

Ein einfacher Mechanismus zur Vermittlung und Abrechnung von Netzteilnehmern auf der Basis von LAN-Standards

A.Tochatschek, M. Wählisch, T.C. Schmidt
{at,mw,schmidt}@fhtw-berlin.de

Fachhochschule für Technik und Wirtschaft Berlin
Hochschulrechenzentrum
Treskowallee 8, 10318 Berlin

Keywords: LAN Accounting, VLAN, RMON

Abstract

Die Untervermittlung von Netzdienstleistungen an rechtlich unabhängige Abnehmer erfordert Technologien, die sowohl Sicherheitsanforderungen als auch dem Anspruch an Verbrauchsabrechenbarkeit genügen. Auf der Basis von Standard Ethernet, 802.1Q VLAN-Techniken und RMON präsentieren wir eine einfache, kostenminimierte Lösung für dieses Problem. Auf der Grundlage dieses Ansatzes stellen wir weiterhin ein Betriebsszenario zur vollautomatischen Konfiguration und Abrechnung vor.

1 Einführung

In größeren lokalen Environments erwächst heute vermehrt die Aufgabe, kleine, rechtlich selbständige Gesellschaften wie Start-Ups oder Spin-Offs in der Brutkastenfunktion des Muttercampus mitzuversorgen und doch gleichzeitig wirtschaftlich und technisch in gebührender Weise getrennt zu behandeln. Die Fachhochschule für Technik und Wirtschaft Berlin betreibt mit eben dieser Zielstellung ein Existenzgünderzentrum, welches 35 Jungunternehmen Gelegenheit bietet, ihre Geschäftsideen unter moderaten wirtschaftlichen Randbedingungen zu etablieren.

Ebenso wie haustechnische Grundversorgungen und Telefondienste benötigen die Start-Ups eine leistungsfähige Internetkonnektivität. On Campus legen dabei Simplizität und Kosten den Einsatz von standard LAN-Techniken nahe, welche allerdings die geforderten Leistungsmerkmale der Netzseparierung und Verbrauchsmessung nicht fertig beinhalten. Nachfolgend beschreiben wir eine einfache Methode zur Implementierung einer skalierbaren, standardbasierten Lösung des Problems.

Unser Papier gliedert sich wie folgt: In Abschnitt 2 stellen wir den technischen Ansatz zur wohlseparierten Konnektivitätsversorgung der Teilnehmer vor. Abschnitt 3 ist dem Konfigurationsmanagement und Accounting gewidmet. Unsere praktische Realisierung wird in Abschnitt 4 vorgestellt und Abschnitt 5 widmet sich der Zusammenfassung und dem Ausblick.

2 Vermittlungsstrukturen auf Layer 2 und 3

Die Teilnehmer der untervermittelten Netze erhalten ihre IP-Grundversorgung durch die Übergabe eines IP-Subnetzes auf einem Ethernetport. Unsere Zielstellung, eine preiswerte und skalierbare Lösung anzubieten, verbietet allerdings, diese Übergabepunkte als Routerports auszubilden. Als Übergabeschnittstelle wählen wir statt dessen einen managebaren Switchport aus einer kaskadierten Switchwolke, welche gesammelt über einen dedizierten Router-Uplink mit dem Wissenschaftsnetz verbunden ist (vgl. Abbildung 1).

Die so erreichte Layer 3 Separierung der Unterteilnehmer zeigt eine klassische Ethernet Switch-Umgebung. Gemäß IEEE 802.1D-bridging Spezifikationen gehören alle Ports innerhalb der Switchwolke einer Broadcast-domain an, jedes Broadcast-Paket würde entlang der Switching-Kaskade an alle Teilnehmer gesendet. Dies genügt freilich noch keinerlei Anforderungen an Vertraulichkeit und gegenseitiger Abschirmung der Teilnehmer untereinander. Die hier gewünschte Topologisierung der Teilnehmerstrukturen muß auf der Subnetzwerkebene erfolgen und bildet eine Lehrbuchanwendung von 802.1Q VLAN-Techniken [1]. In einer 802.1Q-Umgebung ist jeder Switchport oder Frame Mitglied einer logischen Einheit - dem virtuellen lokalen Netz (VLAN). Ein Weiterleiten von Broadcast-Paketen findet nur auf Ports gleicher VLAN-Mitgliedschaft statt.

Die Konfiguration der virtuellen LANs erfolgt demgemäß kanonisch: Pro Teilnehmer und IP-Subnetz wird ein VLAN gespannt und auf jeweils genau einen Switchport gemappt. Die Uplink Ports zwischen den Switches und zum Routerinterface werden als Q-Trunk definiert, so daß jeder Datenverkehr, der sich nicht auf das Netz eines Teilnehmers beschränkt, den Router passieren muß. Als „trunk-link“ wird eine Verbindung zwischen 802.1Q-fähigen Devices bezeichnet, d.h. Geräten, die das VLAN-frame-Format verstehen und den „tag header“ auslesen können. Solch eine Verbindung ermöglicht das Multiplexing von virtuellen LANs zwischen mehreren VLAN-Geräten [1].

3 Konfiguration und Accounting mit SNMP

Ebenso wie die physikalische Verkabelung und die Definition der IP-Strukturen kann die VLAN Partitionierung des Switches im Rahmen einer einmaligen Anfangskonfiguration erfolgen. Das Aktivieren und Deaktivieren der Teilnehmerports ist an den managebaren Switches zur Betriebszeit durch das Management Protokoll SNMP möglich. Wechselnde Teilnehmer können so von einer hardware-unabhängigen Skriptsteuerung erfaßt werden, welche die noch zu lösende Aufgabe der Verbrauchsmessung sinnvoller Weise einschließen sollte.

Ein Trafficaccounting mit dem Ziel einer belastbaren Abrechnung muß zuverlässig, robust und taggenau erfolgen. Eventuell vorhandene interne, dem Übergabepunkt nachgeord-

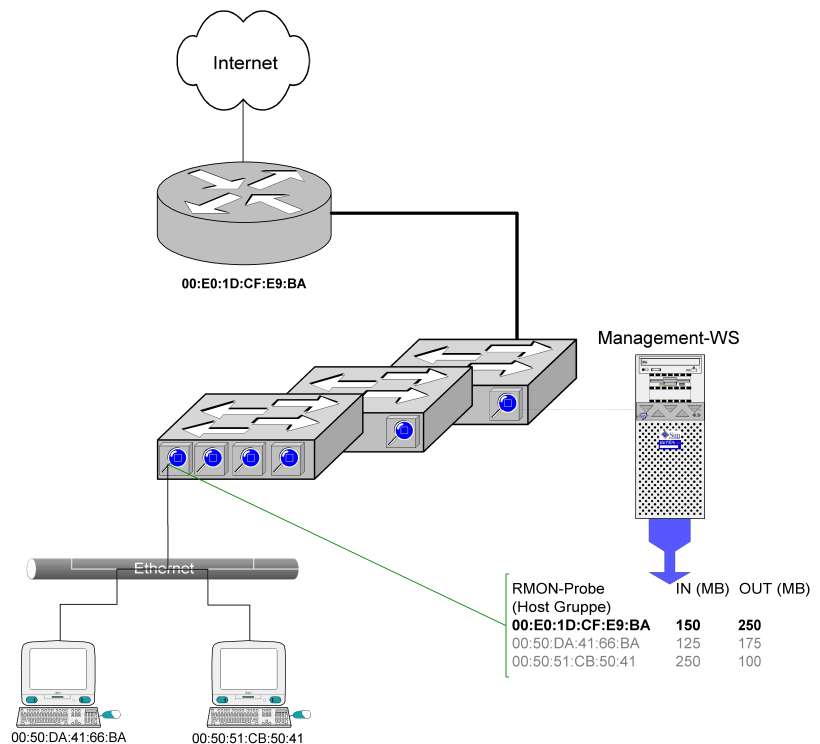


Abbildung 1: LAN Konfiguration mit RMON Probes

nete IP-Kommunikation sollte zudem hiervon nicht erfaßt werden. Das einfache Auslesen der Portcounter in den Switches genügt diesen Anforderungen nicht. Den Datenverkehr auf den teilnehmerspezifischen Internetverbindungskäneln messen wir aus diesem Grunde auf der Basis der Hostgruppe in der RMON MIB [3]. Sie ermöglicht eine Verkehrsanalyse auf Layer 2.

Die eigentliche Idee zur Verbrauchsmessung besteht nun darin, daß RMON Probes auf den einzelnen Switchports konfiguriert werden, und der Datenverkehr über die MAC (Ziel- und Quell-) Adresse des Routers überwacht wird (vgl. Abbildung 1). Auf diese Weise beschränkt sich die Verkehrsmessung auf den tatsächlichen Aussenverkehr der Teilnehmer. Darüber hinaus werden keinerlei Adressinformationen über Hosts der firmenprivaten Netze benötigt. Indem die RMON Probes auf den Schnittstellenports anstelle des zunächst naheliegenden Routerinterfaces instanziiert werden, gewinnt die vorgestellte Lösung zudem eine breite Skalierbarkeit.¹ Die zur Paketmessung bestimmten Counter der RMON Hostgruppe können vollautomatisch per Skript ausgelesen und rückgesetzt werden.

4 Das Einsatzszenario an der FHTW Berlin

Zur Versorgung der 35 Existenzgründer finden in unserem Hause zur Zeit zwei kaskadierte Cabletron SmartSwitches 2200 mit jeweils 24 x 10/100 Ethernetports ihren Einsatz, welche auf einen Fast Ethernet Port unseres Internet Routers Cabletron SSR 8000 geführt werden (vgl. Abbildung 2). Konfiguration und Accounting geschehen vollautomatisch mit Hilfe eines Perlskriptes, welches – gefüttert durch eine Initialisierungsdatei mit den Informationen Firmen-Portmapping sowie An- und Abschaltdatum – nächtlich um 0:00 Uhr Ports konfiguriert sowie Tafficcounter ausliest. Ebenfalls automatisch übernimmt das Skript die monatliche Rechnungslegung, nachdem die Existenzgründer zur Akzeptanz eines emailbasierten Rechnungswesen vertraglich verpflichtet wurden.

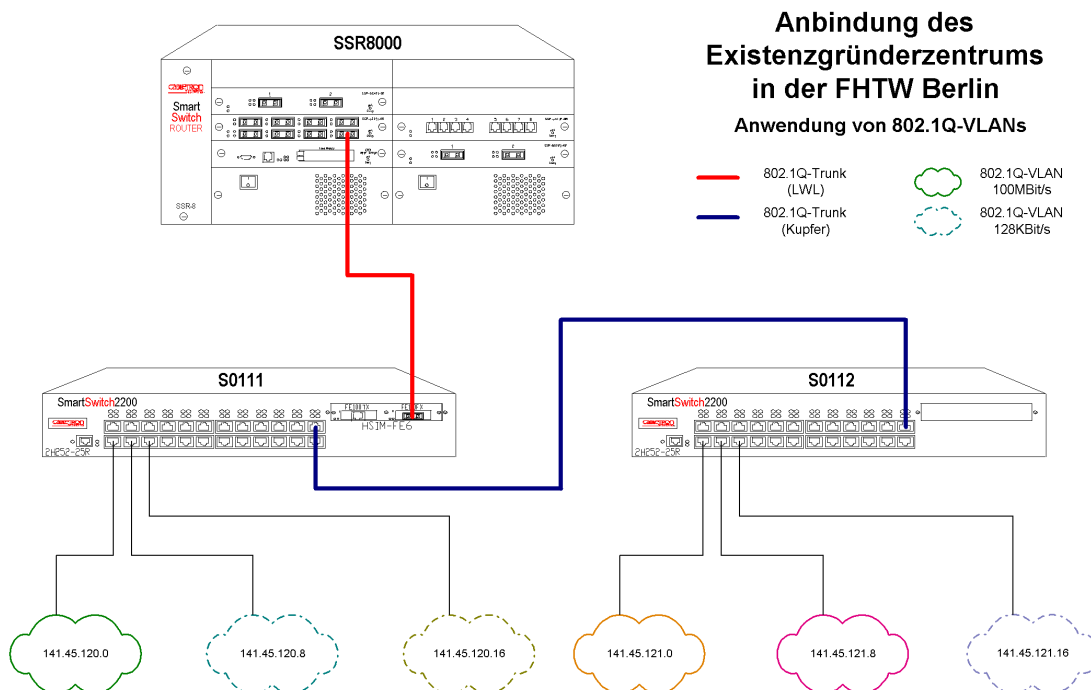


Abbildung 2: Einsatzbeispiel an der FHTW

¹ Bei moderaten Endteilnehmerzahlen jenseits der Portschnittstellen zeigen die in unserem Hause eingesetzten ASIC basierten Switches keinerlei Performanceeinbußen.

Auf der Basis zusätzlicher, teilweise proprietärer Funktionalitäten der Cabletron Switches konfigurieren wir darüber hinaus folgende Leistungsmerkmale [4]:

- Zur Erhöhung der Sicherheit wird im Schnittstellenbereich ausschließlich IP-Verkehr zugelassen sowie die zulässigen IP-Adressen exklusiv an Switchports gebunden [2].
- Als zusätzlichen Service der Kostenkontrolle können Bandbreitenbeschränkungen in den Schnittstellenports vereinbart werden.

5 Zusammenfassung und Ausblick

In dem vorliegenden Papier wurde eine einfache, robuste und skalierbare Lösung zur wohlseparierten Versorgung und Abrechnung von Netzunterteilnehmern vorgestellt, welche allein auf preiswerten, überall verfügbaren LAN-Standards basiert. Die vorgestellte Lösung besteht in einer Lehrbuchanwendung von 802.1Q VLANs sowie einem originellen Einsatz der RMON Hostgruppenfunktionalität.

Die Implementierung skriptgesteuerter Konfigurations- und Abrechnungsfunktionalitäten erlaubt einen stabilen Betrieb ohne technischen Betreuungseinsatz. Aufgrund der guten Skalierbarkeit der vorgestellten Lösung ist der Einsatz unserer Lösung zur kostenstellenbasierten Abrechnung innerhalb eines Hochschul- oder Firmennetzes ebenfalls denkbar.

Literatur

[1] IEEE Standards for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks, P802.1Q, 1998.

[2] Standard for Supplement to IEEE 802.1Q: IEEE Standards for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks: VLAN Classification by Protocol and Port, IEEE Draft P802.1v/D6, November 2000.

[3] S. Waldbusser: Remote Network Monitoring Management Information Base, RFC 2819, May 2000.

[4] Enterasys Networks: SmartSwitch Multilayer Frame Classification, White Paper, <http://www.enterasys.com/products/whitepapers/>, May 2000.