LANCOM Techpaper

Advanced Routing and Forwarding (ARF)

Mit zunehmender Komplexität moderner IP-Netzwerke steigen die Anforderungen an die zugrundeliegende Infrastruktur: Anwendungen wie Telefonie, Fernwartung, Gastzugang, oder Sicherheitsdienste müssen innerhalb einer Infrastruktur parallel und zugleich sicher voneinander getrennt eingerichtet und betrieben werden.

LANCOM Systems bietet über das Advanced Routing and Forwarding eine elegante Möglichkeit, alle IP-Anwendungen über einen zentralen Router zu führen und dabei die verschiedenen Kommunikationskanäle sicher voneinander abzugrenzen.

Dabei wird für jede Anwendung bzw. für unterschiedliche Benutzergruppen jeweils ein eigenes IP-Netzwerk eingerichtet. Über einen virtuellen Router wird der Datenverkehr der Netzwerke untereinander und der Zugang zum Internet und anderen entfernten Netzwerken für jedes IP-Netzwerk separat geregelt. Dieses Verfahren wird auch als Virtualisierung von IP-Netzwerken bezeichnet.

Konvergenz von IP-Diensten

Die Kommunikation von Unternehmen mit Kunden, Lieferanten, Mitarbeitern und externen Dienstleistern basiert auf einer gemeinsamen IP-Infrastruktur.

Oft werden die Möglichkeiten dieser Netzwerke jedoch nicht konsequent genutzt. Denn auch bei optimaler Nutzung aller Sicherheitsmechanismen wird für den firmenexternen Teilnehmer der Kommunikation meistens ein Zugang zum unternehmensinternen LAN (Intranet) eingerichtet – was aus Gründen der Sicherheit in vielen Fällen nicht gewünscht ist. Alternativ wird für jede Komponente ein eigenes Netzwerk mit eigenen Schnittstellen aufgebaut. Bei dieser zweiten Variante entstehen durch die parallelen Netzwerke mit unterschiedlichen Technologien mehr Komplexität und Aufwand für die IT-Abteilungen, anstelle der gewünschten Einsparungen steigen die Gesamtkosten für Kommunikation und Informationsaustausch.

Eigenes IP-Netzwerk für jede Anwendung

Mit dem Advanced Routing and Forwarding (ARF) stellt LANCOM Systems alle Möglichkeiten zur sicheren Reali-

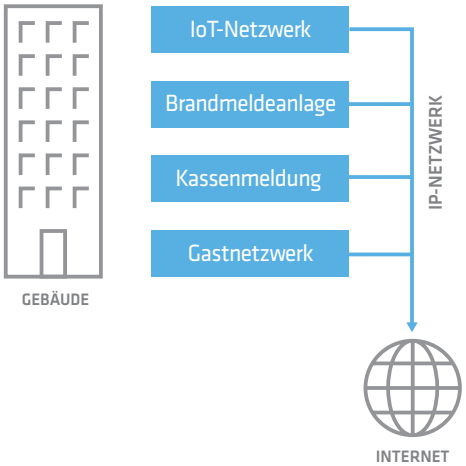

Abb. 1: Klassisches IP-basiertes Netzwerk ohne Anwendungstrennung

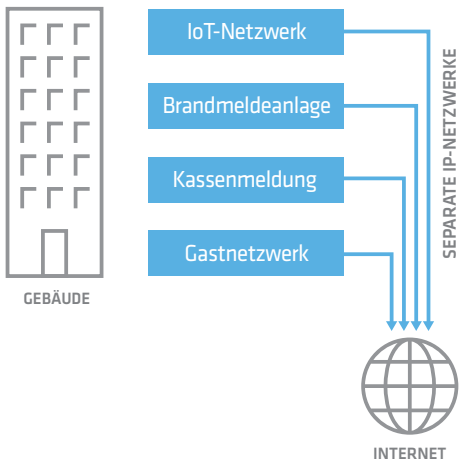

Abb. 2: IP-basiertes Netzwerk mit Anwendungstrennung über ARF

LANCOM Systems

sierung von IP-basierten Netzwerken über einen einzigen zentralen Router bereit. Das Kernstück des ARF ist dabei die Möglichkeit, für unterschiedliche Anwendungen jeweils einen separaten IP-Kontext einzurichten. Jeder IP-Kontext wird wie ein eigenes Netzwerk z. B. mit DHCP- und DNS-Server konfiguriert und gegen alle anderen Netzwerke abgeschirmt. Auf diese Art und Weise können mehrere externe Teilnehmer mit unterschiedlichen Anforderungen in das firmeninterne IP-Netzwerk eingebunden werden, ohne ihnen gleichzeitig einen Zugang zum eigenen Intranet einzuräumen. Damit entfällt der Bedarf für separate Kommunikationsnetze für jede Anwendung, die Wartung und Konfiguration kann zentral von einer Stelle aus vorgenommen werden.

Anwendungsbeispiele

Das Advanced Routing und Forwarding kommt immer dann zum Einsatz, wenn unterschiedliche Anwendergruppen ein gemeinsames physikalisches Medium im IP-Netzwerk nutzen. Die folgenden Beispiele zeigen die Anwendungsmöglichkeiten, die einzeln oder miteinander kombiniert zum Aufbau eines All-IP-Netzwerks genutzt werden können.

Gastzugang für WLAN-Clients

Ein Gastzugang für mobile WLAN-Clients ist in den meisten Unternehmen heute Standard. Darüber können sich die Besucher mit Ihren Notebooks oder Smartphones während einer Besprechung z. B. über VPN in die eigene Firma einwählen und von dort aktuelle Informationen abrufen.
Bei der Nutzung von ARF wird für das Gäste-WLAN ein eigenes IP-Netzwerk aufgesetzt, in dem ein dedizierter DHCP-Server die IP-Adressen verteilt, die z. B. aus einem anderen Adresskreis als dem im Intranet verwendeten kommen. Das IP-Netzwerk für das WLAN wird mit einem Schnittstellen-Tag versehen, über das der Router den Datenverkehr vom Intranet trennen kann.

Gemeinsame Nutzung des WAN-Zugangs

Wenn mehrere Unternehmen ein Gebäude gemeinsam nutzen (z. B. Filialen von größeren Unternehmen), dann muss nicht für jede Firma ein separater Internet-Zugang installiert werden. Die Filialen können einen zentralen Router nutzen, der die entsprechende Weiterleitung der Daten übernimmt. Für jede Filiale wird ein eigenes IP-Netzwerk mit jeweils einem eigenen Schnittstellen-Tag aufgesetzt. Dabei können beide IP-Netze sogar den gleichen IP-Adresskreis nutzen, wenn z. B. von der IT-Abteilung der Zentrale spezielle Adressen gewünscht werden. Im Router werden die Daten anhand des Schnittstellen-Tags identifiziert und können mit eigenen Routing-Regeln behandelt werden. So kann z. B. der Adresskreis 10.0.0.0 aus einer Bankfiliale über VPN in das Netz der Bankzentrale geroutet werden, während der

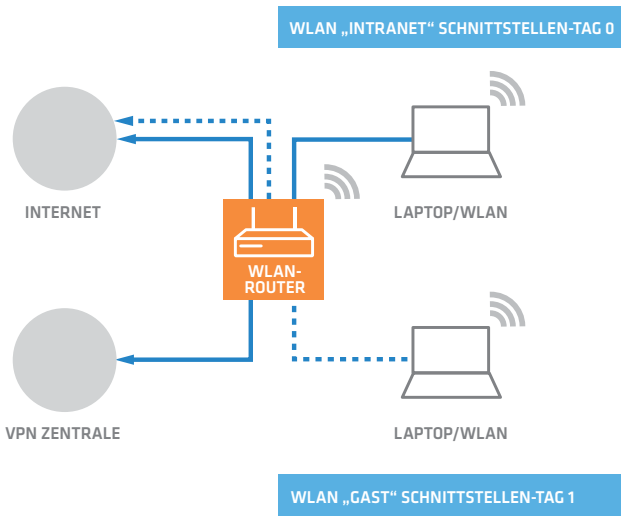

Abb. 3: Gastzugang für WLAN-Clients

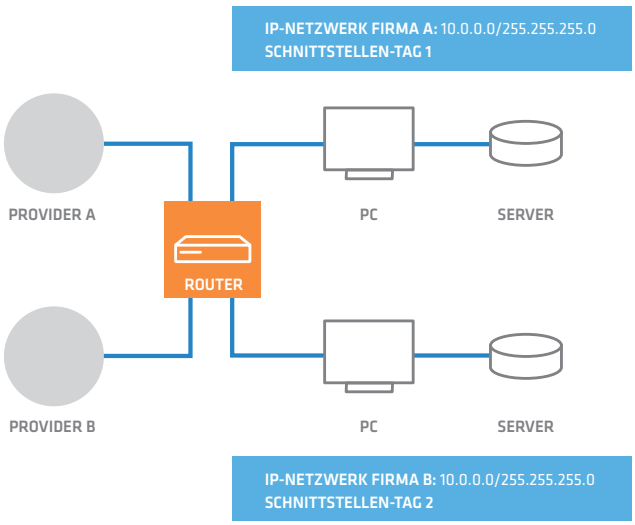

Abb. 4: Gemeinsame Nutzung des WAN-Zugangs

gleiche Adresskreis 10.0.0.0 aus der Versicherungsfiliale in das Netz der Versicherungszentrale geroutet wird.
Als Alternative können die Filialen mit der gleichen Technik auch jeweils den eigenen Internetprovider nutzen. Die Routing-Tabelle kann dazu für jedes IP-Netzwerk eine spezielle Default-Route bereitstellen.

Trennung von privatem und geschäftlichem IP-Netzwerk im Homeoffice

Viele Telearbeiter werden über einen VPN-Router an das Netzwerk der Zentrale angebunden und nutzen so zentrale Mailsysteme, Datenbanken, Fileserver oder VoIP-TK-Anlagen. Bei der üblichen Variante ohne ARF wird dabei das gesamte Intranet aus dem Homeoffice an die Zentrale angebunden mit allen darin angemeldeten Rechnern. Über ARF können im Homeoffice getrennte Netzwerke für die geschäftliche und die private Nutzung eingerichtet werden, sodass nur die Arbeitsstationen für die dienstliche Nutzung über den VPN-Tunnel mit der Firma kommunizieren können. Die privaten Rechner erhalten nur einen Zugang zum Internet. Analog zu dieser Anwendung können z. B. auch die Netzwerke in einer Schule für Schüler und Lehrer getrennt werden, wobei die Schüler nur eingeschränkten Zugriff auf die verfügbaren Ressourcen haben.

Gemeinsame Nutzung von zentralen Ressourcen

Durch den Einsatz von ARF werden die verschiedenen IP-Netzwerke – auch wenn diese das gleiche physikalische Übertragungsmedium nutzen – vollständig voneinander getrennt. Für die gemeinsame Nutzung von zentralen Ressourcen, wie z. B. Netzwerkdruckern o. ä., ist jedoch ein Zugriff aus verschiedenen IP-Netzwerken notwendig. Der Übergang von Daten zwischen verschiedenen Netzwerken wird in den LANCOM Routern von der Firewall geregelt. Dementsprechend kann über die Firewall auch der Zugriff auf bestimmte Geräte oder Dienste in einem gemeinsam genutzten Netzwerk eingerichtet werden.

Einbindung von externen Dienstleistern

Bei den bisher vorgestellten Anwendungen werden die Funktionen des ARF in erster Linie dazu eingesetzt, die Teilnehmer auf Seiten des Routers selbst je nach Anwendergruppe zu separieren und ihnen die erlaubten Dienste bzw. Zugriff auf Ressourcen einzuräumen. Die Möglichkeiten des ARF erlauben es aber auch, gezielt externe Ressourcen oder Unternehmen in die eigene Infrastruktur einzubinden. Als sehr umfassendes Beispiel betrachten wir ein vollständig digitalisiertes Kaufhaus.

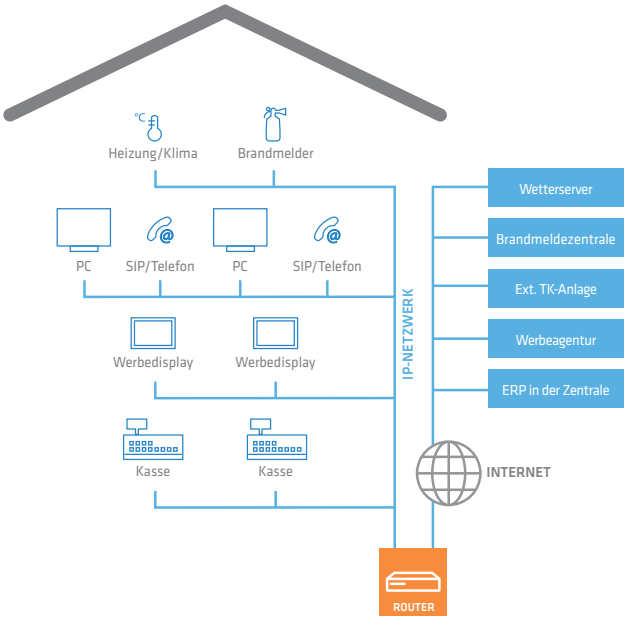

Abb. 5: Beispiel eines digitalisierten Kaufhauses

In diesem Kaufhaus sind die Kassen vernetzt und sollen mehrmals täglich den Warenabfluss an das ERP-System der Zentrale melden, die daraufhin die Nachlieferungen vorbereitet.

- Die Gebäudetechnik ruft von einem Server im Internet die aktuellen Wetterprognosen ab und steuert mit einem entsprechenden Vorlauf die Heizungs- bzw. Klimaanlage.
- Die Videospots in den Werbedisplays werden von einem externen Dienstleister eingespielt und täglich aktualisiert.

- Im ganzen Haus werden VoIP-Telefone verwendet, die an eine TK-Anlage bei einem externen Dienstleister angeschlossen sind.
- Das Alarm- und Schließsystem ist mit der Sicherheitsfirma verbunden, die bei einem Alarm oder einer Störung automatisch informiert wird.

Wie funktioniert das ARF?

Das Advanced Routing and Forwarding besteht aus folgenden Einzelaspekten:

- Im LANCOM Router können mehrere IP-Netzwerke definiert werden.
- Die einzelnen IP-Netzwerke werden untereinander abgeschirmt.
- Die verschiedenen IP-Netzwerke werden getrennt geroutet.

Bis zu 256 IP-Netzwerke in einem Router

Der erste Aspekt ist von der Ausstattung der Hardware abhängig. Je nach Modell können die LANCOM Router bis zu 256 unterschiedliche IP-Netzwerke verwalten und so auch komplexe Szenarien abbilden. Für jedes IP-Netzwerk können dabei der verwendete IP-Adresskreis, die IP-Adresse des LANCOM Routers und wichtige Funktionen wie DHCP- oder DNS-Server separat eingestellt werden.

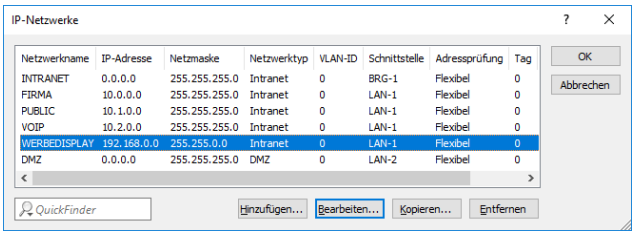

Abb. 6: Konfiguration der IP-Netzwerke

Trennung der Netzwerke

Eine wesentliche Voraussetzung für den sicheren Betrieb von unterschiedlichen IP-Netzwerken in einem Gerät ist die Möglichkeit, den Datenverkehr der einzelnen Netzwerke untereinander abzuschirmen. Die Netzwerke sind über die physikalischen Schnittstellen mit dem Router verbunden. LANCOM Router und LANCOM WLAN-Router bieten für die lokale Anbindung von Workstations und anderen Netzwerkteilnehmern je nach Modell ein oder mehrere Ethernet-Ports und WLAN-Module an. Diese physikalischen Schnittstellen werden aber nicht direkt für das Routing verwendet – um eine möglichst hohe Flexibilität zu erreichen, werden die physikalischen Schnittstellen auf logische Interfaces gebunden.

Bei den kabelgebundenen LAN-Anschlüssen findet diese Zuordnung durch das Ethernet-Port-Mapping statt: für jeden Ethernet-Port kann gezielt die gewünschte Verwendung z. B. als logisches LAN-Interface konfiguriert werden (bei einigen Modellen ist alternativ auch die Verwendung als WAN-Anschluss zur Verbindung mit einem DSL-Modem möglich).

Für die drahtlosen Netzwerkschnittstellen (WLAN-Module) entstehen durch den Aufbau von Point-to-Point-Strecken (P2P) bzw. durch die Verwendung von Multi-SSID auf jedem physikalischen WLAN-Modul mehrere WLAN-Interfaces: bis zu acht WLAN-Netze (Multi-SSID) und bis zu sechs P2P-Strecken pro Modul, die sich für den Router jeweils als logische WLAN- bzw. P2P-Interfaces darstellen.

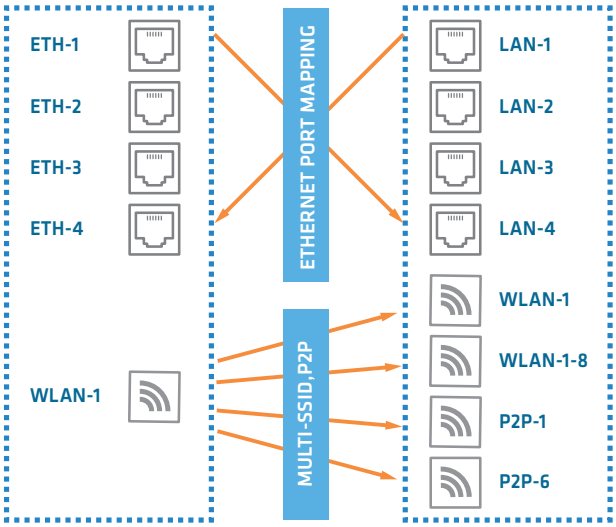

Abb. 7: Logische Trennung der IP-Netzwerke

Jedes IP-Netzwerk kann eines der logischen LAN-, WLAN- oder P2P-Interfaces und darüber die verbundene physikalische Schnittstelle nutzen. Das Netzwerk befindet sich damit in einer separaten Broadcast-Domain und kann

über dieses logische Interface ausschließlich mit dem Routermodul der LANCOM Geräte kommunizieren – eine direkte Datenübertragung in die anderen Netzwerke ist nicht möglich. Eine Broadcast-Domain stellt einen Bereich in einem lokalen Netzwerk dar, in dem eine Broadcast-Nachricht **alle** Teilnehmer erreicht. Broadcasts können auch über Switches oder Bridges hinweg übertragen werden. Erst mit dem Einsatz eines Routers oder durch die Aufteilung des lokalen Netzwerks in VLANs (virtuelle LANs) wird eine Broadcast-Domain begrenzt.

Die Entscheidung über die Datenübertragung zwischen den einzelnen IP-Netzwerken wird also in das Routermodul verlagert, in dem die Datenströme aus allen IP-Netzwerken zusammenlaufen. Grundsätzlich wird dabei das Routing zwischen den verschiedenen lokalen IP-Netzwerken erlaubt. Dazu ein Beispiel:

- Das erste IP-Netzwerk verwendet den Adresskreis 10.0.0.0 und ist über das logische Interface „LAN-1“ an das physikalische Interface „ETH-1“ gebunden.
- Das zweite IP-Netzwerk verwendet den Adresskreis 192.168.0.0 und ist über das logische Interface „WLAN-1“ an das physikalische Interface „WLAN-1“ gebunden.

Für beide IP-Netzwerke ist im LANCOM ein DHCP-Server aktiviert. Obwohl sich die beiden Netzwerke in separaten Broadcast-Domains befinden, ist über den Router ein Zugriff auf Ressourcen im jeweils anderen Netzwerk möglich.

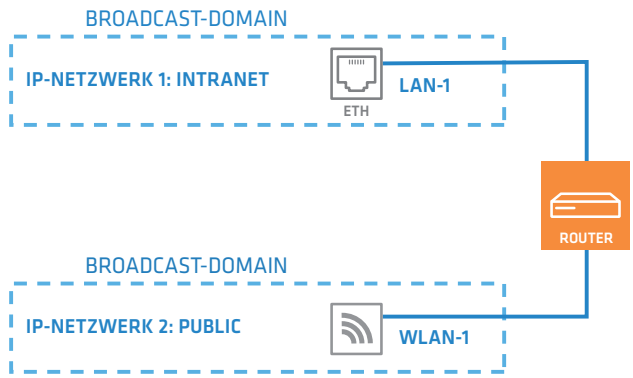

Abb. 8: Begrenzung der Broadcast-Domains durch Router

Ein Ping oder eine Verbindung über die IP-Adresse wird über den Router richtig aufgelöst und durchgeleitet.

Die Zuständigkeit des Routers kann recht einfach getestet werden, indem in der Firewall eine Deny-All-Regel erstellt wird: Der Datenverkehr zwischen allen erreichbaren Netzwerken über den Router wird damit unterbunden, ein Ping in das jeweils andere Netzwerk bleibt ohne Antwort.

Geregeltes Routing mit Schnittstellen-Tags

Neben dem kompletten Abschalten des Routings zwischen den IP-Netzwerken kann über die Firewall auch gezielt eingestellt werden, welches IP-Netzwerk über den Router auf welche anderen Bereiche zugreifen darf. Bei einer größeren Anzahl von Netzwerken können dazu aber recht viele Firewallregeln erforderlich sein. Um das Routing zwischen den logischen Interfaces zu vereinfachen, wird jedes IP-Netzwerk mit einem Schnittstellen-Tag versehen. Dieses Tag regelt auf sehr elegante Art und Weise, welche IP-Netzwerke über den Router miteinander verbunden werden:

- Die Netzwerkgeräte in einem IP-Netzwerk können nur auf Ressourcen in Netzwerken mit dem gleichen Schnittstellen-Tag zugreifen.
- Der Zugriff auf Netzwerke mit abweichenden Schnittstellen-Tags wird im Router unterbunden.
- Das Schnittstellen-Tag „0“ kennzeichnet dabei ein Supervisor-Netzwerk: Geräte in diesem Netzwerk können auf Ressourcen in allen anderen Netzwerken mit abweichenden Schnittstellen-Tags zugreifen.

Das Schnittstellen-Tag steuert die Sichtbarkeit von IP-Netzwerken vom Typ „Intranet“. Neben den Intranets können die Netzwerke auch als „DMZ“ (demilitarisierte Zone) konfiguriert werden. Mit dem Netzwerk-Typ „DMZ“ wird ein IP-Netzwerk definiert, auf dessen Ressourcen die Teilnehmer aus allen anderen IP-Netzwerken zugreifen können – unabhängig von den verwendeten Schnittstellen-Tags.

Als Beispiel wird das Netzwerk der Systemadministratoren mit dem Schnittstellen-Tag „0“ versehen – die Administratoren können auf alle anderen Netzwerke zugreifen. Die

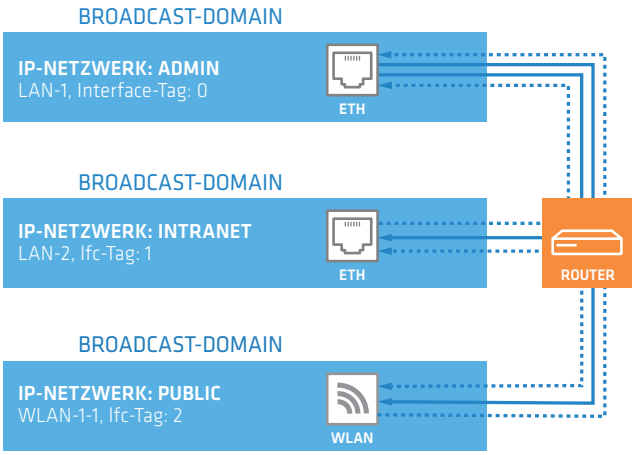

Abb. 9: Beispiel für geregeltes Routing mit Schnittstellen-Tags

Netzwerke für das Intranet und das Gäste-WLAN bekommen die Schnittstellen-Tags „1“ und „2“ – und bleiben damit abgeschottet ohne Zugriff auf eines der anderen Netzwerke.

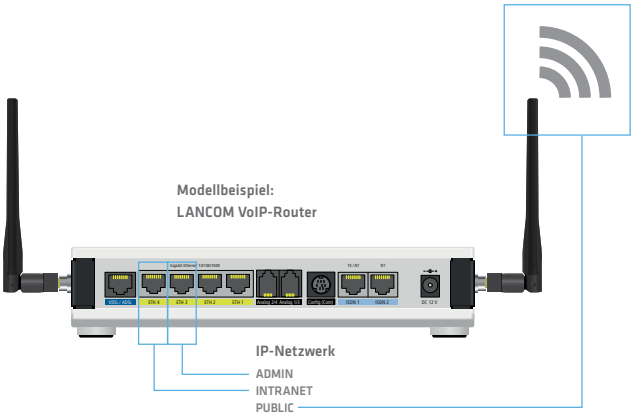

Abb. 10: Modellbeispiel LANCOM VoIP-Router

Wie schon angedeutet, ist die Firewall im Router zuständig für die Vermittlung der Datenpakete. Die Firewall im LANCOM Router ist „stateful“, kann also die Richtung der Datenverbindungen berücksichtigen. Daher wird mit dem Zugriff aus dem Supervisor-Netz mit Schnittstellen-Tag „0“ auf eines der anderen IP-Netzwerke auch gleichzeitig die Tür für den Rückfluss der Daten geöffnet. Der Rechner im Gast-Netz kann also einen Ping beantworten, der von einem Rechner im Supervisor-Netz ausgelöst wurde.

Virtuelle Interfaces

In manchen Anwendungen ist es notwendig, die eindeutige Zuordnung der IP-Netzwerke zu den logischen Interfaces zu erweitern. Dazu können die logischen Interfaces in einem weiteren Schritt auf „virtuelle“ Interfaces abgebildet werden. Je nach Verfügbarkeit der logischen Interfaces sind dabei zwei Varianten möglich:

- Mehrere logische Interfaces werden zu einem virtuellen Interface verbunden: In einem IP-Netzwerk sollen nicht nur Rechner aus einem kabelgebunden LAN, sondern gleichzeitig Stationen aus einem WLAN verbunden werden. In diesem Fall werden die benötigten logischen Interfaces (z. B. ein LAN und ein WLAN für das Intranet) zu einer so genannten „Bridge-Gruppe“ (BRG) zusammengefasst.

Bridge-Gruppen sind in Geräten mit WLAN-Modul vorhanden, um z. B. auch einzelne Layer-2-WLAN-Netze (SSIDs) oder VLANs mit dedizierten Ethernet-Ports gruppieren zu können.

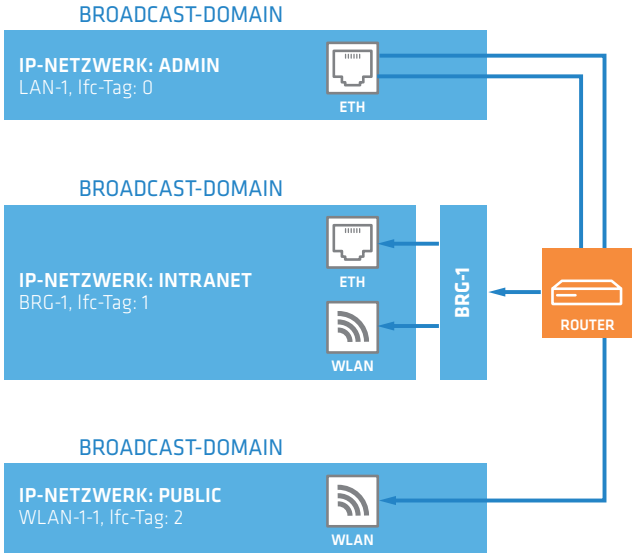

Abb. 11: Zusammenfassung von physikalischen Interfaces über Bridge-Gruppen

Die Bridge-Gruppe spannt eine eigene Broadcast-Domain auf und definiert, welche logischen Interfaces ihr zugeordnet werden und wirkt für den Router wie ein einziges, virtuelles Interface. Zwischen den verbundenen

logischen Interfaces der Bridge-Gruppe ist eine einfache Datenübertragung im Bridge-Modus möglich – alle anderen logischen Interfaces können mit dieser Bridge-Gruppe nur über den Router kommunizieren.

- Ein logisches Interface wird von mehreren virtuellen Interfaces genutzt: Der ungekehrte Fall liegt vor, wenn das Gerät nicht ausreichend viele logische Interfaces bereitstellt, um jedem IP-Netzwerk eine eindeutige Zuordnung zu ermöglichen. In dieser Situation werden mehrere virtuelle LANs (VLANs) definiert, die jeweils das gleiche logische Interface nutzen. Dazu wird dem IP-Netzwerk neben dem logischen Interface eine VLAN-ID zugewiesen. Wenn Datenpakete aus dem IP-Netzwerk versendet werden, wird die VLAN-ID in die Pakete eingefügt. Wird über das logische Interface ein Paket mit dieser VLAN-ID empfangen, kann das Paket dem zugehörigen IP-Netzwerk zugeordnet werden. Die VLANs stellen sich für den Router als separate, virtuelle Interfaces dar – der Datenverkehr der einzelnen VLANs ist jedoch untereinander abgeschirmt, jedes VLAN stellt eine separate Broadcast-Domain dar.

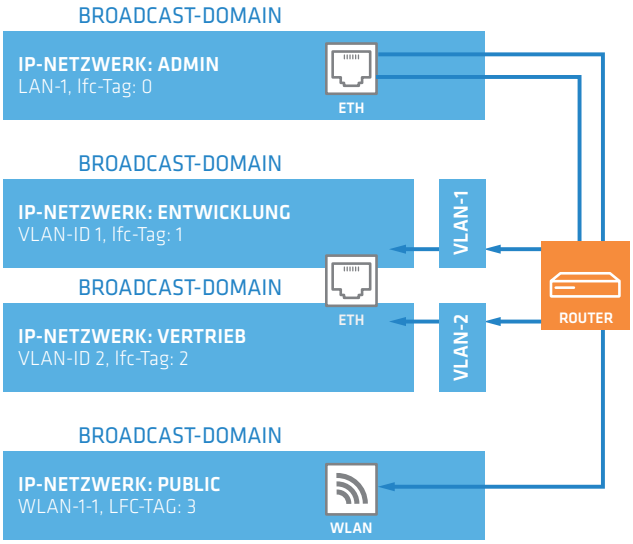

Abb. 12: Logische Trennung per VLAN

So können z. B. an einem logischen LAN-Interface die beiden Netzwerke für die Entwicklung und den Vertrieb mit unterschiedlichen VLAN-IDs eingerichtet werden. Der Router sorgt intern für die richtige Zuordnung und Auswertung der VLAN-Tags. Im LAN werden die Datenpakete anhand der VLAN-Tags entweder in den Netzwerkkarten der Workstations oder in einem vorgeschalteten VLAN-Switch separiert.

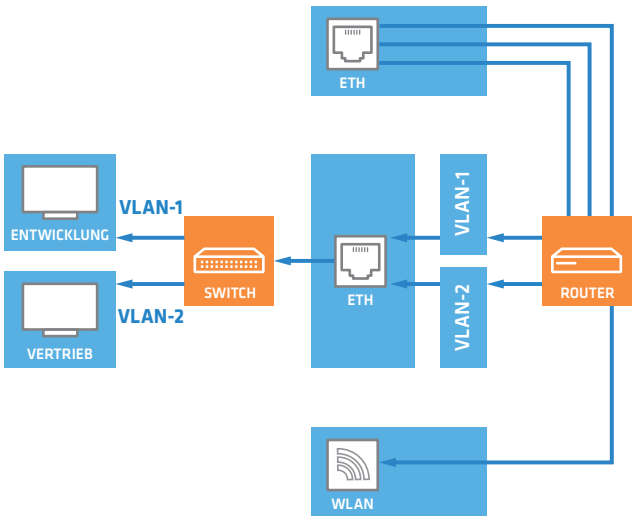

Abb. 13: Logische Trennung per VLAN im Switch

Auch in diesem Szenario wird die Datenübertragung zwischen den VLANs über Schnittstellen-Tags geregelt. Über diese flexible Zuordnung stehen für die IP-Netzwerke neben den logischen Interfaces zusätzlich zahlreiche VLANs und Bridge-Gruppen als virtuelle Interfaces zur Auswahl, mit denen sich in jeder Anwendung der Datenverkehr der Netzwerke untereinander abschirmen läßt.

Virtuelle Router

Mit der Definition der IP-Netzwerke und der Separierung des Datenverkehrs (über Zuordnung von Schnittstellen bzw. Bridge-Gruppen oder VLAN-IDs) wird der parallele Betrieb mehrerer lokaler Netzwerke an einem zentralen LANCOM Router sichergestellt. Für die Verbindung zu anderen Netzwerken ist der IP-Router zuständig. Die in der Routing-Tabelle angelegten Routen sind dabei grundsätzlich für alle an das Gerät angeschlossenen lokalen Netzwerke gültig – anders als z. B. die DHCP-Einstellungen, die für jedes IP-Netzwerk separat eingerichtet werden.

Um für jedes Netzwerk einen separaten Router zu realisieren, wird ebenfalls das Schnittstellen-Tag verwendet. Die Schnittstellen-Tags sind sehr eng mit den Routing-Tags im LANCOM

Router verwandt, die für das „policy-based Routing" eingesetzt werden. Die Routing-Tags können z. B. über die Firewall in die Datenpakete von bestimmten Diensten eingesetzt werden. Der Router nutzt dann für diese Datenpakete zunächst nur die Einträge der Routing-Tabelle, die mit dem entsprechenden Routing-Tag markiert sind.

Ebenso funktionieren im Rahmen des Advanced Routing and Forwarding die Schnittstellen-Tags. Neben der Sichtbarkeit der IP-Netzwerke untereinander steuern diese Tags auch gleichzeitig die Verwendung der Routing-Tabelle: für jedes IP-Netzwerk werden zunächst nur die Einträge genutzt, deren Routing-Tag mit dem Schnittstellen-Tag des IP-Netzwerks übereinstimmt.

Eine Sonderstellung nimmt dabei das Routing-Tag „0" ein: Routen mit diesem Tag gelten für alle Netzwerke, unabhängig vom Schnittstellen-Tag. Durch diese spezielle Auswahl der Routen aus der Routing-Tabelle entsteht für jedes IP-Netzwerk ein eigener, virtueller Router.

Der große Vorteil der virtuellen Router wird in folgendem Beispiel deutlich: Anhand der Quelle eines Datenpakets kann die Firewall üblicherweise ein Routing-Tag zuweisen, das im IP-Router zur Auswahl der geeigneten Route genutzt wird. Dieses Verfahren reicht aber dann nicht mehr, wenn der Router mehrere IP-Netzwerke mit gleichem Adresskreis verwaltet: eine Zuweisung des Tags anhand der Quell-Adresse ist dann nicht mehr eindeutig möglich. Über das Schnittstellen-Tag ist jedoch die Zuordnung der Gegenstelle auch dann möglich, wenn Netzwerkteilnehmer aus unterschiedlichen IP-Netzwerken mit identischen IP-Adressen eine Verbindung aufbauen wollen. Das virtuelle Routing funktioniert nur durch die Auswertung der Schnittstellen-Tags, eine Konfiguration von zusätzlichen Firewallregeln ist nicht notwendig. Für jedes lokale Netzwerk kann so ein separater Provider-Zugang über eine getaggte Default-Route in der Routing-Tabelle angesteuert werden.

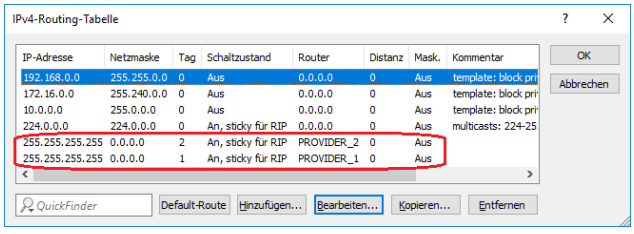

Abb. 14: Beispiel IPv4-Routing mittels Schittstellen-Tags

Die Firewall wird nur dann benötigt, wenn in den lokalen Netzwerken mit gleichen IP-Adressen auch Server stehen, die aus dem Internet erreichbar sind. In diesem Fall wird der Verbindungsaufbau von außen nach innen ausgelöst. Die beim Router-Modul aus dem Internet eintreffenden Datenpakete verfügen zwar nicht über Schnittstellen-Tags, die für die weitere Verarbeitung verwendet werden könnten. In diesem Fall kann aber die Gegenstelle ausgewertet werden, über welche die Pakete empfangen werden. Mit einer speziellen Firewallregel können Verbindungen von dieser Gegenstelle über den entsprechenden Port (z. B. 80 für Webserver) in das jeweilige Netzwerk erlaubt werden, mit dem zugehörigen Port-Forwarding-Eintrag wird gezielt der Webserver angesprochen.

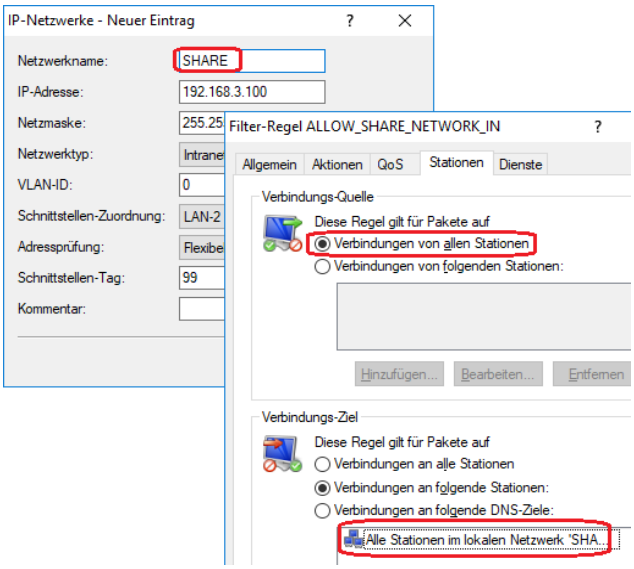

Abb. 15: Beispiel einer Firewall-Regel für Verbindung von Außen

Flexibler Übergang zwischen IP-Netzwerken

Das Advanced Routing and Forwarding realisiert an einem zentralen Router vollständig getrennte IP-Netzwerke. Manche Ressourcen in der Infrastruktur sollen aber vielleicht für mehrere oder alle Netzwerke zur Verfügung stehen, z. B. ein Netzwerkdrucker nicht nur für die eigenen Mitarbeiter im Intranet, sondern auch für die Besucher im Public-Netz. Dazu wird zunächst ein eigenes IP-Netzwerk „SHARE" für die geteilten Ressourcen eingerichtet, das

auf die Schnittstelle(n) gebunden ist, über welche die geteilten Ressourcen angeschlossen sind. Dieses Netzwerk wird außerdem als „Intranet" mit einem eindeutigen Schnittstellen-Tag konfiguriert (z. B. „99"). Damit ist dieses Netzwerk zunächst gegenüber allen anderen Netzwerke abgeschirmt.

Über eine passende Regel in der Firewall wird dann gezielt der Zugang von allen Stationen in anderen Netzwerken in das gemeinsame Netzwerk SHARE ermöglicht. Diese Firewallregel erhält als Routing-Tag das Schnittstellen-Tag des SHARE-Netzwerks. So werden alle Datenpakete, auf welche diese Firewallregel zutrifft, mit dem Tag „99" versehen und können so dem IP-Netzwerk SHARE zugeordnet werden. Bei Bedarf können in der Firewallregel zusätzlich die erlaubten Dienste definiert werden, die im Netzwerk SHARE genutzt werden dürfen.

LANCOM Management Cloud (LMC)

Mit der LANCOM Management Cloud lassen sich komplette Netze unter Einsatz von Software-defined-Networking-Techniken (SDN) per Browser verwalten. Per SD-WAN ist die automatische Einrichtung sicherer VPN-Verbindungen zwischen Standorten, inklusive Netzwerkvirtualisierung und Backup auch über die Weitverkehrsstrecken möglich: Die VPN-Funktionalität wird per Mausklick aktiviert und die gewünschten VLANs werden für den jeweiligen Standort ausgewählt. Die Tunnelendpunkte müssten nicht einzeln konfiguriert werden. Pro standortübergreifendem Netz wird dabei ein VPN-Tunnel benötigt

Somit bietet Advanced Routing and Forwarding (ARF) mit seinen bis zu 256 IP-Kontexten zusammen mit der LMC eine elegante Möglichkeit, alle IP-Anwendungen über einen zentralen Router zu führen und die verschiedenen Kommunikationskanäle sicher voneinander abzugrenzen.

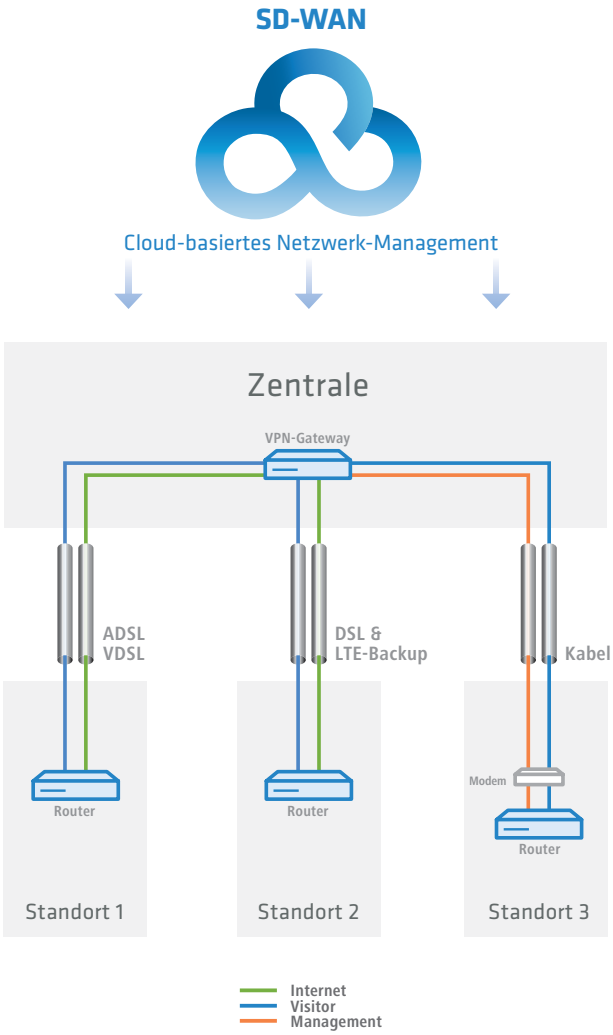

Abb. 16: SD-WAN nutzt ARF, um Kommunikationskanäle logisch zu trennen

Zusammenfassung

Das Advanced Routing und Forwarding in LANCOM Routern bietet die Möglichkeit, mit einem einzigen zentralen Gerät mehrere IP-Netzwerke zu definieren, deren Datenverkehr über die Zuordnung von Ethernet- oder WLAN-Ports bzw. die Zuweisung von Bridge-Gruppen oder VLAN-IDs voneinander abgeschirmt werden kann.

Die Erreichbarkeit der lokalen Netzwerke untereinander wird über den Router geregelt und durch spezielle Schnittstellen-Tags gesteuert.

Über die Schnittstellen-Tags kann für jedes IP-Netzwerk darüber hinaus ein dedizierter, virtueller Router eingerichtet werden, der die Verbindung zum Internet oder anderen externen Gegenstellen herstellt. So kann z. B. ein VPN-Tunnel zu einer Partnerfirma gezielt nur für einzelne Netzwerke erreichbar eingerichtet werden.

Mit diesen Funktionen ermöglichen die ARF-Router den Aufbau von All-IP-Netzwerken, in denen unterschiedliche Anwendungen auf Basis des IP-Protokolls eine gemeinsame Infrastruktur nutzen, dabei jedoch voneinander getrennt bleiben. Auf der lokalen Seite können so mehrere „Intranets“ oder „Gastnetzwerke“ parallel betrieben werden, externen Partnern kann über das Internet gezielt Zugriff auf Teile der lokalen Struktur eingeräumt werden.

Konkrete Beispielkonfigurationen und fertige Scripte finden Sie in der LANCOM KnowledgeBase mit einer Suche nach dem Stichwort „ARF“.
www.lancom-systems.de/knowledgebase/

LANCOM Systems GmbH I Adenauerstr. 20/B2 I 52146 Würselen I Deutschland I E-Mail info@lancom.de

LANCOM Systems