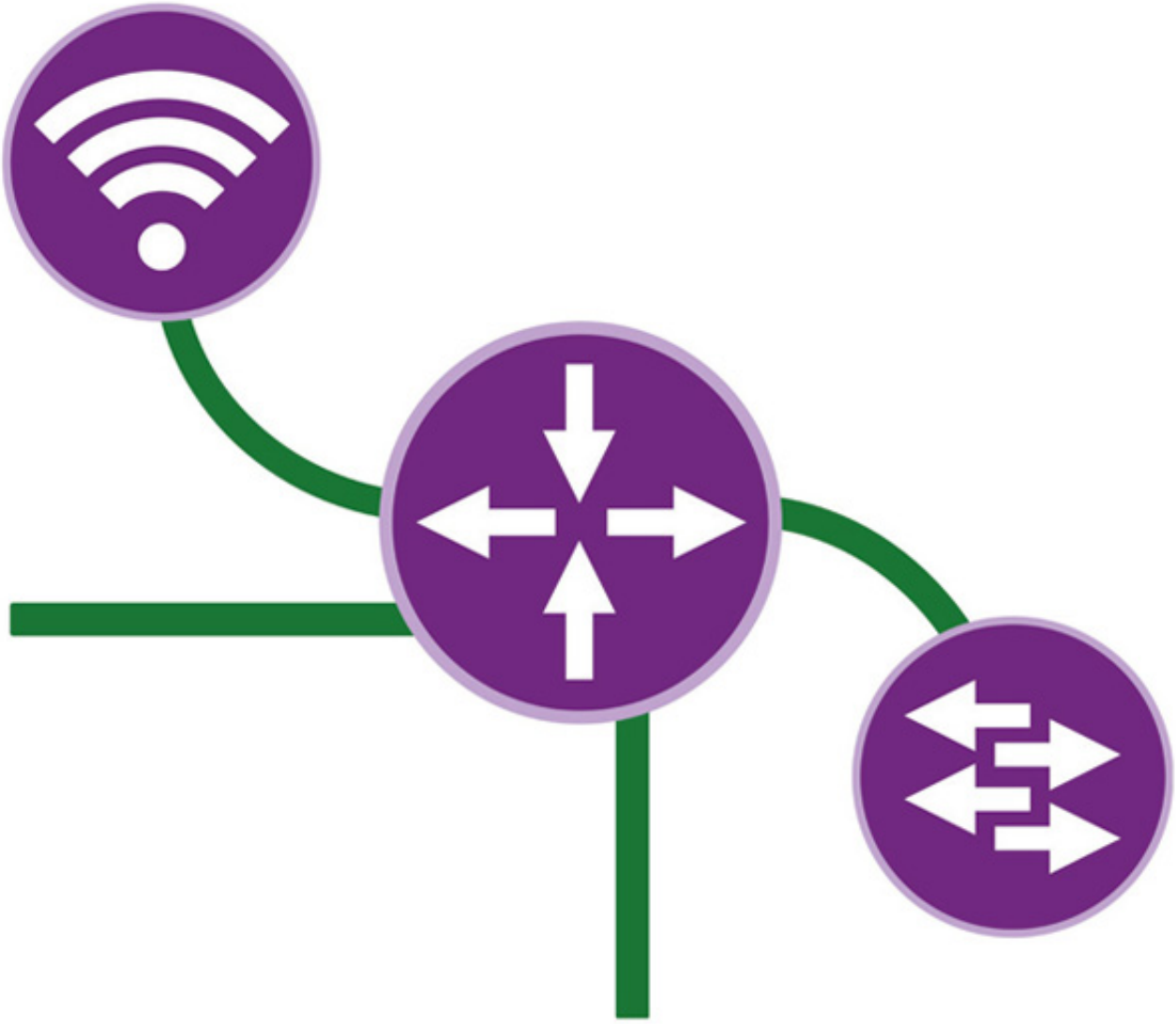

Der OpenWrt-Praktiker

Band 2: Fortgeschritten

Markus Stubbig

Inhaltsverzeichnis

Einleitung

OpenWrt ist ein Open-Source-Betriebssystem für Netzwerkgeräte wie Router, Switches und Accesspoints. Es basiert auf Linux und konzentriert sich auf Themen wie WiFi, Firewall, Adressumsetzung und Routing unter einer einheitlichen Kommandozeile. OpenWrt läuft auf physischer Hardware oder als virtuelle Maschine.

Jeder Netzwerkausrüster stattet seine Komponenten mit dem eigenen Betriebssystem aus. OpenWrt verkauft keine Hardware, sondern bietet eine Linux-Distribution für möglichst viele Geräte an. OpenWrt ersetzt auf *anderen* Routern das Betriebssystem und kann damit durchstarten.

Der erste Band vermittelt einen Einstieg in OpenWrt und behandelt die Grundlagen. Die Kapitel sind eine Schritt-für-Schritt-Anleitung, die Open-Wrt installieren, Netzadapter einrichten und IP-Adressen vergeben. Nach der Ersteinrichtung behandelt Band 1 auch die Kommandozeile UCI, die Paketverwaltung und die Systemadministration mit Überwachung eines OpenWrt-Geräts.

Der vorherige Band richtet sich an Leser, die mit OpenWrt keine Erfahrung haben und ins Thema einsteigen wollen. Wer bereits einen OpenWrt-Router im Einsatz hat, sollte mit dem zweiten Band starten. Der zweite Band baut auf den Grundlagen auf und vermittelt dem Leser fortgeschrittene Themen, Tipps für die Fehlersuche und ein großes Kapitel zur Firewall.

Übersicht

Der Anfang dieses Buchs widmet sich der Sicherheit von OpenWrt: Kapitel 1 beleuchtet die zonenbasierte Firewall und Kapitel 2 demonstriert die Umsetzung von IP-Adressen.

Danach liefert Kapitel 3 ein paar Handgriffe aus dem Tagesgeschäft, die die Arbeit mit OpenWrt vereinfachen. Kapitel 4 macht OpenWrt fit für NetFlow und erfährt damit, welche IP-Verbindungen durch den Router fließen.

Als Nächstes kommt in Kapitel 5 die Hardware unter OpenWrt auf den Prüfstand und darf zeigen, wie viel Durchsatz die Netzadapter unter realen Bedingungen schaffen. Falls das zu wenig Leistung ist, gibt es am Ende des Kapitels einige Tipps für die Steigerung.

Kapitel 6 erklärt die Architektur von OpenWrt und mit welchen Softwarekomponenten die Distribution arbeitet. Wer sich für Open Source interessiert, kann in Kapitel 7 aus dem Quellcode ein fertiges Image für OpenWrt selber zusammenbauen.

Zuletzt beleuchtet Kapitel 8 wie OpenWrt von Cloudanbietern für Logging und Datenablage profitieren kann.

Labornetz

Für den praxisnahen Einstieg erwacht OpenWrt in einem konstruierten Labornetz zum Leben. Die nachfolgenden Kapitel basieren alle auf demselben Netzaufbau. Das vollständige Labornetz ist als Netzdiagramm in Abbildung 1 auf Seite → dargestellt und ist mit dem Diagramm in Band 1 identisch. Es ist als Grundlage für die nachfolgenden Kapitel konzipiert und stellt ein kleines Netzwerk mit mehreren Standorten dar. In den folgenden Kapiteln werden meist nur

Teile dieses Netzwerks zur Untersuchung benutzt. Welches Interface in welchem Netz zu Hause ist zeigt Tabelle 1.

Der stets unveränderte Aufbau des Labornetzes hat den charmanten Vorteil, dass zwischen den Kapiteln nicht umgebaut werden muss. Kein Umverkabeln der Geräte oder Umkonfigurieren der virtuellen Umgebung. Das spart Zeit und verhindert Fehler. Und nach ein paar Kapiteln wird das Labornetz zum vertrauten Begleiter, denn die Namen der Geräte, Netzschnittstellen und IP-Adressen bleiben unverändert.

Wenn ein Abschnitt einen gesonderten Aufbau benötigt oder ein weiteres Gerät untersucht werden soll, gibt es am Anfang der Lektion einen entsprechenden Hinweis mit Erklärung.

Da ein händischer Eingriff nach dem ersten Aufbau nicht mehr notwendig ist, kann das Lab auch „aus der Ferne“ betrieben werden – Remotezugriff vorausgesetzt.

Gerät	**Interface**	**Funktion/Netz**	**IPv4**	**IPv6**
RT-1	eth0	Management	10.5.1.1	fd00:5::1
	eth1	Standort-1	10.1.1.1	fd00:1::1
	eth2	WAN-1	198.51.100.1	2001:db8:1::1
	eth3	WAN-2	192.0.2.1	2001:db8:2::1
RT-2	eth0	Management	10.5.1.2	fd00:5::2
	eth1	Standort-2	10.2.1.2	fd00:2::2
	eth2	WAN-3	203.0.113.2	2001:db8:3::2
	eth3	WAN-1	198.51.100.2	2001:db8:1::2
RT-3	eth0	Management	10.5.1.3	fd00:5::3
	eth1	Standort-3	10.3.1.3	fd00:3::3
	eth2	WAN-3	203.0.113.3	2001:db8:3::3
RT-4	eth0	Management	10.5.1.4	fd00:5::4
	eth1	Standort-4	10.4.1.4	fd00:4::4
	eth2	WAN-3	203.0.113.4	2001:db8:3::4
	eth3	WAN-2	192.0.2.4	2001:db8:2::4
labsrv	eth0	Management	10.5.1.7	fd00:5::7
	eth1	Standort-1	10.1.1.7	fd00:1::7

Tabelle 1: Alle Geräte mit Netzadaptern, Funktion und IP-Adressen

Version

OpenWrt entwickelt sich weiter. Diese positive Tatsache erschwert die Dokumentation und die einheitliche Verwendung einer Versionsnummer. Aus diesem Grund verwenden die Bände der Buchreihe *Der OpenWrt-Praktiker* nicht die gleiche Version, sondern arbeiten stets mit den aktuellen Versionen von OpenWrt. Folglich können Screenshots und Kommandoausgaben zwischen den Bänden und den eigenen Experimenten unterschiedlich ausfallen.

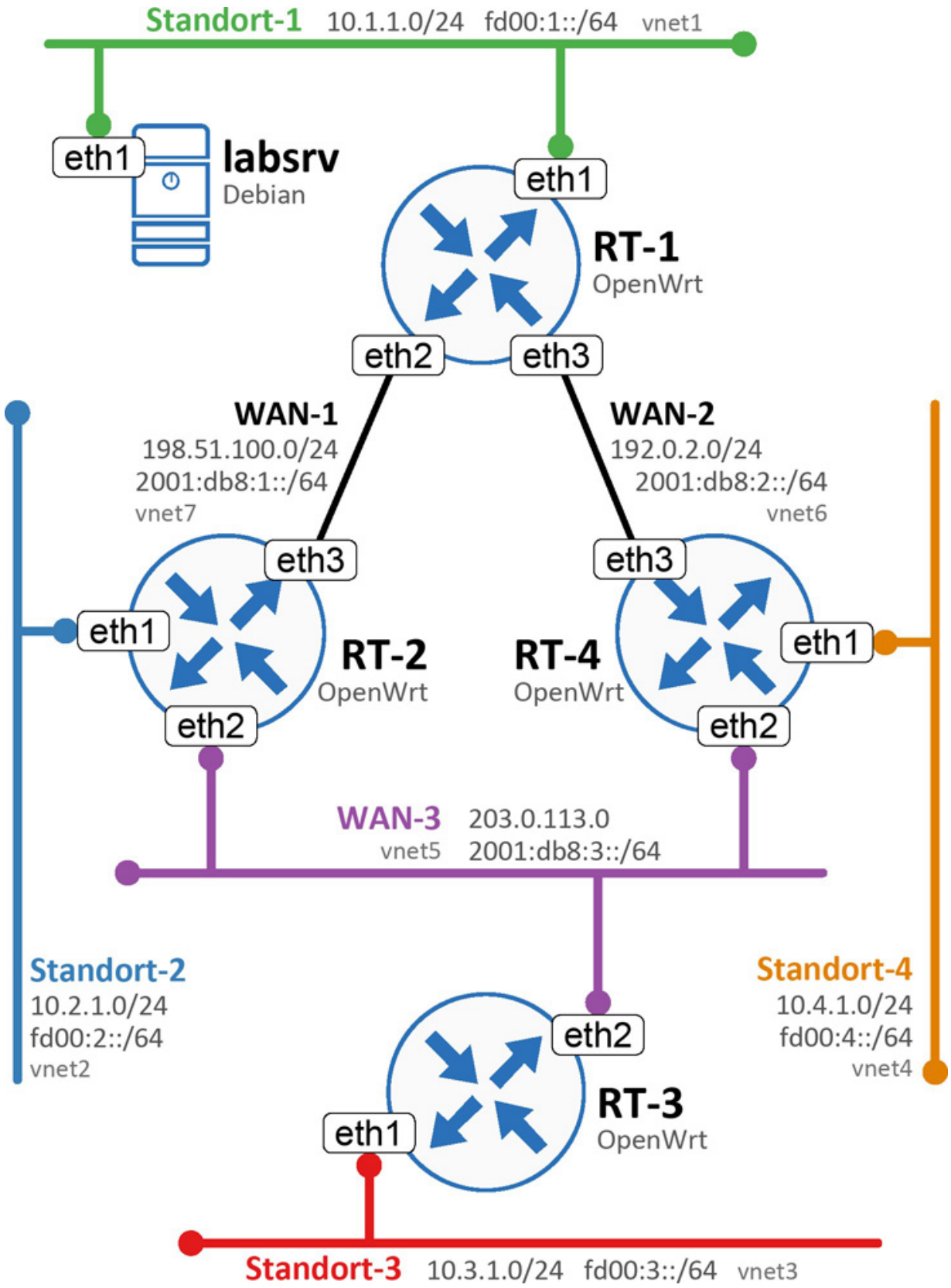

Abbildung 1: Das Labornetzwerk als Vorlage für die folgenden Kapitel

Kapitel 1

Firewall

Eine Firewall ist kein einzelnes Gerät, sondern ein Konzept! Das erklärte Ziel dieses Konzepts ist die Sicherheit zwischen Computernetzen, um Zugriffe zu kontrollieren und Angriffen so lange wie möglich standzuhalten. Umgesetzt wird das Sicherheitssystem meist mit Paketfiltern, Anwendungsgateways (Proxy), demilitarisierter Zone (DMZ), Verschlüsselung und Logging. Ob die Adressumsetzung im Sinne von NAT (vgl. Kap. 2) zur Steigerung der Sicherheit beiträgt, ist umstritten.

Vereinfacht ausgedrückt: Router verbinden Computernetze, Firewalls trennen sie.

Für ein erhöhtes Maß an Sicherheit können auch große Geschütze aufgefahren werden: Systeme zum Erkennen und Verhindern von Einbrüchen suchen im internen Netz nach Paketen, die aufgrund des Regelwerks dort gar nicht sein dürfen.

Beliebt ist auch der Honeypot, welcher ein realistisch aussehendes Netz nachbaut. Genau wie eine Filmkulisse, die aussieht wie eine echte Straßenszene. Der Honeypot lenkt den Angreifer von den wirklichen Zielen ab und erlaubt Angriffsmuster zu studieren.

Allgemein ist der Begriff *Firewall* nicht mit dem Sicherheitskonzept belegt, sondern wird synonym mit

Paketfilter verwendet. Daher bezeichnet das folgende Kapitel ein einzelnes OpenWrt-Gerät und sein Regelwerk als *Firewall*.

OpenWrt als Firewall

Ein Paketfilter besteht aus mehreren Regeln, die IP-Pakete klassifizieren. Jede Regel hat eine oder mehrere Bedingungen, zu denen das Paket passen muss, um weiter bearbeitet zu werden. Sobald ein Paket zu einer Regel passt, wird die hinterlegte Aktion ausgeführt und das Paket wird weitergeleitet oder verworfen.

Diese Beschreibung trifft grundsätzlich auf alle Paketfilter zu. Die meisten Anbieter von Firewalls unterscheiden sich äußerlich dadurch, wie das Regelwerk konfiguriert wird und wie granular die Regeln sein können.

Bei OpenWrt arbeitet das Regelwerk nach dem *First Match*-Prinzip. Die Prüfung des IP-Pakets beginnt bei der ersten Regel und endet, sobald eine der Regeln zutrifft. Wenn keine passende Regel dabei ist, gibt es noch die Standardprozedur, die alles verwirft.

Der Paketfilter von OpenWrt arbeitet verbindungsorientiert. Die *Antwort*pakete einer Verbindung benötigen keine separate Regel, sondern sind automatisch erlaubt.

Durch das *First Match* -Prinzip ist die Reihenfolge der einzelnen Regeln entscheidend. Eine strenge blockierende Regel zu Beginn eines Regelwerks macht nachfolgende einzelne Regeln wirkungslos.

Die Regeln sind meistens nach dem folgenden Schema sortiert:

1. *Anti-Spoofing-Regeln*. Damit lassen sich Pakete mit gefälschten Adressen aufdecken.