



As Built

Eletros - Rede do novo predio da Eletros

ELETROS

Routing, Switching e Wireless

09/08/2023 | Document Version 0.01

Tiago Silva (Americas)

011 3878 6500 | 011989105220

tiago.silva (americas)@global.ntt

NTT contact details

We welcome any enquiries regarding this document, its content, structure, or scope. Please contact:

Tiago Silva (Americas) - Engineering Network, Mobile Phone: 011989105220

NTT Limited

Av Doutor Chucris Zaidan, nº 1.240

11º andar, conjunto 1103

V. Sao Francisco

São Paulo / SP

CEP: 04711-130

☎ 011 3878 6500

☎ 011 3878 6501

✉ [tiago.silva \(americas\)@global.ntt](mailto:tiago.silva (americas)@global.ntt)

Please quote reference in any correspondence or order.

Confidentiality

This document contains confidential and proprietary information of NTT Limited ('NTT'). ELETROS ('ELETROS') may not disclose the confidential information contained herein to any third party without the written consent of NTT, save that ELETROS may disclose the contents of this document to those of its agents, principals, representatives, consultants or employees who need to know its contents for the purpose of ELETROS's evaluation of the document. ELETROS agrees to inform such persons of the confidential nature of this document and to obtain their agreement to preserve its confidentiality to the same extent as ELETROS. As a condition of receiving this document, ELETROS agrees to treat the confidential information contained herein with at least the same level of care as it takes with respect to its own confidential information, but in no event with less than reasonable care. This confidentiality statement shall be binding on the parties for a period of five (5) years from the issue date stated on the front cover unless superseded by confidentiality provisions detailed in a subsequent agreement.

Terms and conditions

This document is valid until 17/08/2023 and, in the absence of any other written agreement between the parties, NTT and ELETROS acknowledge and agree is subject to NTT's standard terms and conditions which are available on request. NTT reserves the right to vary the terms of this document in response to changes to the specifications or information made available by ELETROS. Submission of this document by NTT in no way conveys any right, title, interest, or license in any intellectual property rights (including but not limited to patents, copyrights, trade secrets or trademarks) contained herein. All rights are reserved.

NTT does not assume liability for any errors or omissions in the content of this document or any referenced or associated third party document, including, but not limited to, typographical errors, inaccuracies, or out-dated information. This document and all information within it are provided on an 'as is' basis without any warranties of any kind, express or implied. Any communication required or permitted in terms of this document shall be valid and effective only if submitted in writing.

All contracts with NTT will be governed by Brazilian Law and be subject to the exclusive jurisdiction of the Brazilian courts.



Table of Contents

1	Objetivo	5
1.1.	Hardware.....	6
1.2.	Switch Catalyst C9500-16X.....	6
2	Visão Geral das Tecnologias	9
2.1.	LAN / Switching	9
2.2.	RPVST+ - Rapid per vlan Spanning-tree.....	9
2.3.	Camada de Core	10
2.4.	Camada de Acesso	11
2.5.	Stackwise Virtual	11
2.6.	Stack Wise	13
2.7.	Rapid Per Vlan Spanning-tree Plus (PVTP+)	14
2.8.	Trunk e Port-Channels – Camada de Acesso	14
3	Parte Física	16
3.1.	Switches	16
3.2.	DE/PARA de Conexões	17
3.3.	Parte Lógica.....	21
3.4.	Informações Adicionais	24
4	Detail Design Acceptance Sheet.....	28

List of Figures

Figure 1 - C9500-16X	6
Figure 2 - Switch Catalyst C9200L-48P	7
Figure 3 - Stack Wise Switches 9200	14
Figure 4 – Dispositivos rede Local	16
Figure 5 - Topologia Física.....	20
Figure 6 - Topologia Lógica.....	21

List of Tables

Table 1 - Características Técnicas Switch C9500-16X.....	6
Table 3 - ELE-28-RT-01	17
Table 4 - ELE-28-RT-02	17

Table 5 - ELE-28-SW-EDGE-01	18
Table 6 - ELE-28-SW-CORE-01	19
Table 7 - Vlans Switch Core	22
Table 8 - Links WAN	23
Table 9 - Password	24
Table 10 - NTP.....	24
Table 11 - DNS	24
Table 12 - Domain.....	24
Table 13 – SNMP	24

1 Objetivo

O Objetivo deste documento é descrever a Arquitetura que será implantada no novo Predio do cliente ELETROS.

1.1. Hardware

1.2. Switch Catalyst C9500-16X

Os switches Cisco Catalyst 9500 fazem parte da nova geração de switches para camada de agregação e núcleo de nível corporativo, são equipamentos robustos, construídos com CPU em x86 de 4 núcleos, CPU de 2,4 Ghz, memória de 16 GB e armazenamento interno de 16 GB.

O switch Cisco Catalyst 9500 Séries é a primeira linha de switches Ethernet de 25, 40 e 100 Gigabit Ethernet da indústria, voltada para o campus corporativo. Para as velocidades de 1, 10 e 25 Gigabit Ethernet ele utiliza Small Form-Factor Pluggable Plus (SFP/SFP+/SFP28) e para 40 e 100 Gigabit Ethernet ele utiliza Quad Small Form-Factor Pluggable (QSFP+/QSFP28) e possui densidade de portas granulares para atender as diversas necessidades do campus.

Esses equipamentos suportam serviços avançados de roteamento e infra-estrutura, Cisco Software Defined Access (SDN) com a arquitetura de rede digital Cisco DNA e acesso definido por software SD Access que é uma arquitetura aberta e extensível orientada por software que acelera e simplifica as operações da rede empresarial.

Além disso, os equipamentos da família Catalyst 9500 possuem virtualização de sistemas de rede com a nova tecnologia Cisco Stackwise Virtual, muito utilizada e essencial para o núcleo do campus

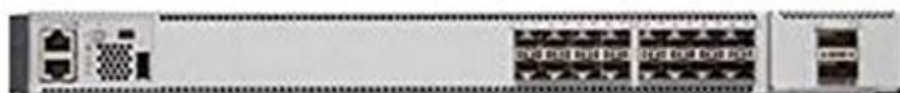


Figure 1 - C9500-16X

Características Técnicas - C9500-16X	
Temperatura ambiente para operação	0 até 40° C
Dimensões (Largura/Profundidade/Altura)	4.4 x 44.5 x 45.7 cm
Peso Chassi	Aproximadamente 9.96 kg
Fluxo de Ar (Air Flow)	Front to Back
Voltagem	90 até 264 VAC

Table 1 - Características Técnicas Switch C9500-16X

1.2.1 Switch Catalyst C9200L-48P

Os switches Cisco® Catalyst® 9200 Series estendem o poder da rede baseada em intenção e da inovação de hardware e software Catalyst 9000 para um conjunto mais amplo de implantações. Com sua linhagem familiar, os switches Catalyst 9200 Series oferecem simplicidade sem concessões - são seguros, sempre ativos e TI simplificada.

Como blocos de construção básicos para a arquitetura de rede digital da Cisco, os switches Catalyst 9200 Series ajudam os clientes a simplificar a complexidade, otimizar a TI e reduzir os custos operacionais, aproveitando a inteligência, automação e experiência humana que nenhum outro fornecedor pode oferecer, independentemente de onde você esteja. jornada de rede baseada.



Figure 2 - Switch Catalyst C9200L-48P

Características Técnicas C9200L-48P	
Temperatura ambiente para operação	0 até 45° C
Dimensões (Largura/Profundidade/Altura)	1.73 x 17.5 x 17.7
Peso Chassi	Aproximadamente 7.27 kg
Fluxo de Ar (Air Flow)	Front to Back
Voltagem	Até 220 VAC

Table 3 - Características Técnicas C9200L-48P

1.2.2 Firepower 2130

Cisco Firepower 2130/2140 Model



O Cisco Firepower 2100 Series é uma família de quatro plataformas de segurança focadas em ameaças que oferecem resiliência comercial e defesa superior contra ameaças.

Eles oferecem um desempenho sustentado excepcional quando as funções avançadas de ameaças estão ativadas. Essas plataformas incorporam exclusivamente uma arquitetura inovadora de CPU dual multicore que otimiza as funções de firewall, criptografia e inspeção de ameaças.

O intervalo de taxa de transferência do firewall da série aborda casos de uso desde a borda da Internet até o data center. Network Equipment Building Standards (NEBS) - a conformidade é suportada pela plataforma Cisco Firepower 2130. As plataformas da série 2100 executam o software Cisco Secure Firewall ASA ou Threat Defense (FMC). Eles podem ser implantados nos modos de firewall e IPS dedicado.

Características Técnicas C9200L-48P	
Temperatura ambiente para operação	0 até 45° C
Dimensões (Largura/Profundidade/Altura)	1.73 x 17.5 x 17.7
Peso Chassi	Aproximadamente 7.27 kg
Fluxo de Ar (Air Flow)	Front to Back
Voltagem	Até 220 VAC

2 Visão Geral das Tecnologias

2.1. LAN / Switching

Segmentação lógica de uma LAN, formando um domínio de broadcast, onde as comunicações entre equipamentos ocorrem como se estivessem conectados ao mesmo “cabo”, quando, de fato, eles podem estar em diferentes segmentos de LAN.

2.2. RPVST+ - Rapid per vlan Spanning-tree

Spanning-Tree Protocol (STP) é um protocolo que permite a criação de uma rede sem loop Layer 2 (L2) mesmo com caminhos redundantes. O padrão IEEE do STP é o 802.1d.

O protocolo Rapid Spanning-Tree é definido no padrão IEEE 802.1w, melhora o tempo de convergência do Spanning-Tree (802.1d), definindo regras para que os links alterem rapidamente ao estado de encaminhamento (forwarding), gerando mensagens BPDUs em vez de apenas retransmitir os BPDUs do Root, oferecendo uma significativa melhora no tempo de convergência da rede.

A Cisco implementa uma versão proprietária e modificada do protocolo, o RSTP, que é o Rapid-PVST (Rapid Per Vlan Spanning-tree), cujas diferenças são apresentadas abaixo:

- A Implementação IEEE envia BPDUs apenas na Vlan 1;
- A Implementação Cisco envia BPDUs em todas as Vlans (Per-Vlan).

Uma das principais melhorias efetuadas no protocolo reduziu o tempo de convergência em caso de falha para 3 Hellos BPDUs (por default 2 segundos cada Hello) ao invés de 10 Hellos BPDUs, como na versão anterior do protocolo.

O RSTP elege o Switch Root da mesma maneira que o 802.1d e o tempo de transição para o estado das portas foi reduzido com 3 operações básicas: Discarding, Learning e Forwarding.

A rápida transição para o forwarding é permitida sem a necessidade de esperar o tempo da configuração, baseando-se na classificação dos equipamentos conectados nas portas do Switch:

- Edge: porta conectada a computadores, telefones IP, impressoras etc;
- Point-to-Point: porta conectada em outro Switch;

Shared: Porta conectada a um Hub.

2.3. Camada de Core

A camada de Core será responsável por realizar o encaminhamento de tráfego de forma eficiente com o mínimo de latência. Essa camada é responsável por conectar todas as camadas de Agregação e seus respectivos Acessos do ambiente.

Essa camada será atendida por equipamentos Cisco Catalyst C9500-16X-E e será implementado a funcionalidade de Multi-Chassis Ethernet (MEC), denominado Stackwise Virtual. A conectividade da camada de Core com as camadas de agregação será em modo L2 (switchport) com configuração de Trunk no Port-Channel de interconexão de camadas e todas as interfaces vlan (SVI) serão configuradas nessa camada.

Para prover roteamento entre a camada de Core e as redes externas via estrutura de WAN e também comunicação com redes atrás de Firewalls, será utilizado roteamento estático, adicionando rotas para os devidos prefixos e redes já conhecidas, e também rota Default para redes externas não conhecidas, as demais camadas da rede utilizam o roteamento do Core para comunicação externa/interna.

2.3.1 Camada de Core Colapsado

Um Core é chamado de colapsado quando as funções de distribuição e núcleo são realizadas na mesma camada, mesclando ambas as camadas em uma só. Essa camada será responsável pela interconexão com todos os switches de acesso da rede, e com isso, a camada de Colapsed Core será o ponto de roteamento da rede e nela serão configuradas todas as interfaces vlan (SVI) pertencentes a rede.

O principal objetivo da arquitetura de Colapsed Core é reduzir custos, complexidade e manter toda a eficiência da rede.

Para a Eletros, essa arquitetura de Core Colapsado foi adotado, ele exerce a função de L2 e L3 de todas as vlans serão roteadas no ambiente.

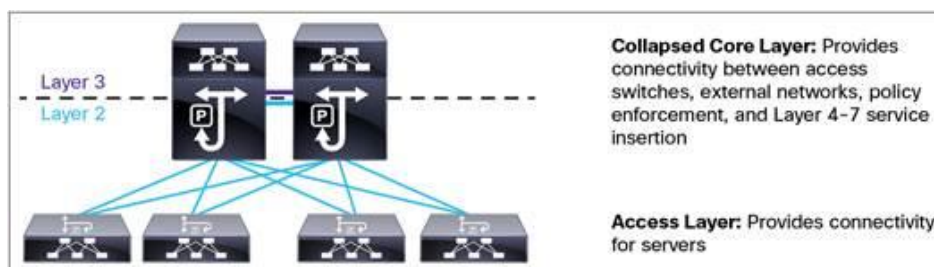


Figure 1 – Exemplo de Core Colapsado

2.4. Camada de Acesso

A camada de Acesso será responsável por conectar dispositivos finais da rede como desktops, telefones, cameras, catracas e etc. Essa camada será atendida por equipamentos Cisco Catalyst 2960-X Séries, que podem ter interfaces até 1 Gbps para conectar dispositivos finais e até 10 Gbps para Uplinks.

Nesta camada teremos a maior densidade de portas ativas.

A camada de Acesso terá conectividade com a camada de Core Colapsado apenas em L2 (switchport), por meio de Trunk e Port-Channels fazendo tag das vlans necessárias.

2.5. Stackwise Virtual

O Cisco Stackwise Virtual é uma tecnologia que combina dois switches em um único switch lógico com maior número de portas, oferecendo assim um único ponto de gerenciamento. Com o Stackwise Virtual em funcionamento, um dos switches é eleito como Active e assume as funções de Control Plane e gerenciamento, enquanto o outro switch é eleito como Standby, porém a grande vantagem dessa tecnologia é que o switch secundário consegue encaminhar tráfego em Data Plane, ou seja, para throughput de dados os dois switches funcionam em conjunto, e apenas as funções de Control Plane são mantidas em funcionamento apenas no switch Active. Um dos benefícios do Stackwise Virtual é simplificar a topologia de rede de camada 3, reduzindo o número de pares de roteamento na rede e se mostrando como um único switch lógico, tendo menor complexidade.

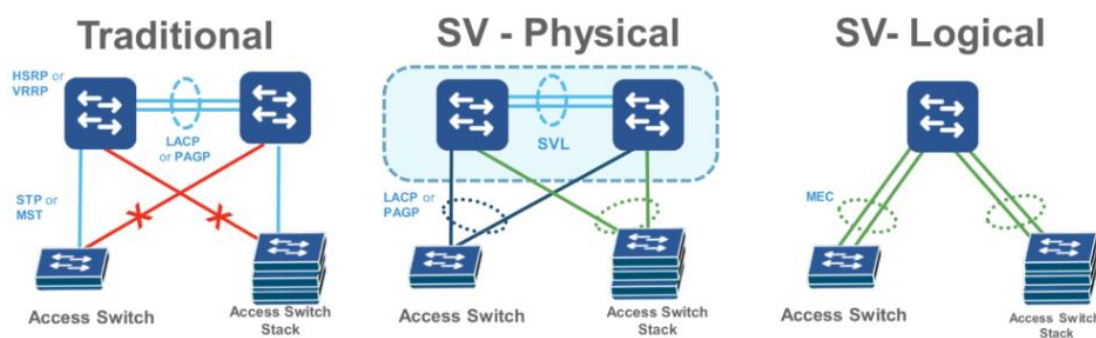


Figure 2 – Rede Tradicional x Stackwise Virtual

2.5.1 Nomenclaturas Stackwise Virtual

- **Stackwise Domain:** É composto por um par de switches Catalyst 9500 se comportando como um equipamento lógico e único;
- **Stackwise Virtual Link:** É composto por até 8 interfaces que tem a função de sincronia de configurações entre o par de equipamentos empilhados;
- **Dual Active Detection:** É composto por interface de 1G, e tem a função de trocar Heartbeat, caso haja queda das interfaces SVL, os equipamentos sabem se o outro lado está realmente Down e se devem entrar em modo Active no Domain;

2.5.2 Arquitetura Stackwise Virtual

O Cisco Stackwise Virtual consegue combinar dois switches em uma única entidade de rede lógica para a perspectiva de gestão. Ele utiliza a tecnologia do sistema Cisco IOS, chamada de Stateful Switchover (SSO), bem como o Non-Stop Forwarding (NSF) para protocolos de roteamento e fornece failover de tráfego contínuo quando um dos dispositivos falha. Para dispositivos vizinhos, um domínio virtual do StackWise aparece como um único switch lógico.

Dentro de um domínio StackWise Virtual um dispositivo é designado como switch Ativo e o outro é designado como switch Standby, entretanto todas as funções de Control Plane são gerenciadas pelo switch Ativo, incluindo:

- Protocolos de Gerenciamento (SSH, TELNET, SNMP);
- Protocolos de camada 2 (BPDU's e protocolos de Link Agregação);
- Protocolos de camada 3 (Roteamento IGP, EGP);
- Caminho de dados;

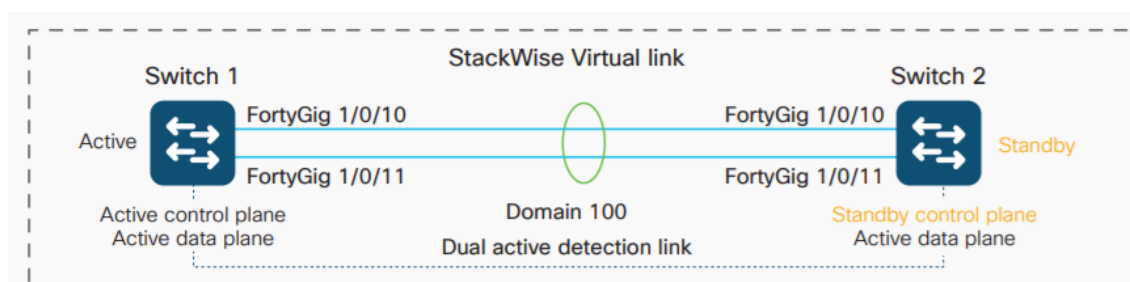


Figure 3 – Stackwise Virtual Detalhado

Como um domínio StackWise Virtual consiste em dois switches mesclados em uma única entidade, é possível designer manualmente o papel de Active ao switch que necessita, por padrão essa designação é determinada de forma automática pelos equipamentos conforme os critérios abaixo:

- Se os equipamentos forem iniciados em momentos diferentes, o switch que é iniciado primeiro se tornará o Active.
- Se os equipamentos forem iniciados simultaneamente, o switch com o endereço MAC mais baixo torna-se o Active.

No Stackwise Virtual, para forçar um switch a se tornar Active naquele domínio basta forçar as prioridades manualmente e com isso o switch com prioridade mais alta, se tornará o Active do domínio.

Para evitar comutação de Active/Standby desnecessárias e não haver interrupções de tráfego desnecessárias, o Stackwise Virtual não oferece função de Preemt, caso seja preciso fazer Switchover da Caixa Active para Standby, é necessário executar manualmente via comando na cli do equipamento.

Caso haja queda de todas as interfaces de SVL do Stackwise Virtual, para que as duas caixas não se tornem ativas na rede e causem problemas de encaminhamento de tráfego, é recomendado a configuração de uma conexão entre os equipamentos denominada Fast Hello, essa conexão fará com que os switches troquem pacotes de Heartbeat que contém o estado do switch, com isso quando o domínio Stackwise Virtual perder todos os SVL, os equipamentos conseguem saber se o outro lado está Up ou Down e para que ambos os switches não virem ativos na rede, um deles é colocado em Recovery Mode e todas suas interfaces são desativadas.

Abaixo temos um exemplo desse cenário:

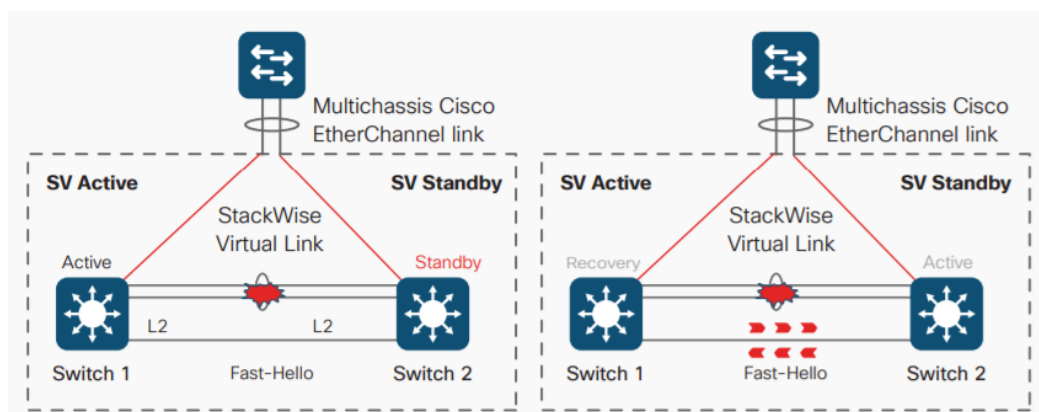


Figure 4 – Stackwise Dual Active

2.6. Stack Wise

Tecnologia StackWise permitindo que vários switches sejam “empilhados” e atuem como um só dispositivo, na prática, os switches empilháveis possuem entradas especiais para conexão dos cabos de empilhamento (stacking cables Cisco), os quais são conectados formando um loop (daisy-chain) e criam um unico switch Virtual.

Principais vantagens do StackWise:

- Possibilidade de empilhar até 8 switches em um mesmo stack, por exemplo, formando uma só pilha lógica de switches.
- Não é preciso fazer nenhuma configuração para inserção de um novo switch na pilha.
- A pilha vai funcionar como um único dispositivo, tendo apenas um IP de gerenciamento único para todos os switches da pilha e sendo configurada a partir do switch definido como “mestre”.



Figure 3 - Stack Wise Switches 9200

2.7. Rapid Per Vlan Spanning-tree Plus (PVTP+)

O Rapid Per Vlan Spanning-Tree Plus se baseia na utilização de uma instância Spanning-Tree por Vlan, porém o domínio criado pelo PVTP+ não será utilizado para bloquear interfaces em situação de rede estável onde o Stackwise Virtual está em perfeito funcionamento pois temos uma topologia lógica de rede livre de loop (loop free), somente em caso de falha do sistema Stackwise Virtual que o Spanning-Tree entrará em ação e bloqueará uma das interfaces do Port-Channel entre a camada de acesso e distribuição.

De acordo com as melhores práticas em implementações de Spanning-Tree e tecnologias Multi-Chassis Ethernet (Stackwise Virtual), o root do domínio STP deve estar localizado na camada de distribuição ou Core (para casos de Core Colapsado ou camada de distribuição em L2), ou seja, é recomendado que a prioridade setada

2.8. Trunk e Port-Channels – Camada de Acesso

Para prover conectividade da camada de acesso para a camada de distribuição com suporte a múltiplas Vlans será utilizado interfaces em modo trunk onde o tráfego ethernet é enviado utilizando tag definidos no documento IEEE 802.1Q. Para suportar contingência de interfaces físicas entre a camada de acesso e a camada de distribuição será utilizada a funcionalidade de Port-Channel, onde temos duas interfaces físicas com velocidade de 1 Gbps ou 10Gbps agregadas e formando um link de 2 Gbps ou 20 Gbps de banda usando mode ON nas portas agregadas.

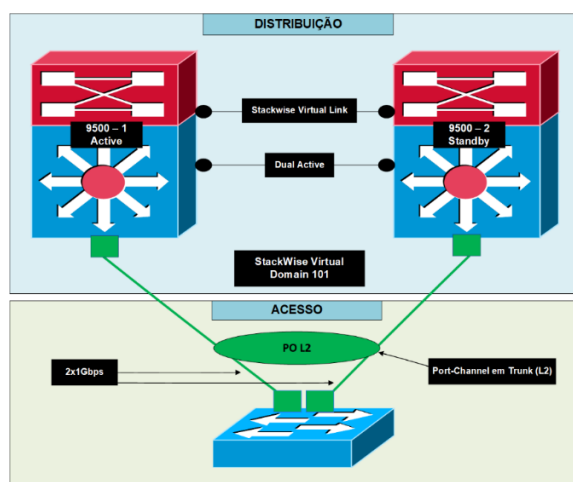


Figure 5 – Exemplo de conexão – Camada de Acesso

3 Parte Física

3.1. Switches

Equipamentos	Hostname	Serial Number	IP Gerência	Descrição
C9500-16X C9500-16X	ELE-28-SW-CORE-01	FJC270523PE FJC27052PZ0	10.226.6.254	Switch Core 28 andar
C9200L-48P-4G C9200L-48P-4G	ELE-28-SW-ACCESS-01	TSP27170024 TSP27170083	10.226.6.4	Switch Borda 27 Andar (distribuição Pontos de Rede)
C9200L-48P-4G C9200L-48P-4G	ELE-28-SW-ACCESS-02	TSP27170262 TSP27170261	10.226.6.3	Switch Borda 28 Andar (distribuição Pontos de Rede)
C9200L-24P-4G-E C9200L-24P-4G	ELE-28-SW-EDGE-01	TSP27022164 TSP27022087	10.226.6.7	Switch Edge 28 Andar
ASR1001-X	ELE-28-RT -01	FXS2114Q0L6	10.226.6.11	Roteador 28 Andar
ASR1001-X	ELE-28-RT -02	FXS2223Q0TE	10.226.6.12	Roteador 28 Andar

Figure 4 – Dispositivos rede Local

3.2. DE/PARA de Conexões

3.2.1 ELE-28-RT-01

	EQ ORIGEM	PORTA ORIGEM	SFP	EQ DESTINO	PORTA DESTINO	SFP
13	ELE-28-RT-01	G0/0/0	GLC-TE	Internet_circuito1	G0/0/0	Interface switch
14	ELE-28-RT-01	G0/0/1	GLC-TE	ELE-28-SW-EDGE-01	G1/0/1	Interface switch
15	ELE-28-RT-01	G0/0/2	GLC-TE	ELE-28-SW-EDGE-01	G2/0/2	Interface switch
15	ELE-28-RT-01	G0/0/3	GLC-TE	ELE-28-RT-02	G0/0/3	Interface switch

Table 2 - ELE-28-RT-01

3.2.2 ELE-28-RT-02

	EQ ORIGEM	PORTA ORIGEM	SFP	EQ DESTINO	PORTA DESTINO	SFP
13	ELE-28-RT-02	G0/0/0	GLC-TE	Internet_circuito2	G0/0/0	Interface switch
14	ELE-28-RT-02	G0/0/1	GLC-TE	ELE-28-SW-EDGE-01	G2/0/1	Interface switch
15	ELE-28-RT-02	G0/0/2	GLC-TE	ELE-28-SW-EDGE-01	G1/0/2	Interface switch
15	ELE-28-RT-02	G0/0/3	GLC-TE	ELE-28-RT-02	G0/0/3	Interface switch

Table 3 - ELE-28-RT-02

3.2.3 ELE-28-SW-EDGE-01

	EQ ORIGEM	PORTA ORIGEM	SFP	EQ DESTINO	PORTA DESTINO	SFP
1	ELE-28-SW-EDGE-01	G1/0/1		ELE-28-RT-01	G0/0/1	
2	ELE-28-SW-EDGE-01	G2/0/2		ELE-28-RT-01	G0/0/2	
3	ELE-28-SW-EDGE-01	G2/0/1		ELE-28-RT-02	G0/0/1	
4	ELE-28-SW-EDGE-01	G1/0/2		ELE-28-RT-02	G0/0/2	
5	ELE-28-SW-EDGE-01	G1/1/1	GLC-LH-SMD - FIBRA	ELE-28-SW-CORE-01	T1/0/5	GLC-LH-SMD - FIBRA
6	ELE-28-SW-EDGE-01	G2/1/1	GLC-LH-SMD - FIBRA	ELE-28-SW-CORE-01	T2/0/5	GLC-LH-SMD – FIBRA
7	ELE-28-SW-EDGE-01	G1/0/7		FW-ELETROS-01	G0/0/0	
8	ELE-28-SW-EDGE-01	G2/0/7		FW-ELETROS-01	G0/0/1	
9	ELE-28-SW-EDGE-01	G1/0/3		FW-ELETROS-01	mgmt	
10	ELE-28-SW-EDGE-01	G1/0/8		FW-ELETROS-02	G0/0/0	
11	ELE-28-SW-EDGE-01	G2/0/8		FW-ELETROS-02	G0/0/1	
12	ELE-28-SW-EDGE-01	G2/0/3		FW-ELETROS-02	mgmt	
13	ELE-28-SW-EDGE-01	G1/0/9		ELE-28-WLC-01-01	G1	
14	ELE-28-SW-EDGE-01	G2/0/9		ELE-28-WLC-01-01	G2	
15	ELE-28-SW-EDGE-01	G1/0/10		ELE-28-WLC-01-02	G1	
16	ELE-28-SW-EDGE-01	G2/0/10		ELE-28-WLC-01-02	G2	

Table 4 - ELE-28-SW-EDGE-01

3.2.4 ELE-28-SW-CORE-01

	EQ ORIGEM	PORTA ORIGEM	SFP	EQ DESTINO	PORTA DESTINO	SFP
1	ELE-28-SW-CORE-01	T1/0/1	GLC-LH-SMD - FIBRA	ELE-28-SW-ACCESS-01	G1/1/1	GLC-LH-SMD - FIBRA
2	ELE-28-SW-CORE-01	T2/0/1	GLC-LH-SMD - FIBRA	ELE-28-SW-ACCESS-01	G2/1/1	GLC-LH-SMD - FIBRA
3	ELE-28-SW-CORE-01	T1/0/3	GLC-LH-SMD - FIBRA	ELE-28-SW-ACCESS-02	G1/1/1	GLC-LH-SMD - FIBRA
4	ELE-28-SW-CORE-01	T2/0/3	GLC-LH-SMD - FIBRA	ELE-28-SW-ACCESS-02	G2/1/1	GLC-LH-SMD - FIBRA
5	ELE-28-SW-CORE-01	T1/0/5	GLC-LH-SMD - FIBRA	ELE-28-SW-EDGE-01	G1/1/1	GLC-LH-SMD - FIBRA
6	ELE-28-SW-CORE-01	T2/0/5	GLC-LH-SMD - FIBRA	ELE-28-SW-EDGE-01	G2/1/1	GLC-LH-SMD - FIBRA

Table 5 - ELE-28-SW-CORE-01

Eletrabras - Rede do novo predio da Eletros
Routing and Switching

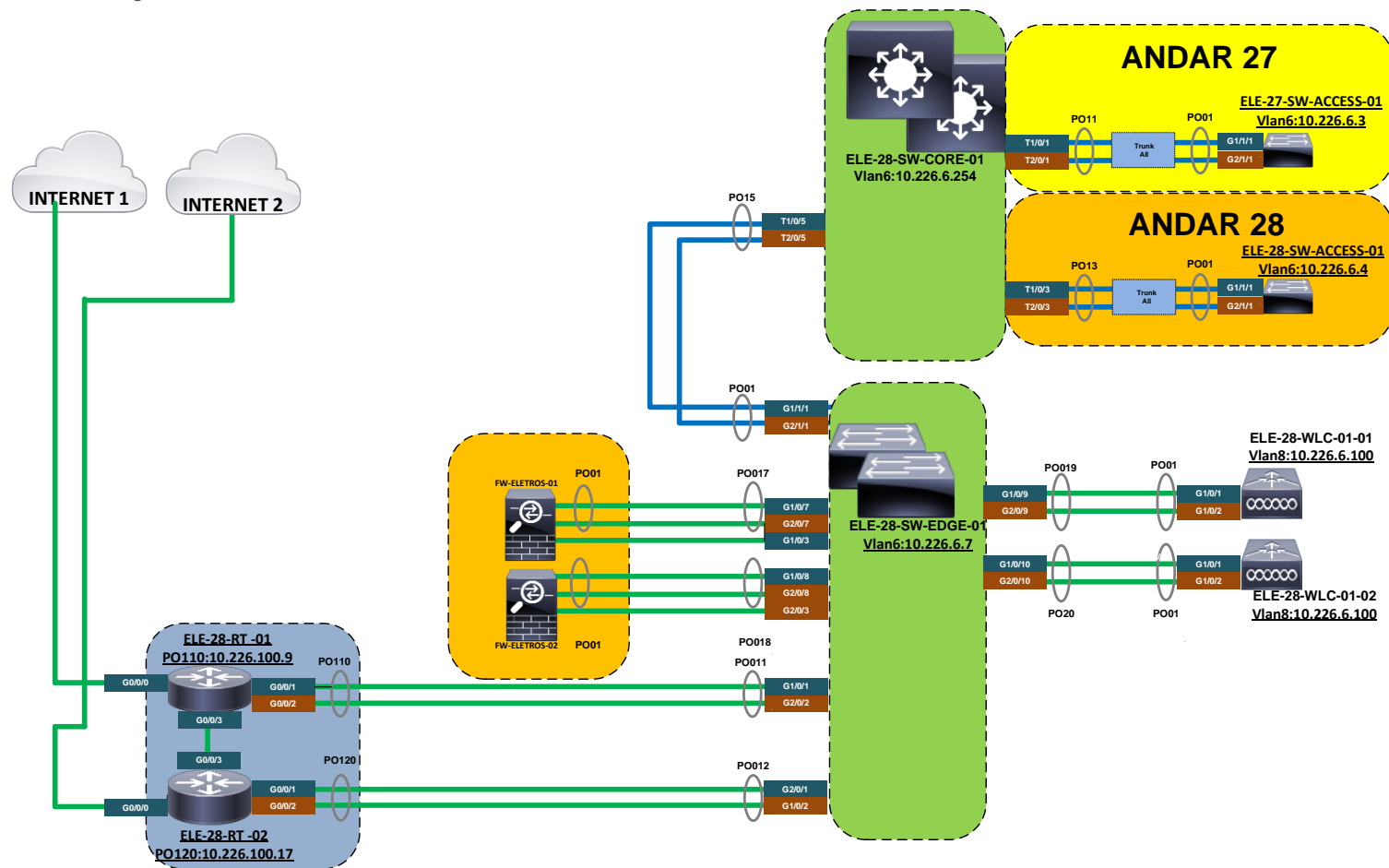


Figure 5 - Topologia Física

3.3. Parte Lógica

3.3.1 Topologia Lógica

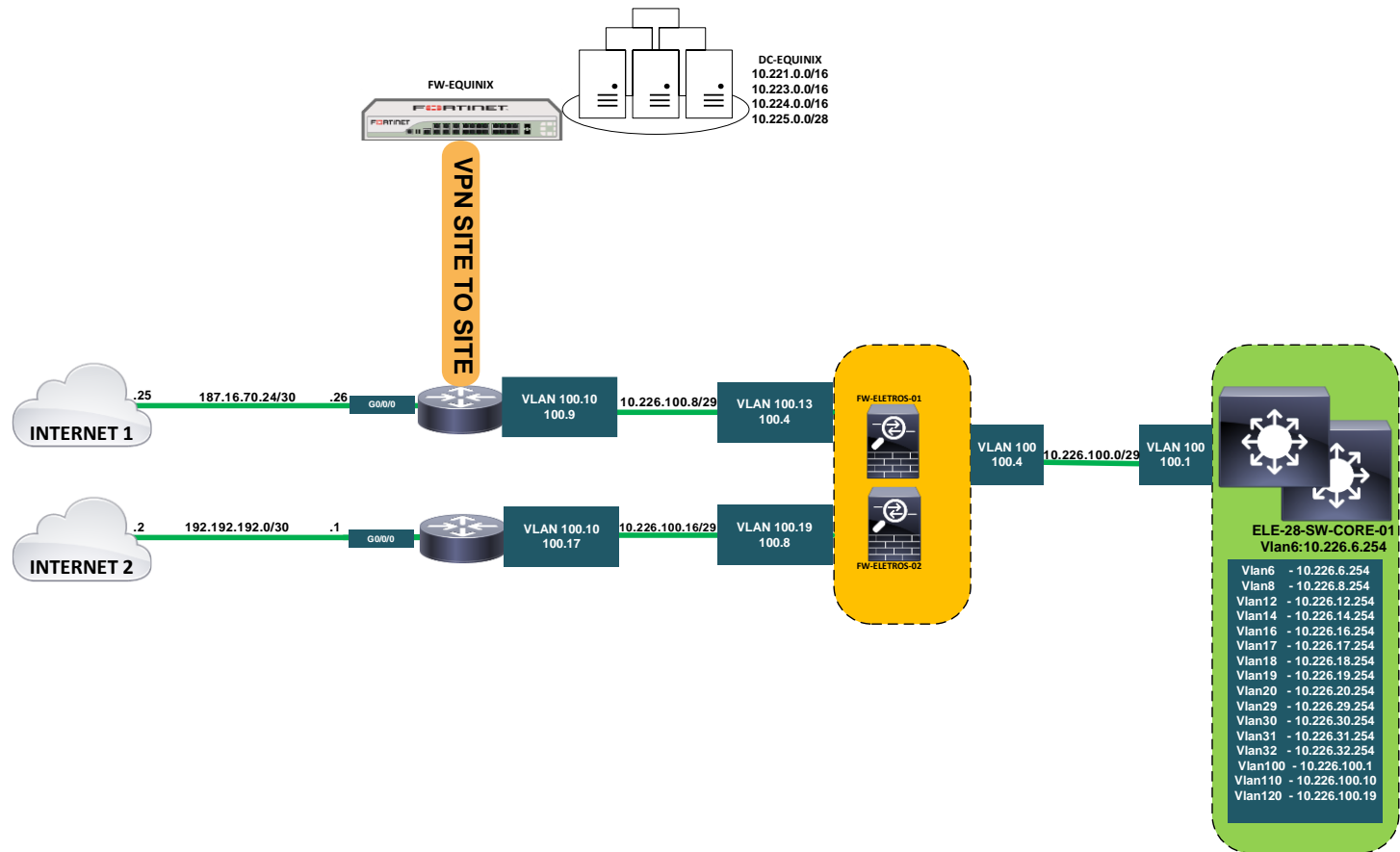


Figure 6 - Topologia Lógica

3.3.2 Vlans rede Interna

O switch Core é o Gateway das Vlans da rede local, segue abaixo tabela com todas as SVIs da rede.

Subredes	VLAN ID	Nome da Vlan	Gateway IP	Descrição
10.226.6.0/24	6	vlan6_ger_switches	10.226.6.254	Rede de Gerência - Switches - Switches e Routers
10.226.8.0/24	8	vlan8_ger_ap	10.226.8.254	Rede Gerência - Aps
10.226.12.0/23	12	vlan12_user_corp_27andar	10.226.12.254	Rede Usuários Corporativa ELETROS (Cabo e Wifi)
10.226.14.0/23	14	vlan14_user_corp_28andar	10.226.14.254	Rede Usuários Corporativa ELETROS (Cabo e Wifi)
10.226.16.0/24	16	vlan16_user_diretoria	10.226.16.254	Rede Usuários Diretoria (Cabo e Wifi)
10.226.17.0/24	17	vlan17_user_convidados	10.226.17.254	Rede Usuários convidados (Cabo e Wifi)
10.226.18.0/24	18	vlan18_Atendimento	10.226.18.254	vlan18_Atendimento (Cabo e Wifi)
10.226.18.0/24	19	vlan19_investimentos	10.226.19.254	vlan19_investimentos (Cabo e Wifi)
10.226.19.0/24	20	vlan20_Diretoria_Beneficio	10.226.20.254	vlan20_Diretoria_Beneficio (Cabo e Wifi)
10.226.29.0/24	29	vlan29_cftv	10.226.29.254	Rede CFTV
10.226.30.0/24	30	vlan30_controle_acesso	10.226.30.254	Rede Controle de Acesso
10.226.31.0/24	31	vlan31_impressoras	10.226.31.254	Rede Impressora
10.226.32.0/24	32	vlan32_videoconf	10.226.32.254	Rede Vídeo Conferência
10.226.100.0/29	100	vlan255_transito_fw	10.226.255.1	Rede de transito para o firewall
10.226.100.8/29	110	vlan110_transito_rt-01_fw	10.226.100.10	Rede de transito com o roteador 01
10.226.100.16/29	120	vlan120_transito_rt-02_fw	10.226.100.19	Rede de transito com o roteador 02

Table 6 - Vlans Switch Core

3.3.3 Links WAN

Os links Wan estão conectados nos roteadores WAN, segue abaixo links WAN do ambiente.

Subredes	Nome da Vlan	Gateway	Descrição
187.16.70.24/29	vlan_internet_circuito1	187.16.70.25/29	Link Internet Primário
N/A	vlan_internet_circuito2		

Table 7 - Links WAN

3.3.4 Roteamento Core x Firewall

Todo tráfego proveniente da rede local passará pelo Firewall, foi criada a VLAN 100 Core e o Firewall, no switch Core foi criado uma rota default que direciona todo tráfego para o Firewall.

3.3.5 DHCP

O switch Core é o servidor DHCP de toda a rede local, o switch é responsável por distribuir os ips para os usuários e demais dispositivos na rede local.

3.3.6 Roteamento Firewall x Roteadores

Todo tráfego que passa pelo Firewall proveniente da rede local passará pelo Firewall, após a inspeção dos pacotes o tráfego será direcionado para os roteadores.

3.3.7 Links de Internet

Os links de Internet estão conectados nos roteadores WAN do site, até o momento somente um link contratado está operando.

3.3.8 Nat usuários

Os roteadores realizam o NAT para que os usuário acessem a Internet, todos os ips internetos são traduzidos pelo 187.16.70.26.

3.3.9 VPN site to SITE

Para comunicação do escritório da Eletros com os servidores que estão alocados na Equinix foi configurado uma VPN site to site no roteador ELE-28-RT-01 com o Firewall Fortinet alocado na Equinix, com essa configuração é possível que os usuários acessem os recursos do Data Center.

3.4. Informações Adicionais

3.4.1 Hardening

3.4.1.1 Password

Device	Role	User	Password
Todos	Privilegio 15	ad	@Eletr05#!

Table 8 - Password

3.4.1.2 NTP

ID	NTP Server	Port
	10.226.100.9	

Table 9 - NTP

3.4.1.3 DNS

ID	DNS Server	DNS Suffix
1	10.223.0.111	intranet.eletros.com.br
2	10.223.0.2	intranet.eletros.com.br
3	10.223.0.102	intranet.eletros.com.br

Table 10 - DNS

3.4.1.4 Domain

ID	Domain Name Port
	intranet.eletros.com.br

Table 11 - Domain

3.4.1.5 SNMP

ID	Community	Server	Version
1	x.x.x.x	x.x.x.x	x.x.x.x
2	x.x.x.x	x.x.x.x	x.x.x.x
3	x.x.x.x	x.x.x.x	x.x.x.x

Table 12 – SNMP

3.4.1.6 DHCP Relay

ID	DHCP Server
1	10.226.6.1
2	10.226.6.1

3.5. Firewalls 2130

Os Firewalls 2130 são usados como borda para internet e estão configurados em Alta Disponibilidade.

3.6. Gerenciamento

Type	Interface	VLAN ID	SITE	IP Address
FW-1	MGMT	6	RJ1	10.226.6.9
FW-2	MGMT	6	RJ1	10.226.6.10

3.7. Interfaces

FW-1

Equipamento	Interface Física	Interface Lógica	Vlan	Vlan Name	IP	Rede
FW-1	Eth1/1 – Eth1/2	Po1.100	100	Inside	10.226.100.4	/24
		Po1.110	101	outside	10.226.100.13	/24
	Giga1/8	Failover	N/A	Failover	1.1.1.1-2	/24

FW-2






















Equipamento	Interface Física	Interface Lógica	Vlan	Vlan Name	IP	Rede
FW-2	Eth1/1 – Eth1/2	Po1.100	100	Inside	10.226.100.4	/24
		Po1.110	101	outside	10.226.100.13	/24
	Giga1/8	Failover	N/A	Failover	1.1.1.1-2	/24

3.8. Versão Software

A versão a ser instalada ou feito update para, segue de acordo com a recomendação do Fabricante

Localidade	Hostname	Versão
Escritorio	FW-01	7.2.4-165
Escritorio	FW-02	7.2.4-165





3.9. Policies Aplicadas

#	NAME	ACTION	SOURCE			DESTINATION			APPLICATIONS	URLS	USERS		ACTIONS
			ZONES	NETWORKS	PORTS	ZONES	NETWORKS	PORTS					
> 1	CFTV	<div> Allow</div>	ANY	10.226.29_24	ANY	ANY	ANY	DNS over UDP HTTP HTTPS RTSP TCP_6000-140... TCP_6600 TCP_6800 TCP_6900 TCP_8000 UDP-6000- 140... UDP_6002 UDP_6800 UDP_6900 tcp-30000-320... tcp_30960 tcp_9010 tcp_9020 udp-30000-32... udp-50000-52... udp-62000-65... udp_8666	ANY	ANY	ANY	 	
> 2	to_datacenter	<div> Allow</div>	ANY	10.226.0.0_16	ANY	ANY	10.223.0.0_24 10.224.0.0_24	ANY	ANY	ANY	ANY	 	
> 3	To_inside	<div> Allow</div>	ANY	10.0.0.201 10.223.0.0_24 10.224.0.0_24	ANY	ANY	10.226.0.0_16	ANY	ANY	ANY	ANY	 	
> 4	to_internet_Un...	<div> Allow</div>	ANY	10.226.0.0_16	ANY	ANY	138.36.219.245 138.36.219.246 168.90.175.0_24 177.126.177.96 177.154.136.0... 177.154.136.141 177.187.10.53 179.107.47.128 187.0.202.0_24 187.0.202.16 187.0.202.19 187.0.217.24 200.143.172.12 200.143.178.14 200.143.178.32 200.143.178.41 200.150.148.87 200.152.32.147 200.155.31.92 200.155.65.21 200.155.9.72 200.198.187.242 200.198.187.3 200.198.187.35 200.198.191.10 200.198.191.144 200.198.191.149 200.198.191.8 200.201.168_24 200.219.200.198 200.219.204.210 200.219.216.2 201.20.39.69 201.20.51.192 201.20.51.235 201.20.8.10 201.20.8.11 201.49.213.176 201.49.213.183 201.49.216.59 analise.eqx-ms... eletros.frogtest... internetbanking...	ANY	ANY	ANY	 		
> 5	from-internet	<div> Allow</div>	ANY	187.0.202.0_128	ANY	ANY	10.226.0.0_16	ANY	ANY	ANY	ANY	 	
> 6	to_internet_Na...	<div> Allow</div>	ANY	10.226.0.0_16	ANY	ANY	ANY	HTTP HTTPS ICMP	ANY	ANY	ANY	 	
> 7	Smart-account...	<div> Allow</div>	ANY	10.226.0.0_16	ANY	ANY	208.67.222.222	DNS over TCP DNS over UDP	ANY	ANY	ANY	 	

Eletronics - Network of the new Eletros

Routing and Switching

> 8	S104A.ELETR...	 Allow	ANY	10.226.0.0_16	ANY	ANY	S104A.ELETR...	FTP RDP	ANY	ANY	ANY	
> 9	strata.ons.org.br	 Allow	ANY	10.226.0.0_16	ANY	ANY	strata.ons.org.br	SSH	ANY	ANY	ANY	
> 10	55pbx	 Allow	ANY	10.226.0.0_16	ANY	ANY	55pbx_group	Ports_55pbx	ANY	ANY	ANY	
> 11	Bloomberg	 Allow	ANY	10.226.0.0_16	ANY	ANY	103.251.205.0... 160.43.13.0_24 160.43.14.0_23 160.43.16.0_23 160.43.166.0_24 160.43.172.0_24 160.43.24.0_24 160.43.250.0_24 160.43.251.0_24 160.43.252.0_24 160.43.253.0_24 160.43.90.0_23 160.43.92.0_22 160.43.96.0_23 160.43.98.0_24 199.105.176.0... 199.105.184.0... 205.183.246.0... 205.216.112.0... 206.156.53.0_24 208.134.161.0... 208.22.56.0_24 208.22.57.0_24 69.184.0.0_16 69.187.16.0_20 69.187.32.0_19 69.187.73.21_26 69.191.176.0_21 69.191.192.0_18 69.191.212.14 69.191.251.78 live.bloom.com	TCP_8194-8198 TCP_8209-8220 TCP_11011 TCP_30206 TCP_8228 TCP_8290-8294 TCP_8292 UDP_10000 UDP_48129-48...	ANY	ANY	ANY	
> 12	fundacao_eletr...	 Allow	ANY	10.226.0.0_16	ANY	ANY	fundacaoeletr... fundacaoeletr... o6tta0.prd.taf.t...	ANY	ANY	ANY	ANY	
> 13	AEBROADCAST	 Allow	ANY	10.226.0.0_16	ANY	ANY	200.196.192.0... 70.36.25.22	TCP_44700-44...	ANY	ANY	ANY	

> 14	Videoconf	 Allow	ANY	10.226.32_24	ANY	ANY	ANY	HTTPS NTP-UDP TCP_1720 TCP_50000-50... TCP_50000-51... TCP_5060 UDP_11780 UDP_1719 UDP_3478-3481 UDP_50000-50... UDP_50000-51... UDP_5060	ANY	ANY	ANY	
> 15	VPN_Eletr...sa...	 Allow	ANY	ANY	ANY	ANY	187.16.75.62	TCP_4433	ANY	ANY	ANY	

4 **Detail Design Acceptance Sheet**

I hereby confirm acceptance and agreement of As Built document for the Eletrabras - Rede do novo predio da Eletros As Built for ELETROS and the contents contained within, excluding the exceptions described in the notes below.

Notes:

<hr/>	
<hr/>	
<hr/>	
<hr/>	
<hr/>	
<hr/>	
<hr/>	
NTT	ELETROS
<hr/>	
Signature	Signature
<hr/>	
Print Name and Title	Print Name and Title
<hr/>	
Date	Date
<hr/>	

ELETROS should send this signed Detail Design Acceptance Sheet to **tiago.silva (americas)@global.ntt**.



Eletrobras - Rede do novo predio da Eletros

Routing, Switching e Wireless

Document Change Control

#	Version	Date	Who	Change Details	Decision
1.	1	2023-03-08	Tiago Luiz da Silva		