interface			SLA				Interface					Interface		
VK	[RT]	[BU]	[BE]	[NC]	[RT]	[BU]	[BE]	[NC]	[RT]	[MM]	[BU]	[BE]	[RT]	[BU]	[BE]
Queue	PQ	WQ	WQ	PQ/ WQ	PQ	WQ	WQ	PQ/ WQ	PQ	PQ/ WQ	WQ	WQ	PQ	WQ	WQ
Conforming <CIR	Fwd.	Fwd.	Fwd.	Fwd.	Fwd.	Fwd.	Fwd.	Fwd.	Fwd.	Fwd.	Fwd.	Fwd.	Fwd.	Fwd.	Fwd.
Exceeding <PIR	Drop	Fwd.	Fwd.	Drop / Fwd.	Drop	Mark	Mark	Drop / Fwd.	Drop	Drop /Mark	Mark	Mark	Drop	Fwd.	Fwd.
Voilating >PIR	-	Fwd.	Fwd.	-	-	Drop	Drop	-	-	-	Fwd,	Fwd.	-	Fwd.	Fwd.
Queue Mgmt.	-	RED	RED	-	-	RED	RED	-	-	-	RED	RED	-	RED	RED

Tabelle 7: Scheduling pro Verkehrsklasse/Netzwerkzone

PQ: Priority Queue

WQ: Weighted Queue

Fwd: Forward Packet ohne Veränderung der DSCP-Werte (DSCP-Transparenz)

Drop: Drop Packet (Policing)

Mark: Re-Mark

RED: Random Early Detect (Active Queue Management)

4.2 Klassifizierung und Markierung

4.2.1 DSCP-Markierung

Die QoS-Vorgabe [AR003] definiert nachfolgende Serviceklassen und DSCP-Werte für die Markierung des Verkehrs von IKT-Endsystemen:

Serviceklasse	DSCP-Name	DSCP-Wert
Telephony	EF	46
Signalling	CS5	40
Multimedia Conferencing	AF41	34
Real time Interactive	CS4	32
Multimedia Streaming	AF31	26
Broadcast Video	CS3	24
Low Latency Data	AF21	18
OAM	CS2	16
High Throughput Data	AF11	10
Standard	DF	0
Low-Priority Data	CS1	8

Tabelle 8: Serviceklassen und DSCP-Werte für die

Ferner wird vorgegeben, welche DSCP-Werte zu welchem Anwendungsverkehr zugewiesen sind

(In der aktuellen Version von [AR003] sind den DSCP-Werten AF41, CS3, AF11 und CS1 keine Anwendungen zugewiesen und werden deshalb von Endsystemen noch nicht verwendet.)

Anwendung	DSCP-Name
Skype for Business (Voice) Avaya Telefonie (Voice) ICA-Stream Very High Priority (Audio) Radar Positionierungsdaten (VBS)	EF
Skype for Business (Signalisierung) Avaya (Signalisierung)	CS5
Skype for Business (Desktop sharing)	CS4
Skype for Business (Video)	AF31
Alle Bundesanwendungen	AF21
Management von IKT-Systemen (Konfiguration und Überwachung)	CS2
Internet Printing Softwareverteilung Backup / Restore ICA-Steam Low Priority (Printing, Port Mapping)	DF

Tabelle 9: Zuweisung Anwendung zu DSCP

Der Ausdruck «Alle Bundesanwendungen» bezeichnet alle bundesinternen Anwendungen, die nicht explizit einer anderen Serviceklasse zugewiesen sind.

Die Zuweisung der DSCP-Werte zu den Anwendungen ist so ausgelegt, **dass nicht jede Anwendung einzeln klassifiziert werden muss. Alle Bundesanwendungen sind prinzipiell der Serviceklasse *Low Latency Data* zugewiesen und dürfen den DSCP-Wert AF21 verwenden** (Default) und werden folglich in der Verkehrsklasse [BU] übermittelt.

Kategorie	Anwendung	DSCP-Name	VK
Standard	Alle Bundesanwendungen	AF21	[BU]

Tabelle 10: Standard Serviceklasse für Bundesanwendungen

Nur Abweichungen davon müssen gesondert betrachtet werden. Diese Anwendungen können (mit Ausnahme von wenigen Spezialfällen) in nachfolgende Kategorien unterteilt werden:

Klasse	Anwendung	DSCP-Name	3VK	4VK
IP-Communications / Skype	Voice	EF	[RT]	[RT]
	Signalisierung	CS5	[RT]	[RT]
	Desktop sharing	CS4	[BU]	[MM]
	Video	AF31	[BE]	[MM]
Best Effort	Internet	DF	[BE]	[BE]
	Printing			
	Softwareverteilung			
	Backup / Restore			
System Management	Management und Überwachung von IKT-Systemen (SSH, SNMP, FTP etc.)	CS2	[BU]	[BU]

Tabelle 11: Abweichungen von der Standard Serviceklasse

In der QoS-Vorgabe [AR003] ist geregelt, dass die Klassifizierung und DSCP-Markierung

- mit erster Priorität immer auf den Endsystemen zu erfolgen hat, sofern dies technisch und betrieblich möglich ist. Dies gilt für Endsysteme im Geltungsbereich der Weisung. Das Netzwerk vertraut den vom Endsystem gesetzten DSCP-Werten und bestimmt damit die Verkehrsklasse für die Übermittlung.
- im Netzwerk erfolgen darf, wenn das Endsystem nicht im Geltungsbereich der Weisung ist, oder die Klassifizierung und Markierung auf dem Endsystem nicht möglich ist. In diesem Fall muss eine IKT-Anforderung auf Stufe Bund (P035) eingegeben werden.
- an Übergängen zu Fremdnetzen, welche nicht im Geltungsbereich der Weisung sind, fallspezifisch zu klären ist.

Abhängig vom Endsystem und der Netzanbindung ergeben sich folgende Grundfunktionen an der Netzgrenze:

QoS-Funktion	Beschreibung
Trust	DSCP-Werten wird vertraut. Scheduling gem. Verkehrsklassenmodell (DSCP-to-Queue Mapping).
Mark	Klassifizierung und Markierung mit DSCP-Werten gem. Tabelle 9

Tabelle 12: Funktionen Klassifizierung/Markierung

Diese Funktionen kommen wie folgt an der *Trust Boundary* zur Anwendung:

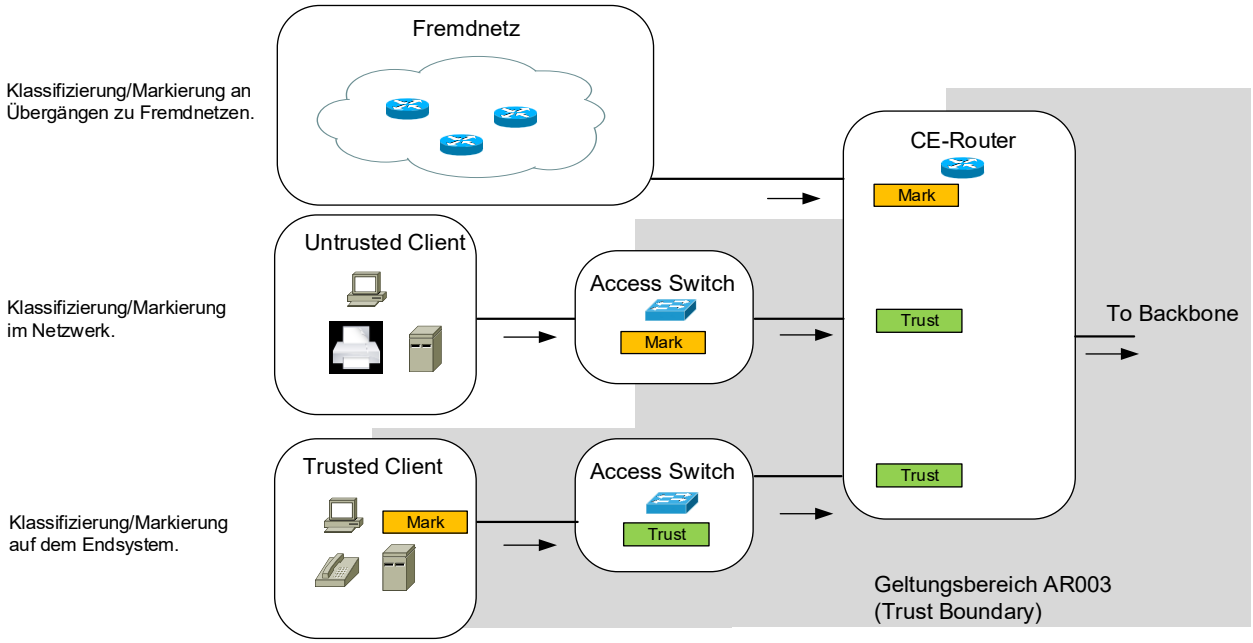


Abbildung 25: DSCP-Markierung

Innerhalb der *Trust Boundary* muss jedes IP-Paket einen gültigen DSCP-Wert besitzen.

Ergänzungen und/oder Änderungen der Anwendungen und der zugewiesenen DSCP-Werte sind mittels IKT-Anforderung auf Stufe Bund [P035] möglich.

4.2.2 Klassifizierung und Markierung auf dem Endsystem

Die Klassifizierung und Markierung des Verkehrs erfolgt bei Systemen im Geltungsbereich [AR003] mit erster Priorität auf dem Endsystem.

Endsysteme erfordern nur eine QoS-Policy für die Markierung des Verkehrs von Anwendungen gem. *Tabelle 10* und Tabelle *11*, die sie auch tatsächlich verwenden. Die Policy sollte auf OS-Ebene umgesetzt werden, so dass das Betriebssystem die DSCP-Markierung aufgrund des auslösenden Prozesses/Applikation, der genutzten TCP/UDP-Ports und/oder der Quell-/Ziel-IP-Adressen vornimmt. Damit kann verhindert werden, dass jeder Betreiber einer Anwendung individuelle QoS-Einstellungen vornehmen muss.

Auch Endsysteme mit Anwendungen welche gem. *Tabelle 10* ausschliesslich der Standardklasse angehören, erfordern eine entsprechende QoS-Konfiguration, **damit der Verkehr mit der korrekten DSCP-Markierung (AF21) gesendet wird. Ohne entsprechende Konfiguration des Endsystems wird der Verkehr üblicherweise mit dem DSCP-Wert DF gesendet und würde somit in der *[BE] Verkehrsklasse* übermittelt werden.**

Das Netzwerk vertraut dann den vom Endsystem gesetzten DSCP-Werten und bestimmt damit, in welcher Verkehrsklasse der Verkehr übermittelt wird.

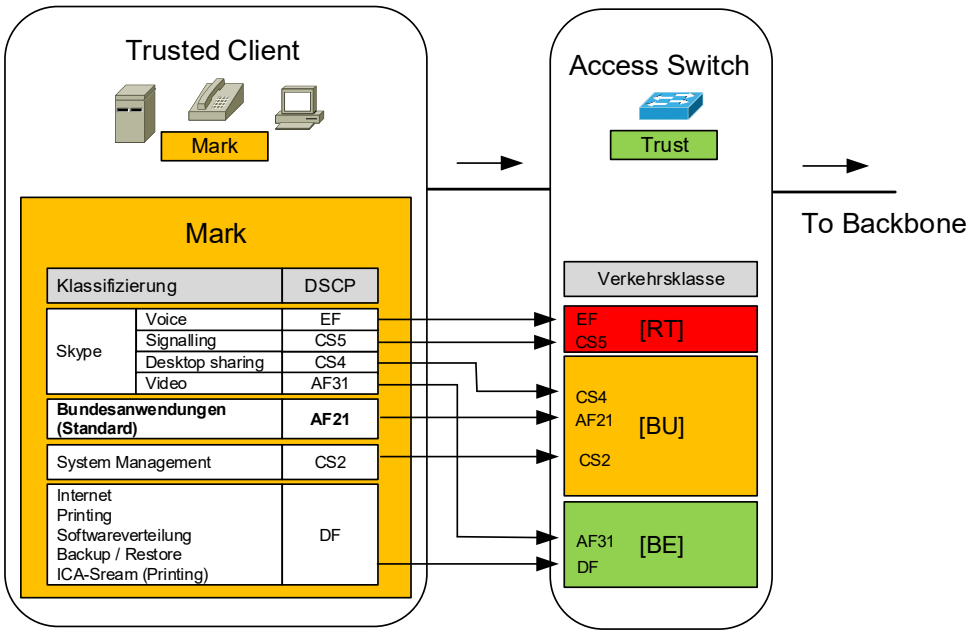


Abbildung 26: Klassifizierung/Markierung auf dem Endsystem (3VK Modell)

4.2.3 Klassifizierung und Markierung im Netzwerk

Falls das Endsystem nicht im Geltungsbereich von [AR003] ist oder die Klassifizierung und Markierung auf dem Endsystem nicht möglich/sinnvoll ist, kann dies im Netzwerk vorgenommen werden. Für Endsysteme im Geltungsbereich [AR003], ist die Klassifizierung und Markierung im Netzwerk nur in Ausnahmefällen zugelassen und erfordert eine IKT-Anforderung Stufe Bund [P035].

Eine einfache Klassifizierung und Markierung im Netzwerk ist möglich, wenn der Verkehr pro VLAN zu nur einem DSCP-Wert gem. *Tabelle 10* oder *Tabelle* 11 zugewiesen werden kann. In diesem Fall kann das Netzelement die Klassifizierung des Verkehrs aufgrund des VLANs vornehmen und die Pakete pro VLAN mit dem entsprechenden DSCP-Wert markieren, bevor sie verarbeitet und in Richtung Backbone weitergeleitet werden.

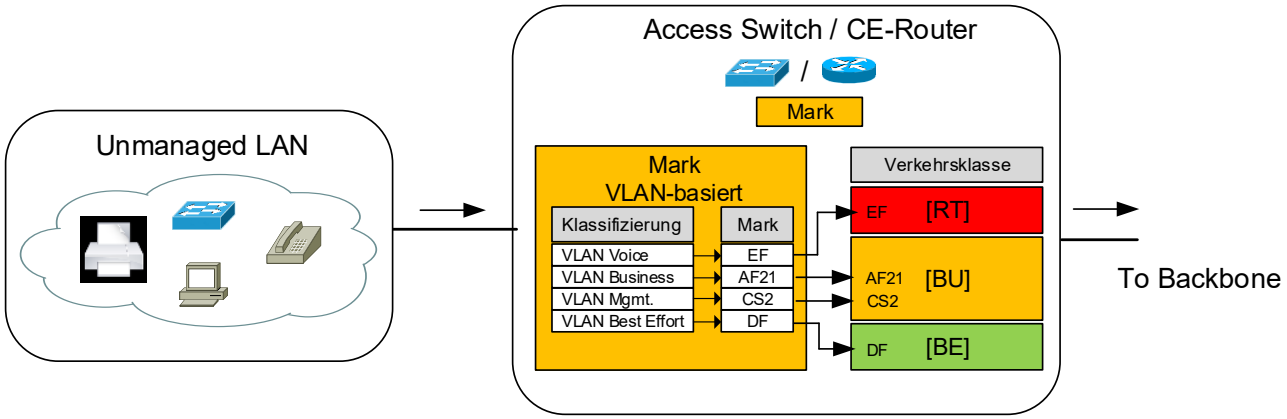


Abbildung 27: VLAN-basierte Klassifizierung/Markierung (3VK Modell)

Eine einfache Klassifizierung und Markierung im Netzwerk ist ebenfalls möglich, wenn der Verkehr pro Netzwerkanschluss (Switchport) zu lediglich einem DSCP-Wert gem. *Tabelle 10* oder *Tabelle 11* zugewiesen werden kann. In diesem Fall kann der Verkehr aufgrund des Netzwerkanschlusses auf dem Netzelement klassifiziert werden. Die Markierung erfolgt dann mit dem entsprechenden DSCP-Wert, bevor der Verkehr verarbeitet und in Richtung Backbone weitergeleitet wird.

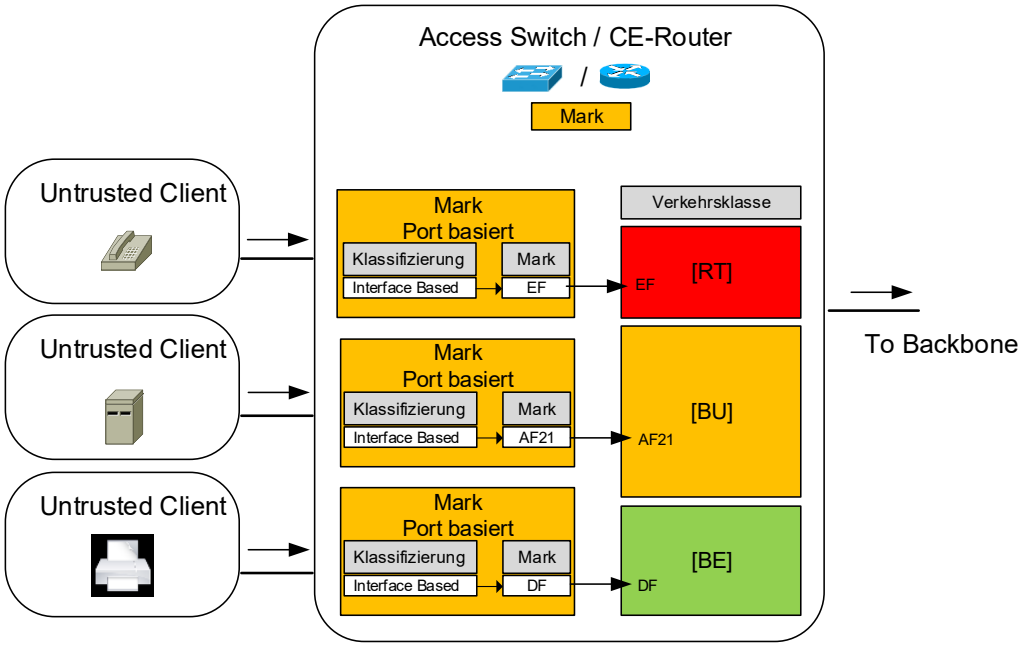


Abbildung 28: Port-basierte Klassifizierung/Markierung (3VK Modell)

In vielen Fällen sollte sich der Verkehr eines Endsystems der Standard-Serviceklasse gem. *Tabelle 10* mit dem DSCP-Wert AF21 zuweisen lassen. Bei der Klassifizierung und Markierung im Netzwerk sollten einfache technische Lösungen «im Sinne von [AR003]» gegenüber komplexen Lösungen mit geringem Nutzen vorgezogen werden.

Falls keine einfache Klassifizierung und Markierung des Verkehrs möglich ist, kann dies auf einem Netzelement anhand von erweiterten Verkehrsmustern stattfinden. Abhängig von den eingesetzten Netzelementen können unterschiedliche Funktionalitäten vorhanden sein, wobei viele Plattformen eine Klassifizierung und Markierung des Verkehrs anhand nachfolgender Kriterien unterstützen:

- Source-/Destination IP Adressen
- Source-/Destination TCP/UDP Ports

Die Markierung erfolgt dann entsprechend der Kommunikationsmatrix der Anwendung mit den entsprechenden DSCP-Werten aus *Tabelle 9.*

Die Klassifizierung und Markierung des Verkehrs sollte jeweils möglichst nahe beim Absender stattfinden, so dass jedes Paket eine gültige DSCP-Markierung besitzt, bevor es in den Backbone weitergeleitet wird. Ohne gültige DSCP-Markierung findet die Übermittlung in der *[BE] Verkehrsklasse* statt. Wenn die Klassifizierung und Markierung «erst» auf dem CE-Router erfolgt, kann ggf. die korrekte Priorisierung des Verkehrs im LAN nicht gewährleistet werden.

4.2.4 Netzübergänge

4.2.4.1 Bundesinterne Netzübergänge

Alle zivilen Bundesnetze unterliegen der QoS-Vorgabe [AR003], womit an den bundesinternen Netzübergängen keine neue DSCP-Markierung des Verkehrs erforderlich ist und den bestehenden DSCP-Werten aus dem Fremdnetz vertraut werden kann.

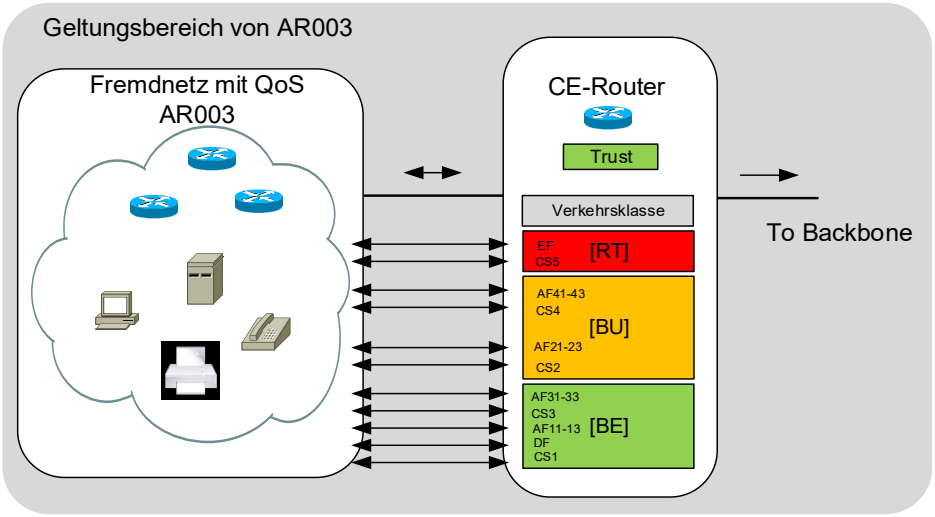


Abbildung 29: Klassifizierung/Markierung an Übergängen zu bundes-internen Fremdnetzen (3VK Modell)

An bundesinternen Netzübergängen müssen alle DSCP-Werte gem. *Tabelle 5* unterstützt werden (ausgenommen davon sind die Serviceklassen für Network Control CS6 und CS7).

4.2.4.2 Externe Netzübergänge

An Übergängen zu externen Fremdnetzen, die nicht im Geltungsbereich von [AR003] sind, muss die Klassifizierung und Markierung fallspezifisch geklärt werden. Der eingehende Verkehr (Downstream) ist am Netzübergang anhand der Anwendungen in *Tabelle 9* zu klassifizieren und mit den entsprechenden DSCP-Werten zu markieren.

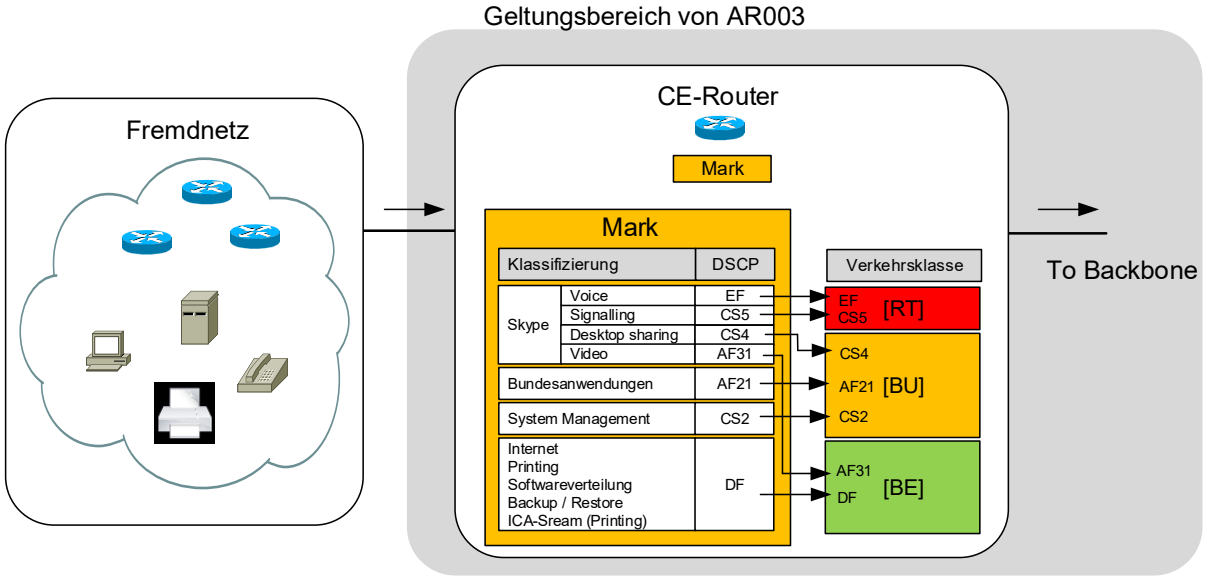


Abbildung 30: Klassifizierung/Markierung an Übergängen zu externen Fremdnetzen (3VK Modell)

In vielen Fällen sollte sich der eingehende Verkehr vom Fremdnetz zur Standard Service-klasse gem. *Tabelle 10* (mit DSCP-Wert AF21) zuweisen lassen. Bei der Klassifizierung und Markierung an Netzübergängen sollten einfache technische Lösungen «im Sinne von [AR003]» gegenüber komplexen Lösungen mit geringem Nutzen vorgezogen werden.

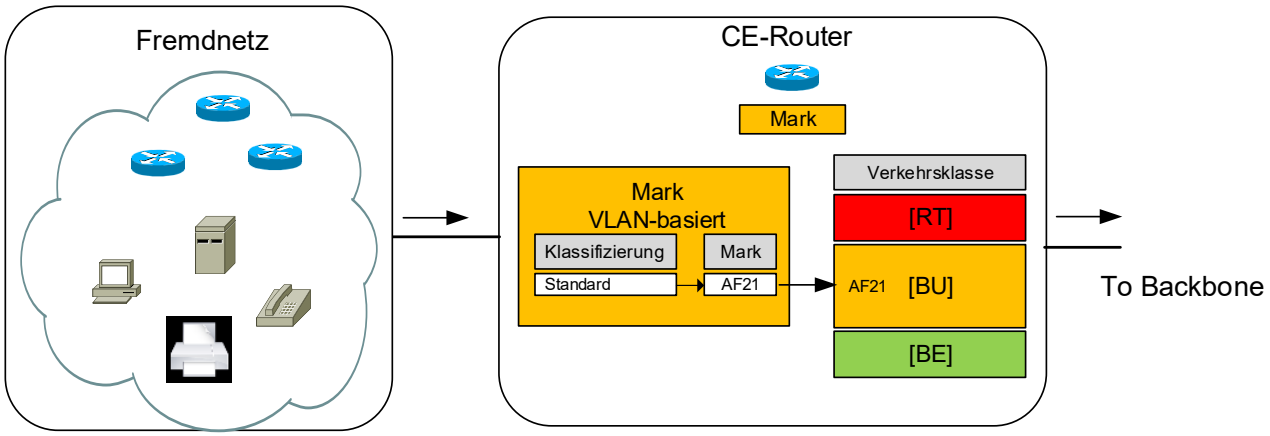


Abbildung 31: Externe Fremdnetze Standard Bundesanwendungen (AF21)

Ausgehender Verkehr aus einem Bundesnetz zu einem Fremdnetz (Upstream) sollte am Netzübergang nur mit DSCP-Werten übermittelt werden, die im Fremdnetz unterstützt wer-den. Bei Übergängen zu Fremdnetzen ohne QoS oder ohne Kenntnis über die QoS-Spezifi-kationen im Fremdnetz wird empfohlen, alle DSCP-Informationen von ausgehendem Verkehr zu löschen und stattdessen mit dem DSCP-Wert DF zu übermitteln.

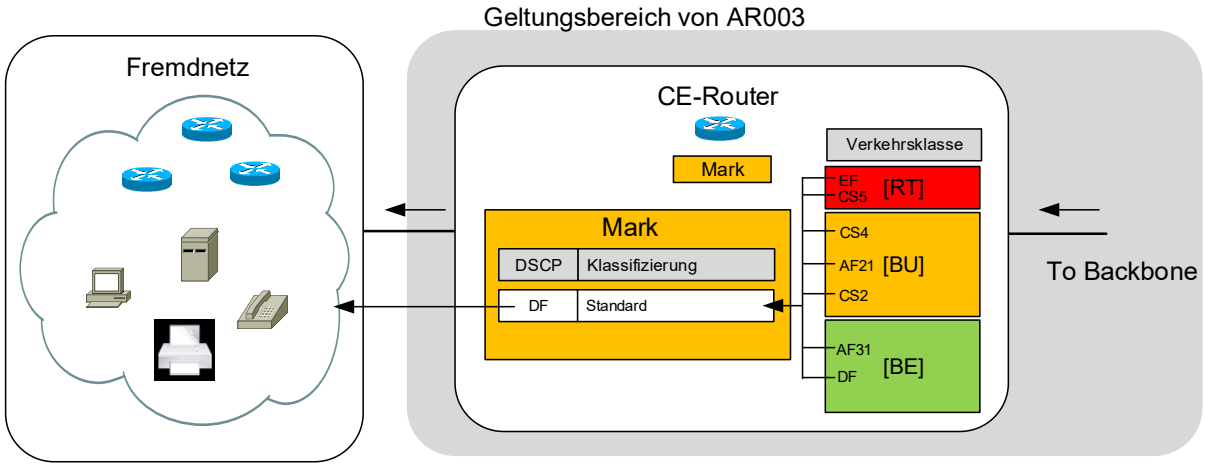


Abbildung 32: Klassifizierung/Markierung an Übergängen zu externen Fremdnetzen (Upstream)

An Übergängen zu externen Fremdnetzen, die einer anderen QoS-Vorgabe als [AR003] unterstellt sind, kann ggf. mittels einer Umsetzungstabelle ein Mapping zwischen den Priorisierungscodepoints im Fremdnetz und den DSCP-Werten von [AR003] erreicht werden.

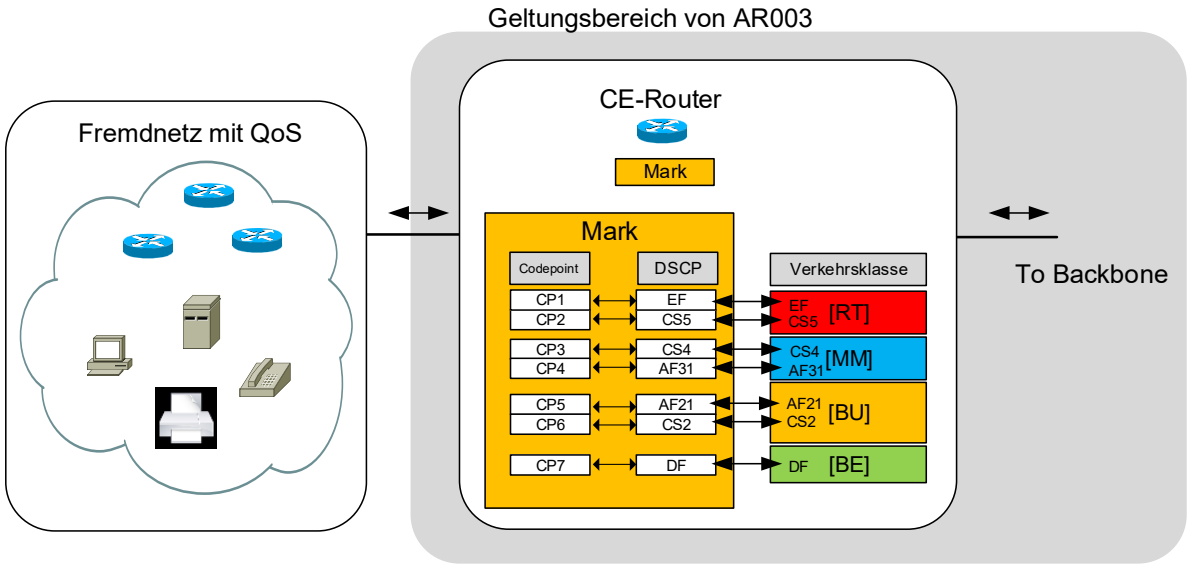


Abbildung 33: Klassifizierung/Markierung an Übergängen zu externen Fremdnetzen (4VK Modell)

Eine genaue Abstimmung zwischen dem Leistungserbringer des Bundes und dem Betreiber des externen Fremdnetzes ist in diesem Fall unerlässlich.

4.3 Admission Control

Mittels *Admission Control* muss das Netzwerk an der *Trust Boundary* und an Netzübergängen geschützt werden, indem

- der Zugang zu der *[RT] Verkehrsklasse* limitiert wird;
- nur zugelassene DSCP-Werte unverändert in die *Trust Boundary* weitergeleitet werden.

Der Schutz erfolgt auf dem *Access Switch* und/oder dem CE-Router und wird in der QoS-Vorgabe [AR003] auf Netzwerkanschlüssen zu Endsystemen wie folgt definiert:

Serviceklasse	DSCP-Name	Funktion Admission Control
Telephony	EF	Policing der Datenrate.
Signalling	CS5	
Multimedia Conferencing	AF41	Übermittlung ohne Veränderung der DSCP-Werte.
Real time Interactive	CS4	
Multimedia Streaming	AF31	
Broadcast Video	CS3	
Low Latency Data	AF21	
OAM	CS2	
High Throughput Data	AF11	
Standard	DF	
Low-Priority Data	CS1	
Alle anderen DSCP-Werte		Re-marking der DSCP-Werte auf DF.

Tabelle 13: Admission Control zu Endsystemen

Auf Netzübergängen zu internen Fremdnetzen ist der Schutz wie folgt definiert:

Serviceklasse	DSCP-Name	Funktion Admission Control
Network Control	CS7	Re-marking der DSCP-Werte auf DF.
Network Control	CS6	
Telephony	EF	Policing der Datenrate.
Signalling	CS5	
Multimedia Conferencing	AF41-43	Übermittlung ohne Veränderung der DSCP-Werte.
Real time Interactive	CS4	
Multimedia Streaming	AF31-33	
Broadcast Video	CS3	
Low Latency Data	AF21-23	
OAM	CS2	
High Throughput Data	AF11-13	
Standard	DF	
Low-Priority Data	CS1	
Alle anderen DSCP-Werte		Re-marking der DSCP-Werte auf DF.

Tabelle 14: Admission Control an Übergängen zu internen Fremdnetzen

Die Policingrate ist entsprechend des Anschlusstyps jeweils durch den Leistungserbringer festzulegen.

5 Fallbeispiele

5.1 Verkehrsklassen

Netzwerkzone	Campus	WAN / Carrier Service	Backbone / Core Netzwerk	Datacenter
Systeme	Router, Switches, Firewalls, Gateways, Loadbalancer, weitere			
Bandbreite	Hoch	Niedrig	Hoch	Sehr hoch
Aggregation	Niedrig	Niedrig	Hoch	Hoch
Netzauslastung	Niedrig-mittel	Hoch	Mittel-hoch	Mittel-hoch
Dynamic Routing	Nein	Ja	Ja	Nein
Verkehrsklassen	3VK	3VK+NC	4VK+NC	3VK
Mapping	DSCP-to-Queue	DSCP-to-802.1p	DSCP-to-Queue	DSCP-to-Queue
DSCP-Transpa-renz	Ja			

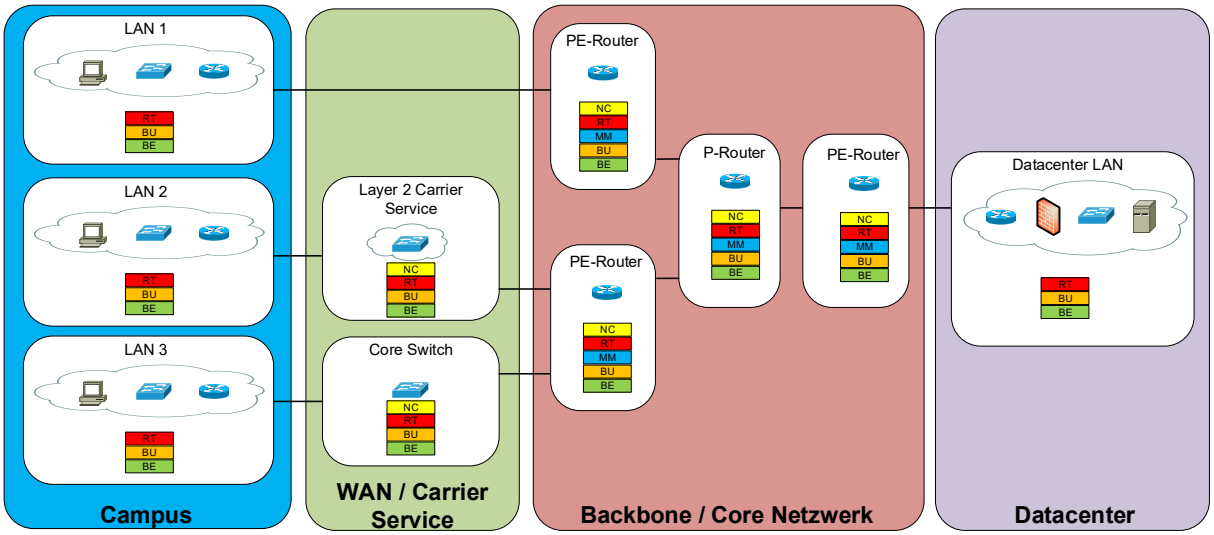


Abbildung 34: Verkehrsklassen

5.2 Klassifizierung und Markierung

5.2.1 Klassifizierung und Markierung im Netzwerk

Netzwerkzone	Datacenter, Campus
Systeme	Spezialsysteme und Systeme welche keine QoS-Konfiguration erlauben (BS2000, TNA, GEBA, Domotik, weitere)
Klassifizierung/Markierung	Port-based oder VLAN-based auf dem Access-Switch. Der gesamte Verkehr auf dem betroffenen Anschluss/VLAN wird als Standard Bundesanwendungen klassifiziert.
DSCP-Werte	Standard Bundesanwendungen (AF21)
Verkehrsklassen	3 VK-Modell am Access-Switch. Mapping des DSCP-Wertes AF21 für Standard Bundesanwendungen zu der Verkehrsklasse [BU]
Bemerkungen	P035 für Endsysteme im Geltungsbereich der Weisung erforderlich.

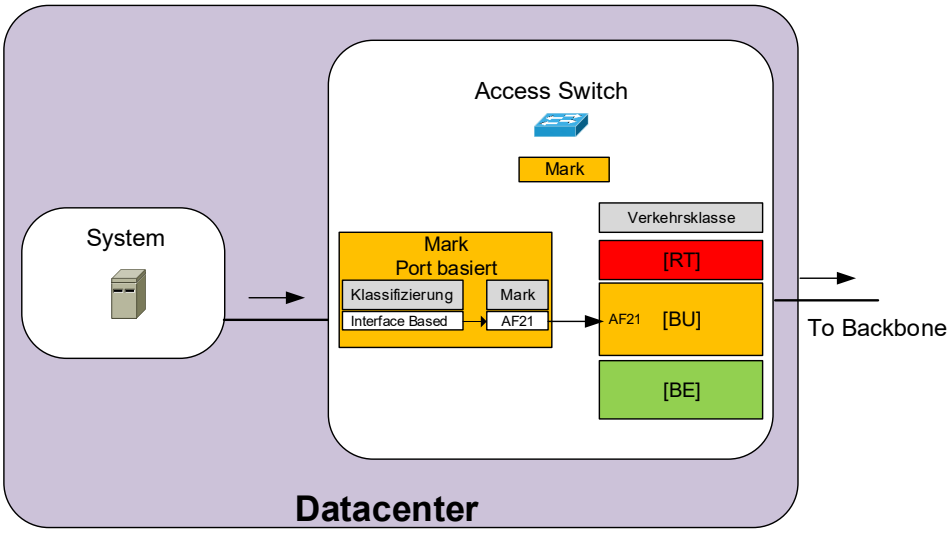


Abbildung 35: DSCP-Markierung im Netz (Port based)

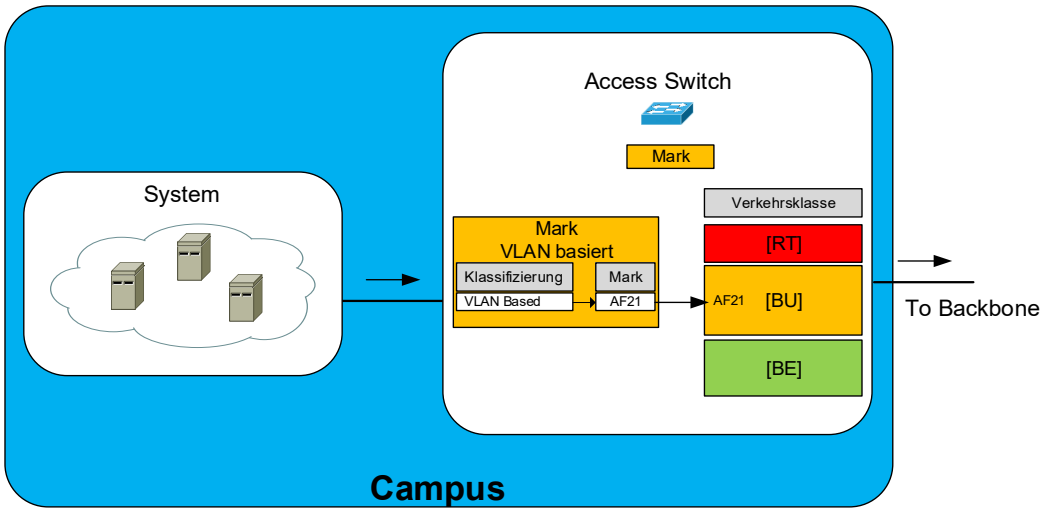


Abbildung 36: DSCP-Markierung im Netz (VLAN based)

5.2.2 Klassifizierung und Markierung auf dem Endsystem

5.2.2.1 BA / Windows Server

Netzwerkzone	Datacenter, Campus
Systeme	*Windows* Server (ausgeschlossen UCC Systeme)
Klassifizierung/Markierung	Mittels «Policy-based QoS» werden auf dem *Windows* Server nachfolgende Anwendungen klassifiziert und in der GPO verwaltet. Internet: Verkehr mit Ziel-IP-Adresse der Internetproxies Printing: Verkehr mit definierten TCP Ports SW-Verteilung: Verkehr mit definierten TCP Ports Backup: Verkehr mit Ziel-IP-Adressen im IP-Range der Backupnetze. Bundesanwendungen: Alles andere wird als Standard Bundesanwendungen klassifiziert.
DSCP-Werte	Internet (DF) Printing (DF) SW-Verteilung (DF) Backup (DF) Standard Bundesanwendungen (AF21)
Verkehrsklassen	3 VK-Modell am Access-Switch. Mapping der Anwendungen/DSCP-Werte zu den Verkehrsklassen: Standard Bundesanwendungen (AF21) in der [BU] Verkehrsklasse. Internet, Printing, SW-Verteilung, Backup (DF) in der [BE] Verkehrsklasse.
Admission Control	Der Access-Switch vertraut grundsätzlich den DSCP-Werten vom Endsystem (Trust). Schutz an der Netzgrenze mittels: Policing von [RT] (obwohl kein Verkehr in der [RT] Klasse erwartet wird). Re-marking von DSCP-Werten ausserhalb Geltungsbereich auf DF.

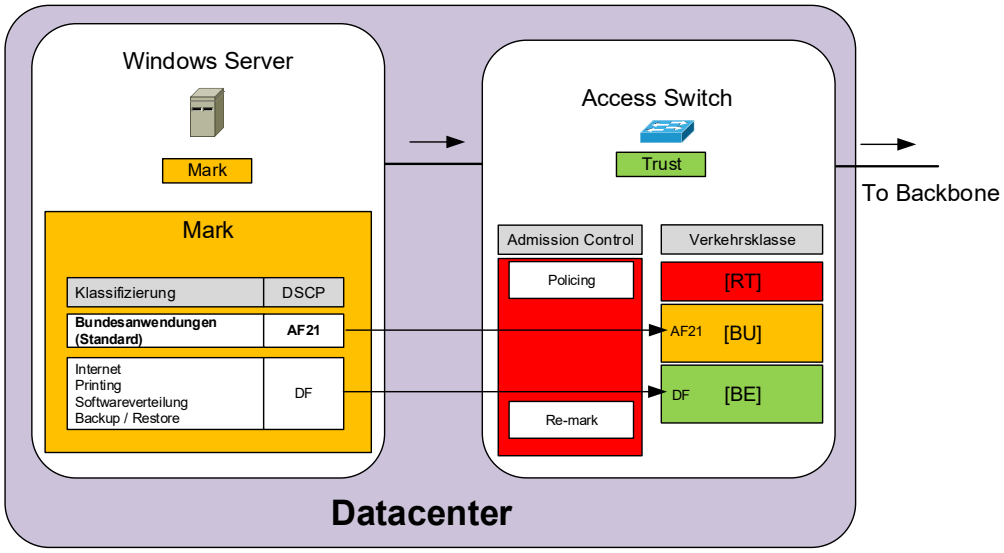


Abbildung 37: DSCP-Markierung Windows Server

5.2.2.2 UCC Server

Netzwerkzone	Datacenter
Systeme	Lync Front-End, Session Border Controller (SBC), IPT-Gateway, weitere
Klassifizierung/Markierung	Mittels «Policy-based QoS» werden auf den *Windows*-Systemen nachfolgende *Skype*-Anwendungen klassifiziert. QoS Policy wird in GPO verwaltet. Voice: Verkehr von «lync.exe» mit definierten UDP Ports Signalisierung: Verkehr von «lync.exe» mit definierten TCP Ports Sharing: Verkehr von «lync.exe» mit definierten TCP Ports Video: Verkehr anhand Ziel-IP-Adressen im IP-Range der Backupnetze klassifizieren. Weitere (nicht *Windows*) UCC Systeme erfordern eine gleichwertige Konfiguration.
DSCP-Werte	Voice (EF) Signalisierung (CS5) Sharing (CS4) Video (AF31)
Verkehrsklassen	3 VK-Modell am Access-Switch. Mapping der Anwendungen/DSCP-Werte zu den Verkehrsklassen: Voice (EF) und Signalisierung (CS5) in der [RT] Verkehrsklasse. Sharing (CS4) in der [BU] Verkehrsklasse. Video (AF31) in der [BE] Verkehrsklasse.
Admission Control	Der Access-Switch vertraut grundsätzlich den DSCP-Werten vom Endsystem (Trust). Schutz an der Netzgrenze mittels: Policing von [RT] (bei zentralen UCC Systemen kann es ggf. besser sein kein Policing zu verwenden). Re-marking von DSCP-Werten ausserhalb Geltungsbereich auf DF.

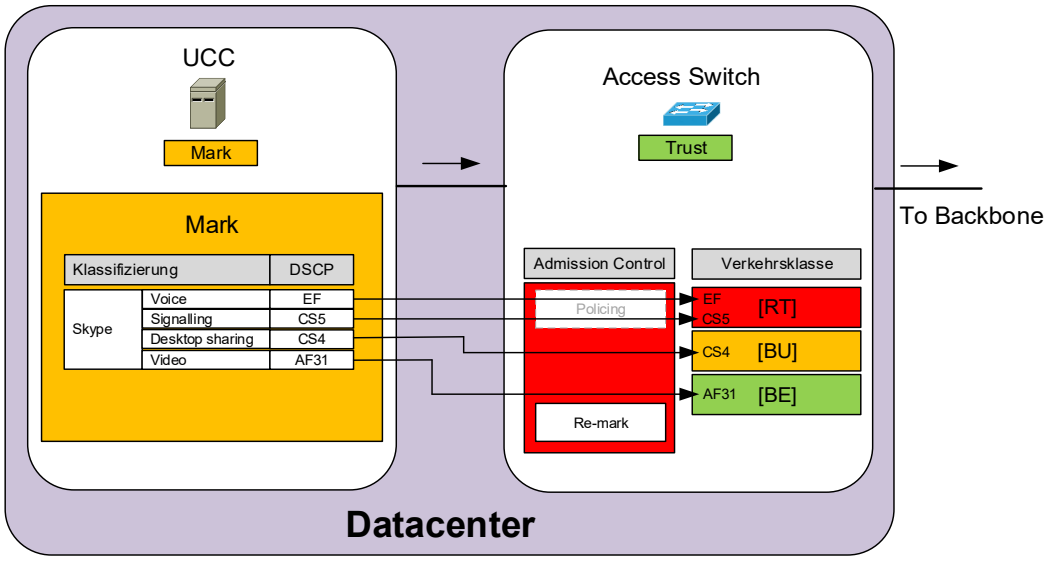


Abbildung 38: DSCP-Markierung UCC Server

5.2.2.3 BA / APS

Netzwerkzone	Campus
Systeme	APS (PC, Laptop, VDI, IP-Hardphone, weitere)
Klassifizierung/Markierung	Mittels «Policy-based QoS» werden die *Windows*-Systeme konfiguriert. Die Einstellungen erfolgen gem. der GPO für *Windows* Server (siehe Kapitel 5.2.2.1) und UCC Server (siehe Kapitel 5.2.2.2). Weitere (nicht *Windows*) BA/APS Systeme erfordern eine gleichwertige Konfiguration.
DSCP-Werte	Voice (EF) Signalisierung (CS5) Sharing (CS4) Video (AF31) Internet (DF) Printing (DF) SW-Verteilung (DF) Standard Bundesanwendungen (AF21)
Verkehrsklassen	3 VK-Modell am Access-Switch. Mapping der Anwendungen/DSCP-Werte zu den Verkehrsklassen: Voice (EF) und Signalisierung (CS5) in der [RT] Verkehrsklasse Standard Bundesanwendungen (AF21) und Skype Sharing in der [BU] Verkehrsklasse. Internet, Printing, SW-Verteilung (DF) und Video (AF31), in der [BE] Verkehrsklasse.
Admission Control	Der Access-Switch vertraut grundsätzlich den DSCP-Werten vom Endsystem (Trust). Schutz an der Netzgrenze mittels: Policing von [RT] Re-marking von DSCP-Werten ausserhalb Geltungsbereich auf DF.

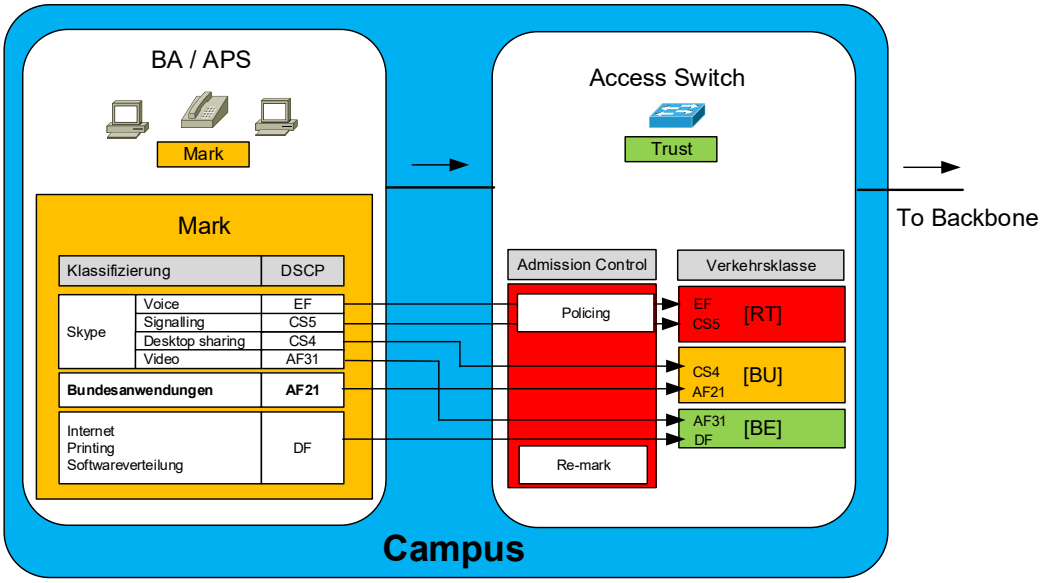


Abbildung 39: DSCP-Markierung BA/APS

5.2.2.4 Unix Server

Netzwerkzone	Datacenter, Campus
Systeme	RedHat, SuSE, AIX, Solaris, zLinux, IBM Host, Appliances, weitere
Klassifizierung/Markierung	Mittels «IP-Tables» auf Linux, «Policyd» auf AIX, «PAGENT» auf IBM-Host werden nachfolgende Anwendungen klassifiziert. Internet: Verkehr mit Ziel-IP-Adresse der Internetproxies Printing: Verkehr mit definierten TCP Ports Backup: Verkehr mit Ziel-IP-Adressen im IP-Range der Backupnetze. Systemmanagement: Verkehr mit definierten Ziel-IP-Adressen der Management Server. Bundesanwendungen: Alles andere wird als Standard Bundesanwendungen klassifiziert.
DSCP-Werte	Internet (DF) Printing (DF) Backup (DF) Systemmanagement (CS2) Standard Bundesanwendungen (AF21)
Verkehrsklassen	3 VK-Modell am Access-Switch. Mapping der Anwendungen/DSCP-Werte zu den Verkehrsklassen: Standard Bundesanwendungen (AF21) und Systemmanagement (CS2) in der [BU] Verkehrsklasse. Internet, Printing, Backup (DF) in der [BE] Verkehrsklasse.
Admission Control	Der Access-Switch vertraut grundsätzlich den DSCP-Werten vom Endsystem (Trust). Schutz an der Netzgrenze mittels: Policing von [RT] (obwohl kein Verkehr in der [RT] Klasse erwartet wird). Re-marking von DSCP-Werten ausserhalb Geltungsbereich auf DF.

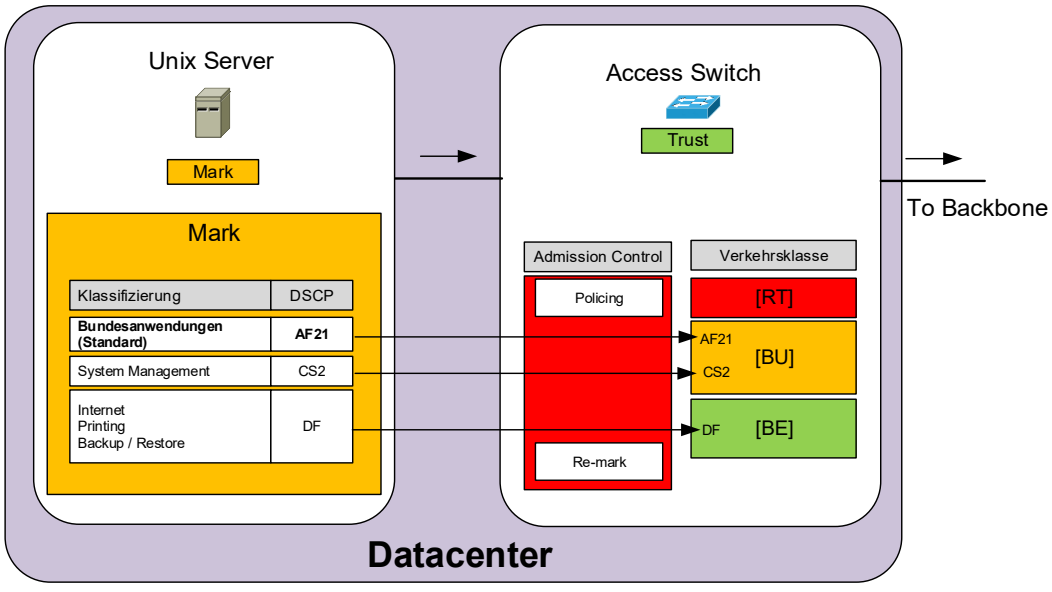


Abbildung 40: DSCP-Markierung Unix Server

5.2.2.5 Virtualisierung

Netzwerkzone	Datacenter
Systeme	*Virtual Windows*, *Virtual Linux* Server, *Cloud Atlantica*, weitere
Klassifizierung/Markierung	Für virtuelle *Windows*-Systeme erfolgen die Einstellungen mittels «Policy-based QoS» gem. der GPO für *Windows* Server (siehe Kapitel 5.2.2.1). Für virtuelle *Linux* Systeme erfolgen die Einstellungen mittels «IP-Tables» (siehe Kapitel 5.2.2.4)
DSCP-Werte	Internet (DF) Printing (DF) SW-Verteilung (DF) Backup (DF) Systemmanagement (CS2) Standard Bundesanwendungen (AF21)
Verkehrsklassen	3 VK-Modell am Access-Switch. Mapping der Anwendungen/DSCP-Werte zu den Verkehrsklassen: Standard Bundesanwendungen (AF21) und Systemmanagement (CS2) in der [BU] Verkehrsklasse. Internet, Printing, SW-Verteilung, Backup (DF) in der [BE] Verkehrsklasse.
Admission Control	Der Access-Switch vertraut grundsätzlich den DSCP-Werten vom Endsystem (Trust). Schutz an der Netzgrenze mittels: Policing von [RT] (obwohl kein Verkehr in der [RT] Klasse erwartet wird). Re-marking von DSCP-Werten ausserhalb Geltungsbereich auf DF.

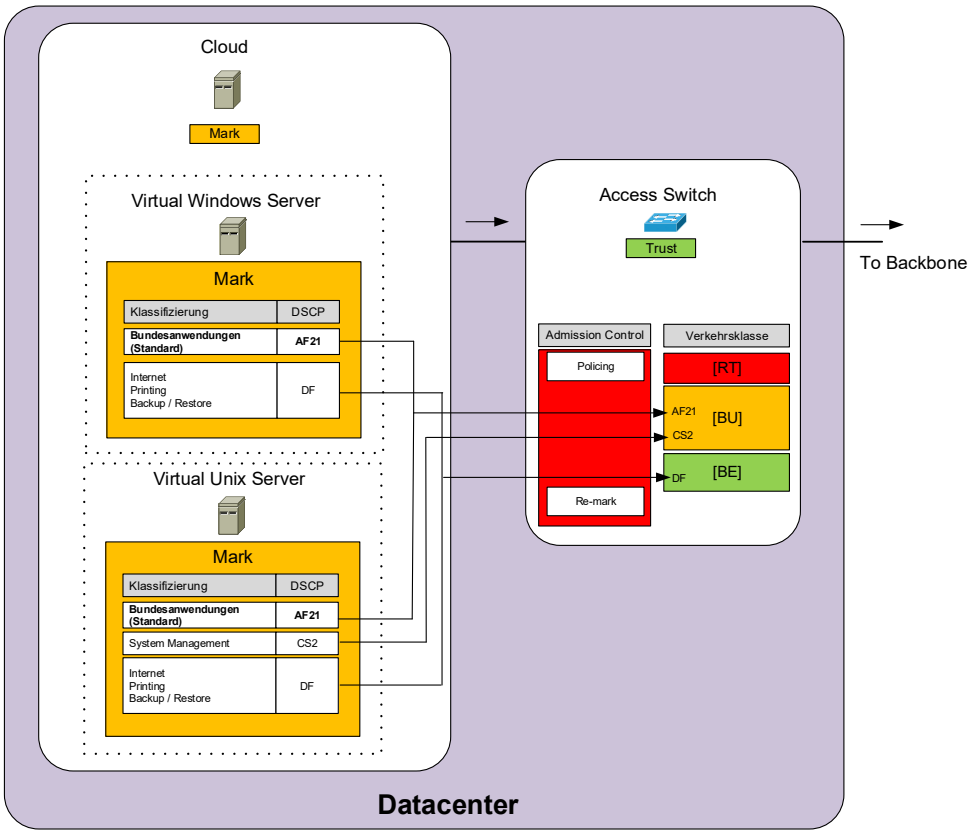


Abbildung 41: DSCP-Markierung Cloud

5.3 UCC

Netzwerkzone	End-to-End
Systeme	APS (PC, Laptop, VDI, IP-Hardphone), Lync Front-End, Session Border Controller (SBC), IPT-Gateway, weitere
Klassifizierung/Markierung	Auf den UCC Systemen gem. Kapitel 5.2.2.2 und Kapitel 5.2.2.3
DSCP-Werte	Voice (EF) Signalisierung (CS5) Sharing (CS4) Video (AF31)
Verkehrsklassen	3VK-Modell: Voice (EF) und Signalisierung (CS5) in der [RT] Verkehrsklasse. Sharing (CS4) in der [BU] Verkehrsklasse. Video (AF31) in der [BE] Verkehrsklasse. 4VK-Modell: Voice (EF) und Signalisierung (CS5) in der [RT] Verkehrsklasse. Sharing (CS4) und Video (AF31) in der [MM] Verkehrsklasse.

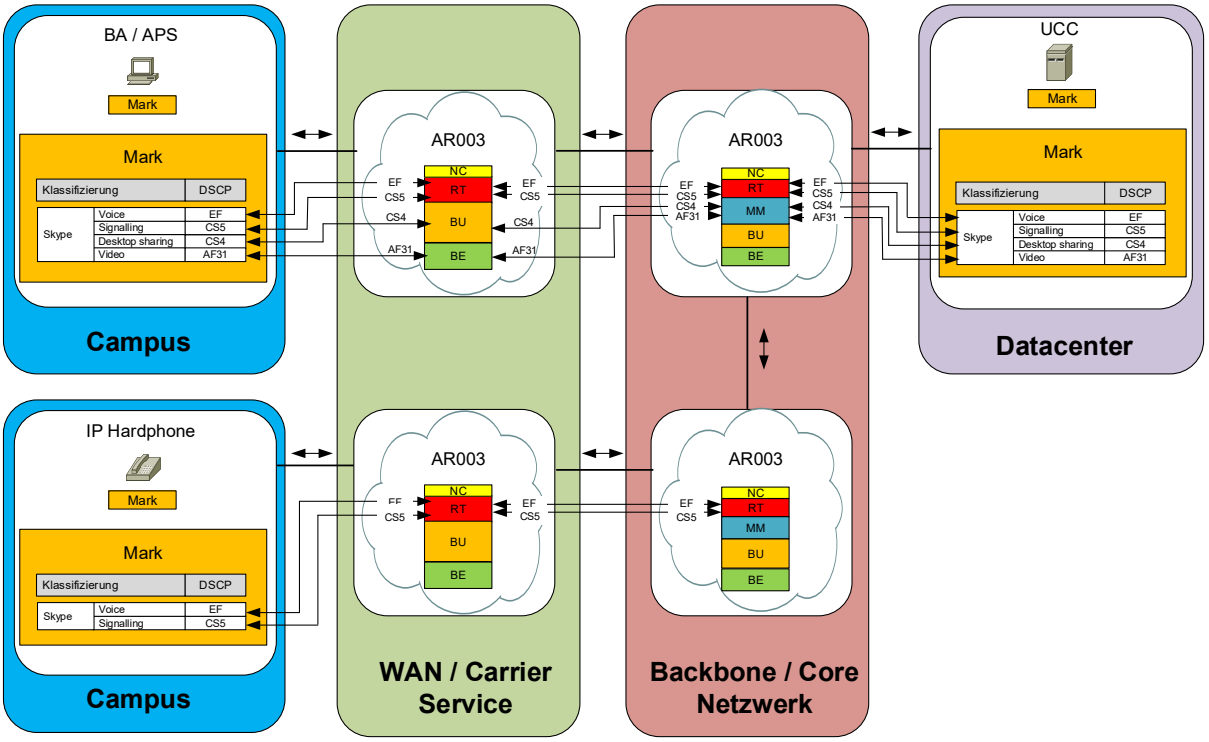


Abbildung 42: UCC

5.4 Softwareverteilung

Netzwerkzone	End-to-End
Systeme	APS (PC, Laptop, VDI), *Windows* Server (Domäne)
Klassifizierung/Markierung	Auf den Endsystemen gem. Kapitel 5.2.2.1 und Kapitel 5.2.2.3
DSCP-Werte	SW-Verteilung (DF)
Verkehrsklassen	3VK/4VK-Modell: SW-Verteilung (DF) in der [BE] Verkehrsklasse.

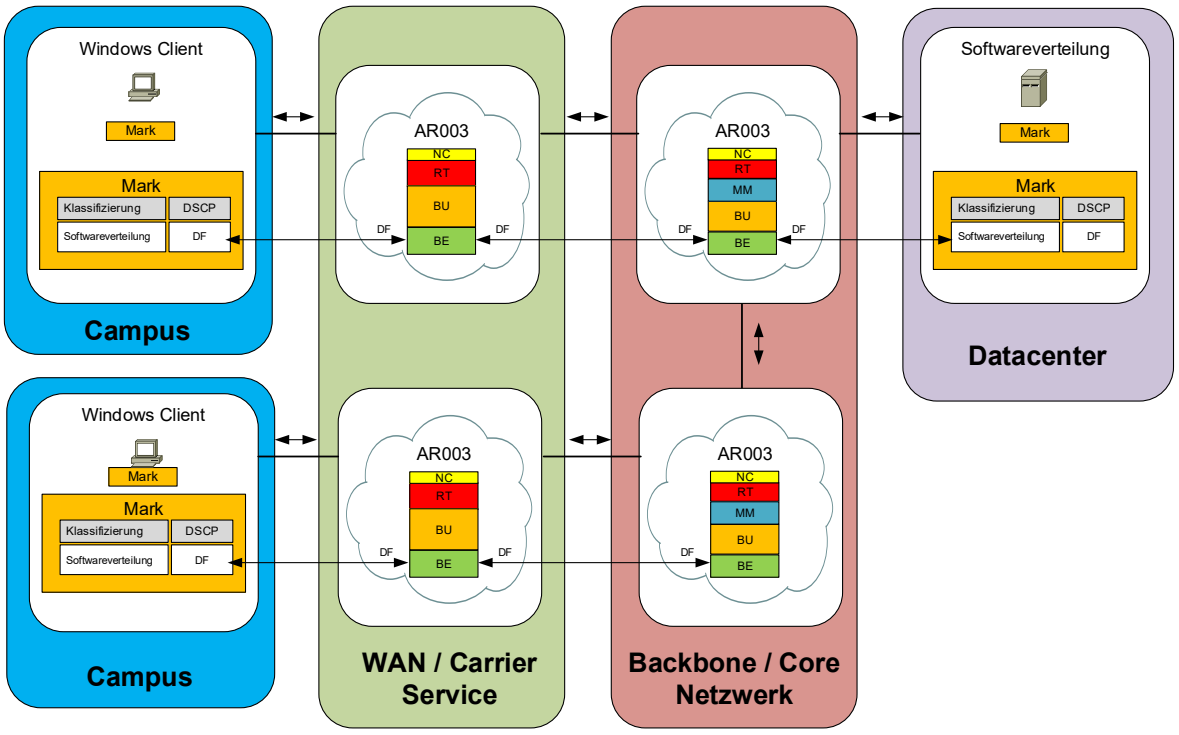


Abbildung 43: Softwareverteilung

5.5 Printing

Netzwerkzone	End-to-End
Systeme	APS (PC, Laptop, VDI), Windows Server (Domäne), Printserver, Drucker, weitere
Klassifizierung/Markierung	Auf den Endsystemen gem. Kapitel 5.2.2.1 und Kapitel 5.2.2.3
DSCP-Werte	Printing (DF)
Verkehrsklassen	3VK/4VK-Modell: Printing (DF) in der [BE] Verkehrsklasse.

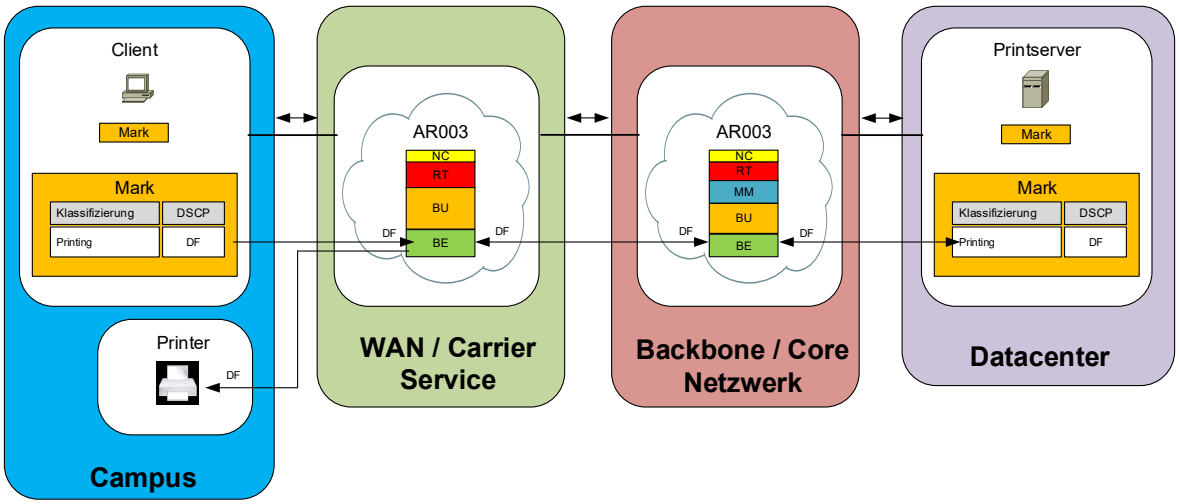


Abbildung 44: Printing

5.6 Internet

Netzwerkzone	End-to-End
Systeme	APS (PC, Laptop, VDI), Server, Proxy
Klassifizierung/Markierung	Auf den Endsystemen gem. Kapitel 5.2.2.1 Kapitel 5.2.2.3 und Kapitel 5.2.2.4
DSCP-Werte	Internet (DF)
Verkehrsklassen	3VK/4VK-Modell: Internet (DF) in der [BE] Verkehrsklasse.

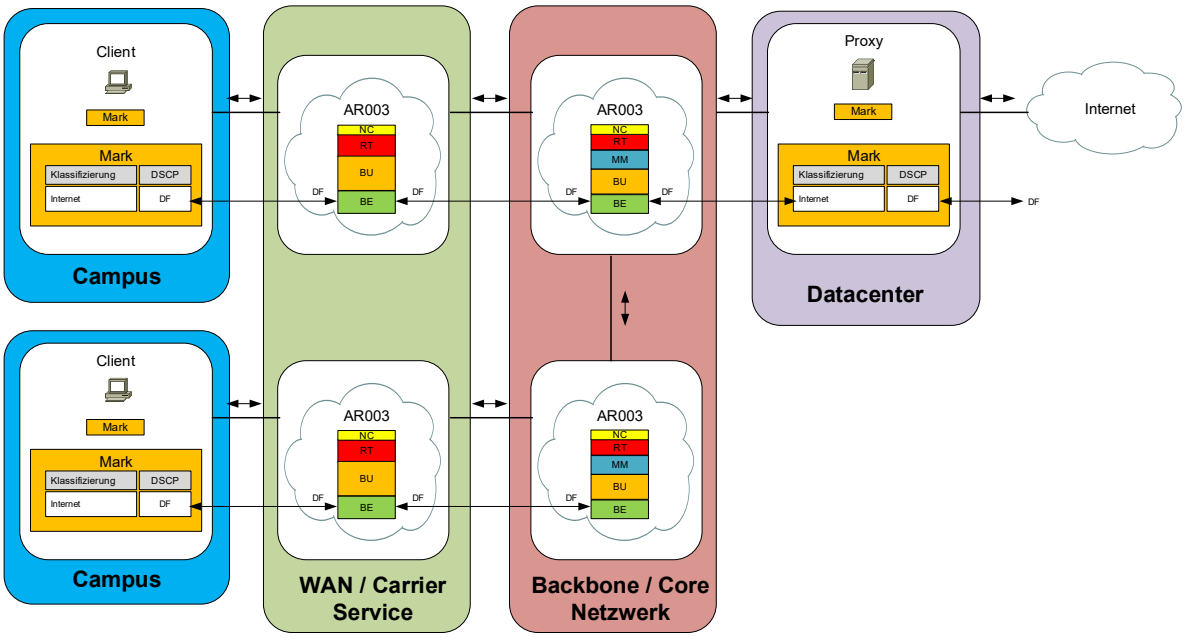


Abbildung 45: Internet

5.7 VDI

BA / APS Policy auf VM installiert

ICA Multistream

Netzwerkzone	End-to-End
Systeme	APS (PC, Laptop), VDI Thinclient, VDI Host
Klassifizierung/Markierung	Auf den Endsystemen gem. Tabelle 9
DSCP-Werte	ICA-Stream Very High Priority (EF) ICA-Stream High Priority (CS4) ICA-Stream Medium Priority (AF21) ICA-Stream Low Priority (DF)
Verkehrsklassen	3VK-Modell: ICA-Stream Very High Priority (EF) in der [RT] Verkehrsklasse. ICA-Stream High Priority (CS4) und Medium Priority (AF21) in der [BU] Verkehrsklasse. ICA-Stream Low Priority (DF) in der [BE] Verkehrsklasse. 4VK-Modell: ICA-Stream Very High Priority (EF) in der [RT] Verkehrsklasse. ICA-Stream High Priority (CS4) in der [MM] Verkehrsklasse. ICA-Stream Medium Priority (AF21) in der [BU] Verkehrsklasse. ICA-Stream Low Priority (DF) in der [BE] Verkehrsklasse.

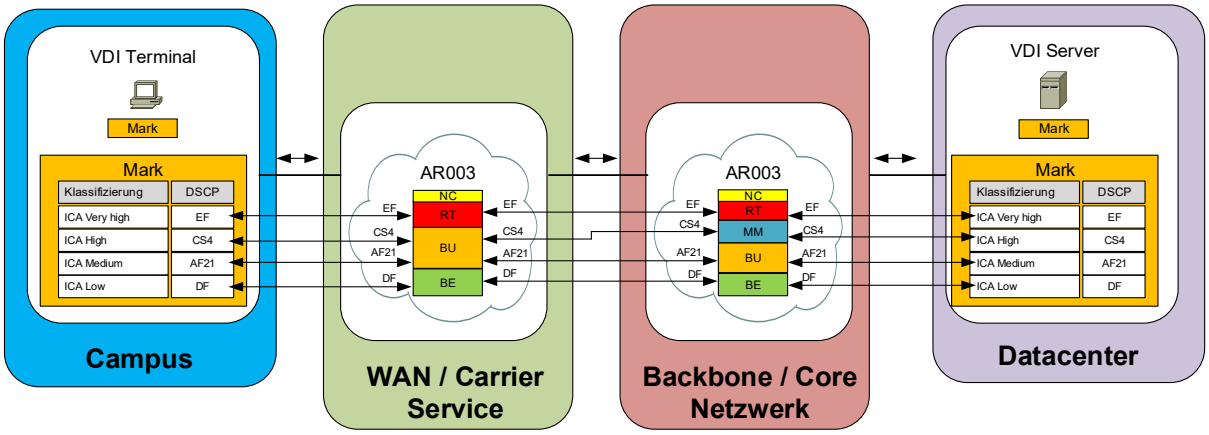


Abbildung 46: VDI

Anhänge

A. Änderungen gegenüber Vorversion

Keine (Ersterstellung)

B. Referenzen

ID	Referenz
[AR003]	AR003 – Architektur QoS
[DiffServ]	RFC 2475 – An Architecture for Differentiated Services
[P035]	P035 – Umgang mit Anforderungen und Vorgaben zur Bundesinformatik

C. Abkürzungen

Kürzel	Bedeutung
CIR	Committed Information Rate
DSCP	Differentiated Service Code Point
QoS	Quality of Service
PHB	Per Hop Behavior
RED	Random early detection