Zusammenfassung:

Die Aufgabe dieser Projektarbeit ist ein Unternehmensnetzwerk im Labor der HTW Chur zu planen, aufzubauen und zu Dokumentieren. Das ganze Netzwerk soll redundant aufgebaut werden, um ausfallsicher zu sein, und ausserdem wird IPv4 und IPv6 verwendet.

Abstract:

The goal of this project is to achieve a working corporate network. Beside redundancy, the clients should be able to use IPv4 and Ipv6. Clients from a department should only be able to communicate with users from the same department, even in other sites.

Fallbeispiel:

Sie sollen ein neues Netzwek für die Mittelgrosse Firma HAC Home Audio Center AG aufbauen, welche 80 Mitarbeiter an den 3 Standorten Chur, Buchs, St. Gallen beschäftigt. Die Firma hat ihren Hauptsitz mit 70 Mitarbeitern in Chur und Niederlassungen mit je 5 Mitarbeitern in Buchs und St. Gallen. Die Standorte sind durch ein Layer-3 MPLS VPN miteinander verbunden(durch einen einfachen Swich simuliert).

Die Netzwerkkomponenten sind bereits vorhanden, die physische Netzstruktur aufgrund der Gebäudetopographie und der Skalierbarkeit zu einem grossen Teil vorgegeben.

Die verfügbaren Komponenten sind:

-Standort Chur:

- 1x Router (Cisco 1941) mit 2x FastEthernet und 2x GigabitEthernet Anschlüssen

- 2x Layer-3 Switch (Cisco 3750)

- 2x Layer-3 Switch (Cisco 3560)

- 2x Layer-2 Switch (Cisco 2960)

-Standort Buchs:

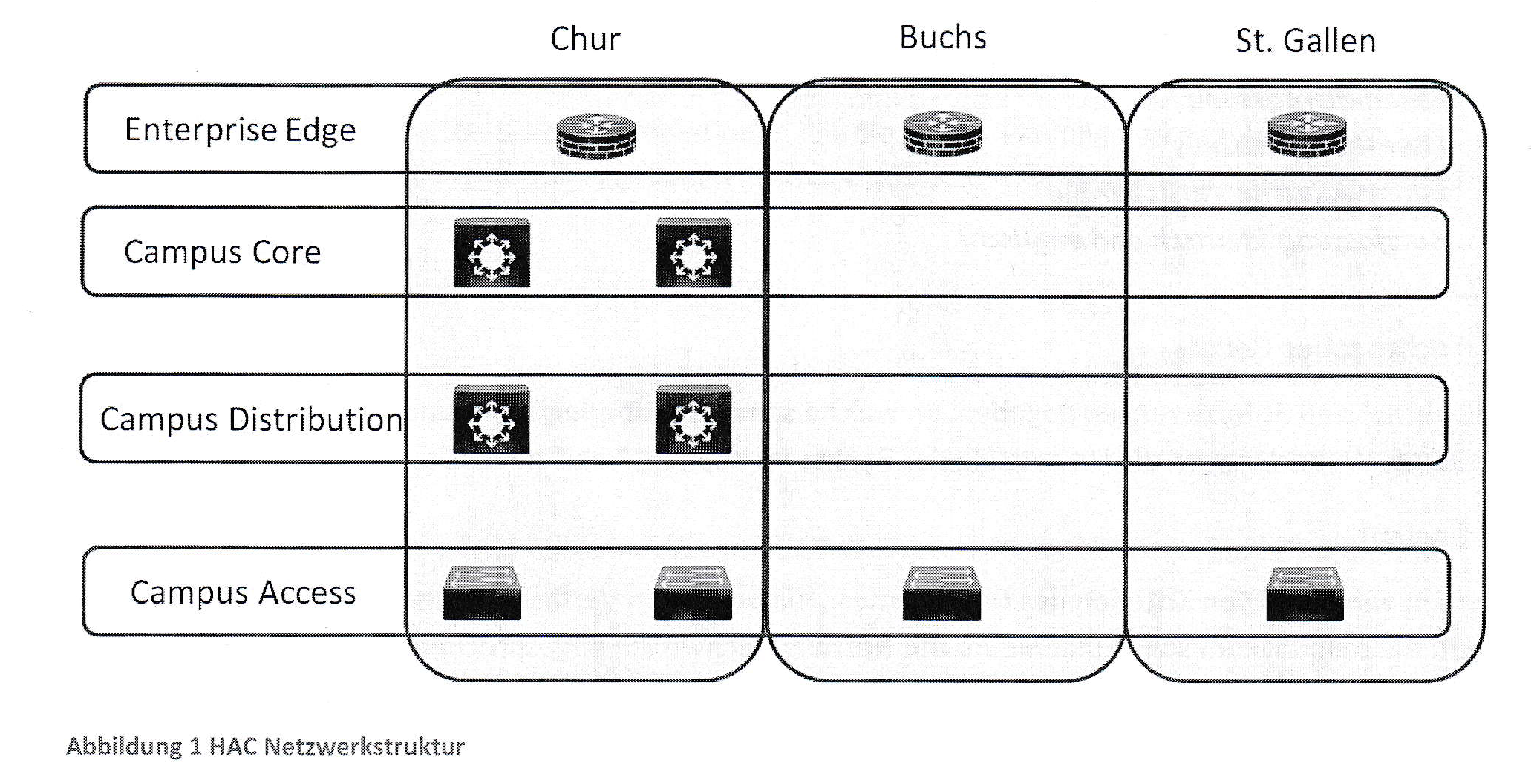
- 1x Router (Cisco 1920)

- 1x Layer-2 Switch (Cisco 2960)

-Standort St.Gallen:

- 1x Router (Cisco 1921)

- 1x Layer-2 Switch (Cisco 2960)

Die vorgegebene Netzwerkstruktur sieht folgendermassen aus:

Ipv4 Adresskonzept:

Das folgende Konzept gilt nur für IPv4, immer wenn von Adressen die Rede ist, sind nur IPv4 Adressen gemeint.

Für das private Netz werde Adressen aus dem 10.0.0.0/8 Netz ausgewählt. Für jeden Standort und für die Netze welche nicht einem Standort zugeornet werden können wird ein /16 Netz ausgewählt, so hat jeder Standort 65534 Ip-Adressen. Dies sollte für die nahe Zukunft genügen,

Die Aufteilung sieht folgendermassen aus:

Chur 10.1.0.0/16

St. Gallen 10.2.0.0/16

Buchs 10.3.0.0/16

Transfer 10.4.0.0/16

Für die Vlans werden die Netze der Standorte nochmals unterteilt, die gelben Sterne im Vlan-Plan stehen für die Standorte. Mit /24 Netzen stehen jeder Abteilund pro Standort 256 Adressen zur Verfügung.

Vlan 10 Geschäftsleitung 10.\*.10.0/24

Vlan 20 Buchhaltung 10.\*.20.0/24

Vlan 30 Entwicklung 10.\*.30.0/24

Transfer 10.\*.40.0/24

Vlan 99 Management 10.\*.99.0/24

Ipv6 Adresskonzept:

Das folgende Konzept gilt nur für IPv6, immer wenn von Adressen die Rede ist, sind nur IPv6 Adressen gemeint.

Die Aufgabenstellung besagt, dass ein /48 Netz zur Verfügung steht, das Ziel ist nun dies in einer ähnlichen Art wie bei IPv4 zu gestalten.

Standortabhängigkeiten:

Chur 2001:620:3101:1::/64

St. Gallen 2001:620:3101:2::/64

Buchs 2001:620:3101:3::/64

Da es bei IPv6 keine Vlans gibt, sondern alles über Layer-3, sprich IP, geschieht. Muss auch ein “Vlan-Konzept” für IPv6 erstellt werden. Dies wird analog zu IPv4 gemacht. Die gelben Sterne stehen für die Standortadresse.

Netze der Abteilungen:

Vlan 10 Geschäftsleitung 2001:620:3101:\*010::/64

Vlan 20 Buchhaltung 2001:620:3101:\*020::/64

Vlan 30 Entwicklung 2001:620:3101:\*030::/64

Transfer 2001:620:3101:\*040::/64

Vlan 99 Management 2001:620:3101:\*099::/64

weitere Überlegungen:

Bei genügender Zeit hätte man noch einiges erreichen können. Einige Punkte welche wichtig sind werden nun erläutert:

- Passwort setzen: Im Moment ist auf keinem Gerät ein Passwort gesetzt, da es während der Konfiguration mühsam ist immer wieder das Passwort einzugeben, deshalb sollte dies ganz am Schluss geschehen.

- Fernwartung: Auf allen Geräten ist eine Management Adresse konfiguriert. Wenn jetzt der Fernzugriff aktiviert würde, müssten die Anzahl Zugriffe aus dem Internet begrenzt werden, damit nicht mit Bruteforce das Passwort geknackt werden kann.

- OSPF Areas: Die einzelnen Standorte hätten noch mit einem eigenen OSPF Area konfiguriert werden können, dies hätte den Vorteil dass nicht alle über OSPF Teilnehmer über das ganze Netz bescheid wissen müssen und so bedeutend weniger Traffic auf den Leitungen ist.

- Vlan: Es hätte noch ein GästeVlan eingerichtet werden können, welches nur zum Internet zugriff hat, dies ist jedoch nicht Teil der Aufgabenstellung und könne im Bedarfsfall schnell nachgerüstet werden.

- Device Backups: Wenn im Moment Device Backups gemacht werden müssen, muss jeder einzelne Router und Switch mittels kopieren der running-config gebackupt werden. Dabei könnte man mit einem Kron-Script die Backups zeitgesteuert auf einen TFTP Server speichern. So spart man sich wöchentliche Arbeit und man vergisst es auch sicher nicht.

Stack:

Stacken ist das Zusammenschliessen zweier physischen Switches zu einem logischen. Dies ist nicht mit allen Switches möglich, doch in diesem Fall ist es bei den Beiden Distribution-Switches möglich, da diese ein Stack-Interface auf der Rückseite haben. Dies erspart eine Menge an Arbeit, wenn man weiss wie dies funktioniert. In diesem Fall war dies leider nicht der Fall, da noch nie mit gestackten Switches gearbeitet wurde, die Anweisungen zur Konfiguration des Stackes bezieht sich hier nur auf die Cisco Catalyst 3750 Switches, da nicht bekannt ist ob es noch Besonderheiten bei der Konfiguration anderer Switches gibt. Als erstes musste festgestellt werden, dass der 3750er nur LACP und kein PagP unterstützt. Ausserdem müssen die gestackten Switches auf Active geschalten werden, falls sie auf passive

Routing Konzept:

Innerhalb unseres Unternehmens werden die verschiedenen Standorte miteinander über OSPF geroutet. Am Hauptstandort in Chur wird ab dem Distributions-Switch (D) ebenfalls mit OSPF geroutet. Beim Interface mit dem Internetanschluss wird eine default-Route gesetzt, da diese immer die Gleiche ist. Damit die Clients immer den gleichen default-Gateway haben, ist auf R1 noch ein Loopback-Interface erstellt worden, dieses darf nicht vergessen werden bei der Konfiguration von OSPF.

NAT Konzept:

Meistens ist es für ein Unternehmen nicht rentabel sich die gesamte Anzahl benötigter IP-Adressen zu kaufen. Deshalb werden private IP-Adressen verwendet und danach können mit einem NAT ganze Subnetze zu einer öffentlichen Adresse zugeordnet werden. Dies ist eine komfortable Lösung, ausserdem können dann die privaten Adressen so gestaltet werden, dass man nur schon beim anschauen weiss an welchem Standort und zu welchem Vlan die Adresse gehört.

IPv4:

Für die öffentlichen Adressen steht ein /28 Netz zur Verfügung. Für die Verwendung von NAT können alle Adressen des Netzes benutzt werden, die Netz- und Broadcast-Adresse werden nicht benötigt. Somit stehen 16 öffentliche Adressen zur Benutzung, hier wurde für jeden Vlan an jedem Standort eine eigene Adresse verteilt. Dies ergibt 12 Adressen, die restlichen 4 Adressen sind für Reserven eingeplant.

IPv6:

Bei IPv6 ist kein NAT notwendig, da ein öffentliches /48 Netz gebraucht wird. Es sind also mehr Adressen vorhanden als je in diesem Kleinunternehmen gebraucht werden.

ACL:

Mit ACL's wird der Zugriff der Abteilungen untereinander verhindert, lediglich das Management-Vlan hat auf alles Zugriff, da dies für die reibungslose Verwaltung des Netzes erforderlich ist.

Die ACL's werden auf den Routern R2, R3 und auf dem Switch D konfiguriert, für die 3 Vlans der Abteilungen wird je der Zugriff der anderen Vlans verboten, danach werden alle anderen IP und TCP Pakete erlaubt. Dies wird für IPv4 und IPv6 gleich gemacht, als erstes wird eine ACL pro Vlan erstellt, danach wird diese ACL dem Vlan-Interface zugewiesen.

Serverservices:

DHCP:

DNS:

Glossar:

LACP: Link Aggreagtion Protocol von der IEEE (funkt)

PagP: Port Aggregation Protocol von Cisco (funktioniert nur auf Cisco Geräten)

lacp funktioniert auf gestackten switches, PAgP funktioniert nicht auf gestackten switches(gestackte switches müssen active sein, mit desirable funktionierts nicht)

auf port-channel no switchport kommando funktioniert nicht, es erscheint die Fehlermeldung not a convertible port

http://www.groupstudy.com/archives/cisco/200511/msg00242.html 13.11.2015 no switchport

falls nicht funktioniert vlan pro port-channel

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

umbedingt zuerst port-channel erstellen, bevor ein interface dem channel-port channel hinzugefügt worden ist. !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

NAT Tabelle:

172.176.242.17 VLan 10 Chur 10.1.10.0/24

172.176.242.18 VLan 20 Chur 10.1.20.0/24

172.176.242.19 VLan 30 Chur 10.1.30.0/24

172.176.242.20 VLan 99 Chur 10.1.99.0/24

172.176.242.21 VLan 10 Buchs 10.2.10.0/24

172.176.242.22 VLan 20 Buchs 10.2.20.0/24

172.176.242.23 VLan 30 Buchs 10.2.30.0/24

172.176.242.24 VLan 99 Buchs 10.2.99.0/24

172.176.242.25 VLan 10 St.Gallen 10.3.10.0/24

172.176.242.26 VLan 20 St.Gallen 10.3.20.0/24

172.176.242.27 VLan 30 St.Gallen 10.3.30.0/24

172.176.242.28 VLan 99 St.Gallen 10.3.99.0/24

Beide Core Layer 3 Switches sind mit Gigabit Glasfaser verbunden

Distribution Layer 3 Switches sind gestackt

auf S1/2 & A1/2 nur management vlans mit ip

auf D1/2 geswichte ports ohne ip, auf switch selbst alle vlans mit ip (wegen stack wahrscheinlich nur 1IP pro vlan)

13.11.2015

lacp funktioniert auf gestackten switches, PAgP funktioniert nicht auf gestackten switches(gestackte switches müssen active sein, mit desirable funktionierts nicht)

auf port-channel no switchport kommando funktioniert nicht, es erscheint die Fehlermeldung not a convertible port

http://www.groupstudy.com/archives/cisco/200511/msg00242.html 13.11.2015 no switchport

falls nicht funktioniert vlan pro port-channel

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

umbedingt zuerst port-channel erstellen, bevor ein interface dem channel-port channel hinzugefügt worden ist. !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

20.11.2015

Port Channels auf allen Switches und Router konfigurieren

Vlan auf Switches erstellen

Management Ip-Adresse erstellt

Passwörter ganz am schluss setzten, da sonst nur im weg.

Glasfaserkabel zwischen C1 und C2 verbunden, haben mit Auge geschaut welches Kabel geleuchtet hat, dann gekreuzt

eingesetzt.

04.12.2016

ip routing auf c1 aktivieren, auf c2 nicht mehr nötig gewesen.

Abgabetermin am 11.Januar 2016 per E-Mail an Beat Bigger

Template musste gewechselt werden um IPv6 zu aktivieren

interface vlan 10

ip address 10.1.10.1 255.255.255.0

interface vlan 20

ip address 10.1.20.1 255.255.255.0

interface vlan 30

ip address 10.1.30.1 255.255.255.0

interface vlan 99

ip address 10.1.99.1 255.255.255.0

für redundante verbindung zum dhcp server auf r1 muss auf r1 ein loopback interface inklusive ip adresse angelegt werden.

Auf D kann dann die Loopbackadresse als DHCP helper address angegeben werden, diese ist dann auch immer verfügbar

10.12.2015

Die gestackten Switches waren falsch angenommen, D1 ist 2/ und D2 ist 1/ . Deshalb hat OSPF auf diese Interfaces nicht funktioniert. umkonfigurieren

18.12.2015:

Native Vlan mismatch auf A2 auf physischen Ports mussten die nativ vlans noch angepasst werden.

sobald die ports g0/1 und g0/2 die nativ vlan eingegeben wurden gingen die ports up,

Nat konfigurieren. nat ip adresse muss doppelt eingegeben werden. acl für nat muss umkonfiguriert werden.

----d---

ipv6 access-list c10

deny ip 2001:620:3101:1020/64 2001:620:3101:1010/64

deny ip 2001:620:3101:1030/64 2001:620:3101:1010/64

deny ip 2001:620:3101:2020/64 2001:620:3101:1010/64

deny ip 2001:620:3101:2030/64 2001:620:3101:1010/64

deny ip 2001:620:3101:3020/64 2001:620:3101:1010/64

deny ip 2001:620:3101:3030/64 2001:620:3101:1010/64

permit ip any any

permit tcp any any

exit

interface vlan 10

ipv6 traffic-filter c10 in

end

ipv6 access-list c20

deny ip 2001:620:3101:1010/64 2001:620:3101:1020/64

deny ip 2001:620:3101:1030/64 2001:620:3101:1020/64

deny ip 2001:620:3101:2010/64 2001:620:3101:1020/64

deny ip 2001:620:3101:2030/64 2001:620:3101:1020/64

deny ip 2001:620:3101:3010/64 2001:620:3101:1020/64

deny ip 2001:620:3101:3030/64 2001:620:3101:1020/64

permit ip any any

permit tcp any any

exit

interface vlan 20

ipv6 traffic-filter c20 in

end

ipv6 access-list c30

deny ip 2001:620:3101:1010/64 2001:620:3101:1030/64

deny ip 2001:620:3101:1020/64 2001:620:3101:1030/64

deny ip 2001:620:3101:2010/64 2001:620:3101:1030/64

deny ip 2001:620:3101:2020/64 2001:620:3101:1030/64

deny ip 2001:620:3101:3010/64 2001:620:3101:1030/64

deny ip 2001:620:3101:3020/64 2001:620:3101:1030/64

permit ip any any

permit tcp any any

exit

interface vlan 30

ipv6 traffic-filter c30 in

end

-----r2-----

ipv6 access-list b10

deny ip 2001:620:3101:1020/64 2001:620:3101:2010/64

deny ip 2001:620:3101:1030/64 2001:620:3101:2010/64

deny ip 2001:620:3101:2020/64 2001:620:3101:2010/64

deny ip 2001:620:3101:2030/64 2001:620:3101:2010/64

deny ip 2001:620:3101:3020/64 2001:620:3101:2010/64

deny ip 2001:620:3101:3030/64 2001:620:3101:2010/64

permit ip any any

permit tcp any any

exit

interface g0/0.10

ipv6 traffic-filter b10 in

end

ipv6 access-list b20

deny ip 2001:620:3101:1010/64 2001:620:3101:2020/64

deny ip 2001:620:3101:1030/64 2001:620:3101:2020/64

deny ip 2001:620:3101:2010/64 2001:620:3101:2020/64

deny ip 2001:620:3101:2030/64 2001:620:3101:2020/64

deny ip 2001:620:3101:3010/64 2001:620:3101:2020/64

deny ip 2001:620:3101:3030/64 2001:620:3101:2020/64

permit ip any any

permit tcp any any

exit

interface g0/0.20

ipv6 traffic-filter b20 in

end

ipv6 access-list b30

deny ip 2001:620:3101:1010/64 2001:620:3101:2030/64

deny ip 2001:620:3101:1020/64 2001:620:3101:2030/64

deny ip 2001:620:3101:2010/64 2001:620:3101:2030/64

deny ip 2001:620:3101:2020/64 2001:620:3101:2030/64

deny ip 2001:620:3101:3010/64 2001:620:3101:2030/64

deny ip 2001:620:3101:3020/64 2001:620:3101:2030/64

permit ip any any

permit tcp any any

exit

interface g0/0.30

ipv6 traffic-filter b30 in

end

-----r3-----

ipv6 access-list s103

deny ip 2001:620:3101:1020/64 2001:620:3101:3010/64

deny ip 2001:620:3101:1030/64 2001:620:3101:3010/64

deny ip 2001:620:3101:2020/64 2001:620:3101:3010/64

deny ip 2001:620:3101:2030/64 2001:620:3101:3010/64

deny ip 2001:620:3101:3020/64 2001:620:3101:3010/64

deny ip 2001:620:3101:3030/64 2001:620:3101:3010/64

permit ip any any

permit tcp any any

exit

interface interface g0/0.10

ipv6 traffic-filter s10 in

end

ipv6 access-list s20

deny ip 2001:620:3101:1010/64 2001:620:3101:3020/64

deny ip 2001:620:3101:1030/64 2001:620:3101:3020/64

deny ip 2001:620:3101:2010/64 2001:620:3101:3020/64

deny ip 2001:620:3101:2030/64 2001:620:3101:3020/64

deny ip 2001:620:3101:3010/64 2001:620:3101:3020/64

deny ip 2001:620:3101:3030/64 2001:620:3101:3020/64

permit ip any any

permit tcp any any

exit

interface g0/0.20

ipv6 traffic-filter s20 in

end

ipv6 access-list s30

deny ip 2001:620:3101:1010/64 2001:620:3101:3030/64

deny ip 2001:620:3101:1020/64 2001:620:3101:3030/64

deny ip 2001:620:3101:2010/64 2001:620:3101:3030/64

deny ip 2001:620:3101:2020/64 2001:620:3101:3030/64

deny ip 2001:620:3101:3010/64 2001:620:3101:3030/64

deny ip 2001:620:3101:3020/64 2001:620:3101:3030/64

permit ip any any

permit tcp any any

exit

interface g0/0.30

ipv6 traffic-filter s30 in

end